cybereason | WHITEPAPER

INSIDE COMPLEX
RANSOMWARE OPERATIONS
AND THE RANSOMWARE ECONOMY

RansomOps

Introduction

Ransomware operations have transformed dramatically over the last few years from a small cottage industry conducting largely nuisance attacks to a highly complex business model that is extremely efficient and specialized with an increasing level of innovation and technical sophistication. Several factors have contributed to the maturation of ransomware operations, resulting in a significant surge in ransomware attacks with record-breaking, multi-million dollar ransom payouts. This has created a gold rush in the cybercrime world, and a good portion of the illicit funds generated are invested right back into their operations, further increasing their capabilities and spawning an ecosystem of technologies and services that bolster the operations.

There are a few key factors driving the ransomware economy. First, organizations are more reliant on digital infrastructure than they were in the past, especially following the increase in remote work in response to the pandemic. Second, the burgeoning Ransomware-as-a-Service (RaaS) industry has lowered the technical bar for many would-be attackers by making complex attack infrastructure available to low-skilled threat actors.

Third, ransomware actors continue to benefit from the pseudo-anonymity that cryptocurrency provides for the collection and laundering of proceeds derived from their elicit operations. Cryptocurrency is digital, decentralized and for the most part anonymous—with still maturing oversight from any government, legal or regulatory entity—which is why attackers demand that victims pay their ransom using cryptocurrency.

Lastly, ransomware is an extremely lucrative model with little-to-no risk involved for the threat actors, as they often operate in countries with no extradition treaty with the target nations and where the governments turn a blind eye, which allows them to operate with near impunity. Couple this with the willingness of most victim organizations to pay the ransom demand swiftly under the assumption it will return business operations to normal, and we have a serious problem with no easy remedies.

Ransomware purveyors are moving away from high-volume attacks with low ransom demands in favor of **more focused, custom attacks** aimed at individual organizations selected for the ability to pay multi-million dollar ransom demands

To further complicate matters, ransomware purveyors are moving away from high-volume attacks with low ransom demands in favor of more focused, custom attacks aimed at individual organizations selected for the ability to pay multi-million dollar ransom demands. In some cases, ransomware gangs are even brazen enough to compromise insurance companies to steal lists of clients with cyber insurance policies that will cover the costs of the attack.

A joint report issued by the United States, Australia and the United Kingdom in early February of 2022 and published by the Cybersecurity and Infrastructure Security Agency (CISA) specifically noted the increasing complexity observed in ransomware operations, stating that, "ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally."

These more complex ransomware operations, or **RansomOps™** involve highly targeted, complex attack sequences by sophisticated threat actors. Unlike early iterations of ransomware attacks that relied on "spray-and-pray" tactics to infect large numbers of victims while seeking relatively small ransom demands, RansomOps attacks are much more intricate and akin to the stealthy operations conducted by nation-state threat actors. RansomOps are typically "low and slow" attacks that seek to remain clandestine and spread through as much of the target network as possible before the ransomware payload is delivered and a ransom demand is issued.

RansomOps are typically "low and slow" attacks that **seek to remain clandestine and spread through as much of the target network** as possible before the ransomware payload is delivered and a ransom demand is issued.

INSIDE RANSOMOPS

RansomOps also involve a great deal of reconnaissance on the targets which are carefully chosen for their ability to pay huge ransom demands and high likelihood to pay given they may be in an industry with the potential for significant ripple effects should their operations be disrupted, such as with healthcare and other critical infrastructure organizations.

RansomOps attacks rely on organized criminal syndicates and typically involve multiple players from the burgeoning Ransomware Economy, each with their own specializations, including:

FOUR COMPONENTS OF RansomOps

- **Initial Access Brokers (IABs):** Infiltrate target networks, establish persistence and move laterally to compromise as much of the network as possible, then sell access to other threat actors
- **Ransomware-as-a-Service (RaaS) Providers:** Supply the actual ransomware code, the payment mechanisms, handle negotiations with the target and provide other "customer service" resources to both the attackers and the victims
- **Ransomware Affiliates:** Contract with the RaaS provider, select the targeted organizations and then carry out the actual ransomware attack
- **Cryptocurrency Exchanges:** Launder the extorted proceeds

