



The Near and Far Future of Ransomware Business Models

Feike Hacquebord, Stephen Hilt, and David Sancho



TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

**Feike Hacquebord, Stephen Hilt,
and David Sancho**

Stock image used under license from
Shutterstock.com

Contents

3

Executive Summary

5

Introduction

6

Current Ransomware Evolution

12

Contemporary Ransomware
Building Blocks

17

Triggers for a Paradigm Shift

25

What Ransomware Looks Like
When It Goes Through an Evolution

41

What Ransomware Looks Like
When It Goes Through a Revolution

50

Conclusions

52

References

Executive Summary

This research paper explores the position of ransomware in cybercrime and what would trigger changes in ransomware business models. Ransomware has evolved into a malware used to cause major problems for enterprises, governments, healthcare, and critical infrastructure, but other cybercriminal business models — ones that can generate significantly more illicit profit — raises an interesting question: what would make ransomware actors change their criminal business models?

Geopolitical events, like Russia's invasion of Ukraine in 2022, can trigger or force ransomware actors to change. The trigger for ransomware actors can also come from both combative and defensive strategies by law enforcement, government, and private industries: cloud adoption, hardening networks, arrests, sanctions on cybercriminal gangs and facilitating services, and the regulation of cryptocurrency to make it more difficult to launder money.

We believe that most of these strategies will lead to gradual changes in ransomware, like the usage of more zero-day vulnerabilities in the initial access phase, better operational security (OpSec), more automation to optimize revenues, increased targeting of Linux cloud servers and targeting of exotic platforms — all of which will be covered in more detail in this report.

Meanwhile, ransomware actors will only start to rethink their business and make drastic changes when they are pushed harder or realize there is much more money to be made elsewhere. For example, actors can abandon ransomware and use other more profitable payloads in the kill chain while still leveraging many of their core specialist skills. This report will detail scenarios that include the following:

- Theft of intellectual property and other sensitive data
- Business email compromise
- Stock manipulation schemes, such as “short and distort”
- Theft of cryptocurrencies at scale

Moreover, ransomware actors are likely to move and be more active in cryptocurrency theft and fraudulent schemes with crypto assets, especially once they realize how profitable these schemes are. Illicit profits in cryptocurrency are expected to grow because of the popularity of bitcoin and upcoming technologies like Web3 and the metaverse.

One of the core problems in ransomware attacks is initial access. Initial access of enterprise networks can happen through:

- Tailored attacks against enterprises, which can include advanced social engineering.
- Mass email campaigns with a malicious payload, plus filtering of the most valuable victims.
- N-days and zero-day exploits of vulnerabilities in internet-facing systems.
- Supply chain attacks.
- Leveraging misconfigurations of cloud services and theft of cloud management keys.
- Vulnerabilities in cloud instances.

Given the pivotal place of initial access in the ransomware kill chain, defenses against ransomware should not focus on ransomware alone, or ransomware will simply be replaced by other payloads with much higher profits and damage potential. Defenses need a combination of strategies such as:

- Hardening of internet-facing systems.
- Hardening of internal corporate systems.
- Transitioning to cloud services.
- Combating initial access providers should have priority over combating ransomware alone.
- Imposing sanctions on major actors and facilitators will make the costs for ransomware demands increase even more.
- Implementing regulations of cryptocurrency that will reduce privacy and protect consumers against fraud. The upcoming regulations in the EU are an example, and will make money laundering a lot harder.
- Preparing for the possibility that ransomware actors might move to another cybercrime like cryptocurrency fraud and cryptocurrency theft.

When law enforcement authorities and the private cybersecurity industry work closely together, the problem of ransomware will be reduced and prevent cybercriminals from moving on to other areas of cybercrime.

This research paper explores the position of ransomware¹ in cybercrime and under what circumstances that position can and will change. The problems that ransomware have caused to society have escalated dramatically over the past few years. This has led to a strong response from the private cybersecurity industry, which has heavily invested in better defenses, international law enforcement chasing bad actors, and governments imposing sanctions on ransomware gangs and some service providers, such as cryptocurrency exchanges and crypto mixers, that facilitate money laundering. But we have yet to see whether this increased counteroffensive will have a lasting effect.

There are indications that the fight is not enough. For example, there are multiple reports that the infamous Evil Corp circumvented sanctions imposed by the US government by setting up ransomware affiliate programs with new names.² Ransomware victims end up paying Evil Corp continuously almost three years after the group was added to the US sanction list.

Some of the REvil (tracked by Trend Micro as Water Mare) actors were arrested by the Russian authorities in early 2022³ while the Tor-hidden website of REvil was already down in October 2021.⁴ But somebody took control of the REvil ransomware-as-a-service (RaaS⁵) Tor-hidden sites again in spring of 2022 and seem to have resumed business.⁶

Conti (tracked by Trend Micro as Water Goblin) took a pro-Russia stance after the invasion of Ukraine. This provocative action prompted a security researcher, who had access to Conti's internal systems for more than a year, to come out of the shadows.⁷ He posted revealing internal chat logs and server information on the internet regarding Conti, which gave an unprecedented public insight into Conti's operations and accelerated the disbandment of Conti as a well-known RaaS group.

However, it was, by no means, the end of the activities for former Conti affiliates. Some of Conti's affiliates had been working for other RaaS groups simultaneously, or just moved elsewhere to start working for another group like BlackCat (also known as Alpv, Alphav, and AlphaVM).^{8,9} Likewise, the multitude of operational security (OpSec) blunders of other RaaS groups provided significant insight into their operations, but do not seem to be fatal to their daily operations.

This raises the question of what actions can the security industry, governments, and law enforcement take to stop or slow down ransomware attacks. When would the actors, who found their cozy home in a RaaS program, pack up and move elsewhere?

This research paper attempts to provide the answers by studying realistic scenarios in which, for example, risk assessments of getting caught would be unfavorable for ransomware actors. In other scenarios, ransomware actors might simply find more profitable ways to commit crimes. In our analysis, we explicitly do not rule out that ransomware will initially gradually evolve further before the actors make drastic changes in their business models because they are forced to do so by an external trigger or simply because they discovered more profitable cybercrimes.

Escalations in ransomware might occur when actors manage to leverage complicated vulnerabilities in cloud service providers' (CSPs) solutions, and when, for example, ransomware attacks get combined with stock manipulation. Given the growth in the use of cryptocurrency because of emerging technologies like the metaverse and Web3, ransomware actors might follow the lead of nation state actor Lazarus, who not only has deployed ransomware in the past, but also earns more money by hacking cryptocurrency wallets and cryptocurrency exchanges.

We start this paper with an overview of today's state of ransomware. Then we discuss what could trigger ransomware actors to change their different business models. We have characterized these changes as evolutions and revolutions, discussing both changes in separate sections. Throughout the paper, we make recommendations on combating ransomware and how to prepare for future changes in the criminal business models of ransomware actors.

Current Ransomware Evolution

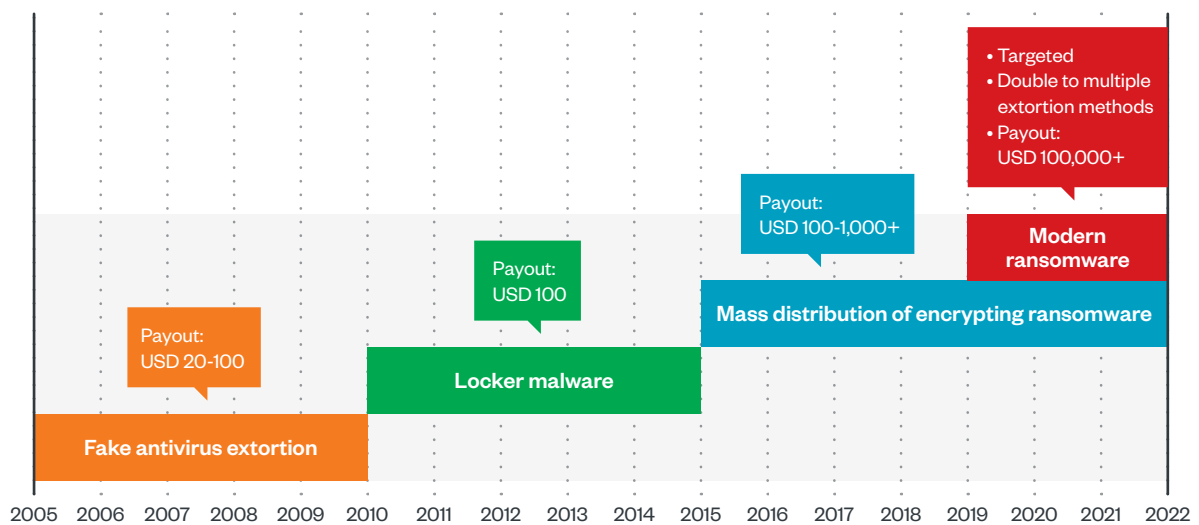


Figure 1. Summarized timeline of ransomware changes¹⁰

The current ransomware threats can be traced back to the earliest modern forms of ransom-requesting malware: “Fake Antivirus” software and “Locker” malware. In those two forms, the attacker hijacks the computer and the malware demands a payment from the user. The main difference is the narrative behind the attack and how each tries to convince the user to pay.

Fake antivirus software was a common threat to internet users from around 2005 to 2010. This fake security software detects a false threat in the system. Then, the fake AV continuously harasses the user to acquire a software license to clean the system. This strategy was successful for the attackers for a few years, but the media coverage they ended up getting was extensive. This forewarned a lot of users so the threat became less effective. On top of that, payments were usually made with regular credit cards. When victims realized they had been scammed, they often made complaints and credit card processors ended up shouldering the cost. This meant attackers were often being denied further transactions as they were blacklisted on the processors’ end.

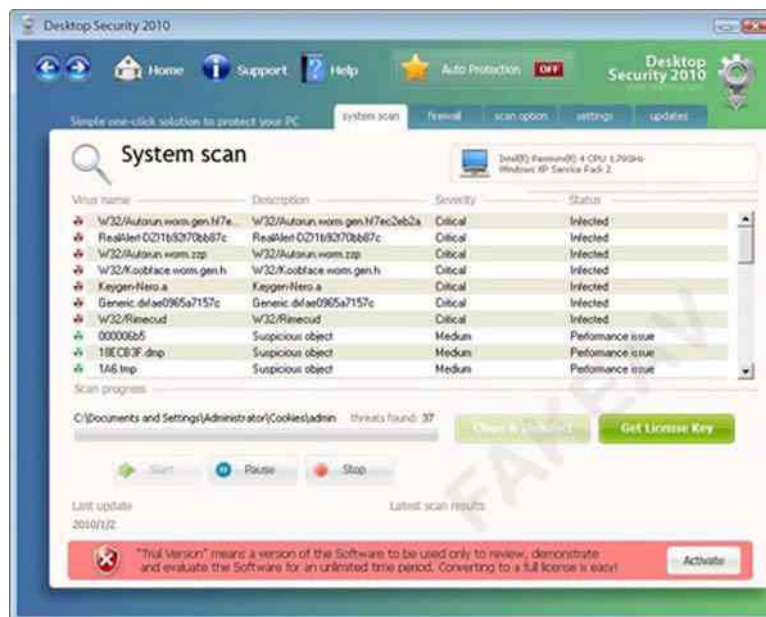


Figure 2. A screenshot of the fake antivirus software “Desktop Security 2010.”

The names changed very often, sometimes weekly.

The next iteration in this evolution was Locker malware, which started to become common around 2010 until around 2015. Locker malware had a simple idea: Once it infects the machine, it disables user access to the computer. The user is presented a warning that offers to unlock access in exchange for payment. The attackers usually masked this threat as if the access lock came from a law enforcement agency and the payment is a fine for a supposed misdemeanor. Again, after a few years, this social engineering trick received such media coverage that victims already knew the scheme was a ploy to steal their money.

As an improvement to fake AV attacks,¹¹ Locker malware requested payment by means of cash vouchers. These were commonly sold in gas stations and other small shops, and allowed consumers to make small payments when they provided the serial number of the voucher to the recipient. Often, the voucher companies that were most used were UKash and Paysafecard. Both companies were victims in this game and therefore fought hard to eradicate Locker malware along with the law enforcement agencies the attackers impersonated.



Figure 3. The lock screen of Locker malware impersonating the UK Police, circa 2010.
 Notice the cash voucher prompt on the right side requesting payment.

The next evolution from these attacks was ransomware as we currently know it. Ransomware attacks started to be common around 2015 and have become rampant today.

These threats scour the system looking for valuable files (such as user photos, documents, and spreadsheets, among others) and encrypt them with a strong algorithm. They then proceed to ask for payment to decrypt those files. This is a more efficient way to force the user into making a payment because it does not matter if they are forewarned or not: There is no need to fool the user. Once the computer is successfully infected, the trap is sprung. This is a more technical and less social kind of threat.

The payment was facilitated by the rise in popularity of Bitcoin and other cryptocurrencies. This enabled attackers to better avoid law enforcement tracking, receive payments easier internationally, and this helped ramp up the number of ransomware attacks. Common ransomware groups of this era were CryLock and Dharma/CrySIS.¹²

The earlier forms of ransomware were mainly mass-mailed to as many users as possible. In the beginning, ransomware downloaders were attached to infectious email messages. When clicked, these attachments would download the rest of the attack chain and finally infect the computer. Later, links on the email text would perform the same function. This change often bypassed antispam filters along the way.

This infection vector was indiscriminate and aimed to reach as many victims as possible. The more victims infected, the higher the bottom line for the attackers.

In the latest evolution, ransomware has become more targeted. Around 2019, the newer ransomware versions entered the network manually through a hacking attack or other similar means. Once inside, the intruders assess the network, try to move laterally searching for valuable data, and often end up elevating their privileges and becoming network administrators. Once the data has been located, they first exfiltrate it through the network, encrypt it, and demand a ransom. Common ransomware groups include Conti, Clop, and LockBit. More on these recent ransomware variants can be found in our Ransomware Spotlight Series.¹³

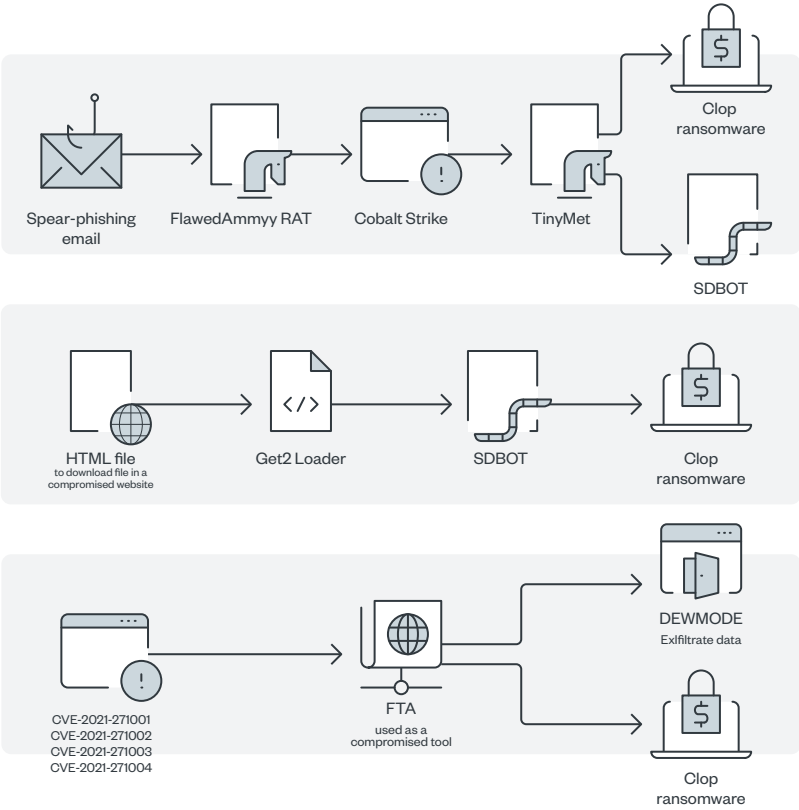


Figure 4. Clop ransomware’s routine changes deployed by different groups

These newer ransomware types not only differ in the way they enter the network, but also in how the attackers exert pressure to force their victims to pay. Early ransomware attacks just encrypted the data and hoped that the victim cared enough to pay to get it back, but these newer attacks publish the data bit by bit and use other techniques to force the victim to pay.

The additional pressure point on the victim — appearing as explicit threats to disclose the stolen data — is known as double extortion.¹⁴ This has further evolved into triple and quadruple extortion wherein ransomware groups use additional arguments to threaten the victim and elicit payment. Threats of conducting distributed denial of service (DDoS) attacks on the victim’s network and harassing the victim via social networks (through clients and suppliers) are the pressure points most often used beyond regular ransom demand and data disclosure.

In the move from mass-produced to targeted ransomware, it is clear that the main players are forming criminal groups that show increased professionalism. In fact, some players draw from over a decade of experience, stemming from a time when they ran some of the world’s most successful banking trojans.¹⁵ This shows in the maturity of their attacks and the way they interact with others in the criminal underground. At the same time, there has been a huge increase in the other supporting players that the main actors rely on to commit their crimes.

A good example of this is “Access as a Service” (AaaS).¹⁶ While AaaS has been around as a concept for some time, there was a noticeable increase of these sellers from approximately 2019, offering access to corporate networks in the form of credentials or other ways of directly connecting to internal networks. The rise of this new criminal offering has made it possible for ransomware groups to now target bigger victims in a more reliable and professional manner.

At the same time, the security industry has been constantly reporting on advanced persistent threat (APT) groups, and the emergence of the MITRE ATT&CK matrix has made it clear to attackers what a full-blown kill chain should look like. This has informed attackers of methods they could attempt to replicate to improve their offensive techniques.

Lastly, another factor could be the appearance of more powerful red team tools for penetration testers. This has made the pen testers’ arsenal a lot stronger, so the attackers’ teams are more dangerous than they would have been otherwise.

This quick history lesson on ransomware evolution cannot be complete without a mention of how the payouts have grown over time. Fake antivirus software used to ask for a license fee of around \$20-\$100. PC lockers increased their ransom demands to around \$100. Mass-produced ransomware also started ransom demands around that range, but increased up to the low thousands over time, depending on the group. Modern ransomware demands, however, are customized to fit the victim’s revenue and tend to be upward of \$100,000 and, in some cases, several millions of dollars. The difference between the older threats and current ransomware is dramatic.



Figure 5. Ransomware demand payment from earlier types of ransomware like Fake AV and PC Locker

In summary, the most dangerous ransomware attacks today are hacking operations with a ransomware payload. This is important to understand because stopping or minimizing these attacks is very different compared to stopping their earlier iterations. Today, much of the emphasis is placed on protecting systems from this final payload. But this comes at the very end of the attack kill chain and is only deployed after complete control of the network has been achieved. Defending against ransomware is like defending against targeted attacks: users and teams need to protect systems in as many layers as possible as far to the left of the kill chain as they can.

