SANS

Analyst Program

Whitepaper

SANS 2022 Ransomware Defense Report

Written by Matt Bromiley

March 2022

Gigamon®

©2022 SANS™ Institute

The Ransomware Era

The years 2020 and 2021 were undoubtedly the years of ransomware. In the ongoing waves of the COVID-19 pandemic, a growing remote workforce, and widespread adoption of new technologies, adversaries had no shortage of opportunities. These changes were coupled with a flurry of critical, widespread vulnerabilities and large-scale supply chain compromises that left many organizations at risk to ransomware attacks.

The European Union Agency for Cybersecurity, or ENISA, found that ransomware attacks increased 150% between April 2020 and July 2021.[1] The report also found that ransomware adversaries have become more brazen in their demands and approaches over the past year, with the ransomware-as-a-service (RaaS) business model setting new trends and breaking records. RaaS only exacerbates the ransomware issue, as it lowers the entry barrier for a ransomware attack to literally anyone with access to cryptocurrency.

However, while the landscape for ransomware adversaries and attacks has only gotten worse, organizations and security teams are not left high and dry. The past two years have shown an advancement in cybersecurity detection and response technologies. In fact, many organizations are successfully focusing on preventing ransomware and malware attacks, intending to stay ahead of adversaries who might seek to evade detection. Many organizations currently embrace solutions and platforms that provide a holistic point of view into the enterprise. Other teams leverage the changes that resulted from pandemic shifts to increase security spend, acquire new tools, or advance projects that were once thought dead in the water.

The cliché holds that experience is one of the best teachers. However, in the case of data breaches and ransomware, we'd prefer to study our adversaries ahead of time and ensure that they never get unfettered access to our networks! Use this paper to help identify potential weaknesses in your environment and then close those doors before an adversary can walk in.

In this whitepaper, we address both high-level concepts: With respect to ransomware, what are the current adversary trends, and then what can organizations do to defend themselves (or better defend themselves)? The basic concept of ransomware remains the same: Encrypt data and demand money for decryption. If you've been through a ransomware incident, however, you know it's just not that simple. It seems like things have gotten worse, especially when we realize that adversaries do their homework and know their targets well.

Just as adversaries have changed their techniques, organizations have as well. Let's examine both and look for areas where security teams can find success. Are processes or tools available that can prevent or detect attacks on the environment earlier in the attack chain? Does a "choke point" exist in ransomware attacks that provides an opportunity for detection? Even better—do adversaries share tactics in common, and can we use one to stop many?

[1] www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Adversary Trends

Unfortunately, ransomware threat actors have kept up with modernizing their operations and updating their techniques, tactics, and procedures (TTPs). So much so that we've seen ransomware actors sarcastically advise organizations on their security capabilities and implementations. That's not to say they're entirely wrong, but often these specific threat capabilities have either been harnessed by ransomware threat actors or used to rapidly conduct ransomware attacks.

Knowledge of Operational and Attack Surface of Victim Environments

Don't let an adversary know more about your perimeter than your security team knows. Whether you like it or not, adversaries do their homework on their victims during the initial reconnaissance stage of an attack. This background research helps increase threat credibility when they demand a ransom payment and allows them to potentially lock up more of the environment.

Time and time again, and perhaps increasingly so over the past two years, ransomware actors have researched and gained knowledge about victim environments prior to an attack. This knowledge often includes operational and financial details, such as annual budgets, employee counts, and/or revenue statistics. For example, in April 2021, a ransomware attack attempted to hold hostage Broward County Public Schools in Florida. When the adversaries asked for a whopping $40 million ransom payment, they reminded the school district that this demand represented only 1% of the school district's $4 billion annual budget.[2]

Adversary knowledge of their victims also often includes knowledge of the victim's overall attack surface. An organization's attack surface may include things such as:

- Internet-facing systems and services
- Vulnerabilities or unpatched systems
- Use of specific technology, such as security solutions or third-party vendors
- Potential cloud footprint

We posit that acquiring this information may prove not only to be good adversary tradecraft but also may increase the odds that an adversary gets paid (because they seem more "knowledgeable" about their victims). It might also allow the adversary to hold the victim organization to ransom in multiple ways, especially if the organization has a weak security posture, which allows the adversary a chance to get back in.

We never want to applaud adversaries for good TTPs or tradecraft, but we must agree that doing "homework" on a victim organization is a clever tactic.

Defense Tip

You cannot control every aspect of your digital footprint, but being aware of it is the first step. In some cases when the security team may be directly responsible, lack of patching or use of outdated or otherwise vulnerable software can leave an organization open to significant risk. Don't wait for an adversary to learn more about, and then exploit, your attack surface before you start attempting to prevent or respond to an attack.

[2] "Large Florida school district hit by ransomware attack," https://apnews.com/article/technology-fort-lauderdale-florida-ac217a0759194dc3c717b421ae05bd0c

Rapid Weaponization

Upon the announcement of a new vulnerability, a race often starts between adversaries and defenders to determine who can either exploit or patch, respectively. The adversary often wins because they can more easily write exploit code than an organization can issue a patch inside of change control processes or, even worse, during a change freeze. One trend among ransomware threat actors is to not only win the race of weaponization but to win it quickly.

We need only look to the Exchange vulnerabilities of March and April or Log4j in December, all 2021, to examine the speed at which adversaries moved from vulnerable code to working exploit. In a matter of hours after the announcement of the vulnerabilities, working proof-of-concept (PoC) code was available on the internet, and adversaries were quickly taking advantage of vulnerable systems before some security teams were even aware of a patch.