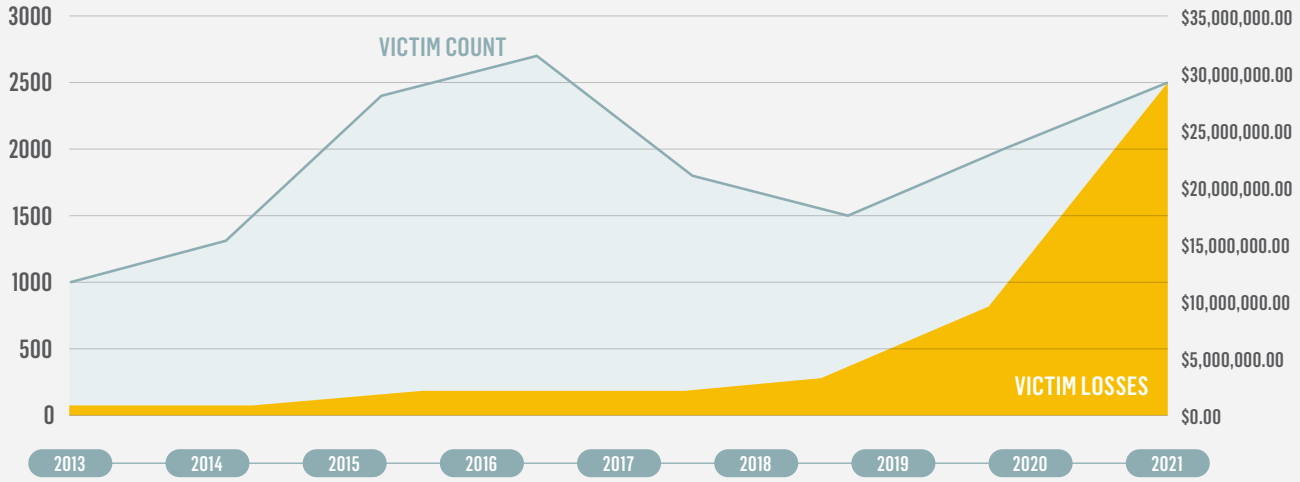
RansomOps attacks rely on organized criminal syndicates and typically involve multiple players from the burgeoning Ransomware Economy, each with their own specializations

The maturity of a given industry or organization can be determined by the level of specialization in the roles and support structure, and today we see a mature ransomware economy given the complex networking and specialization in the support structure. Some ransomware groups even go as far as to crowdsource information and collaborate with other malware developers on attacks, where one malware family is used for data exfiltration prior to the delivery of the ransomware payload that encrypts the targeted systems.

"For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0," the joint report published by CIS stated. "In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors."

Ransomware groups also share tactics, infrastructure, and information on potential targets. This helps to keep the costs low and the development in-house with core R&D (research and development) and coding teams in place, as well as the option to outsource to other groups when desired. They use cloud environments for testing in attack simulations, machine learning for attack optimization, and leverage legitimate pentesting tools like CobaltStrike that are designed to automate reconnaissance and infiltration to establish footholds within an environment for more effective ransomware operations.

RANSOMWARE MARKET



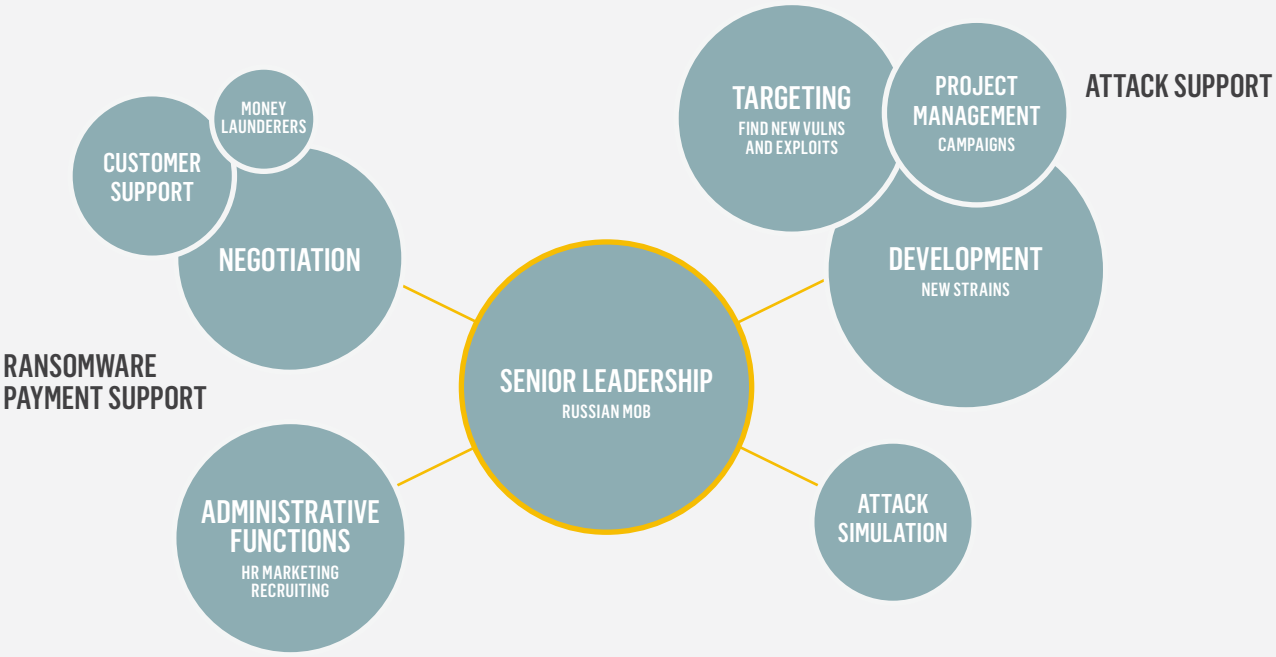
RANSOMWARE STRAINS OVER TIME

POWERWARE | ZCRYPTOR | GOLDENEYE | GANDCRAB
CRYPTOLOCKER | TESLACRYPT | LOCKY | PETYA | JIGSAW | WANNACRY | CONTI/RYUK | MAZE | REVIL/SODINOKIBI

Scale of the Ransomware Economy over time (from reported IC3 ransomware cases)

RansomOps attacks yield enormous financial gains for the adversaries, and ransomware gangs today operate like legitimate companies that can be as agile as a startup and as well-funded as a mature company. For example, reports estimate that the REvil ransomware gang makes more than $100M per year.