This section has outlined how ransomware attacks may be viewed as an evolution of previously related threats thus far. As good as any of them have been for the attackers, these attacks never stayed static. The threat has been constantly evolving, and today's ransomware is another step in the evolution of these threats. What will the next point be in that gradual evolution? That is what we are trying to predict in this paper.

Contemporary Ransomware Building Blocks

We present some building blocks of the current ransomware threat landscape to give some context to the criminal business plans behind the threat. Then, we discuss the scenarios on ways the current ransomware threat may evolve.

Key Underground Services That Enable Ransomware

Today's ransomware is a part of a criminal ecosystem that has multiple building blocks. Different actors are usually involved before and after the ransomware payload is deployed on the victims' networks. The different phases include:

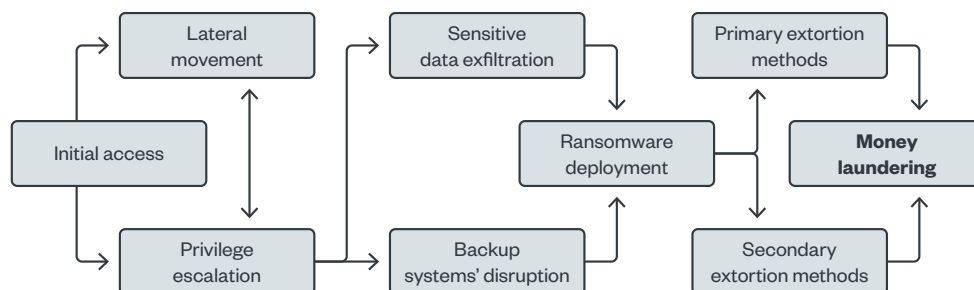


Figure 6. Building blocks of a modern ransomware ecosystem

- **Initial access**

Initial access to a network can be established in various ways. One way is to choose the victims with the highest potential from a large set of infections via mass email campaigns with a backdoor payload.¹⁷ Another way involves targeting enterprises with tailored social engineering campaigns.¹⁸ Other ransomware players gain initial access by using vulnerabilities in internet-facing systems. Initial access can be bought from sellers of specialized services or be done by the ransomware actors themselves.

- **Lateral movement and privilege escalation**

In this phase, an attacker tries to penetrate deeper into the victim's network and tries to get elevated privileges with standard or custom hacking tools.

- **Sensitive data exfiltration**

When the lateral movement phase is a success, the attacker is likely to get their hands on private data and will try to exfiltrate it. In addition, the stolen data is analyzed to determine the ransom amount and whether the company has cyber insurance

- **Backup systems' disruption**

The attacker tries to lower the chances of the victim's capability to potentially restore systems from backups by disrupting the backup processes and systems.

- **Ransomware payload deployment**

In this phase, an attacker deploys ransomware that can lead to serious problems for the victim: data files are encrypted and IT systems become unusable.

- **Extortion**

The attacker extorts the victim. There are two ways that are particularly harmful: the victim gets a decryption key for the encrypted data only after paying a ransom, or the threat actor threatens to release stolen data if the victim does not pay a ransom. There are secondary extortion methods that can be imposed in addition to the primary extortion method if the victim does not pay the ransom, such as DDoS attacks, phone calls or emails to customers and suppliers, and public posts on social media.

- **Money laundering**

In case the ransom is paid, the actors need to launder their ill-gotten gains, which are usually paid in cryptocurrency. Money laundering can make use of cryptocurrency mixers, multiple cryptocurrency exchanges, and various tricks to conceal the final beneficiaries.

All the services needed in the phases above can be done by one cybercrime gang alone, but in practice, actors are often specialists in one task (like initial access)

Current Types of Ransomware Actors and Motivations

To understand whether ransomware will move to other criminal business models in the future, it is important to understand the current motivations of ransomware actors. Not all motivations are the same even though this might not be immediately obvious when looking at the actions of ransomware actors alone. For example, the H0lyGh0st ransomware actors looked like any other medium-sized ransomware group. The group attacks small- and medium-sized businesses and threatens to leak stolen data of

victims on their leak site. This picture changed after Microsoft linked H0lyGh0st to North Korean actors, and even found links to the DarkSeoul actors who are known to have attacked the energy sector in Asia and the US.¹⁹ The H0lyGh0st actors are likely to follow a different criminal career path than, for example, a Canadian affiliate of the large Netwalker RaaS group who has been charged for both drug-related crimes and cybercrime.²⁰

Big Game Hunters

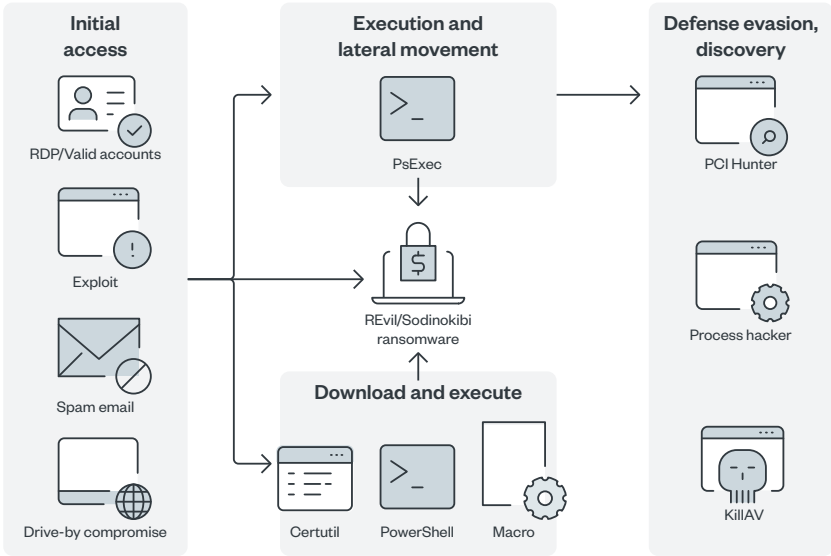


Figure 7. REvil's general infection chain, which uses highly customizable tools and malware depending on the target's environment

First, there are the actors who are associated to RaaS affiliate programs that lead to headlines repeatedly because they break into the networks of multibillion dollar companies, steal, leak confidential data, deploy ransomware in the corporate network, and boldly demand millions of dollars in ransom. Some of these actors are unscrupulous when it comes to attacks against the healthcare sector and critical infrastructure.²¹ Even though the OpSec of these actors often is not optimal (for example, the servers of REvil were allegedly hacked by international law enforcement²²), none of the major arrests made a lasting effect. Some of the affiliates just hop from one RaaS group to another. For instance, in an analysis published by Microsoft, it is reported that one affiliate group deployed the ransomware of Ryuk, Conti, and Hive, and later deployed ransomware from BlackCat.²³ Another affiliate worked with Ryuk, REvil, BlackMatter, and Conti, and later also worked with BlackCat. The big hunters take the largest risks as their downfall will surely be high on the priority list of international law enforcement.

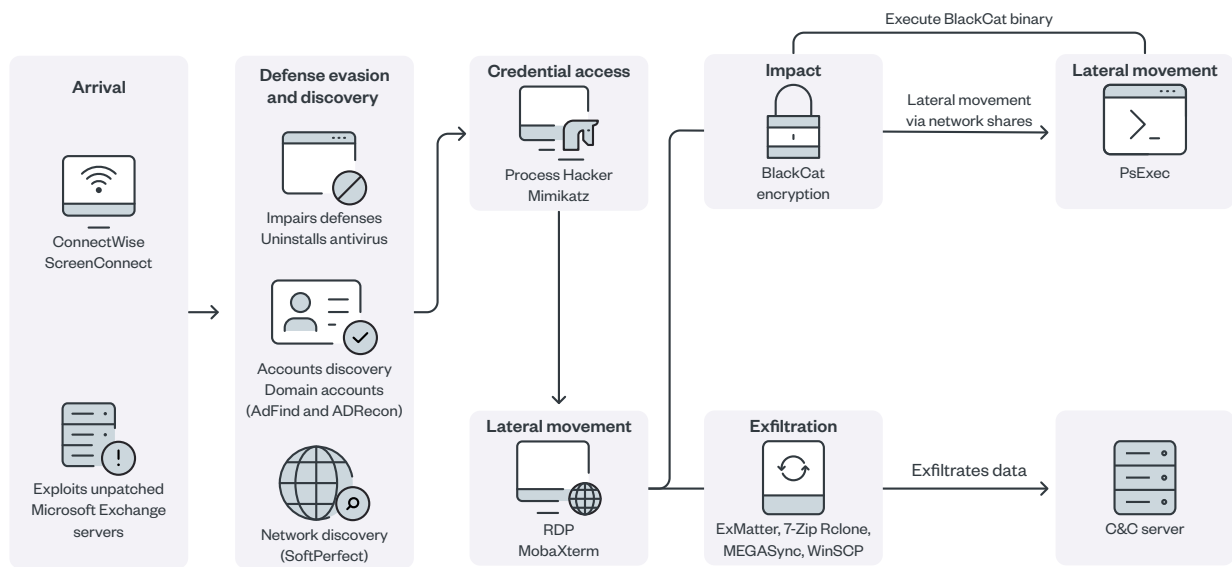


Figure 8. BlackCat ransomware's infection chain

Traditional Cybercriminals

Second, there are ransomware actors who have been around for a long time: they maintain a low profile, operate with automation that minimizes the need of contact between victim and perpetrator, have good OpSec, and make no extravagant ransom demands. These actors are playing the numbers game, trying to infect as many victims as possible with very little manual effort and collect moderate ransoms from each of them. They can still earn millions of dollars per year. But because of the havoc their big game hunter colleagues are causing, they might not get the full attention of law enforcement and the security industry, simply because these big ransomware incidents must be prioritized. An example is Cerber, who earned at least \$7 million in bitcoins in 2016, according to research published by Google and other researchers.²⁴ As of this writing, Cerber is believed to be still around.²⁵

Nation-State Actors

The third type are ransomware actors who can be considered nation-state actors. These actors have the resources and time to prepare their attacks. The motives of these actors can vary. They demand ransoms from their victims and the money might flow to governments or elites who are in power in their countries. But it is also possible that government-related actors use ransomware deployments as a night job for their own benefit.

Nation-state actors might use ransomware to cause chaos and disruption, like in the WannaCry 2.0 incident in 2017 that, according to US law enforcement, was the work of North Korean state-sponsored actors.^{26,27} In other attacks, nation-state actors are suspected of using ransomware as a smokescreen to confuse the victim and incident response (IR) handlers on the true reason why ransomware is being deployed. The actual goal of the initial intrusion might not be ransomware, even when it is being deployed

and crippling a corporate network. In reality, the goal can be espionage through the theft of confidential information or deployment of a destructive wiper attack. According to a report by Symantec, prior to the 2022 Russian invasion into Ukraine, several Ukrainian organizations were targeted with ransomware at the same time when they were hit with destructive wiper malware.²⁸ This might have been an attempt to hide the destructive wiper attacks. An example of espionage was also suggested for ransomware attacks by an alleged Chinese actor believed to be state-sponsored.²⁹ This actor reportedly deployed ransomware families like LockFile, AtomSilo, Rook, Night Sky, and Pandora ransomware in a sequential timeline. These ransomware families are based on publicly available ransomware source codes. After the actor stopped using Pandora ransomware it started to use Lockbit 2.0 ransomware.³⁰

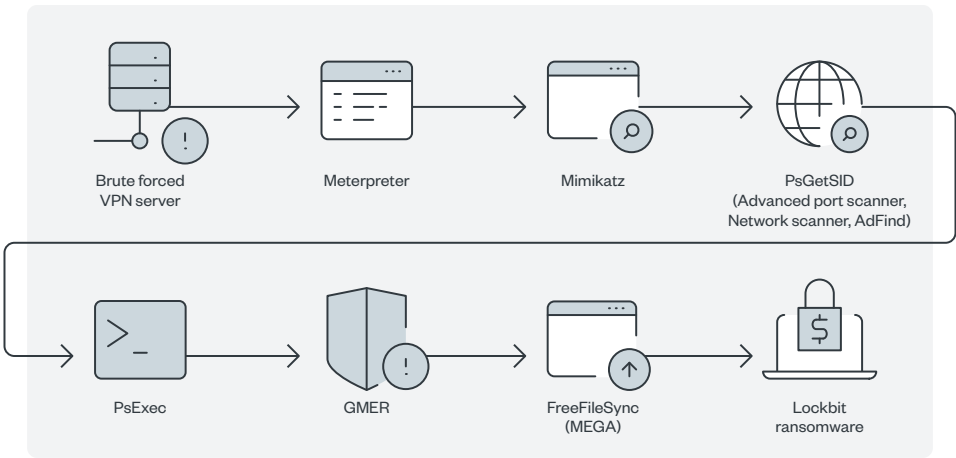


Figure 9. Lockbit 2.0 ransomware with automated data exfiltration (Stealbit)

Other examples of alleged state-sponsored ransomware actors are: Maui Ransomware^{31,32} and H0lyGh0st,³³ both allegedly deployed by North Korean state actors. Moses Staff ransomware is believed to originate from Iran.³⁴

There can also be an overlap between the different types of actors. For example, US law enforcement agencies have alleged that the leader of Evil Corp has worked for the Russian intelligence service FSB, and he was in the process of getting permission to work with classified information in Russia.³⁵

Actors with different motives will most likely have different triggers to change the way they use ransomware. The next sections will discuss the triggers that could change ransomware.

Triggers for a Paradigm Shift

From time to time, a regular business owner will rethink the way they do business. The business could continue to do the same thing, renovate the office, expand the office, or even relocate to a different location and start something entirely new. The need for change will be triggered by external or internal factors. For example, the market has changed, government regulations have changed, new technologies have emerged, or the entrepreneur wants to enter a different, more profitable business.

The same shifts hold true for a cybercriminal: There will be triggers that make cybercriminals change their business model. In the following sections, we explore what could make ransomware evolve with small gradual changes (evolutions) and what could cause drastic changes in the criminal business model of ransomware (revolutions).

Trigger 1: Increase in Successful Law Enforcement Activities Against Ransomware Groups

If law enforcement were able to regularly perform multi-jurisdictional takedowns of ransomware groups, this would prove to be a big factor in the future of ransomware. As an example, if there were players in the US, the UK, and the Netherlands operating in the same ransomware group, there would need to be an arrest of all these people at the same time to effectively take down the ransomware group in one effort. In the recent past, there were announcements specifically from these countries that more resources would be used against these criminals, including intelligence agencies.^{36, 37, 38} If this was ever successful at scale, this would highlight the collaborative strength of international law enforcement, which might have hindered the ransomware groups from being as successful as they are today – or at least have some of those involved focus on a criminal business model with a lower profile.

Security researchers around the world are also constantly monitoring ransomware groups, trying to continuously make it more difficult for these players to deploy ransomware payloads on computers. Because of these efforts, it can cause some paranoia within the illicit groups that they are under surveillance or even have someone on the inside working with security researchers or law enforcement. In the published Conti Leaks, members felt that they were being monitored and followed.³⁹ This can dissuade criminals from this line of attack.

In cases where law enforcement is unable to apprehend an entire group at once, this could unfortunately strengthen the remaining ransomware businesses and allow for people left free to go into hiding, feel more justified in their attacks, improve their operational security, and make them bolder. Additional members of the group can also rise from the ranks to replace those who have been arrested and move to countries that allow this type of activity with little recourse.

Trigger 2: Change in Russia's Stance Regarding the Arrest of Ransomware Actors

In early 2022, ransomware groups were put on edge in Russia when local authorities announced the arrest of 14 members of the group known as REvil.⁴⁰ If actions like this continue in Russia, ransomware actors might feel they no longer have a safe harbor in the country in which they reside. It has commonly been considered the case that if they do not target Russian citizens or interests, they are very unlikely to face consequences; something commonly seen in discussions and even rules of cybercriminal communities. This could result in actors changing their business models, avoid deploying ransomware payloads, and forcing a change in their business models.

In a separate incident in 2021, Ukrainian officials arrested a ransomware actor that was operating within their country. The US Department of Justice announced that \$6.1 million in assets had been seized in Ukraine for an actor that was linked to the attack on Kaseya, an IT management company. The actor arrested in Ukraine was a Russian national who was later linked to the same group that Russia had actions against the following year, REvil.⁴¹ As mentioned in the previous section of this report, this should be a cross-jurisdictional effort to take down the group. In the case of REvil, there was even an arrest in Romania in December of 2021.⁴² However, all these efforts were short-lived because the group had returned to action in mid-2022.⁴³ This is likely because Russian authorities were not serious with arresting prominent REvil actors or were unable to do so, and this allowed for the group to quickly resume their previous operations. If governments in countries that are traditionally seen as safe havens for cybercriminals change their approach to actively targeting them, this will have a noticeable disruptive effect.

If governments do act on the actors behind ransomware groups, previous examples have shown that the efforts need to be on the whole group and not just parts of it. This is the same mentality when going after other organized crime groups since there are people who will rise from the lower ranks to become the new leaders and continue the groups' operations. It will only truly stop if the risks of running and being part of the group outweigh the risks of participating in a ransomware group.

Trigger 3: Government Regulations on Cryptocurrency

Without cryptocurrency, ransomware would not be as big a problem as it is today. This is because cryptocurrency allows for easy cross-border money transfers with possibilities to obscure the beneficiary's identity. Therefore, stringent regulations on cryptocurrency can potentially reduce the monetary incentive for criminals to deploy ransomware.

Many governments around the world are already considering regulations for cryptocurrency. However, their main motives for doing so are driven by concern for the stability of the financial system and protecting investors and consumers. As the cryptocurrency market grows, it gets more interconnected with the traditional financial system. Big fluctuations in the value of cryptocurrency could cause a ripple effect on the financial markets. Other reasons for regulations include stimulating innovation in cryptocurrencies, gaining better control of money flows, and preventing capital flight. Money laundering and crimes using cryptocurrencies are a concern, too. Research done by the cryptocurrency industry suggests that the percentage of money laundering compared to the illicit use of cryptocurrency is much lower than illicit use in fiat currency.^{44,45} But independent academic research suggests that crime in cryptocurrency is a much bigger problem, with crime involved in 46% of bitcoin transactions.⁴⁶ Regardless, cryptocurrency and other virtual currencies are widely preferred as a payment method for cybercriminals, so cryptocurrency regulations are expected to help governments combat cybercrime.

An extreme case in which a country outlaws cryptocurrency completely would greatly hinder ransomware actors because victims would potentially be unable to pay the ransom. However, this will not be relevant to multibillion companies with a global presence. When a branch in a country with stringent cryptocurrency regulations is attacked, the extortionists can demand payment from another branch of the same victim in a country with less regulations.

Some countries have already implemented strict regulations on the use of cryptocurrencies. In 2017, China banned trading on its domestic cryptocurrency exchanges. Later in 2021, China banned cryptocurrency transactions and cryptocurrency mining. As a result, some of the Chinese exchanges moved their headquarters abroad. Yet, blockchain technologies like NFTs are not outlawed in the country. In fact, we expect no country can effectively outlaw blockchain technologies. This means that ransomware actors would still be able to demand a ransom in the form of virtual currencies. Despite the strict regulations in China, the actors behind Qlocker have been targeting Chinese users in 2022 with 7locker ransomware, demanding a ransom of 1 BTC.⁴⁷

In January 2022, the Russian central bank advocated to ban cryptocurrency exchanges and cryptocurrency mining in Russia.⁴⁸ This would have had a big impact on cybercrime as several cryptocurrency exchanges located in Moscow allegedly have more than the average share in money laundering.⁴⁹ However, later in the year, the Russian government announced it wants to legalize cryptocurrency as a payment method and strict regulation to better track the transactions.⁵⁰

In March 2022, the Biden administration issued an executive order to US agencies to come up with recommendations for regulations on cryptocurrency.⁵¹ Different agencies can look at the problem from different angles, but we can expect that when the US finally regulates cryptocurrency, it will be primarily focused on making the industry more robust and aimed at protecting consumers and investors.

In June 2022, the European Parliament agreed on new legislation regulating cryptocurrency: Markets in Crypto-Assets (MiCA). MiCA aims to protect investors and make cryptocurrency more stable.⁵² Crypto-asset service providers (CASPs) will have to follow strong (security) requirements and educate their clients on risks. CASPs will also need authorization to operate within the EU. This is viewed as a major milestone in regulating crypto assets. But the EU also intends to introduce new legislation that would demand that all crypto transactions will have information on the payer and the beneficiary.⁵³ This new legislation does not have a transaction threshold, meaning criminals cannot split a transfer in smaller transfers that might not get noticed by an automated monitoring system. If this proposal makes it to becoming a real law, it will likely hurt cybercriminal operations that involve receiving money through cryptocurrency payments. This would not only have an impact on ransomware but on all payments to cybercriminals. It is expected that the financial industry will push back on the proposed law as one of the key elements — privacy — will be taken away from crypto, so it remains to be seen if this legislation takes effect soon.

Currently, government regulations on cryptocurrency do not pose an immediate threat to cybercriminals. But the European MiCA law that will take effect in 2025, and the yet-to-be finalized EU legislation mandating information on the payer and payee for cryptocurrency transactions, will make payments to cybercriminals and money laundering more difficult and trigger changes in criminal business models. The MiCA law is expected to be in effect not earlier than 2025, so criminals still have time to adapt to the new situation.

Trigger 4: More Sanctions on Ransomware and Enabling Services

Economic sanctions on countries, organizations, and individuals are generally used as a foreign policy tool. Multiple countries have sanction lists. The most well-known are the ones of the UN and the US Treasury Department's Office of Foreign Assets Control (OFAC). Sanctions against cybercrime-related persons and companies are relatively new. The EU, for example, imposed cybercrime-related sanctions against Russian hackers that attempted to hack the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague and APT10 actors for the very first time on July 30, 2020.⁵⁴ The US imposed cybercrime-related sanctions on December 29, 2016, when the alleged author of the infamous data stealer Zeus malware was designated on the US sanction list. Since then, some ransomware-related actors have been added to the sanction list, including Evil Corp and Lazarus. Alleged facilitators of money laundering schemes, such as cryptocurrency exchanges and bitcoin mixers, have also been designated by OFAC since September 2021. The earliest OFAC designations of two Chinese individuals who allegedly helped Lazarus with money laundering of stolen cryptocurrency was in March 2020. Long before OFAC started designating some cryptocurrency exchanges and crypto mixers, other virtual currency companies have been taken down: US law enforcement took down Liberty Reserve in 2013.⁵⁵

Date	Organization	Reason of OFAC designation
Dec. 29, 2016	Individual	Developer of Zeus malware
Dec. 29, 2016	Individual	Major data breaches
Nov. 28, 2018	Two individuals	SamSam ransomware
Sept. 13, 2019	Lazarus Group	WannaCry 2.0 ransomware, cryptocurrency hacks
Sept. 13, 2019	Bluenoroff	Attacks against financial institutions
Sept. 13, 2019	Andariel	ATM hacks, banking attacks
Dec. 5, 2019	Evil Corp	Development of Dridex malware
Dec. 5, 2019	17 individuals	Related to Evil Corp
Dec. 5, 2019	Six cooperations	Related to Evil Corp
Mar. 20, 2020	Two individuals	Assisted Lazarus Group with money laundering
Sept. 21, 2021	Suex OTC	Virtual currency exchange – Money laundering
Nov. 8, 2021	Chatex	Virtual currency exchange – Money laundering
Nov. 8, 2021	Three businesses	Related to Chatex
Apr. 5, 2022	Hydra market	Marketplace
May 6, 2022	Blender.io	Cryptocurrency mixer
Aug. 8, 2022	Tornado Cash	Cryptocurrency mixer

Table 1. Some examples of OFAC designations related to ransomware and cryptocurrency cybercrime

Some have speculated that ransomware actors residing in Russia are less active because of the international sanctions imposed on Russia since its invasion of Ukraine.⁵⁶ However, whether sanctions are really causing the drop in ransomware activity remains to be seen. While the sanctions might make the money laundering phase more difficult, actors can hold their cryptocurrency in wallets that are in other jurisdictions. It has also been theorized that threat actors have changed tactics by posting less victim data publicly and interact with victims more in private.⁵⁷ Unfortunately, it's not easy to get reliable statistics on ransomware activity. Statistics based on companies that are listed as a victim on RaaS websites are potentially unreliable and do not reflect the actual number of victims per se. For example, a French journalist found that Lockbit had 60 unfounded claims of data leaks published on their RaaS site (out of 400 cases).^{58,59} In a research paper on PYSA ransomware, it was found that the real number of victims of PYSA was 747, while the number of exposed victims on PYSA's RaaS site was only 309.⁶⁰

Cybercriminals have been reportedly trying to evade sanctions by renaming the brand name of their ransomware family. The clearest example is Evil Corp, which was designated on the OFAC in December 2019. In 2022, Evil Corp reportedly moved away from their own ransomware and used RaaS Lockbit instead.⁶¹ Yet it is an open question whether cybercriminals rename their ransomware to evade sanction lists alone: Evil Corp already used different ransomware names, such as Bitpaymer, Doppelpaymer, and Wastedlocker, before OFAC sanctioned them. Other actors allegedly from China are not on the sanction list, but still they have been observed changing ransomware names frequently.⁶² Regularly changing ransomware family names could also be part of good operations security to make the work of security researchers and law enforcement more difficult.

Even if a ransomware actor is on the OFAC sanction list, that does not necessarily mean no payment to the actor is ever made. In 2021, it was reported that a large insurance company in the US paid \$40 million to the Phoenix Locker actors.⁶³ Phoenix Locker is believed to be a ransomware of Evil Corp.

It is too early to tell how far sanctions will contribute to the fight against ransomware and cybercrime. Sanctions will lead to disruptions of cybercriminal business operations and will likely lead to monetary losses for criminals, just like how the takedown of Liberty Reserve in 2013 did. However, cybercriminals can relatively easily choose other bitcoin mixers and cryptocurrency exchanges to launder their ill-gotten money in future crimes. Sanctions target yesterday’s problems of money laundering and do not solve today’s problems in cybercrime. We expect that sanctions, as they are currently implemented, affect how cybercriminals do their business, but they will not stop them from committing future crimes.

Trigger 5: Changes in the IT Security Landscape and Move to the Cloud

As more companies move to decentralize their datacenters and employ a more remote workforce, it changes the threat landscape, targets for the ransomware groups, and their victims. Today cloud systems are often accidentally left exposed to the internet, and are less secured than systems in a traditional IT system.⁶⁴ This provides more potential for the attackers to find new ways into victim’s networks and critical systems, leveraging these flaws as organizations are still growing their maturity in cloud security to the level they already have for their on-premise environments.

As security becomes a more important topic around the world, IT and security professionals are trying to reduce the risk to their enterprise network. To prevent attacks, it is a common recommendation that everyone should work to reduce the number of internet-facing devices on corporate systems. However, an intent to be more secure and reality do not always align. As an example, according to the trends section of Shodan, we see that remote desktop protocol (RDP) exposures have increased since 2018.

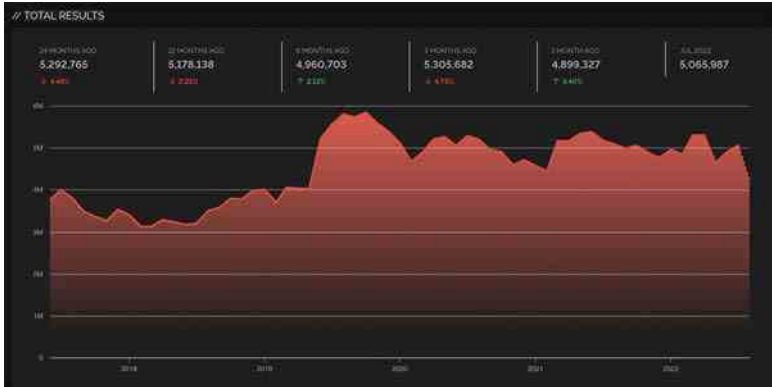


Figure 10. Shodan trends for port 3389 exposed to the internet⁶⁵

This port is just one service known to be attacked to gain initial access to systems for ransomware groups. Once on an RDP session, attackers can pivot through the network to see what else they might have access to. This shows that in traditional on-premise setups, there is currently no major change needed for ransomware actors to carry out their operations. However, this will certainly change as more companies move larger parts of their core infrastructure to cloud environments. The number of attack opportunities from their preferred access methods will decrease.

Since cloud environments do not have some of the same classic attack vectors of a corporate system such as phishing and remote access attacks (such as the virtual private network or VPN and RDP, among others), this will require an attacker to look to the potential of developing and utilizing a new group of vulnerabilities to be exploited not currently being leveraged at scale in ransomware attacks. Palo Alto mentioned that 24% of cloud instances are vulnerable to exploits in 2019.⁶⁶ This has likely grown since this research was done with more companies moving to cloud infrastructures for everything from file storage to active directory systems.

Trigger 6: Poor OpSec, Which Leads to Business Reevaluation

Many RaaS groups make OpSec mistakes. For numerous Tor-hidden websites of RaaS groups, we were able to determine the clear web IP addresses. Common mistakes include leaving more services exposed on the Tor-hidden websites than needed, no proper access management, and leaving unique fingerprints on the hidden websites that can be found back on the clear web using internet scanning services such as Shodan.io and Censys.io. One notorious ransomware group had an SSH server running on their Tor-hidden service and used the same public key for an SSH server on the clear web backend server.

In 2021, servers of the infamous REvil ransomware gang were reported to have been compromised by an unknown party and the leak site was taken down.⁶⁷ Later in 2022, it appeared that some of the REvil infrastructure came back online, but at the time of writing this research, it is unclear who exactly controls the REvil-related infrastructure today.

REvil was not the only major RaaS group that got compromised in recent years. Other security researchers have reported that they were able to get access to restricted areas of several RaaS websites. A researcher of Danish security company CSIS was able to obtain detailed data on affiliates and victims of the Nemty ransomware affiliate site.⁶⁸ In 2021, Prodaft researchers were able to infiltrate some of the servers of the infamous Lockbit ransom group and the infamous Conti group.^{69,70} Prodaft also appeared to have had access to management panels of the PYSA ransomware group.⁷¹ In February 2022, it appeared that a Ukrainian security researcher was deep into Conti's systems for a long time, and they collected detailed information on the daily operations of Conti. The researcher leaked revealing information on Conti in late February 2022.⁷² The leak included chat logs, Conti's server infrastructure, passwords to systems, and source codes.^{73, 74, 75, 76} In April 2022, security researchers of Infinitum IT used information from the Conti leaks to break into the group's systems and found a relation between Conti and the Karakurt hacking

team. The researchers claimed to have used a vulnerability to break into the leak site of Karakurt and find detailed data on the group’s operations.⁷⁷ In May 2022, yet another in-depth analysis on Conti’s relation to the larger cybercrime group Wizard Spider (overlaps with Water Goblin) was published.⁷⁸

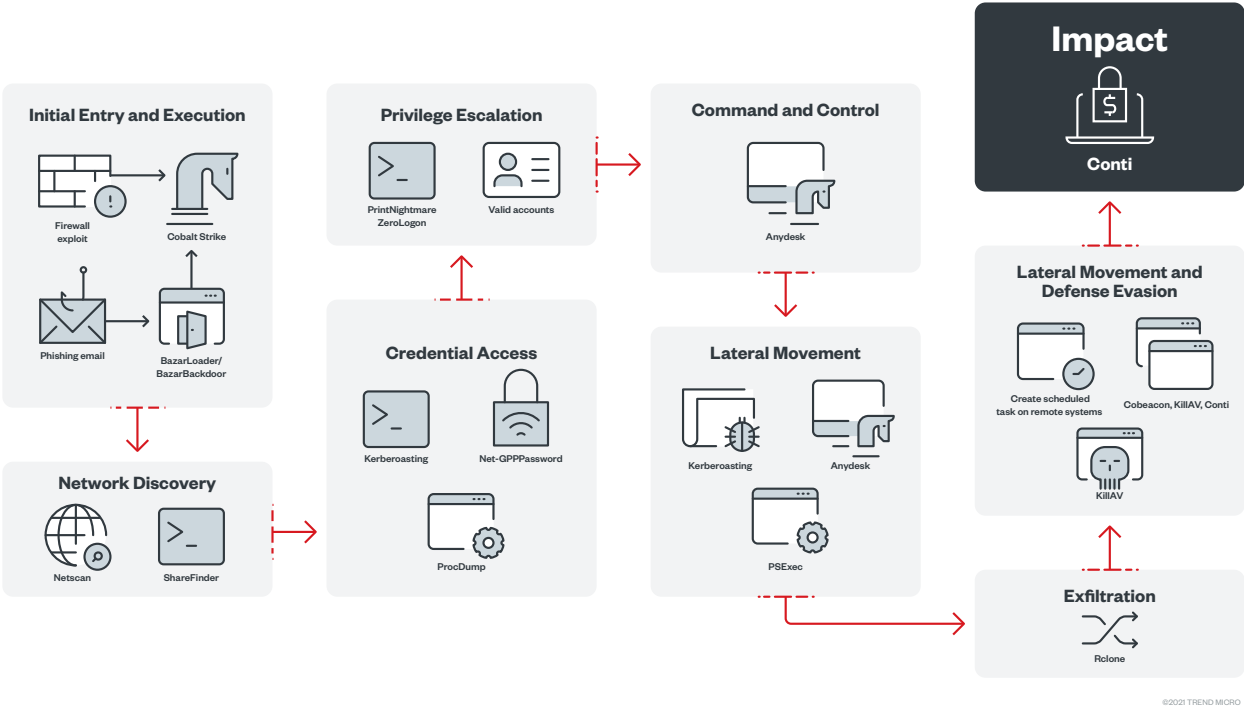


Figure 11. Conti ransomware infection chain

It took Conti until June 22, 2022 – months after the first leaks on Conti appeared on the internet – to shut down all known servers.⁷⁹ However, servers of Karakurt are still up at the time of writing this report. This is a clear indication that Wizard Spider did not stop its operations despite all the horrible security issues the Conti group faced.

Internet-facing servers of ransomware actors, including their Tor-hidden servers, appear to be a major Achilles heel for them. Multiple ransomware actors suffered from serious breaches by private industry researchers. These researchers appear to be willing to use offensive tactics, which could potentially hinder law enforcement in their active investigations. As far as we know, major OpSec mistakes of ransomware actors did not lead to concrete arrests yet, but whenever RaaS actors realize they made major OpSec mistakes, they are forced to shut down their services sooner or later. This could either lead to the cybercriminals starting over and hardening their server infrastructure, or force them to stop altogether and try another cybercriminal business model.

What Ransomware Looks Like When It Goes Through an Evolution

The previous sections described what could trigger ransomware actors to change their business models. Changes are to be expected over time, but some will be a gradual evolution where small parts of the ransomware extortion model are tweaked. Other changes will be much bigger, such as if the ransomware payload gets replaced with something else in the kill chain.

First, we describe how ransomware could evolve in the coming years. After that, we discuss the bigger changes (revolutions) in the ransomware extortion model that could happen soon.

Evolution 1: Replace the Ransomware Payload With Only One Data Extortion

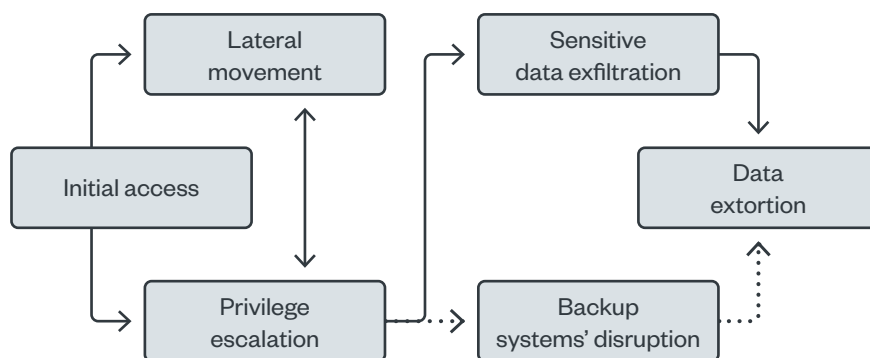


Figure 12. Shifting from ransomware attacks to data extortion

It has been said that one of the main reasons companies pay the ransom is the fear that the data exfiltrated by the criminals contain information that can harm the company with items like passwords, sensitive files, or even emails of its employees.⁸⁰ Ransomware attacks are very noticeable to victims once the payload has been deployed as ransom messages appear and files are encrypted, and they significantly affect companies with a high need for availability and uptime, such as companies in manufacturing, power production and transmission, healthcare, and financial industries. For these companies, a traditional ransomware payload is one of the more devastating things that an attacker can do to their business and are more likely to pay the ransom just to stop the attack and get their business operational again.