This is because ransomware operators have adopted proven business models from legitimate industries to speed and scale their efforts: they have product roadmaps, development engineers, marketing and support teams to smooth operations, and more:



Ransomware Gang Internal Functions

"The market for ransomware became increasingly 'professional' in 2021, and the criminal business model of ransomware is now well established," the joint report published by CIS stated. "In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals."

Simply put, ransomware operations are more mature and structured than ever before, with proven playbooks, thriving development and an organized network of participants. Without the burden of legitimate business expenses like taxes, a good portion of the extorted funds are being funneled back into R&D to create improved ransomware variants and methods of attack. This is why we can expect continued innovation from these groups in the development of novel Tactics, Techniques, and Procedures (TTPs).

GEOPOLITICAL FACTORS

Tensions between the U.S. and Russia over ransomware incidents have escalated because the majority of ransomware comes from Russia and/or former Soviet Bloc states, and the Russian Government is well aware of the issue but looks the other way when it serves their geopolitical interests.

Russian ransomware gangs are closely aligned with the Russian mob, which has longstanding ties with Russian Intelligence, so as long as attacks don't run afoul of Russian interests, the groups remain free to operate as they please. Some ransomware gangs have vowed not to attack some critical infrastructure entities in an effort to avoid retaliation or or sanctions from the United States, although the sincerity of those pledges is suspect and the attacks against organizations in healthcare, education, energy and food production continue unabated.

Moscow's financial district is also a hub for ransom money laundering, with some 50 or so crypto exchanges located there, making it a global center for crypto exchanges. And ransom payment laundering has been traced back to several companies based in Moscow, with some located in the tallest and most prestigious building in the city.

Some ransomware variants are even hardcoded to abort an attack in certain regions like Eastern Europe and Russia, or if Cyrillic keyboards are detected in use. It is also suspected that Russian Intelligence influences some targeting by ransomware gangs, as with the DarkSide attack on Colonial Pipeline or the REvil attacks that leveraged Kaseya to infect their client base.

Essentially, it has become difficult if not impossible for private-sector Defenders to draw a clear distinction between attacks supporting nation-state geopolitical interests and many of the more complex ransomware attacks we are seeing today.

RANSOMOPS AND APT OPERATIONAL OVERLAP

Essentially, it has become difficult if not impossible for private-sector Defenders to draw a clear distinction between attacks supporting nation-state geopolitical interests and many of the more complex ransomware attacks we are seeing today—and it's not just Russia that is driving this trend. For example, Cybereason recently documented a previously unidentified state-sponsored cyberespionage campaign Operation GhostShell, a highly-targeted cyber espionage campaign attributed to Iranian threat actor MalKamak. During the investigation, the Nocturnus Team uncovered a previously undocumented and stealthy RAT (Remote Access Trojan) dubbed ShellClient which was employed as the primary espionage tool.

Using this RAT, the threat actors were first observed conducting reconnaissance and the exfiltration of sensitive data from leading Aerospace and Telecommunications companies in the Middle East region, and was later observed targeting the same industries in other regions including the U.S, Russia and Europe.

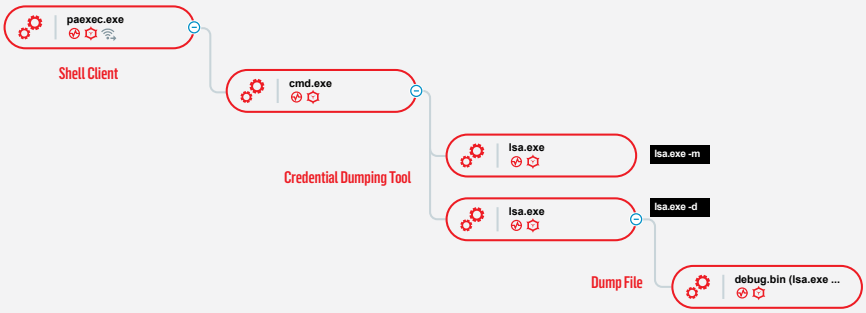
The attackers leveraged PAExec to:

- Execute a CMD shell as SYSTEM on remote machines
- Perform remote service related operations like start, stop, restart, status and more
- Exfiltrate organizational Active Directory structure using a remotely executed csvde.exe -f < output file > command
- Check internet connectivity using ping to reach Google.com
- Gather host information by executing ipconfig, tasklist and net use

In order to exfiltrate data, the attackers used WinRar to compress important files before data exfiltration using a renamed rar.exe WinRar file:

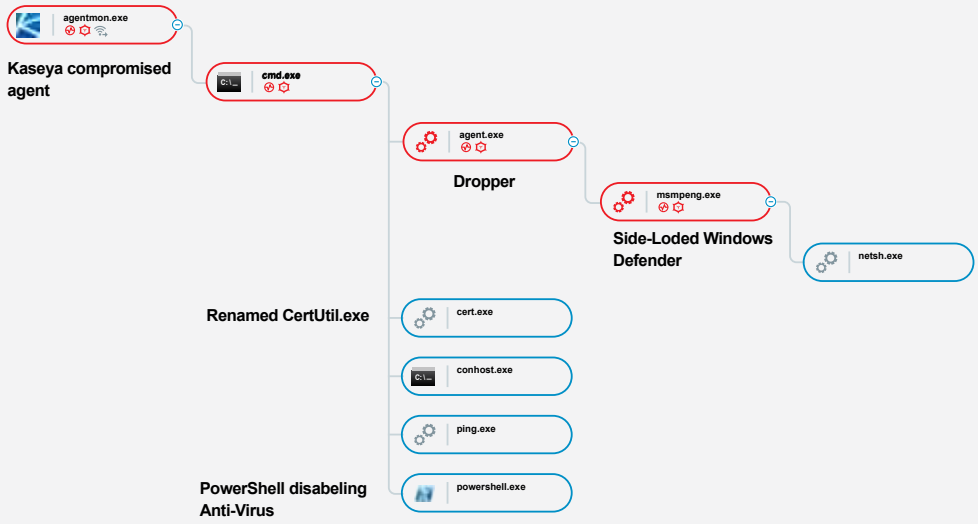
APT Operation GhostShell: ShellClient leveraging PAExec as observed in the Cybereason XDR Platform

During the observed attacks, the ShellClient RAT activity group deployed and executed an unknown executable named lsa.exe to perform credential dumping. Although Cybereason was unable to retrieve the lsa.exe executable, we speculate the tool might be a variation of the tool **SafetyKatz** based on the debug.bin dump file the tool creates, which is also the name of the dump file created by SafetyKatz that was previously tied to Iranian threat actors:



APT Operation GhostShell: ShellClient credential dumping as observed in the Cybereason XDR Platform

Similarly, the REvil ransomware cybercrime gang's attack on IT services provider Kaseya in July of 2021 was highly targeted and designed to ultimately compromise the company's customer base. This supply chain attack displayed a level of complexity more on par with a nation-state operation like the **Operation GhostShell** attack described above than a typical cybercrime operation:



REvil RanomOps:: Kaseya attack tree as shown in the Cybereason XDR Platform

These campaigns highlight the increasingly blurred line between nation-state and cybercrime threat actors, where **ransomware gangs are more often employing APT-like tactics to infiltrate** as much of a targeted network as possible without being detected, and APTs leveraging cybercrime tools like ransomware to distract, destroy and ultimately cover their tracks.

The attack exploited the web interface for Kaseya VSA Servers which are used by Kaseya customers to monitor and manage their infrastructure, enabling authentication bypass and remote code execution. The Kaseya Agent Monitor was abused to initiate the ransomware dropper which writes the encoded payload to disk and executes a series of command line instructions that disabled the Windows Defender security and antivirus tools as well as evading other other detection rules for the processes. The attack also employed advanced techniques like DLL Side-Loading and exploited a number of zero-day vulnerabilities in the Kaseya VSA software. In short, the Kaseya attack was very complex and more closely resembled an APT-type operation one would expect to see from a nation-state as opposed to typical cybercrime initiative.

These campaigns highlight the increasingly blurred line between nation-state and cybercrime threat actors, where ransomware gangs are more often employing APT-like tactics to infiltrate as much of a targeted network as possible without being detected, and APTs leveraging cybercrime tools like ransomware to distract, destroy and ultimately cover their tracks. For Defenders in the private sector, there is no longer a significant distinction between nation-state adversaries and sophisticated cybercriminal operations.

SCOPE OF THE RansomOps THREAT

It may come as no surprise that the number of global ransomware attacks is on the rise, but how big is the threat? According to recent reports, the global volume of ransomware operations reached 304.7 million attacks in the first half of 2021—a year-over-year increase of 151%, and 100,000+ more attack attempts than in all of 2020. Research by Cybersecurity Ventures estimated a ransomware attack occurs about every 11 seconds. That translates to about 3 million ransomware attacks over a year.

The 2021 Data Breach Investigations Report (DBIR) noted that 13% of all security incidents included a ransomware component, and that ransomware was a factor in 10% of all reported data breaches—double the frequency year-over-year—to become the third most-prevalent attack action in data breach events.