For other companies, data leakage has had a larger impact. Some groups in recent years have gained traction being an extortion-only group such as LAPSU\$. This group has been able to successfully extort companies around the world without deploying a ransomware payload. This group is believed to have attacked Microsoft, NVIDIA, and Brazil's Ministry of Health.⁸¹ LAPSU\$ operated like a ransomware group leveraging the data exfiltration part of today's common double-extortion models. It would post proof that it hacked their claimed victims almost like a leak site for those who refuse to pay the ransom. This was shown with their evidence of hacking one Microsoft employee's account in March 2022.⁸² In September 2022, Uber⁸³ and RockStar Games⁸⁴ were hit by an attacker that resembled those of the LAPSU\$ group and is rumored to be members of the same group.⁸⁵ Leaked information from both companies were posted on the internet, and while investigations are ongoing at the time of writing, the UK Police has arrested a teenager in connection to these attacks.⁸⁶ These attacks, however, were more destructive and brazen in nature compared to past ransomware attacks and represent a possible evolution in approach. This group also seems to be after trophies than actual money from a ransomware extortion, to build its name for going after large targets and using this notoriety against later victims with a message of "look at what we did to those companies, do you want to be next?"

In the future, ransomware groups can also take this approach and move to a model where multiple final business models are deployed depending on the victim. These groups will be better at making a business decision and develop playbooks to help decide between deploying ransomware (when availability and uptime is of key importance to the victim), prioritizing data extortion (when brand damage or breach concerns are of key importance to the victim), or even walking away from a target where the negative attention outweighs potential earnings. In hindsight, this could have been something the DarkSide group, the group who attacked the Colonial Pipeline in the US, would have chosen to do. While their attack caused Colonial Pipeline to shut down their systems and pay the ransom, it caused unwanted attention to the group that eventually led them to rebrand their ransomware efforts.⁸⁷ If this group had elected not to deploy a ransomware payload at the time and only extort the company, it may not have caused as much unwanted attention, including statements from US President Joe Biden.⁸⁸

The increase of data extortion groups will likely be an avenue that some actors, including ransomware affiliates, could favor more in future. This will allow these groups to prepare for a landscape where increased pressure from the security industry and law enforcement makes ransomware attacks more difficult, but from which they can still leverage the expertise they have developed in deep network penetration and data theft – by simply replacing the final stage of the payload – and continue to cause harm to generate revenue from their victims.

Evolution 2: Replace the Ransomware Payload With Data Monetization

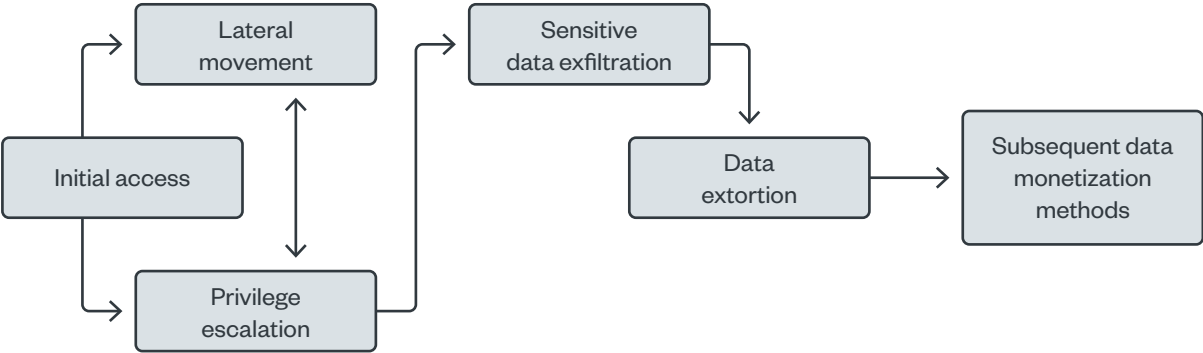


Figure 13. Adding data monetization methods after exfiltration

At this point, it is useful to remember that modern ransomware groups run hacking teams and use encryption only as their final payload. If they see the opportunity or are forced to, groups can switch business plans by simply using a different payload.

Currently, stealing data as part of the extortion plan seems to be the norm. At some point, these groups might also realize that they can monetize these stolen data directly. Mining the data on the client side is a real possibility. For instance, searching the infected system for credit cards or other easily monetizable data is a relatively easy thing to do. Searching for financial plans, source code, salary spreadsheets, and other valuable company secrets can also be accomplished on the infected machine. In fact, several groups already appear to have the tools to do this as part of their data exfiltration stage.

Alternatively, all this data mining could be performed in the criminal's servers after stealing the data wholesale in a less discriminating way. To do this, the criminals would need to invest in data mining experts who can filter the data looking for gold nuggets in the pile. The monetization for this data would need to be thought out very carefully. The information could be financial (such as the company's bottom line and future projections), strategic (for example, contracts and source codes) or personal (such as salaries and medical data).

Perhaps some criminals are already looking to sell the most interesting information.⁸⁹ What ransomware actors could do instead is identify the right data and try to make money directly from it. Data monetization has been one of the longest running criminal business models, but ransomware groups are currently not known for doing it. Doing so, however, has another advantage for the longevity of such groups. It moves them from the end of the kill chain towards the middle as they become suppliers to other groups, who ultimately make use of the stolen sensitive data. In doing so, they also move lower under law enforcement's radar compared to the more visible data brokers who sell the data they have stolen.

If these groups changed this stance, they would need to partner with others, perhaps hire data specialists or merge with other groups who are already doing it. This is a recurring theme in this paper: ransomware criminals could partner with other criminal groups to reinforce their business models. For instance, selling email data to BEC actors⁹⁰ or financial data to stock market fraudsters.

Evolution 3: Spin Out the DDoS Department as a Separate Entity

DDoS attacks provide an alternative way to extort organizations that is different from ransomware. Ransomware can cripple the victim's network for days without the attacker doing anything else after the ransomware has been deployed successfully. A DDoS attack can also lead to an outage of an organization, but a sustained outage is expensive and labor intensive for the attacker to maintain. A DDoS attack is especially harmful for companies who cannot afford to be offline, even for relatively short time periods. These companies include voice over internet protocol (VoIP) telephony service providers, banks, cryptocurrency exchanges, and gambling websites, among others. Some of these companies have lost millions of dollars from DDoS attacks that caused outages.⁹¹ Any company that relies on the internet is potentially vulnerable to DDoS attacks, so in theory, the pool of potential DDoS victims is large.

There have been reports of DDoS attacks claimed to come from the REvil ransomware gang,^{92,93} but there is no evidence that the group was really behind these attacks. In the past, variations of other well-known actor names were being used, including "Fancy Bear" and "Fancy Lazarus,"⁹⁴ so the idea that actors are using well-known names for fear-mongering purposes is plausible. Simply using a known name to send DDoS threats could already generate hundreds of thousands of dollars in profits.⁹⁵

Some RaaS actors have used DDoS techniques as an extra method to pressure victims into paying the ransom,^{96,97} but it is still unknown if this strategy actually makes ransomware victims more willing to pay the ransom. As a business model on its own, DDoS attacks are believed to be less profitable than ransomware. But the threat of DDoS is growing rapidly: Google reported that the size of attacks show exponential growth in the period between 2010 and 2020.⁹⁸ We do not expect ransomware actors to move to DDoS attacks exclusively. However, when the trend in DDoS attacks continue to grow in the coming years, it's likely to become more profitable and this would make DDoS extortion schemes more attractive as a separate criminal business model for large cybercrime groups that are already active in ransomware.

Evolution 4: Change of Targeted Endpoints – Cloud

Moving to the cloud has seen a large push in recent years. This is changing the endpoint landscape for cybercriminal attacks, including ransomware. The security industry has already moved to protect the cloud and help users secure cloud infrastructures that are not behind a typical enterprise router or firewall. While decentralized cloud infrastructures provide easier targets for attackers in some cases due to misconfigurations or unpatched vulnerabilities, the ability to map successful compromises to a

given organization can prove more difficult if there is no domain name pointing to the system or if it's a shared resource. This leads us to see a lot of attacks for systems' idle resources instead, such as cryptocurrency mining groups attacking known vulnerabilities.⁹⁹ However, if these groups begin to either deploy ransomware themselves or sell access to the systems for more profit than they might be able to make with crypto mining, this will start a quick evolution for ransomware actors to migrate to attacking cloud infrastructure more frequently. In March 2021, a crypto mining group named TeamTNT started looking for cloud keys that they could steal and use for later attacks.¹⁰⁰ In most cases, the keys are easy to extract from a compromised computer as they are stored in default locations on the computer, ones that are well-known to attackers. Attackers can also look for keys in the data that has been exfiltrated from companies with regular expression search patterns as the keys are predictable in format. Once an attacker has these keys, they can use these for further exploitation of databases and other systems in cloud systems.

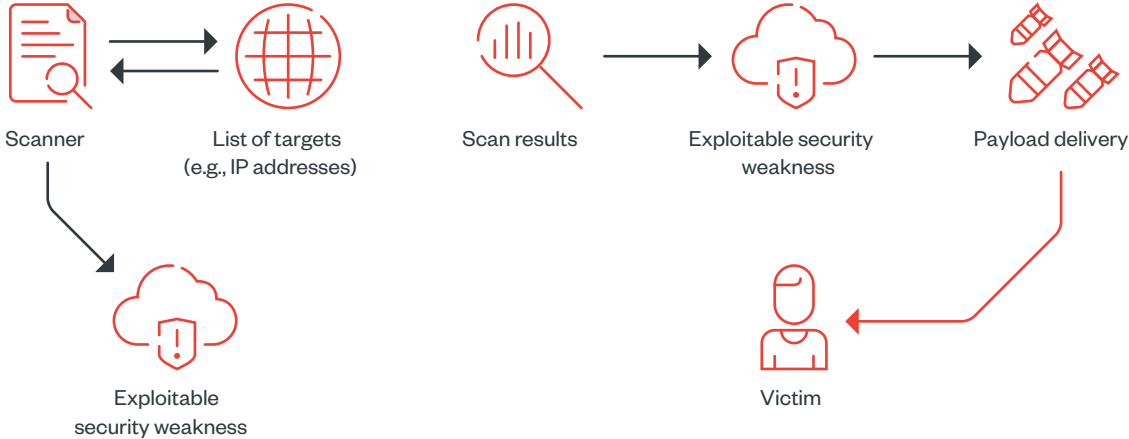


Figure 14. A typical TeamTNT infection chain targeting the cloud and containers that can be copied by ransomware groups

As this evolution happens with the continued move to the cloud, we expect that not only will attackers have to switch to targeting vulnerabilities associated to cloud deployments, but also begin to mature by targeting those unique to them. It is more likely that the criminals will be going after cloud administrator panels rather than the data directly in the cloud because this gives a higher level of access to all the cloud assets owned by the company and not just to a single instance. In June 2022, there was an observed zero-day gap in Microsoft's Azure Synapse, a product that allows users to mount Azure file share to their Apache Spark pools with a script that would then execute with elevated privileges.¹⁰¹ This led to an issue where there was no separation between tenants in the cloud that could allow an attacker to pivot through data in the back end of Azure file systems. This vulnerability was found by an ethical hacker and reported to Microsoft. However, what if a criminal ransomware group was the one who found this vulnerability? In this example, it is a Microsoft-specific vulnerability, however, this could exist in any of the cloud providers as this will always be a risk with sharing resources between other systems and even other companies.

As ransomware actors start targeting the administrator interface accounts of the cloud services, they can also get into the systems and remove backups, start up new servers from which to perform attacks, and lock out other users from the systems. As they become more familiar with cloud infrastructures, we expect their business models to also evolve and adapt. Ransomware will likely evolve to cloud-oriented models in two phases:

- First, criminals will adapt their current business models to work in cloud environments, treating instances as standard data to be encrypted. During this stage of evolution, attackers will also likely make use of cloud environments as initial beachheads to pivot back into the on-premise networks of the victims where possible, and from there carry out their traditional ransomware operations.
- Second, they will gain maturity in understanding their targets and cloud environments, and create more cloud-specific ransomware families designed specifically with unique cloud services in mind, creating new forms of ransomware attacks.

Beyond this level, however, this constant game of attack and defense will continue to evolve. As more corporate systems are put into cloud infrastructures, implement stronger architecture, and deploy the best available cloud native defenses, these movements will force ransomware actors to change their attack methods once again to compensate.

Evolution 5: Change of Targeted Endpoints – Internet of Things (IoT)/Linux

Modern day attackers are very aware of the fact that there are many new platforms connected to the internet. From routers to network attached storage (NAS) servers, all sorts of once “exotic” — but now commonplace — internet of things (IoT) devices are internet endpoints. Attackers have realized that this is a great opportunity because these devices:

- Are powerful enough to support very functional capabilities.
- Are connected to the internet 100% of the time.
- Often host very valuable data, personal or otherwise.
- Have poorly supported and unpatched vulnerabilities.

The trend of targeting these new platforms has already started with ransomware that supports NAS devices¹⁰² and bare metal hypervisors,¹⁰³ but it would be naïve to think that attackers will stop there. To be clear, we are not discussing attacks against cloud platforms in this section even though they are often hosted on Linux servers. We are focusing specifically on Linux-embedded devices and regular non-cloud Linux servers.

The inflection point that marked the trend to target these devices can be traced to the advent of the Mirai botnet in 2016. While this was not ransomware, Mirai was the first mass attack against embedded Linux devices wherein the source code was openly shared with the internet. After that point, anybody with the interest and the skillset to infect Linux-based routers could just download and recompile the old Mirai code and start building their own botnet.

There has been a dramatic increase in router infections afterward, and ransomware authors have been paying attention. From the source code sharing to adding new capabilities (like data encryption and ransom request) to the infectious code, it was just a matter of time. The only other thing needed was to find target Linux-based devices that held valuable data. NAS devices have been the obvious choice. This has already been seen from high profile groups that traditionally targeted Windows environments such as Lockbit.¹⁰⁴ This transition to new targets tells us two important things about these attackers:

1. They have the code ready to target any Linux-based device. There is little effort involved in generating code for other similar devices.
2. As soon as there are valid targets with available internet-facing vulnerabilities, the attacks will start pouring in. They are just ready.

There are two possible ways in which ransomware threats will evolve in the mid-term: attackers will either find new Linux-based targets, or they can tweak the threat to target other platforms.

Regarding the first possibility – finding new Linux-based devices to attack – there are a few possible developments:

- Attackers will start focusing on regular Linux servers. Targeting these servers allow attackers to reach new data stored on them. While file storage servers are valuable, Linux-based databases can be great targets. We have not seen ransomware groups targeting specifically databases at the file level. Any valuable data stored on these servers may be at risk. But if intruders can identify where the database stores data, they could stop the database service and encrypt the appropriate files on the filesystem. Then, attackers extort the company to get those files back. The same thing could be done against web content or any other valuable data on the Linux server.
- Attackers will start targeting backup servers. This could be an additional layer of the main attack: the encryption of file backup servers. This can affect the physical media (such as corrupting, overwriting, or encrypting the tapes, among others), or at the file-level like corporate online file backup systems. The latter would be very similar to the previous bullet point, but the cloud-based software might not be storing the file on disk exactly as the original file. The software can alter them, encrypt them, or even store them on a database. All of those would be valid targets for future ransomware strains to encrypt and demand ransom.

- Attackers will start targeting other IoT Linux-based devices. These devices will preferably hold valuable data that the user may want to pay for to recover. These can be digital photo frame devices (used for storing and displaying user photos), or even cryptocurrency hardware wallets (used to secure storage for encryption private keys). We believe that in the future, ransomware attackers will keep an eye on any new devices coming to the market that can be targeted.

Evolution 6: Change of Targeted Endpoints – Uncommon Platforms

It is important to think about what other platforms attackers might go against for the purpose of ransomware. If an attacker can gain access to an unconventional system that likely does not have backups or is business critical, it could result in a higher chance of a payout and a higher payout amount. While most of what this topic covers will be examples of what researchers have done, it is important to remember that an attacker can look at the proofs of concept (PoCs) and perform the same attacks once they find these systems in a victim's network or just exposed to the internet. In many cases, these exotic platforms might be a more dangerous ransomware attack target.

In 2017, researchers from Georgia Institute of Technology were able to successfully make a proof of concept for creating ransomware for a Program Logic Controller (PLC).¹⁰⁵ The researchers were able to successfully encrypt the logic of a PLC so that only the attacker could decrypt the information upon payment. While these systems can be rebuilt, in some cases the downtime to replace this equipment might cost more than the ransom itself. The victim could find it appealing to pay just to get it back up and running.

If you look at more classic infrastructure and how some business-critical systems are still running on them, these include systems such as mainframes and super computers. In 2017, Trend Micro researchers investigated the number of mainframes exposed on the internet.¹⁰⁶ The research mentioned that compromise of these systems can lead to business process compromise (BPC), which involves silently altering parts of business processes. If an attacker has the access needed to alter processes, they can also choose a noisy approach and decide to hold the company ransom for their mainframe. While mainframe systems are more difficult to attack, they are not immune to compromise as anything that is networked is. Attackers can leverage a few different attacks including phishing, insider threat, and exposure to the internet either on purpose or by accident.¹⁰⁷ When these systems are exposed, sometimes there is a belief that they are some of the most secure systems and therefore cannot be attacked. But with enough motivation and skill, there is an opportunity for an attacker. These systems might also not be backed up, backups might not have been tested for completeness, or the backups take a long time to perform. Often, businesses use these systems to contain information critical to the function of the businesses. Off-the-shelf security tools are available to attack mainframes to show their insecurities, and it would not be hard for a ransomware actor to get hold of these tools and start trying to break into mainframes.

Another possibility is attacking networking equipment that would allow an attacker to turn off ports, reconfigure routes, or encrypt the configuration files of the networking equipment. If an attacker took control of a network router, in theory they could change the administrative passwords and then change routes via static or dynamic routing protocols, maybe even route all the traffic to a specific location to show a ransomware message. To perform this, an attacker would have to compromise the credentials of a network administrator and gain access to the switch or router to perform changes to the networking equipment. This could include changing dynamic routing protocol keys and then changing the routes to remove any redundant routes through the network, making it harder to reboot the networking equipment and recover the equipment without taking longer and potentially cause more costly outages. Once this is done, they can introduce new routes to show the ransomware message to all users in the network, then change the administrative passwords in the central server and the local passwords, preventing the administrators from getting back into the networking equipment.