This increase likely reflects the extent to which RansomOps include additional extortion tactics, like the exfiltration of sensitive data prior to encryption with the threat to leak or sell it if the ransom demand is not met. The additional extortion tactics complicate the targeted organizations' recovery efforts and enable ever higher ransom demands by the attackers. Other double extortion methods that gained prevalence include threats to sell sensitive data to unscrupulous competitors or to investors who can short the victim company's stock, as well as threatening denial of service (DOS) attacks in addition to the ransomware infection.

"After encrypting victim networks, ransomware threat actors increasingly used 'triple extortion' by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders, or suppliers about the incident," the joint report published by CISA noted. "The ACSC continued to observe 'double extortion' incidents in which a threat actor uses a combination of encryption and data theft to pressure victims to pay ransom demands."

Additional extortion leverage wasn't the only new technique that helped ransomware grab the third spot in the DBIR ranking of attack actions. RansomOps are also increasingly exploiting software vulnerabilities as a means of capitalizing on weak vulnerability management and patching practices. For example, the Ragnarok ransomware gang used a Citrix vulnerability (CVE-2019-19781) to download attack tools disguised as Windows Certificate Services to execute a malicious binary before deleting the entry from the user certificate cache, and the Black Kingdom ransomware gang leveraged the Pulse flaw (CVE-2019-11510) as a way of preying upon unpatched enterprise assets.

COMMON DATA TYPES TARGETED FOR DOUBLE EXTORTION

The growth in extortion schemes raises an important question: what types of data do ransomware attackers tend to target for exfiltration to leverage for double extortion? It usually depends on the affected organization, but there are some common data categories that ransomware actors tend to target more than others. Provided below are four of those information types:

- **Protected Health Information (PHI):** PHI includes information like medical records, diagnosis details, and patient medical insurance data. Attackers changed their tactics during the COVID-19 pandemic to include exfiltration of PHI, which can also be leveraged for blackmail.
- **Personally Identifiable Information (PII):** PII includes information like birth dates, physical addresses, Social Security numbers (SSNs) and other sensitive and protected details about individuals. Ransomware actors can also monetize the information and sell it on the Dark Web for identity theft, fraud, or spear-phishing attacks.
- **Account Credentials:** Consisting primarily of usernames and passwords, account credentials are valuable to ransomware actors who seek to move laterally across the network so that they can encrypt even more data and devices in order to demand an even larger ransom amount.
- **Intellectual Property (IP):** IP includes new product releases and/or details that are integral to an organization's line of business. As with the theft of sensitive personal details, ransomware actors can monetize a victim's IP on the Dark Web or hand it over to a state-sponsored threat actor to be leveraged for an economic advantage.

RANSOMOPS IMPACT TO THE BUSINESS

Taken together, these tactics have escalated the costs to targeted organizations from ransomware attacks. The Cost of a Data Breach Study 2021 estimated the average ransomware attack cost victim organizations $4.62 million to recover from, a figure that doesn't even include the costs associated with paying the ransom demand and other fallout from an attack.

So, what does the cost of a ransomware attack include? A Cybereason study from 2021, titled Ransomware: Attacks and the True Cost to Business provides some indication. Consider the following statistics:

- **Loss of Business Revenue:** Two-thirds of organizations said that they suffered significant revenue loss following a ransomware attack.
- **Damage to Brand and Reputation:** More than half of organizations said that they suffered damage to their brand and reputation after an attack.
- **Loss of C-Level Talent:** Approximately one third of respondents said that they lost C-Level talent after suffering a ransomware attack.
- **Employee Layoffs:** About thirty percent indicated that they were forced to lay off employees due to the financial pressures caused by a ransomware attack.
- **Business Interruption:** A quarter of organizations temporarily ceased business operations after experiencing a ransomware attack.

Another attacker strategy worth noting is the tendency for attackers to hit organizations on weekends and holidays when they are typically running skeleton crews. Notable weekend/holiday ransomware attacks in 2021 included the DarkSide attack on Colonial Pipeline that occurred over Mother's Day weekend, the REvil attack against JBS Meat Packing over Memorial Day weekend and the attack on Kaseya during the Fourth of July weekend.

A follow-up report from Cybereason, titled Organizations at Risk: Ransomware Attackers Don't Take Holidays, revealed that 60% of organizations said a weekend or holiday ransomware attack resulted in longer periods to assess the scope of an attack. As a result, 50% said they required more time to mount an effective response, and 33% said they required a longer period to fully recover from the attack.

COMMON RANSOMOPS ATTACK VECTORS

Ransomware attacks involve a variety of infection vectors, but RansomOps actors prefer some attack methods over others. Researchers found that unsecured Microsoft Remote Desktop Protocol (RDP) connections accounted for over half of all ransomware attacks, followed by phishing emails and exploitation of software vulnerabilities. Here is how these three leading delivery vectors lead to a ransomware attack:

- **Unsecured RDP:** A proprietary protocol developed by Microsoft, RDP enables users to remotely connect to other computers over a network connection. The issue is when organizations leave their RDP ports exposed online that threat actors leverage for brute-force attacks to establish persistence on a target network.
- **Phishing Emails:** A typical attack attempt begins when a user receives an email that instructs them to click on a malicious link that delivers ransomware or an exploit kit as a payload, or instructs the recipient to open a tainted PDF, ZIP archive, or Microsoft Office file with enabled macros that downloads ransomware or initiates command and control for lateral movement on the network.
- **Exploitation of Vulnerabilities:** Exploit kits can evaluate web browsers, operating systems, and other software for exploitable vulnerabilities to activate exploit code and install ransomware on the victim's machine or initiate command and control for lateral movement.