In 2022, it was reported that an APT actor known as Sandworm was able to take control of WatchGuard routers by escaping the administrative shell and getting to the base Linux operating system (OS) to configure scripts and their own proxy system. If the attacker, in this case, took the time to also take a few steps to hold the device for ransom, it could have led to one of the first ransomware attacks on networking equipment.¹⁰⁸ It is also important to note that while WatchGuard is an enterprise router, these groups are also attacking consumer-grade equipment, which, while cheaper to replace, can be just as problematic for the end users. The criminal group could hold an individual's internet access for ransom.¹⁰⁹

If you were watching television and it displayed a message that said, "Your TV has been encrypted, pay BTC to continue watching," would you pay? Given that TVs are not overly expensive, this would not be a very high payout for the attacker and at most cost a replacement. However, when combined with a social engineering lure such as impersonating law enforcement and a claim that there was an unpaid TV License, this could prove effective as a mass ransomware business model, reusing the "Police Ransomware" method of previous years.

In early 2022, we saw ransomware trying to extort not only the users, but also a NAS vendor to pay for the master decryption key for all the customers that were affected.¹¹⁰ While no vendor paid, it is interesting to note that the number of NAS users and the number of people who have TVs in their residences are different and might have a larger impact if it was successful on a TV vendor. This does not just apply to TVs since one of the more popular OS for TVs is Android-based. This style of attack can be replicated to affect other types of devices that also run an Android-based OS, such as the display on a smart refrigerator.

As more electric vehicles and smart cars hit the road every year, there are more computers running the cars and their features for the passengers. In a 2019 Trend Micro Zero Day Initiative (ZDI) event called Pwn2Own, participants successfully hacked a Tesla Model 3.¹¹¹ This attack was done by just using the browser built into the vehicle's entertainment system. Imagine a parent sitting in line at school to pick up their child, deciding to use the car's browser to look something up, then suddenly finding a ransom

demand on the screen stating that the car has been held hostage, and they need to pay the ransom if they want to go anywhere. This could create fear, especially given the number of cameras these cars have, and would likely lead to a high payout rate for the actor.

Evolution 7: Scale Up Through More Automation

Ransomware actors who go after big targets have been successful in attacking large enterprises and other organizations around the world, especially because their attacks have been tailored to the targets and because parts of the attack in the kill chain were done manually. Tailored, manual attacks are more likely to succeed, but they come at a cost: scalability. These costs are not prohibitive for ransomware gangs because they will still be able to ask for huge ransoms, leading to big profits. But for ransomware attackers who want to maximize profits, scaling will be different. It is a matter of calculating what will bring more revenue: automating attacks might reduce the revenue per ransomware victim. But with more automation, the overall revenue might increase because of scaling advantages. Another reason to automate tasks is that more manual work means more risk. Human errors are made easily, and manual work means that more people must be hired. All the workers are potential risks to the criminal ransomware operation. In the past, there have been instances where disgruntled cybercriminals doxed other cybercriminals or leaked information to the internet.

Initial access and lateral movement make for a substantial cost in ransomware operations. More automation in these phases will lead to faster operations and lower costs. Some affiliates might be able to offer initial access at a lower cost through better automation and scalability. In an extreme scenario, the affiliates can be cut out of the ransomware business model completely and be replaced by automation, for example, via mass exploitation or worm-like behavior in the initial compromise phase. This would greatly reduce the costs for a ransomware operation as affiliates usually get a big share of the profits.

The lateral movement phase and finding valuable information in a corporate environment is costly, especially when this is mostly being done manually. Algorithms for wading through massive amounts of data and identifying the most valuable data would also be quicker and cheaper.

Negotiating with the victim about the ransom amount to be paid is labor intensive as well. This phase can be replaced with full automation using a chatbot. Sending the decryption key automatically after ransom payment by using a smart contract has been theorized in literature,¹¹² and this would reduce the communication between perpetrator and victim.

Big volume ransomware actors like Cerber already have more automation in place. For example, Cerber already used blockchain technology to communicate the location of a command and control (C&C) server in 2017.¹¹³ It is plausible that big game hunters will evolve towards more automation as well once they realize they could potentially earn more and reduce the risks.

Evolution 8: Scale Up Through Increased Professionalism

Some ransomware actors have been interviewed by the media.^{114, 115, 116} While it might have been a rational choice to increase notoriety, some of the interviewees' RaaS infrastructure were already compromised and closely monitored by security researchers by the time they talked to journalists.

Many RaaS groups have a website on a Tor-hidden server. For operational security, it would benefit malicious actors not to assume that the real clear web IP address will never be found by either researchers or law enforcement. Naturally, law enforcement will always be on the lookout for deanonymizing attacks on Tor, and there is evidence there are offensive organizations who spend significant resources on deanonymizing it. For example, an unknown party, dubbed KAX17, allegedly has operated close to 1,000 Tor entries, middle relay, and exit nodes since 2017. These nodes could be used to try to identify the real location of Tor-hidden services.¹¹⁷ But even when using simple methods, we found the clear web IP address of numerous Tor-hidden servers. This means that potentially, any data on those backend servers that are not encrypted are an easy target for law enforcement.

In contrast to the brashness of some of the more notorious actors, there are also ransomware actors who have better OpSec, who do not speak to the press, who minimize interactions with victims, and who did not have documented compromises of their network. If the biggest and most infamous RaaS groups would follow the example of their more careful colleagues in crime with an increased level of professionalism, this could have a big impact on the longevity of their RaaS programs.

Evolution 9: Nation State Ransomware as a Key Cyber Weapon

An incident response (IR) team that gets called in to contain and remediate a compromise that looks like a typical ransomware infection will lose valuable time when the actual goal of the attacker is different from extortion through ransomware. In addition, the ransomware might hinder attribution of the attack and even turn out to be a false flag. This would make it harder for the victim company to understand the possible consequences of the attack.

In the past, there have been examples of APT actors that used ransomware to disguise the actual goal: creating chaos and destruction of the targets' computer systems. In these attacks, the intent was never to force the victim to pay a ransom and then give a decryption key to get encrypted data back in its original form. Examples include the infamous NotPetya attacks from 2017 that hit Ukraine and other countries hard.¹¹⁸ NotPetya was a variant of the ransomware family Petya. It even showed a ransom note, but paying the ransom would not help to get the data back and systems up and running again. Lazarus, alleged to be a nation state-sponsored actor group from North Korea, crippled hundreds of thousands of computers worldwide in May 2017.^{119, 120} The motivation of the attack was most likely not monetary but to create chaos.

In 2022, just before the invasion of the Russian army into Ukraine started, HermeticRansom was deployed on systems in Ukraine that were also hit with a destructive malware called HermeticWiper.¹²¹ Though we do not have definite proof of a relation between the deployment of HermeticRansom and the military invasion, the timing and the choice of targets definitely points to the use of ransomware as a cyberweapon. In early January 2022, Ukrainian organizations were hit by a destructive malware called Whispergate.¹²² Whispergate posed as ransomware, but it did not have a mechanism to restore files.

Particularly concerning is the possibility of using ransomware to cover the tracks of espionage and data stealing campaigns. In the usual kill chain of a ransomware attack, when the actor is done with stealing information, they could first deploy non-ransomware payloads to utilize the stolen data in other schemes. When the time is right, the actor deploys a ransomware payload to cover their tracks and real intentions. We will discuss some of the possible extra payloads in the following sections, with examples including BEC and short-and-distort schemes.

Attribution might also get obscured for IR teams or researchers. When attribution gets obscured, the victimized company gets less understanding of the context and scope of the compromise. In a research by SecureWorks, an actor is described responsible for deploying ransomware families like LockFile, AtomSilo, Rook, Night Sky, and Pandora ransomware in a sequential order.¹²³ These ransomware families are based on publicly available ransomware source codes. After the actor stopped using Pandora ransomware, they started to use Lockbit 2.0 ransomware.¹²⁴ On the surface, this looked like any other criminal affiliate of RaaS programs with a monetary motivation. But according to the report, this was most likely an APT actor allegedly from China whose goal was espionage rather than ransoming victims.

The source codes of ransomware are available to attackers, and the source codes of some RaaS programs were leaked online. These make it easy for attackers to create their own kinds of ransomware and use it to obscure their real intentions, making attribution harder. Nation state actors have already been doing this for a while and have added ransomware to their cyberweapons since at least 2017.

Evolution 10: Adding Zero-Day Research/Purchase to Remove the Need for Access Brokers and Affiliates

Let us come back to the point we made about modern ransomware being a hacking operation with a ransomware payload. These groups are currently set up as pentesting teams that proactively find their way into and around the victim's network.

Currently, these hacking teams often look for a way into the network through a number of ways:

1. They buy stolen users' credentials from "Access-as-a-Service" (AaaS) sellers in the criminal underground. These sellers collect credentials from many sources, from data leaks to malware logs. These credentials can be used to access the company's VPN to join the internal network. They can also be used to access internal servers and cause further havoc.

2. They rely on affiliates who find the way into the network and pass access to the ransomware group in exchange for a share of the ransom or a fixed fee.
3. They use known vulnerabilities to open their own way into the network. To do this, they study the software installed on the target network and check if it is affected by known vulnerabilities that can be exploited. Then they acquire the exploits to make their way in.

A possible evolution is that these hacking groups start allocating resources to develop their own exploits for unknown (zero-day) vulnerabilities. If these groups are already willing to hire skilled hackers, they might as well hire an exploit developer. Having this skillset in-house would allow them to reuse a vulnerability over and over before it could be publicly known and patched, giving them a unique advantage over others in the ransomware space. In the long run, the return of investment generated by finding your own backdoor to victims might outweigh the cost and effort of finding exploitable zero-day vulnerabilities. To our knowledge, most of these groups are not yet doing vulnerability research, but this is a very real possibility.

This evolution would mean that these groups might upgrade their current hacking teams to become vulnerability research and exploitation teams. This is not out of the question, and it would also depend on the availability of people who could perform these tasks.

In cases where such availability is scarce, these groups could also have “first refusal” agreements with known high-profile exploit developers who have a proven track record of zero-day discoveries – especially in web-facing services that could be used for initial access. In this setup, instead of having a full-time internal exploit team, they would be paying to have the first look and right to buy any newly discovered exploits before the developer sells them to their normal clients on the criminal underground, via bug bounty programs, or to governments and similar customers.

The first sign that something like this might happen is the LockBit3.0 bug bounty program where the LockBit ransomware group offered hackers to buy vulnerabilities.¹²⁵ On September 17, 2022, LockBit posted a message they had awarded \$50,000 to somebody who found a weakness in LockBit’s encryption algorithm.



Figure 15. LockBit 3.0 bug bounty program payout announcement

Though Lockbit's bug bounty program is meant to reward vulnerability reports in its own infrastructure or encryption routines, a similar program could be set up to buy zero-day exploits in legitimate software.

Regardless of the exact method used, any initial access zero-days exploit could lead to a surge of successful attacks for the group that possess it, even long after official patches are available due to the length of corporate patch cycles.

Evolution Summary

Ransomware has been in an escalatory spiral in the last couple of years, with more and more enterprises, government institutions, hospitals, and even critical infrastructure falling victim to unscrupulous attacks with steadily increasing ransom demands. In 2022, the disruption and monetary losses due to ransomware has stabilized and will probably appear to have dropped at the end of the year. But that does not mean the ransomware problem has gone away. We expect that ransomware will be endemic, evolving gradually all the time with occasional periods of revolution — at which point, it will branch off and become something different. When ransomware actors act in a rational way, we might see more professionalism in the coming years: better operational security, the realization that Tor-hidden servers do not always remain hidden for determined security researchers and law enforcement, and more automation to increase revenue.

Recently, several reports were published showing ransomware is being utilized by nation state actors. Not so much with a monetary motive that would benefit dictators and their elites in countries that are subject to economic sanctions, but rather to create a smokescreen that covers the real intent. That intent could be espionage or destruction. This part of ransomware is expected to stay at least until ransomware is no longer popular among cybercriminals.

Evolutions that will have a big effect are the use of more zero-day exploits and attacking the cloud infrastructure. If initial access brokers start spending more resources on finding zero-days, vulnerabilities, and misconfigurations in cloud infrastructure, these could have a big impact on the success rate of ransomware and we might end up in an escalatory spiral again.

Some of the ransomware actors will go further than evolutionary steps, though. They will try big changes, especially if they are triggered by internal or external factors that force them to innovate their criminal business models. One large incentive to change a business model is the expectation to earn even more money. We will discuss possible revolutions that may be triggered by that and other factors in the next sections.

Trigger: A More Profitable Business Model Emerges

Statistics that have been published by the FBI in the Internet Crime Report 2021 show that there are several criminal business models whose estimated annual revenue far exceeds the annual revenue of ransomware.¹²⁶ These models include business email compromise (BEC), investment scams, tech support scams, advanced fee, identity theft, and more.

By Victim Loss			
	▼ ▲ = Trend from previous Year		
Crime Type	2021	2020	2019
Advanced Fee	\$98,694,137 ▲	\$83,215,405 ▼	\$100,602,297 ▲
BEC/EAC	\$2,395,953,296 ▲	\$1,866,642,107 ▲	\$1,776,549,688 ▲
Civil Matter	\$85,049,939 ▲	\$24,915,958 ▲	\$20,242,867 ▲
Confidence Fraud/Romance	\$956,039,739 ▲	\$600,249,821 ▲	\$475,014,032 ▲
Corporate Data Breach	\$151,568,225 ▲	\$128,916,648 ▲	\$53,398,278 ▼
Credit Card Fraud	\$172,998,385 ▲	\$129,820,792 ▲	\$111,491,163 ▲
Crimes Against Children	\$198,950 ▼	\$660,044 ▼	\$975,311 ▲
Denial of Service/TDoS	\$217,981 ▼	\$512,127 ▼	\$7,598,198 ▲
Employment	\$47,231,023 ▼	\$62,314,015 ▲	\$42,618,705 ▼
Extortion	\$60,577,741 ▼	\$70,935,939 ▼	\$107,498,956 ▲
Gambling	\$1,940,237 ▼	\$3,961,508 ▲	\$1,458,118 ▲
Government Impersonation	\$142,643,253 ▲	\$109,938,030 ▼	\$124,292,606 ▲
Health Care Related	\$7,042,942 ▼	\$29,042,515 ▲	\$1,128,838 ▼
Identity Theft	\$278,267,918 ▲	\$219,484,699 ▲	\$160,305,789 ▲
Investment	\$1,455,943,193 ▲	\$336,469,000 ▲	\$222,186,195 ▼
IPR/Copyright and Counterfeit	\$16,365,011 ▲	\$5,910,617 ▼	\$10,293,307 ▼
Lottery/Sweepstakes/Inheritance	\$71,289,089 ▲	\$61,111,319 ▲	\$48,642,332 ▼
Malware/Scareware/Virus	\$5,596,889 ▼	\$6,904,054 ▲	\$2,009,119 ▼
Non-Payment/Non-Delivery	\$337,493,071 ▲	\$265,011,249 ▲	\$196,563,497 ▲
Other	\$75,837,524 ▼	\$101,523,082 ▲	\$66,223,160 ▲
Overpayment	\$33,407,671 ▼	\$51,039,922 ▼	\$55,820,212 ▲
Personal Data Breach	\$517,021,289 ▲	\$194,473,055 ▲	\$120,102,501 ▼
Phishing/Vishing/Smishing/Pharming	\$44,213,707 ▼	\$54,241,075 ▼	\$57,836,379 ▲
Ransomware	\$49,207,908 ▲	\$29,157,405 ▲	\$8,965,847 ▲
Real Estate/Rental	\$350,328,166 ▲	\$213,196,082 ▼	\$221,365,911 ▲
Re-Shipping	\$631,466 ▼	\$3,095,265 ▲	\$1,772,692 ▲
Spoofing	\$82,169,806 ▼	\$216,513,728 ▼	\$300,478,433 ▲
Tech Support	\$347,657,432 ▲	\$146,477,709 ▲	\$54,041,053 ▲
Terrorism/Threats of Violence	\$4,390,720 ▼	\$6,547,449 ▼	\$19,916,243 ▲

Figure 16. Cybercriminal business models' profitability statistics

Data taken from the FBI's Internet Crime Report 2021¹²⁷

These statistics raise an interesting question: Why don't ransomware actors move to other business models altogether? There can be several reasons for this. Ransomware needs other skills than BEC, for example, which requires advanced social engineering and a good grasp of languages that may be foreign to the actors. Another reason is that ransomware is a very visible threat that gets a lot of media attention, and the fact that ransomware has been very profitable for criminals. Why change the mode when money is pouring in?

What Ransomware Looks Like When It Goes Through a Revolution

Sooner or later, ransomware actors will be triggered to change their criminal business models. This could happen through an evolution of relatively small changes, as described in the previous sections, or by more radical changes. In the coming sections, we discuss some of the more radical changes. In a lot of the scenarios we describe, the ransomware payload gets replaced by another payload or scheme while still allowing the attackers to leverage their core skillset. These alternative payloads are profitable by themselves, but would lead to even more profits when they become a part of the typical kill chain of today's targeted ransomware.

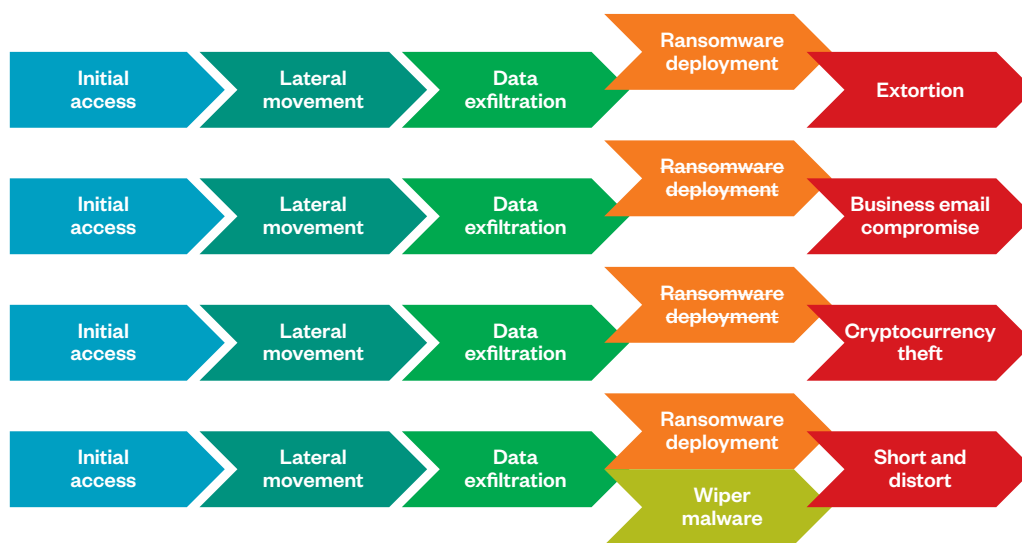


Figure 17. Potential changes from ransomware in adopted cybercriminal business models

Revolution 1: Hacking Into Crypto Exchanges/ Stealing Cryptocurrency

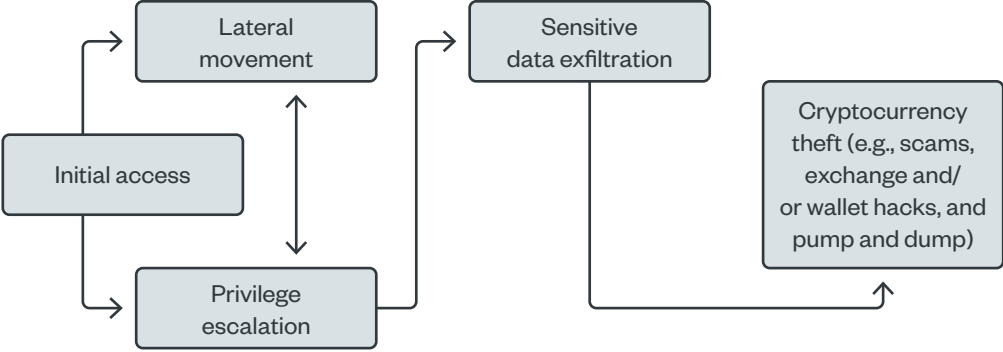


Figure 18. Shifting attention to cryptocurrency theft-related activities

Criminal actors make a lot of money with ransomware, but stealing cryptocurrency and fraud with cryptocurrency are even more profitable. In the 2022 crime report of Chainalysis, illicit activity involving cryptocurrency in 2021 was estimated to be at least \$14 billion.¹²⁸ This figure is in the lower bound that is likely to be corrected to a higher amount when more knowledge on illicit activities are known. The amount includes all known criminal activities, including ransomware payments, sales on Darknet websites, scams, and theft. Almost \$8 billion comes from scams where, for example, investors were duped after buying Decentralized Finance (DeFi) tokens whose code was not audited. More than \$3 billion worth of cryptocurrency was stolen in 2021, the majority of it done via compromised cryptocurrency exchanges. The growing trend of billions in stolen cryptocurrencies continued in Spring 2022.¹²⁹ In comparison, the profit made with ransomware is relatively modest — well under \$700 million in 2021.¹³⁰

This raises the question of why ransomware actors would stick with ransomware when they could earn a lot more with cryptocurrency schemes. Part of this could simply be because ransomware just works for a lot of actors, and they don't have any incentive to change their business tactics. However, a lot of today's ransomware attacks start with the breach of a company's network, and methodologies that used to get this initial access can also be applied to break into the networks of cryptocurrency exchanges. Once inside, the attackers can try to steal cryptocurrency instead of deploying ransomware.

The Lazarus group is one example of an actor group that has used ransomware and has stolen cryptocurrencies. This is a group that utilized the big potential by breaking into traditional and new financial service providers, and perhaps realized there is less money to be made with ransomware. Only a few documented ransomware incidents with an apparent monetary motive were attributed to the Lazarus actor.¹³¹ The group's biggest ransomware attack was WannaCry, which caused a lot of disruption for relatively low profit.¹³² But Lazarus made big profits with cryptocurrency theft and bank heists.

We expect that some of the large ransomware actors will become less active in ransomware and more active in hacking into cryptocurrency exchanges once they realize the potential and when they are triggered to change their business plans. The Conti leaks already suggested that ransomware actors developed an interest in cryptocurrency.¹³³ It was even suggested that Conti was involved in the Squid Game-themed crypto coin that first rose to a value of around \$2,862 per coin, and later collapsed to almost zero when the anonymous creators abandoned the project and exchanged many of the Squid coins for cash.¹³⁴ This is an example of a so-called rug-pull scheme,¹³⁵ which is basically a variant of pump and dump. A lot of the fraud schemes known to be used in stock manipulation can also be used on cryptocurrencies. Cybercriminals have been familiar with stock market pump and dump schemes for years.¹³⁶ It is, therefore, to be expected that cybercriminals will play their part in cryptocurrency fraud as well.

The big-volume ransomware actors could turn to other profitable schemes like stealing cryptocurrencies from wallets by either spreading stealer malware that are specifically designed to steal from various wallets, or doing credential phishing campaigns. Given the popularity of cryptocurrency among younger users, it is plausible there is more money to be made from internet users by stealing their cryptocurrency than by asking for a ransom after encrypting their personal files.

Revolution 2: Key Players Work for Governments

As ransomware actors gain more attention by breaking into large companies, this can gain the attention of the governments of the countries in which the actors reside, but for recruitment and not for prosecution. There have been previous examples of criminal hackers being recruited by companies and governments trying to shape them into non-criminal security practitioners. The United Kingdom has a program in which the National Crime Agency (NCA) aimed at reforming teenaged hackers in hopes to change them into more ethical hackers that could apply their skills in the information security field.¹³⁷ However, what if a country with different ethics encourages them to hack on behalf of the country instead? The skillsets built up in today's standard big game hunting ransomware business models are very transferrable to intrusions also favored by nation state actors. This can benefit APT groups to get more access to systems on the target list of the nation state groups.

In most countries around the world, this more offensive-oriented scenario is unlikely. However, there might be the cases wherein a ransomware actor is arrested and then convinced to become a hacker for the government as part of a deal to shorten the sentence. This can even be combined with being allowed to continue their criminal activities, as long as they are restricted to targeting regions considered of political interest to the state. This would likely be one of the scenarios that play out given ransomware actors will not want to give up their larger paychecks to work for a government that historically pays lower than the private industry, let alone large-scale crime.

During times of patriotism and national pride, some actors move towards government or pro-government hacktivism. This could include things from doing DDoS, web defacements, and even hacking on behalf of the government towards its enemies and opposition groups. In July of 2022, Killmilk, the leader of a pro-Russian DDoS hacktivism group called Killnet, announced they were leaving the group and that an actor known as BlackSide would be leading the group. In a statement, it said that BlackSide was experienced in other hacking activities including ransomware.¹³⁸ While this is not directly working with the government, it is working for pro-government groups going after high profile targets such as Lockheed Martin, not only with a DDoS attack but possibly even a breach of their networks within weeks after BlackSide was said to have joined the group.¹³⁹

It also has been alleged that in the 2022 war against Ukraine, initial access brokers who previously worked for the Conti RaaS shifted to helping the Russian government in an effort against Ukraine assets.¹⁴⁰ This shows that during times when patriotism is high, criminal hackers will help what they feel is the cause of their country's government or the country they support to aid efforts in the cyber side of conflicts and wars. This can also be done for self-preservation — for example, if they appear to be acting in the interest of their country of residence, then this could help them avoid negative consequences for their actions.

Such high-profile graduation from crime to government roles could see several major players leave the ransomware market in the future, only for their tactics, techniques, and procedure (TTP) of choice to later emerge in attacks attributed to more APT groups.

Revolution 3: Crossing Paths With Traditional Organized Crime/Mafia

Cyber criminology is still under development with limited scientific literature on the relation between traditional organized crime and cybercrime, but existing studies have provided insight into how organized cybercrime is. There is an argument that there are some relations between organized crime and cybercrime,¹⁴¹ but there is no convincing evidence that organized crime is taking over cybercrime; traditional organized crime is rather using IT and the internet to make their operations more efficient.

Mafia and traditional organized crime work differently than cybercriminals. Involuntary protection for a fee is a common mafia-related scheme, but this kind of protection is not observed among cybercriminals. Cybercriminals rather need protection against law enforcement, who could take their business down and make arrests. Hence, cybercriminals have more incentive to get protection from politicians and/or law enforcement, for example, by paying bribes or working for governments too.

Another clear difference is that the Mafia wants to control criminal businesses in a certain geographical area, while cybercriminals are not bound by their location to commit crimes.

There are a few areas where cybercriminals and traditional organized crime meet: money laundering, facilitating crime, and a few instances of cybercrime. A report by Jonathan Lusthaus mentioned examples where organized crime helped cybercriminals launder money: the Citibank hack of 1994 and carding.¹⁴² In other cases, traditional organized crime hired cybercriminals to facilitate a drug crime, like hacking computers of container terminals in Antwerp¹⁴³ and ATM cash-out incidents. In 2013, Europol announced the arrest of more than 100 suspects who were involved in BEC, a very profitable cybercrime business.¹⁴⁴ Some of the suspects were said to be related to the Mafia in Italy.

The Conti leaks did not show any evidence that the group is working with traditional crime groups. But we can envision that sooner or later, traditional organized crime will be interested in ransomware, simply because of the enormous criminal revenues RaaS groups are making. While this would require a noticeable step up in technical skillsets, a shake-up in the world of cybercrime is then to be expected. We foresee faster and more professional money laundering schemes, more investments in cybercrime businesses, and rivalries between different cybercrime gangs.

Revolution 4: Leverage the Same Kill Chain for Stock Market Manipulation

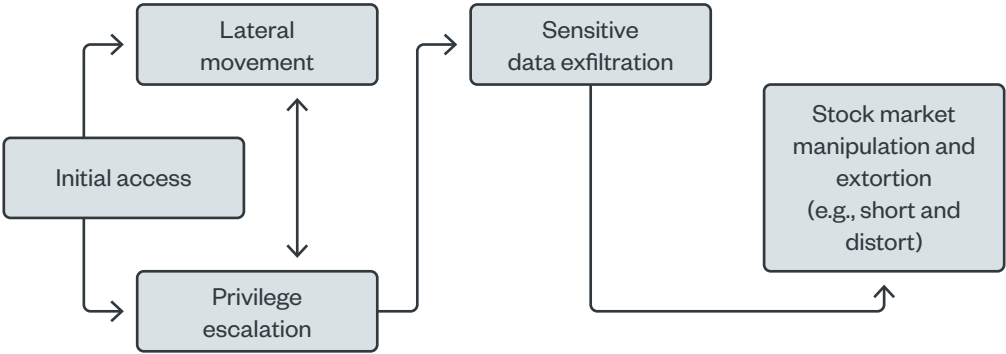


Figure 19. Shifting to stock market manipulation via short and distort

In 2021, the RaaS group Darkside presented another way to extort their victims who are listed on the stock exchange.¹⁴⁵ Prior to making a ransomware infection public, Darkside planned on informing stock traders who could leverage the expected dip in the stock price of the ransomware victim by shorting the victim’s stocks. In this scheme, the trader would borrow stocks from an investor, sell them to another investor, and buy them back when the stock price has dropped. The trader would then make a profit from the difference in stock price.

At first sight, this looks like a naive approach that would not bear much fruit. The time window to act for rogue traders is limited and unusual patterns in short selling of stocks might get noticed by regulating authorities. Darkside aimed to use this scheme as an extortion method and that is most likely not going to work very well.

However, there is a variant of the Darkside plans that could net the cybercriminals a larger profit. In this variant, the cybercriminal would use a form of what is known as “short and distort”.¹⁴⁶ In a “short and distort” scheme, a trader takes a short position on a stock of a company and then starts to spread false rumors on the company that drives the stock price down.

In case a cybercriminal has breached a corporate network of a large enterprise, the actor can quietly look around on the network and collect sensitive data for several weeks. During that time, the cybercriminal has time to go short on the stocks of the victimized company. When the time is right, the cybercriminal can either start to spread sensitive information from the victim company, make it public that the company has been breached, or disrupt operations by deploying destructive malware. In all cases, the stock is expected to drop immediately. Even if this drop is temporary, the potential profits could be huge.

For this to work, the cybercriminal needs some capital to be able to buy short positions and it must have knowledge of stock trading. These are not real obstacles as ransomware actors have earned millions in earlier attacks they could invest in a more profitable crime, and cybercriminals already have shown that they are capable of working with other schemes that manipulate stock prices, like pump and dump.¹⁴⁷

It has been reported that investors are not that concerned when companies suffer from a data breach or ransomware infection. However, there is anecdotal evidence of noticeable drops in stock prices on the day a breach or ransomware infection is made public.¹⁴⁸ A temporary drop in the stock price is enough for a short-and-distort scheme.

Research suggests that profits of short-and-distort schemes can amount to hundreds of millions of dollars.¹⁴⁹ This exceeds the profits made by ransomware actors by far, so we think there is an incentive for cybercriminals to replace their ransomware payload with such a scheme in case they have breached a large enterprise with a stock listing.

Revolution 5: Merger With a Top-Tier Non-Ransomware Group

To increase profits and efficiency, a RaaS group could merge with or acquire another non-ransomware group. As an example, a top-tier AaaS group could decide to start working for a RaaS group exclusively and even merge with the RaaS group. Or a money laundering-as-a-Service group could be acquired to work exclusively for a group like Water Goblin, the larger group that owned Conti. The obvious advantages of these mergers or acquisitions are efficacy and a way for ransomware actors to cut costs. Their larger size can also help them become a market leader in the cybercriminal underground.

To explore other criminal business models outside their current focus, a RaaS group could also look into acquiring other criminal organizations that have a specialized expertise in a particular field. This is especially relevant when a RaaS actor wants to make more radical steps and invest money in other criminal businesses with potentially large returns, such as cryptocurrency fraud, stock market fraud, and BEC.

Just as in traditional businesses, such mergers and acquisitions can allow a successful, well-run RaaS group to either strengthen their core business, or to quickly gain market share in a new criminal vertical backed by an initial large investment.

Revolution 6: Supply Chain Compromise as a Service

Supply chain attacks have been a tool of cybercriminals for at least a decade.¹⁵⁰ With the rise of targeted ransomware over the past few years, supply chain attacks also happened for the purpose of spreading ransomware to as many victims as possible. This was observed with the 2021 attack on Kaseya, an IT solutions company that sells network management software. A vulnerability was leveraged in one of the company's popular products, which allowed REvil-affiliated attackers to deploy ransomware through their managed software providers. About 800 to 1,500 companies were estimated to have fallen victim because of this supply chain attack.¹⁵¹ Even if only a few of these victims paid the ransom, this would have been a very profitable attack for the criminals.

In 2017, there was the well-known attack called NotPetya. NotPetya leveraged an attack on a software company called MeDoc, a software platform used primarily in Ukraine, but not exclusively.¹⁵² Almost 80% of companies in Ukraine were estimated to have been using MeDoc software prior to the attack.¹⁵³ This company became a prime target for the attackers who wanted to hit as many victims in a specific region as possible. But NotPetya was found to have used ransomware as a smokescreen — its real intent was to create chaos and destroy computer systems. The attack has been attributed to a nation state actor called Sandworm.¹⁵⁴

Supply chain attacks have been increasing in recent years and the fear of them being utilized in ransomware attacks is being realized. The issue at hand is that a lot of software around the world depends on other software that is authored and maintained by developer companies. Compromising these companies allows attackers to push malicious updates that customers trust implicitly. While supply chain attacks have been a fear for national security networks for a long time, it is likely that ransomware actors will try to compromise software supply chains more often to extort as many victims as possible. Compromising a supply chain would allow ransomware groups to cut out the outsourced initial access of their business models while giving them a unique, scalable, and repeatable source of new victims.

Revolution 7: Replace Ransomware Payload With Business Email Compromise (BEC)

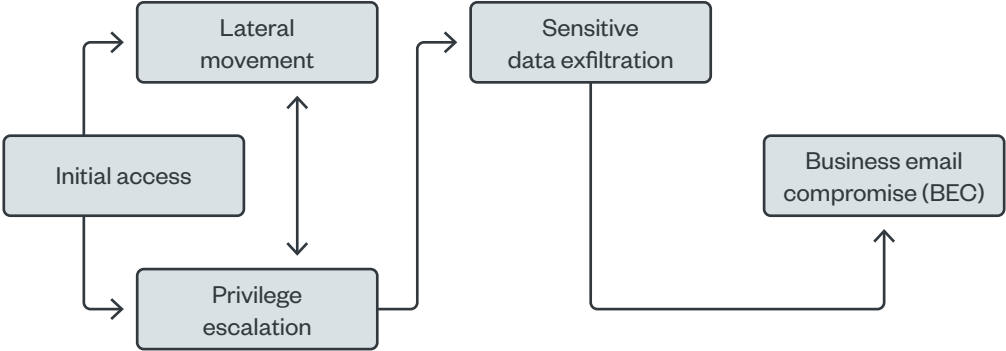


Figure 20. Shifting to BEC

Business email compromise (BEC) attacks are a scam that involves tricking high ranking employees in a company into wiring a large sum of money to an attacker.¹⁵⁵ BEC often utilizes publicly available information on company’s executives. No malware or credential phishing is needed per se, though there are cases where a compromise of the corporate network or a supplier is also involved. BEC is highly profitable: In 2016, the average losses per victimized company was estimated at \$160,000 USD. In May 2022, the FBI reported that the losses worldwide between June 2016 and December 2021 due to BEC amounted to \$43 billion.¹⁵⁶ This shows that BEC is a huge problem and that results in higher profits for cybercriminals compared to ransomware.

This naturally raises the question why actors would not replace the ransomware payload in the kill chain with a BEC attack. After the initial access phase, the lateral movement phase and theft of sensitive information, an attacker could choose not to deploy ransomware but to utilize the stolen information for a BEC attack. Compared with a BEC attack that starts from data obtained from open-source intelligence methods alone, this would give the attacker much more powerful tools in hand as it is based on actual (stolen) insider information.

When a ransomware actor turns to BEC, he will start with a different business model that needs different skills. The attacker will no longer bluntly demand a ransom and will instead need to socially engineer executives into wiring fiat money to a banking account. That is different from receiving cryptocurrency after deploying ransomware that makes files and computer systems inaccessible. The costs of the learning curve will most likely pay off for the ransomware actor, so we expect it to be just a matter of time before more ransomware actors turn to BEC schemes. Alternatively, they could hire new team members with previous expertise in this area.

A comparison between ransomware and BEC was also recently presented at the 2022 RSA conference.¹⁵⁷

Conclusions

We can trace the current ransomware business model back to other various threats that aimed to extort money from victims with increasingly aggressive arguments. The criminal groups designing and operating these threats always strive to improve their business plans to be more effective and lucrative. The attacks we are seeing today are a step in their evolution, but they really became a major problem to society as actors drastically changed their business model from some of the world's most successful banking trojans to targeted ransomware. It is exactly these actors that could be triggered to change their business model again in the future.

What will the future be like for ransomware attacks? In what possible ways will they continue to evolve? Our thinking is that there could be a smooth evolution and gradual improvement of ransomware and a revolution of the ransomware business plan that branches off, either simultaneously or in the long term.

The evolution route is something we have come to expect from criminals that compete against each other. They regularly try to improve their attacks to be more effective and earn them more money. We enumerated many ways that criminals could enhance their creations, from focusing on data monetization to improving their payloads to new platforms. There are many possible ways criminals could enhance their processes based on how they already operate today: increase automation, improve their professionalism, start their own zero-day research, or focus on DDoS attacks to complement their income.