Researchers found that unsecured Microsoft Remote Desktop Protocol (RDP) connections accounted for over half of all ransomware attacks, followed by phishing emails and exploitation of software vulnerabilities.

"These infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021," the joint report published by CISA stated. "This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching."

To that end, it is worth noting that ransomware gangs typically also have access to multiple zero-day vulnerabilities they can leverage in attacks, and a good deal of their R&D efforts go into finding new zero-days to exploit, keeping them well ahead of the defenders. A zero-day is an as-yet-unknown software vulnerability with no available patch, fix or response—and they are a vital tool adversaries can utilize to gain access to a victim environment.

RANSOMOPS ATTACK SEQUENCE

Spray-and-pray ransomware attacks typically begin with mass spam email campaigns or drive-by attacks leveraging malicious websites. Unwitting targets open malicious documents or click on malicious links which executes the ransomware on the target device. At that point, the ransomware encrypts the victim's files and a ransom note is displayed, usually demanding payment in the hundreds of dollars. Once they've received the ransom payment, the attackers may send a decryption utility to the victim, may make additional demands, or may do nothing in response.

RansomOps follow a similar progression, but often involves a level of sophistication in target selection, infection, and network penetration that are more similar to complex nation-state operations to gain persistence, move laterally on the target network, exfiltrate sensitive information from the victim for double extortion, and more.

RansomOps also typically include several threat actors working in unison: a ransomware developer making their malicious code available on the black market; affiliates using choosing an infection vector to launch an attack on a target using the RaaS-supplied infrastructure, then sharing a portion of the ransom proceeds with the RaaS provider, the negotiator, the crypto exchange, and so on.

The typical RansomOps attack sequence includes the following stages:

- **Reconnaissance and Target Selection:** For highly targeted RansomOps attacks, target selection is important. Threat actors typically seek to target organizations of consequence to compel swift payment of the ransom demand, such as healthcare and others that are deemed as critical infrastructure or whose business operations are essential.
- **Initial Access:** RansomOps attackers typically gain an initial foothold on the targeted network through phishing attacks or the exploitation of a vulnerable component. A variety of TTPs may be at play at this stage of the operation. Once persistence is established on the targeted network, the initial threat actor may opt to sell access to the network to another attacker or group.
- **Command and Control:** The attackers begin communications with the Command and Control (C2) server to import additional tools or commence abuse of legitimate tools already available on the network to spread laterally and escalate privileges.
- **Credential Theft and Privilege Escalation:** The abuse of user identities through credential theft allows the attackers to further spread through the targeted network and escalate privileges.
- **Data Exfiltration:** Sensitive data is exfiltrated for use in double extortion or to be monetized for sale on Dark Web.
- **Encryption:** The ransomware payload is delivered and the compromised systems and data are encrypted. They become inaccessible to the victim organization, and a ransom demand is levied.
- **Negotiation:** After the network assets are encrypted and the ransom demand issued, the negotiation stage begins to determine the final ransom amount and process for decryption.
- **Ransom Payment:** Victims can opt to pay the ransom with the expectation that a decryption key will be provided, but there are no guarantees the key will work or that no data will be corrupted in the process. Victims can also opt to not pay the ransom and restore systems from backups, but any exfiltrated data is still at risk of exposure. Either option is labor intensive and costly for the impacted organization.

TO PAY OR NOT TO PAY?

After falling prey to a ransomware attack, most organizations are faced with the decision of whether they're going to pay the ransom demand. We'll save you some time: it's not worth it. There are three primary reasons why it does not pay to pay:

NO GUARANTEES

Paying the ransom doesn't mean that you will regain access to your encrypted data. The decryption utilities provided by those responsible for the attack sometimes simply don't work properly. In our recently published ransomware report, Ransomware: The True Cost to Business, nearly half of respondents (46%) who fulfilled their attackers' demands regained access to their data following payment only to find that some–if not all–of their data was corrupted. Just 51% said that they successfully recovered all their data after paying, with three percent admitting that they didn't get any of their data back after payment. 80% of organizations who paid a ransom demand ended up incurring another attack–often by the same threat actors (46%).

LEGAL IMPLICATIONS

Organizations could inadvertently incur penalties from the U.S. government for paying ransomware actors who may reside or operate out of countries who are subject to U.S. sanctions. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) made this point clear in an advisory published in October 2020 where OFAC added some malicious actors including ransomware attackers to its list of sanctioned entities. The initiative empowers OFAC to impose penalties on U.S. persons who provide material assistance and/or other methods of support to any designated individuals, even if someone didn't know that they were dealing with a sanctioned individual beforehand.