On the other hand, if the economic or geopolitical environment forces ransomware attackers to alter their business plan significantly, we could witness a larger change — a revolution, in our terminology. This is not unlikely since we have already seen this threat significantly change a few times in the past.

It is possible that these groups join forces with other groups with different business plans: governments, organized crime, or other non-ransomware groups. They could also replace their current ransomware payloads to create a new business plan: phishing for crypto-wallets, stock manipulation, supply chain compromise, or even BEC. Hacking cryptocurrency exchanges could also be a potentially fruitful avenue for them.

Whether any of these possibilities come to pass, ransomware will undoubtedly change from its current state. Performing this thought exercise can allow network defenders to prepare ahead of time and assess if their future defense strategies may be enough to counter newer potential criminal business plans.

As for the current breed of ransomware, defenders need to keep in mind that these groups run hacking operations with a ransomware payload. Those who plan to defend their organization must have full visibility on all possible ongoing intrusions. Merely detecting the ransomware encryption guarantees that you are too late. Instead, focus on finding signs that somebody is trying to break in and move around the organization. This is better accomplished with detection and response (XDR) software solutions that raise flags whenever there are separate signs of a potential intrusion, and protecting systems as far to the left in the kill chain as possible.

On the other hand, government sanctions are only marginally effective as a countermeasure, and, if implemented well, can probably only force an evolution of the threat to its next iteration. To succeed in the fight against ransomware, law enforcement agencies need to team up with the security industry for impactful and longer lasting results, with a particular focus on initial access brokers and those that enable initial compromise of organizations at scale.

Overall, we cannot allow ourselves to be distracted by the very visible final payload of these attacks and miss what enables them to exist in the first place.

References

- 1 Trend Micro. (n.d.) *Trend Micro*. “Ransomware.” Accessed on Nov. 2, 2022, at <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>.
- 2 Mandiant Intelligence. (June 2, 2022). *Mandiant*. “To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions.” Accessed on Oct. 17, 2022, at <https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions>.
- 3 Ivan Nechepurenko. (Jan. 14, 2022). *The New York Times*. “Russia Says It Shut Down Notorious Hacker Group at U.S. Request.” Accessed on Oct. 17, 2022, at <https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html>.
- 4 Trend Micro Threat Research. (Dec. 20, 2021). *Trend Micro*. “Ransomware Spotlight: REvil.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil>.
- 5 Trend Micro. (n.d.) *Trend Micro*. “Ransomware as a Service (RaaS).” Accessed on Nov. 2, 2022, at <https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas>.
- 6 Lawrence Abrams. (May 1, 2022). *Bleeping Computer*. “REvil ransomware returns: New malware sample confirms gang is back.” Accessed on Oct. 17, 2022, at <https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/>.
- 7 Sean Lyngaas. (Mar. 20, 2022). *CNN*. “I can fight with a keyboard’: How one Ukrainian IT specialist exposed a notorious Russian ransomware gang.” Accessed on Oct. 17, 2022, at <https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html>.
- 8 Microsoft Defender Threat Intelligence. (June 13, 2022). *Microsoft*. “The many lives of BlackCat ransomware.” Accessed on Oct. 17, 2022, at <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>.
- 9 Trend Micro Research. (Oct. 27, 2022). *Trend Micro*. “Ransomware Spotlight: BlackCat.” Accessed on Nov. 2, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat>.
- 10 Coveware. (July 28, 2022). *Coveware*. “Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022.” Accessed on Oct. 17, 2022, at <https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>.
- 11 Trend Micro. (April 6, 2020). *Trend Micro*. “Information on how you can unmask Fake Antivirus (AV).” Accessed on Oct. 17, 2022, at https://community-trendmicro.force.com/dcx/s/solution/1055340-information-on-how-you-can-unmask-fake-antivirus-av?language=en_US.
- 12 Raphael Centeno. (May 8, 2019). *Trend Micro*. “Dharma Ransomware Uses AV Tool to Hide Activities.” Accessed on Oct. 17, 2022, at https://www.trendmicro.com/en_ie/research/19/e/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities.html.
- 13 Trend Micro. (n.d.) *Trend Micro*. “Ransomware Spotlight.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight>.
- 14 Mayra Fuentes, et. Al. (June 8, 2021). *Trend Micro Research*. “Modern Ransomware’s Double Extortion Tactics and How to Protect Enterprises Against Them.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them>.
- 15 Trend Micro. ((Dec. 6, 2019). *Trend Micro*. “US, UK Governments Unite to Indict Hacker Behind Dreaded Dridex Malware.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/us-uk-governments-unite-to-indict-hacker-behind-dreaded-dridex-malware>.
- 16 Trend Micro Research. (Nov. 30, 2021). *Trend Micro*. “Investigating the Emerging Access-as-a-Service Market.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market>.
- 17 Trend Micro Research. (Dec. 1, 2021). *Trend Micro*. “Ransomware Spotlight: Conti.” Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 18 Vlad Stolyarov and Benoit Sevens. (Mar. 17, 2022). *Google Threat Analysis Group*. “Exposing initial access broker with ties to Conti.” Accessed on Oct. 17, 2022, at <https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/>.
- 19 Microsoft Threat Intelligence Center and Digital Security Unit. (July 14, 2022). *Microsoft*. “North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware.” Accessed on Oct. 17, 2022, at <https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/>.
- 20 Catalin Cimpanu. (Feb. 7, 2022). *Recorded Future*. “NetWalker ransomware affiliate sentenced to seven years in prison.” Accessed on Oct. 17, 2022, at <https://therecord.media/netwalker-ransomware-affiliate-sentenced-to-seven-years-in-prison/>.

- 21 Trend Micro Research. (Dec. 1, 2021). *Trend Micro*. "Ransomware Spotlight: Conti." Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti>.
- 22 Trend Micro Research. (Dec. 20, 2021). *Trend Micro*. "Ransomware Spotlight: REvil." Accessed on Oct. 17, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil>.
- 23 Microsoft Defender Threat Intelligence. (June 13, 2022). *Microsoft*. "The many lives of BlackCat ransomware." Accessed on Oct. 17, 2022, at <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>.
- 24 Elie Bursztein, Kylie McRoberts, and Luca Invernizzi. (July 26, 2017). *Google*. "Tracking desktop ransomware payments." Accessed on Oct. 17, 2022, at <https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf>.
- 25 Cyble. (June 17, 2022). *Cyble*. "Cerber2021 Ransomware Back in Action." Accessed on Oct. 17, 2022, at <https://blog.cyble.com/2022/06/17/cerber2021-ransomware-back-in-action/>.
- 26 US Department of Justice. (Sept. 6, 2018). *US Department of Justice*. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." Accessed on Oct. 17, 2022, at <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>.
- 27 US Department of Justice. (Feb. 17, 2021). *US Department of Justice*. "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe." Accessed on Oct. 17, 2022, at <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>.
- 28 Symantec Threat Hunter Team. (Feb. 24, 2022). *Symantec*. "Ukraine: Disk-wiping Attacks Precede Russian Invasion." Accessed on Oct. 17, 2022, at <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia>.
- 29 Counter Threat Unit Research Team. (June 23, 2022). *SecureWorks*. "BRONZE STARLIGHT Ransomware Operations Use HUI Loader." Accessed on Oct. 18, 2022, at <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>.
- 30 Microsoft Defender Threat Intelligence and Threat Intelligence Center (MSTIC). (May 9, 2022). *Microsoft*. "Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself." Accessed on Oct. 18, 2022, at <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>.
- 31 FBI Internet Crime Complaint Center (IC3). (July 6, 2022). *Internet Crime Complaint Center*. "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector." Accessed on Oct. 18, 2022, at <https://www.ic3.gov/Media/News/2022/220706.pdf>.
- 32 Silas Cutler. (June 7, 2022). *Stairwell*. "Maui ransomware." Accessed on Oct. 18, 2022, at <https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf>.
- 33 Microsoft Threat Intelligence Center and Digital Security Unit. (July 14, 2022). *Microsoft*. "North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware." Accessed on Oct. 17, 2022, at <https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/>.
- 34 Cybereason Nocturnus. (Feb. 1, 2022). *Cybereason*. "StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations." Accessed on Oct. 18, 2022, at <https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations>.
- 35 US Department of the Treasury. (Dec. 5, 2019). *US Department of the Treasury*. "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware." Accessed on Oct. 18, 2022, at <https://home.treasury.gov/news/press-releases/sm845>.
- 36 Trevor Hunicutt. (July 4, 2021). *Reuters*. "Biden orders probe of latest ransomware attack". Accessed on Oct. 18, 2022, at <https://www.reuters.com/technology/biden-says-uncertain-who-is-behind-latest-ransomware-attack-2021-07-03/>.
- 37 Cybersecurity and Infrastructure Security Agency (CISA). (Feb. 9, 2022). *National Security Agency/Central Security Service*. "CISA, FBI, NSA and International Partners Issue Advisory on Ransomware Trends from 2021." Accessed on Oct. 18, 2022, at <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2928709/cisa-fbi-nsa-and-international-partners-issue-advisory-on-ransomware-trends-fro/>.
- 38 Catalin Cimpanu. (Oct. 7, 2021). *Recorded Future*. "Netherlands can use intelligence or armed forces to respond to ransomware attacks." Accessed on Oct. 18, 2022, at <https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/>.
- 39 Matt Burgess. (Mar. 18, 2022). *Wired*. "Leaked Ransomware Docs Show Conti Helping Putin From the Shadows." Accessed on Oct. 18, 2022, at <https://www.wired.com/story/conti-ransomware-russia/>.

- 40 Ivan Nechepurenko. (Jan. 14, 2022). *The New York Times*. "Russia Says It Shut Down Notorious Hacker Group at U.S. Request." Accessed on Oct. 17, 2022, at <https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html>.
- 41 US Department of Justice. (Nov. 8, 2021). *US Department of Justice*. "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya." Accessed on Oct. 18, 2022, at <https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>.
- 42 Catalin Cimpanu. (Dec. 13, 2021). *Recorded Future*. "Ransomware affiliate arrested in Romania." Accessed on Oct. 18, 2022, at <https://therecord.media/ransomware-affiliate-arrested-in-romania/>.
- 43 Lawrence Abrams. (May 1, 2022). *Bleeping Computer*. "REvil ransomware returns: New malware sample confirms gang is back." Accessed on Oct. 17, 2022, at <https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/>.
- 44 Kim Grauer and Henry Updegrave. (2021). *Chainalysis*. "The 2021 Crypto Crime Report." Accessed on Oct. 18, 2022, at <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.
- 45 Kim Grauer, Will Kueshner, and Henry Updegrave. (2022). *Chainalysis*. "The 2022 Crypto Crime Report." Accessed on Oct. 19, 2022, at <https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf>.
- 46 Sean Foley, Jonathan R. Karlsen, and Tālis J Putniņš. (2019). *Oxford University Press*. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?" *The Review of Financial Studies*, Vol. 32, Issue no. 5, p. 1798–1853.
- 47 CN-SEC Chinese Net. (June 6, 2022). *CN-SEC Chinese Net*. "警惕WEB服务漏洞! 7Locker勒索来袭" Accessed on Oct. 18, 2022, at <https://cn-sec.com/archives/1092089.html>.
- 48 Elena Fabrichnaya and Alexander Marrow. (Jan. 21, 2022). *Reuters*. "Russia proposes ban on use and mining of cryptocurrencies" Accessed on Oct. 18, 2022, at <https://www.reuters.com/business/finance/russian-cbank-proposes-banning-cryptocurrencies-crypto-mining-2022-01-20/>.
- 49 Andrew E. Kramer. (Dec. 6, 2021). *The New York Times*. "Companies Linked to Russian Ransomware Hide in Plain Sight." Accessed on Oct. 18, 2022, at <https://www.nytimes.com/2021/12/06/world/europe/ransomware-russia-bitcoin.html>.
- 50 Reuters. (Jul. 8, 2022). *Reuters*. "Russia to improve crypto transaction monitoring as regulation draws closer." accessed on Oct. 18, 2022, at <https://www.reuters.com/technology/russia-improve-crypto-transaction-monitoring-regulation-draws-closer-2022-07-08/>.
- 51 The White House. (Mar. 9, 2022). *The White House*. "President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets." Accessed on Oct. 18, 2022, at <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/>.
- 52 Council of the EU. (June 30, 2022). *Council of the European Union*. "Digital finance: agreement reached on European crypto-assets regulation (MiCA)." Accessed on Oct. 18, 2022, at <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.
- 53 European Parliament Committee on Economic and Monetary Affairs. (Mar. 31, 2022). *European Parliament*. "Crypto assets: new rules to stop illicit flows in the EU." Accessed on Oct. 19, 2022, at <https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu>.
- 54 Council of the EU. (July 30, 2022). *Council of the European Union*. "EU imposes the first ever sanctions against cyber-attacks." Accessed on Oct. 19, 2022, at <https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>.
- 55 The US Attorney's Office. (May 28, 2013). *US Department of Justice*. "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A \$6 Billion Money Laundering Scheme." Accessed on Oct. 19, 2022, at <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest>.
- 56 Danny Palmer. (May 10, 2022). *ZDNet*. "Ransomware has gone down because sanctions against Russia are making life harder for attackers." Accessed on Oct. 19, 2022, at <https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/>.
- 57 Tim Starks. (Aug. 17, 2022). *The Washington Post*. "The Cybersecurity 202: Is the drop in ransomware numbers an illusion?" Accessed on Oct. 19, 2022, at <https://www.washingtonpost.com/politics/2022/08/17/is-drop-ransomware-numbers-an-illusion/>.

- 58 Valéry Rieß-Marchive. (Dec. 10, 2021). *LeMagIT*. “Ransomware : comment la franchise LockBit 2.0 gonfle artificiellement ses chiffres” Accessed on Oct. 19, 2022, at <https://www.lemagit.fr/actualites/252510802/Ransomware-comment-la-franchise-LockBit-20-gonfle-artificiellement-ses-chiffres>.
- 59 Valéry Rieß-Marchive. (Feb. 2, 2022). *LeMagIT*. “Ransomware : LockBit ne semble pas avoir touché le ministère de la Justice.” Accessed on Oct. 19, 2022, at <https://www.lemagit.fr/actualites/252512817/Ransomware-LockBit-ne-semble-pas-avoir-touche-le-ministere-de-la-Justice>.
- 60 PRODAFT Threat Intelligence Team. (Apr. 14, 2022). *PRODAFT*. “PYSA (Mespinoza) In-Depth Analysis.” Accessed on Oct. 19, 2022, at https://www.prodaft.com/m/reports/PYSA_TLPWHITE_3.0.pdf.
- 61 Mandiant Intelligence. (June 2, 2022). Mandiant. “To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions.” Accessed on Oct. 17, 2022, at <https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions>.
- 62 Counter Threat Unit Research Team. (June 23, 2022). *SecureWorks*. “BRONZE STARLIGHT Ransomware Operations Use HUI Loader.” Accessed on Oct. 18, 2022, at <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>.
- 63 Kartikay Mehrotra and William Turton. (May 21, 2022). Bloomberg. “CNA Financial Paid \$40 Million in Ransom After March Cyberattack.” Accessed on Oct. 19, 2022, at <https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack>.
- 64 Magno Logan (Oct. 8, 2022). *Trend Micro*. “Minding the Gaps: The State of Vulnerabilities in Cloud Native Applications.” Accessed on Oct. 19, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications>.
- 65 Shodan. (n.d.). Shodan. “Shodan Trends: Port 3389.” Accessed on Oct. 19, 2022, at <https://trends.shodan.io/search?query=port%3A3389>.
- 66 Jay Chen. (Aug. 12, 2019). Palo Alto Networks Unit 42. “Hunting the Public Cloud for Exposed Hosts and Misconfigurations.” Accessed on Oct. 19, 2022, at <https://unit42.paloaltonetworks.com/hunting-the-public-cloud-for-exposed-hosts-and-misconfigurations/>.
- 67 Joseph Menn and Christopher Bing. (Oct. 22, 2021). *Reuters*. “Governments turn tables on ransomware gang REvil by pushing it offline.” Accessed on Oct. 19, 2022, at <https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/>.
- 68 Benoit Ancel. (Jan. 25, 2021). *CSIS TechBlog*. “The Nemty affiliate model.” Accessed on Oct. 19, 2022, at <https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b>.
- 69 PRODAFT Threat Intelligence Team. (June 18, 2021). *PRODAFT*. “LockBit RaaS In-Depth Analysis.” Accessed on Oct. 19, 2022, at https://www.prodaft.com/m/reports/LockBit_Case_Report__TLPWHITE.pdf.
- 70 PRODAFT Threat Intelligence Team. (Nov. 18, 2021). *PRODAFT*. “Conti Ransomware Group In-Depth Analysis.” Accessed on Oct. 19, 2022, at https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf.
- 71 PRODAFT Threat Intelligence Team. (Apr. 14, 2022). *PRODAFT*. “PYSA (Mespinoza) In-Depth Analysis.” Accessed on Oct. 19, 2022, at https://www.prodaft.com/m/reports/PYSA_TLPWHITE_3.0.pdf.
- 72 Sean Lyngaas. (Mar. 20, 2022). *CNN*. “‘I can fight with a keyboard’: How one Ukrainian IT specialist exposed a notorious Russian ransomware gang.” Accessed on Oct. 17, 2022, at <https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html>.
- 73 Brian Krebs. (March 1, 2022). *Krebs on Security*. “Conti Ransomware Group Diaries, Part I: Evasion.” Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>.
- 74 Brian Krebs. (March 2, 2022). *Krebs on Security*. “Conti Ransomware Group Diaries, Part II: The Office.” Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/>.
- 75 Brian Krebs. (March 4, 2022). *Krebs on Security*. “Conti Ransomware Group Diaries, Part III: Weaponry.” Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>.
- 76 Brian Krebs. (March 7, 2022). *Krebs on Security*. “Conti Ransomware Group Diaries, Part IV: Cryptocrime.” Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/>.
- 77 Infinitum IT. (April 8, 2022). *Infinitum IT*. “Conti Ransomware Group Behind the Karakurt Hacking Team.” Accessed on Oct. 20, 2022, at <https://www.infinitumit.com.tr/conti-ransomware-group-behind-the-karakurt-hacking-team/>.
- 78 PRODAFT Threat Intelligence Team. (May 16, 2022). *PRODAFT*. “Wizard Spider In-Depth Analysis.” Accessed on Oct. 20, 2022, at https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf.

- 79 Lawrence Abrams. (June 24, 2022). *Bleeping Computer*. "Conti ransomware finally shuts down data leak, negotiation sites." Accessed on Oct. 20, 2022, at <https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/>.
- 80 Perry Carpenter. (July 9, 2021). *Forbes*. "Ransomware: Five Reasons Why Victim Organizations Pay Up." Accessed on Oct. 20, 2022, at <https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/09/ransomware-five-reasons-why-victim-organizations-pay-up/?sh=39030d124f66>.
- 81 Brian Krebs. (March 23, 2022). *Krebs on Security*. "A Closer Look at the LAPSUS\$ Data Extortion Group." Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/>.
- 82 Lawrence Abrams. (March 22, 2022). *Bleeping Computer*. "Lapsus\$ hackers leak 37GB of Microsoft's alleged source code." Accessed on Oct. 20, 2022, at <https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/>.
- 83 Uber. (Sept. 16, 2022). *Uber*. "Security Update." Accessed on Oct. 20, 2022, at <https://www.uber.com/newsroom/security-update>.
- 84 Lawrence Abrams. (Sept. 18, 2022). *Bleeping Computer*. "GTA 6 source code and videos leaked after Rockstar Games hack." Accessed on Oct. 20, 2022, at <https://www.bleepingcomputer.com/news/security/gta-6-source-code-and-videos-leaked-after-rockstar-games-hack/>.
- 85 Lily Hay Newman. (Sept. 27, 2022). *Wired*. "The Dire Warnings in the Lapsus\$ Hacker Joyride." Accessed on Oct. 20, 2022, at <https://www.wired.com/story/lapsusdollar-uber-rockstar-breach-multifactor-authentication-weaknesses/>.
- 86 Carly Page. (Sept. 26, 2022). *TechCrunch*. "UK police arrest teenager suspected of Uber, GTA 6 hacks." Accessed on Oct. 20, 2022, at https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACZOFRx-NQOZGstKZ2VykdMCDp6T9wL3MXZT8wXGbagpW0qqCBP_shEBCTYDlomMuEshB6TvojRB8euphC6Olqab22Fla2CrrJvn8Ya7.
- 87 Charlie Osborne. (May 13, 2021). *ZDNet*. "Colonial Pipeline ransomware attack: Everything you need to know." Accessed on Oct. 20, 2022, at <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>.
- 88 The White House. (May 13, 2022). *The White House*. "Remarks by President Biden on the Colonial Pipeline Incident." Accessed on Oct. 20, 2022, at <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/>.
- 89 Vladimir Kropotov and Fyodor Yarochkin. (Nov. 16, 2020). *Trend Micro*. "Cybercriminal 'Cloud of Logs'." Accessed on Oct. 20, 2022, at <https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data>.
- 90 Accenture. (Aug. 11, 2022). *Accenture*. "How cybercriminals are weaponizing leaked ransomware data for follow-up attacks." Accessed on Oct. 20, 2022, at <https://www.accenture.com/us-en/blogs/security/cybercriminals-weaponizing-leaked-ransomware-data>.
- 91 Bandwidth. (Oct. 26, 2021). *SEC*. "Bandwidth Announces Preliminary Third Quarter 2021 Revenue Results Exceeding Guidance and Estimated Full Year Revenue Impact of DDoS Attack." Accessed on Oct. 20, 2022, at <https://www.sec.gov/Archives/edgar/data/1514416/000151441621000280/q32021exh991-preliminaryth.htm>.
- 92 Larry Cashdollar. (May 25, 2022). *Akamai*. "REvil Resurgence? Or a Copycat?" Accessed on Oct. 20, 2022, at <https://www.akamai.com/blog/security/revil-resurgence-or-copycat>.
- 93 Nelli Klepfish. (Mar. 4, 2022). *Imperva*. "Imperva Mitigates Ransom DDoS Attack Measuring 2.5 Million Requests per Second." Accessed on Oct. 20, 2022, at <https://www.imperva.com/blog/imperva-mitigates-ransom-ddos-attack-measuring-2-5-million-requests-per-second/>.
- 94 Lily Hay Newman. (Oct. 16, 2020). *Wired*. "Fancy Bear Imposters Are on a Hacking Extortion Spree." Accessed on Oct. 20, 2022, at <https://www.wired.com/story/ddos-extortion-hacking-fancy-bear-lazarus-group/>.
- 95 Matthew Prince. (Apr. 25, 2016). *Cloudflare*. "Empty DDoS Threats: Meet the Armada Collective." Accessed on Oct. 20, 2022, at <https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/>.
- 96 FBI Internet Crime Complaint Center (IC3). (March 17, 2022). *Internet Crime Complaint Center*. "Indicators of Compromise Associated with AvosLocker Ransomware." Accessed on Oct. 20, 2022, at <https://www.ic3.gov/Media/News/2022/220318.pdf>.
- 97 FBI Internet Crime Complaint Center (IC3). (Oct. 28, 2021). *Internet Crime Complaint Center*. "Tactics, Techniques, and Indicators of Compromise Associated with Hello Kitty/FiveHands Ransomware." Accessed on Oct. 20, 2022, at <https://www.ic3.gov/Media/News/2021/211029.pdf>.

- 98 Damian Menscher. (Oct. 17 2020). *Google*. "Exponential growth in DDoS attack volumes." Accessed on Oct. 20, 2022, at <https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks>.
- 99 Mayra Rosario Fuentes, et. Al. (Mar. 29, 2022). *Trend Micro*. "A Floating Battleground Navigating the Landscape of Cloud-Based Cryptocurrency Mining." Accessed on Oct. 20, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-navigating-the-landscape-of-cloud-based-cryptocurrency-mining.pdf.
- 100 David Fiser and Alfredo Oliveira. (March 9, 2022). *Trend Micro*. "APT & Targeted Attacks TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_us/research/21/c/teamtnt-continues-attack-on-the-cloud--targets-aws-credentials.html.
- 101 Microsoft Security Response Center. (Sept. 1, 2022). *Microsoft*. "Vulnerability Fixed in Azure Synapse Spark." Accessed on Oct. 20, 2022, at <https://msrc-blog.microsoft.com/2022/09/01/vulnerability-fixed-in-azure-synapse-spark/>.
- 102 Stephen Hilt, Éireann Leverett, and Fernando Mercês. (June 6, 2022). *Trend Micro*. "Closing the Door: DeadBolt Ransomware Locks Out Vendors With Multitiered Extortion Scheme." Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_no/research/22/f/closing-the-door-deadbolt-ransomware-locks-out-vendors-with-mult.html.
- 103 Arianne Dela Cruz, et. Al. (May 25, 2022). *Trend Micro*. "New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code." Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-esxi-devices.html.
- 104 Junestherry Dela Cruz. (Jan. 24, 2022). *Trend Micro*. "Analysis and Impact of LockBit Ransomware's First Linux and VMware ESXi Variant." Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_us/research/22/a/analysis-and-impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html.
- 105 Georgia Tech Research. (Feb. 13, 2017). *Georgia Institute of Technology*. "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls." Accessed on Oct. 21, 2022, at <https://rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls>.
- 106 Roel Reyes, et. Al. (July 13, 2017). *Trend Micro*. "Do Online Mainframes Compromise Business Processes?" Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_us/research/17/g/online-exposed-mainframes-business-process-compromise.html.
- 107 Christopher Perry. (May 20, 2019). *BMC Software*. "Are Mainframes Your Weakest Link?" Accessed on Oct. 21, 2022, at <https://www.bmc.com/blogs/are-mainframes-your-weakest-link/>.
- 108 National Cyber Security Centre. (Feb. 23, 2022). *National Cyber Security Centre*. "New Sandworm malware Cyclops Blink replaces VPNFilter." Accessed on Oct. 21, 2022, at <https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter>.
- 109 Feike Hacquebord, Stepen Hilt, and Fernando Mercês. (Mar. 17, 2022). *Trend Micro*. "Cyclops Blink Sets Sights on Asus Routers." Accessed on Oct. 21, 2022, at https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html.
- 110 Stephen Hilt, Éireann Leverett, and Fernando Mercês. (June 6, 2022). *Trend Micro*. "Closing the Door: DeadBolt Ransomware Locks Out Vendors With Multitiered Extortion Scheme." Accessed on Oct. 21, 2022, at https://www.trendmicro.com/en_no/research/22/f/closing-the-door-deadbolt-ransomware-locks-out-vendors-with-mult.html.
- 111 Catalin Cimpanu. (March 23, 2019). *ZDNet*. "Tesla car hacked at Pwn2Own contest." Accessed on Oct. 21, 2022, at <https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/>.
- 112 Christos Karapapas, et. Al. (March 9, 2020). *arXiv*. "Ransomware as a Service using Smart Contracts and IPFS." Accessed on Oct. 20, 2022, at <https://arxiv.org/abs/2003.04426>.
- 113 Stijn Pletinckx, Cyril Trap, and Christian Doerr. (2018). *Cyber Threat Intelligence*. "Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware." Accessed on Oct. 21, 2022, at <https://www.cyber-threat-intelligence.com/publications/CNS2018-Cerber.pdf>.
- 114 Dmitry Smilyanets. (Oct. 26, 2021). *Recorded Future*. "An interview with LockBit: The risk of being hacked ourselves is always present." Accessed on Oct. 21, 2022, at <https://therecord.media/an-interview-with-lockbit-the-risk-of-being-hacked-ourselves-is-always-present/>.
- 115 Dmitry Smilyanets. (March 16, 2021). *Recorded Future*. "'I scrounged through the trash heaps... now I'm a millionaire:' An interview with REvil's Unknown." Accessed on Oct. 21, 2022, at <https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/>.
- 116 Dmitry Smilyanets. (Feb. 4, 2022). *Recorded Future*. "An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe'." Accessed on Oct. 21, 2022, at <https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/>.

- 117 Catalin Cimpanu. (Dec. 3, 2021). *Recorded Future*. "A mysterious threat actor is running hundreds of malicious Tor relays." Accessed on Oct. 21, 2022, at <https://therecord.media/a-mysterious-threat-actor-is-running-hundreds-of-malicious-tor-relays/>.
- 118 Brian Cayanan and Anthony Melgarejo. (June 27, 2017). *Trend Micro*. "Petya Ransomware Attack In Progress, Hits Europe." Accessed on Oct. 20, 2022, at https://www.trendmicro.com/en_us/research/17/f/large-scale-ransomware-attack-progress-hits-europe-hard.html.
- 119 US Department of Justice. (Sept. 6, 2018). *US Department of Justice*. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." Accessed on Oct. 17, 2022, at <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>.
- 120 US Department of Justice. (Feb. 17, 2021). *US Department of Justice*. "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe." Accessed on Oct. 17, 2022, at <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>.
- 121 ESET Research. (March 1, 2022). *ESET*. "Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper." Accessed on Oct. 21, 2022, at <https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/>.
- 122 Microsoft Security. (Jan. 15, 2022). *Microsoft*. "Destructive malware targeting Ukrainian organizations." Accessed on Oct. 20, 2022, at <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>.
- 123 Counter Threat Unit Research Team. (June 23, 2022). *SecureWorks*. "BRONZE STARLIGHT Ransomware Operations Use HUI Loader." Accessed on Oct. 18, 2022, at <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>.
- 124 Microsoft Defender Threat Intelligence and Threat Intelligence Center (MSTIC). (May 9, 2022). *Microsoft*. "Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself." Accessed on Oct. 18, 2022, at <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>.
- 125 Trend Micro Threat Research. (Feb. 8, 2022). *Trend Micro*. "Ransomware Spotlight: LockBit." Accessed on Oct. 21, 2022, at <https://www.trendmicro.com/vinfo/in/security/news/ransomware-spotlight/ransomware-spotlight-lockbit>.
- 126 FBI Internet Crime Complaint Center (IC3). (2021). *Internet Crime Complaint Center (IC3)*. "Internet Crime Report 2021." Accessed on Oct. 21, 2022, at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- 127 FBI Internet Crime Complaint Center (IC3). (2021). *Internet Crime Complaint Center (IC3)*. "Internet Crime Report 2021." Accessed on Oct. 21, 2022, at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- 128 Kim Grauer, Will Kueshner, and Henry Updegrave. (2022). *Chainalysis*. "The 2022 Crypto Crime Report." Accessed on Oct. 19, 2022, at <https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf>.
- 129 Chainalysis. (Apr. 14, 2022). *Chainalysis*. "Hackers Are Stealing More Cryptocurrency From DeFi Platforms Than Ever Before." Accessed on Oct. 21, 2022, at <https://blog.chainalysis.com/reports/2022-defi-hacks/>.
- 130 Kim Grauer, Will Kueshner, and Henry Updegrave. (2022). *Chainalysis*. "The 2022 Crypto Crime Report." Accessed on Oct. 19, 2022, at <https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf>.
- 131 Trellix. (May 3, 2022). Trellix. "The Hermit Kingdom's Ransomware play." Accessed on Oct. 21, 2022, at <https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html>.
- 132 Arjun Kharpal. (May 15, 2017). *CNBC*. "Hackers who infected 200,000 machines have only made \$50,000 worth of bitcoin." Accessed on Oct. 20, 2022, at <https://www.cnn.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html>.
- 133 Brian Krebs. (March 7, 2022). *Krebs on Security*. "Conti Ransomware Group Diaries, Part IV: Cryptocrime." Accessed on Oct. 20, 2022, at <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/>.
- 134 Amy Cheng. (Nov. 2, 2021). *The Washington Post*. "'Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam." Accessed on Oct. 21, 2022, at <https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/>.
- 135 Valerio Puggioni. (Feb 6, 2022). *CoinTelegraph*. "Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it." Accessed on Oct. 21, 2022, at <https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it>.
- 136 Brian Krebs. (Sept. 5, 2006). *The Washington Post*. "Don't Be a Pump-and-Dump Chump." Accessed on Oct. 20, 2022, at http://voices.washingtonpost.com/securityfix/2006/09/dont_be_a_pumpanddump_chump.html.
- 137 Dan Simmon. (July 25, 2017). *BBC*. "UK's first boot camp hopes to reform teenage hackers." Accessed on Oct. 21, 2022, at <https://www.bbc.com/news/av/technology-40655656>.

- 138 Joe Uchill. (July 29, 2022). *SCMedia*. "Founder of pro-Russian hacktivist Killnet quitting group." Accessed on Oct. 21, 2022, at <https://www.scmagazine.com/analysis/cybercrime/founder-of-pro-russian-hacktivist-killnet-quitting-group>.
- 139 Kevin Townsend. (Aug. 12, 2022). *Security Week*. "Killnet Releases 'Proof' of Its Attack Against Lockheed Martin." Accessed on Oct. 20, 2022, at <https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin>.
- 140 Threat Analysis Group. (Sept. 7, 2022). *Google*. "Initial access broker repurposing techniques in targeted attacks against Ukraine." Accessed on Oct. 20, 2022, at <https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/>.
- 141 Jonathan Lusthaus. (Aug. 8, 2018). *BlackHat*. "Is the Mafia Taking Over Cybercrime?" Accessed on Oct. 21, 2022, at <https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf>.
- 142 Jonathan Lusthaus. (Aug. 8, 2018). *BlackHat*. "Is the Mafia Taking Over Cybercrime?" Accessed on Oct. 21, 2022, at <https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf>.
- 143 European Cybercrime Centre (EC3). (June 2013). *Europol*. "Hackers deployed to facilitate drugs smuggling." Accessed on Oct. 21, 2022, at https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf.
- 144 European Cybercrime Centre (EC3). (June 2013). *Europol*. "Hackers deployed to facilitate drugs smuggling." Accessed on Oct. 21, 2022, at https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf.
- 145 Catalin Cimpanu. (Apr. 22, 2021). *Recorded Future*. "Ransomware gang wants to short the stock price of their victims." Accessed on Oct. 20, 2022, at <https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/>.
- 146 Joshua Mitts. (2020). University of Chicago Press. "Short and Distort." *The Journal of Legal Studies*, Vol. 49, Issue no. 2, p. 287–334.
- 147 Brian Krebs. (Sept. 5, 2006). *The Washington Post*. "Don't Be a Pump-and-Dump Chump." Accessed on Oct. 20, 2022, at http://voices.washingtonpost.com/securityfix/2006/09/dont_be_a_pumpanddump_chump.html.
- 148 Paul Bischoff. (Sept. 23, 2021). *CompariTech*. "How ransomware affects stock market share prices: report." Accessed on Oct. 21, 2022, at <https://www.comparitech.com/blog/information-security/ransomware-share-price-analysis/>.
- 149 Adele Ferguson. (Dec. 7, 2020). *The Age*. "Caught in a bear trap: How 'short and distort' attacks are costing Australian investors billions." Accessed on Oct. 21, 2022, at <https://www.theage.com.au/business/markets/caught-in-a-bear-trap-how-short-and-distort-attacks-are-costing-australian-investors-billions-20201204-p56ksl.html>.
- 150 Paul Roberts. (June 8, 2022). *Reversing Labs*. "A (Partial) History of Software Supply Chain Attacks." Accessed on Oct. 21, 2022, at <https://blog.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks>.
- 151 Charlie Osborne. (July 23, 2021). *ZDNet*. "Updated Kaseya ransomware attack FAQ: What we know now." Accessed on Oct. 21, 2022, at <https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/>.
- 152 David Maynor, Matt Olney, and Yves Younan. (July 5, 2017). *Cisco Talos*. "The MeDoc Connection." Accessed on Oct. 21, 2022, at <https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>.
- 153 BBC. (July 4, 2017). *BBC*. "Ukraine cyber-attack: Software firm MeDoc's servers seized." Accessed on Oct. 21, 2022, at <https://www.bbc.com/news/technology-40497026>.
- 154 Anton Ivanov and Orkhan Mamedov. (June 28, 2017). *Secure List by Kaspersky*. "ExPetr/Petya/NotPetya is a Wiper, Not Ransomware." Accessed on Oct. 21, 2022, at <https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>.
- 155 Trend Micro. (n.d.). *Trend Micro*. "Business Email Compromise (BEC)." Accessed on Oct. 21, 2022, at [https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-\(bec\)](https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)).
- 156 FBI Internet Crime Complaint (IC3). (May 4, 2022). *FBI Internet Crime Complaint (IC3)*. "Business Email Compromise: The \$43 Billion Scam." Accessed on Oct. 21, 2022, at <https://www.ic3.gov/Media/Y2022/PSA220504>.
- 157 Crane Hassold. (June 6, 2022). *RSA Conference 2022*. "BEC & Ransomware: Two Sides of the Same Cybercrime Coin." Accessed on Oct. 21, 2022, at https://static.rainfocus.com/rsac/us22/sess/1626998728821001aNZu/finalwebsite/2022_USA22_AFD-M03_01_BEC-%26-Ransomware-Two-Sides-of-the-Same-Cybercrime-Coin_1654098902815001gKMP.pdf.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



| research 