INCENTIVIZING RANSOMWARE ATTACKS

Incentivizing Ransomware Attacks: Organizations who pay ransomware attackers are sending the message that extortion schemes work– a message that can only fuel continued ransomware attacks and extortion schemes. In general, the FBI advises that organizations refrain from paying ransoms because it simply emboldens malicious actors by telling them that extortion works. Those attackers can then justify expanding their operations and continue to target organizations, making everyone less safe. In 2021, according to one source, the average ransom payment was $570,000, a 518% increase from 2020. For perspective, this average is relatively low compared to recent ransom demands that have hit as high as $50 million dollars or more.

"Cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent," the joint report published by CISA stated. "Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model."

DEFENDING AGAINST RANSOMOPS

The utility of data backups has changed given the increasing prominence of double extortion, where backups might allow a victim to recover their encrypted information, but it won't prevent an attacker from leaking their stolen data online. This tactic thus helps to put additional pressure on victims to pay up. Zero trust is an inherently complicated goal for infosec teams, as sending and receiving data in only prescribed circumstances is unrealistic in the average enterprise that is more distributed than ever before. Interfacing through the internet means that we do normal business over the same channels that attackers operate on, which is like sending a commercial ship through known pirate routes.

In addition—and through no fault of their own due to human bandwidth issues and resource constraints—the average security team doesn't have full visibility of their ecosystems, can't patch vulnerable systems in short order, and have not fully implemented security basics across their environment. This gives sophisticated attackers many options to gain access to the IT infrastructure of a targeted organization, and opponents will use every tool at their disposal to gain access.

Many organizations that have prepared for a ransomware attack have resorted to cyber insurance as a failsafe against financial losses. Due to its prevalence, cyber insurance payouts are in a sense funneling money to adversaries and directly helping to prop up the industry. The insurance itself is often insufficient, with many loopholes for coverage and red tape that tips the scales in the advantage of the insurers. Just as venture capital is a conduit for infusing monies into the legitimate software market, cyber insurance is becoming a conduit for infusing monies into the illegitimate software market of ransomware.

"Criminal activity is motivated by financial gain, so paying a ransom may embolden adversaries to target additional organizations (or re-target the same organization) or encourage cyber criminals to engage in the distribution of ransomware," the joint report published by CISA advised. "Paying the ransom also does not guarantee that a victim's files will be recovered. Additionally, reducing the financial gain of ransomware threat actors will help disrupt the ransomware criminal business model."

The utility of data backups has changed given the increasing prominence of **double extortion,** where backups might allow a victim to recover their encrypted information, but it won't prevent an attacker from leaking their stolen data online.

Just as venture capital is a conduit for infusing monies into the legitimate software market, cyber insurance is becoming a conduit for **infusing monies into the illegitimate software market of ransomware.**

It is possible for organizations to defend themselves at each stage of a ransomware attack. What's important to understand about RansomOps is that prior to the delivery of the ransomware payload, the attackers have engaged in weeks or even months of detectable activity on the target network. This is where understanding RansomOps and strategies to detect and disrupt them early in the kill chain can turn what would have been a potentially devastating ransomware attack into a less consequential intrusion or data exfiltration attempt.

For example, during the reconnaissance stage, Defenders can investigate network mapping and discovery attempts launched from unexpected sources. In the initial access stage, Defenders can disrupt phishing attempts, disable tainted links in emails, and disable malicious macros in email attachments. Defenders can also detect and block binaries that are attempting to create new registry values or other suspicious activity on endpoints. Defenders can block outbound connections to attack infrastructure when the operation attempts to establish command and control. As well, Defenders can prevent the abuse of legitimate services, block unapproved scripts and the execution of payloads from running on the system. The joint report published by CISA provides a detailed list of controls and policies to implement to better defend against ransomware attacks, as well as steps to take when initiating incident response following a ransomware attack.

What's important to understand about RansomOps is that prior to the delivery of the ransomware payload, **the attackers have engaged in weeks or even months of detectable activity** on the target network.

Until recently the task of **correlating attack telemetry across the disperate and often distributed assets** that together make up today's network ecosystems was a difficult and resource-heavy endeavor that was impossible to scale.

Defenders can also use behavioral detections to prevent account compromise and credential theft attempts from unknown attacks, to flag attempts to gain access to other network resources with which they don't normally interact, to discover attempts to exfiltrate data as well as encrypt files, and to block the execution of malicious code prior to encryption of systems, and so on. Unfortunately, until recently the task of correlating attack telemetry across the disparate and often distributed assets that together make up today's network ecosystems was a difficult and resource-heavy endeavor that was impossible to scale and let attackers essentially hide in the network seams.

The advent of Extended detection and Response (XDR) solutions offer the opportunity for organizations to identify not only what systems were hit with ransomware, but also what business applications, user identities, and cloud deployments may have been involved as well to identify root cause so they can mitigate against the threat of future similar attacks. XDR solutions can also reveal the full impact of the compromise and whether the attackers pivoted into other systems, cloud infrastructure or into ICS systems, for example. The ability for XDR to surface the full attack sequence from reconnaissance to initial intrusion to data exfiltration allows Defenders to quickly understand the full scope of the attack, which in turn will allow the organizations the chance to improve their overall security posture for the future.

Clearly, there are multiple opportunities to detect RansomOps prior to the final ransomware payload delivery and presentation of the ransom note if Defenders have the right tools in place. The issue is that organizations can't achieve visibility into the early stages of a highly-targeted RansomOps attack by only relying on Indicators of Compromise (IOCs) derived from known attacks, as the tools and techniques are likely unique to the individual target environment in a RansomOps attack.

Hence the need for organizations to embrace an operation-centric approach which enables organizations to visualize a MalOp™ (malicious operation) in its entirety from root cause across every single affected device and account. To do so requires drawing on both known IOCs and Indicators of Behavior (IOBs), the more subtle signs of compromise. IOBs can allow Defenders to identify potential security incidents earlier based upon chains of behavior that produce circumstances that are either extremely rare, or that present a distinct advantage to an attacker—even when those behaviors in isolation are common or expected to be seen in the network environment.

IOBs can thus provide insight into attack chains that are novel or have never been detected prior, because at some point early in the attack sequence, these chains of behavior will distinguish the attack from normal network activity even if the individual behaviors are considered "normal." Organizations need the visibility afforded by tracking both IOCs and IOBs if they are to successfully defend against a RansomOps attack at the earliest stages.

The ability for XDR to surface the full attack sequence from reconnaissance to initial intrusion to data exfiltration allows Defenders to **quickly understand the full scope** of the attack.

Organizations can't achieve visibility into the early stages of a highly-targeted **RansomOps attack by only relying on Indicators of Compromise (IOCs)** derived from known attacks, as the tools and techniques are likely unique to the individual target environment in a RansomOps attack.

Conclusion

The impact to organizations from successful ransomware attacks are becoming ever more dire across every region and industry vertical, and ransomware attacks can have far-reaching effects that can shake an organization to its core. Often, the outcome is damage to reputation, loss of jobs, and loss of revenue. While good risk management requires organizations to have contingency plans in place for dealing with the aftermath of a ransomware attack on all levels, the most prudent strategy to avoid significant losses for your organization is always going to be a strong effort around proactive defense strategies.

Even with robust prevention capabilities in place that can block the majority of ransomware attacks, organizations must invest in comprehensive detection and response capabilities as well. The legacy security stack has clearly fallen short, and given the trend where ransomware purveyors are increasingly conducting complex attack sequences similar to what we have seen with national-state sponsored attackers, it is also clear that conventional approaches are simply no match for sophisticated RansomOps tactics.

Similarly, ransomware has demonstrated such a high level of success that we are seeing more evidence that nation-state attackers have begun to incorporate it into their arsenals as a means to thwart forensic investigations and damage targeted systems after they have completed their geo-political objectives. Along with this shift from nuisance attacks with limited impact to events that threaten critical infrastructure, economic viability and ultimately national security, has come a highly specialized ransomware economy that is agile, innovative, and rivals legitimate industries in both scale and return on the attacker's investment.

The legacy security stack has clearly fallen short, and given the trend where **ransomware purveyors are increasingly conducting complex attack sequences** similar to what we have seen with national-state sponsored attackers, it is also clear that conventional approaches are simply no match for sophisticated RansomOps tactics.

This blurring of the lines between tools and techniques of statecraft and those of criminal syndicates makes the job of successfully defending against complex attack even more imperative. Emerging technology approaches like Extended Detection and Response (XDR) solutions do offer some hope for Defenders by delivering proactive threat hunting and enriched telemetry correlations across patchworked networks, and well as addressing alert fatigue caused by a complicated security stack and the shortage of skilled personnel to staff security teams. XDR allows Defenders to move response efforts further to the left and the opportunity to intercept a ransomware attack proactively, long before the actual ransomware payload can be delivered.

In addition, leveraging Indicators of Behavior (IOBs)--the chains of behavior that surface attacks earlier and enable faster remediation–is a key advantage of an AI-driven XDR solution. IOBs can allow defenders the ability to detect and end malicious activity on the network, even when that activity consists of otherwise benign behaviors that one would expect to see on the network. This combination of increased visibility across siloed network assets to produce context-rich correlations based on chained attacker behaviors is at the heart of an AI-driven XDR solution. It also represents the opportunity for paradigm shift in how we can collectively reverse the adversary advantage and return the high ground to the Defenders.

XDR allows Defenders to move response efforts further to the left and **the opportunity to intercept a ransomware attack proactively,** long before the actual ransomware payload can be delivered.

This combination of increased visibility across siloed network assets **to produce context-rich correlations based on chained attacker behaviors** is at the heart of an AI-driven XDR solution.

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason AI-Driven XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.