Defense Tip

Patching is often easier said than done. Unfortunately, it's sometimes the most efficient way to defend against an incoming exploit—even if that means subverting change controls or waking someone up in the middle of the night. After all, you'll find issuing an emergency patch much better than responding to an active intrusion. Knowing your cybersecurity risk is the first step toward resolving it. Unpatched vulnerabilities are some of the biggest, and they are the first attack vectors that adversaries use. Remote work and digital transformation have made managing holes in critical software harder. The best solutions simplify and automate your vulnerability management by prioritizing those applications your team uses most coupled with unpatched vulnerabilities that are known risks, and thus ensure that you can reduce the greatest risks first in the most efficient way.

Of course, rapid weaponization does not necessarily equate to a ransomware attack. Advanced state-nexus threat actors also move at a rapid speed to weaponize vulnerabilities and gain persistence inside of an environment. In fact, in some cases, this has resulted in multiple threat actors attempting to enter a target organization via the same vulnerability. This creates a unique one-to-many situation for defenders: They need to apply only one patch to shut out multiple threat actors.

However, if you cannot patch a vulnerable and/or external-facing system as quickly as you want, consider looking at network and endpoint alternatives as a stopgap. Utilize the technology controls you have in place to look for prevention, detection, and response opportunities. A quick network rule or endpoint signature and behavioral protection are examples of reliable defenses that can hold you over until the organization can assess patching feasibility.

The recent Log4j vulnerability provides a perfect example of using signatures to mitigate patching and to buy time. Multiple signatures, both network and endpoint, were available, and organizations could use them to detect incoming malicious packets and post-compromise activities. Organizations that could quickly deploy these signatures had a chance to give the application team time to assess options and respond appropriately.

Fileless or Malware-less Attacks

A growing post-exploit trend adversaries use is to bring as little "malware" to the intrusion as possible. This reflects adversarial attempts to evade detection as much as possible, until after they have introduced the actual ransomware encryptor into the environment. Some adversary TTPs take advantage of fileless or memory-only attacks and/or take advantage of native binaries so as not to introduce additional malware to the environment. Let's briefly discuss each:

- **Fileless malware** includes malware that leaves little to no malware on disk, instead relying on other locations, such as the Windows Registry or a remote location, to store malicious code. At a high level, fileless malware signals an attempt to evade traditional file-based detections or indicators of compromise (IoCs). Fileless malware may also be memory-only, which classifies malware and/or malicious code that exist only in memory. Adversaries download and deploy code directly into memory, again evading file-based or traditional detections.
- The use of **native binaries** on a system is yet another adversary technique to evade traditional detections and remain hidden in plain sight during an intrusion. Living-off-the-land binaries (lolbins) are executables already present within an operating system. Adversaries have uncovered dozens of ways to manipulate these files to achieve malicious objectives, such as loading code into memory, downloading a file, or running a custom script.

In the same vein, adversaries can also shift away from compiled binaries and instead rely on custom scripts or exploit kits on a victim system. Over the past few years, adversaries have increasingly used PowerShell and post-exploitation frameworks, such as Cobalt Strike, to assist in achieving their objectives. Although scripts and exploit kits can still leave on-disk artifacts, they also provide an attacker with a multitude of easy-to-use ways to compromise multiple systems and stay in memory.

Defense Tip

Relying on legacy defenses, such as disk-based file analysis and detections, can result in an adversary easily slipping through the cracks. Unfortunately, once an adversary has compromised the right set of credentials, there's little they cannot do. So, to defend against these advanced techniques, organizations must look at preventive capabilities that provide in-memory analysis and protections.

> **Technology now enables us to implement strong prevention capabilities, allowing in-memory analysis of code, loaded libraries, and other activity. By placing prevention and detection capabilities in memory, we get closer to the adversary than ever before. This provides a higher level of fidelity for detection, but also may provide an opportunity for wily adversaries to defeat endpoint monitoring. Tweak your rules accordingly and examine how multiple alerts may coalesce to tell one story.**

In-memory protections are one way to limit the success of these techniques. Runtime analysis and in-memory code examination are just two of the technological developments that help organizations defend against advanced adversaries. We encourage you to assess the capabilities of your current tooling and ask about their ability to stop fileless malware or to analyze usage of lolbins to identify malicious activity.

Although not an adversary tactic, another notable change from the past two years (mentioned earlier) is the explosion in ransomware-as-a-service (RaaS). Offering complete ransom capabilities, some adversaries have made more money as middlemen than they would have made as front-line attackers. However, even though the explosion in RaaS does not change the ransomware attack, it may change who is behind the keyboard or which TTPs they use.

Increased Automation

Another area where ransomware adversaries achieve success and/or get the better of a victim organization is in the level of automation they utilize. This area is no joke. We used to measure the speed with which an adversary moved in days, but we now measure that speed in hours or minutes. A November 2021 blog post from The DFIR Report describes an intrusion that went from zero to domain admin control and ransomware deployed within 42 hours.[3] Another post describes an adversary that went from zero control to full control in two hours.[4] We cannot overstate how, with a plethora of open source tools and automated processes, adversaries can be "done" before a security team has even detected them.

Luckily, adversary automation creates a predictable, and therefore easily detectable, sequence of events. Adversaries usually write attack scripts in OS-based programming languages like PowerShell or bash with repeatable commands, many of which security teams can use to create signatures for detection. Furthermore, adversaries increasingly use offensive security tools, including any open source toolkits and scripts. Although these give the adversary the advantage of time to quickly deploy, they leave predictable marks that an organization can use to disrupt an intrusion early on.

Defense Tip

Interestingly, automation represents both the problem and the solution. Just as adversaries have found it advantageous to automate parts of their attack and infrastructure, security teams should find benefits in doing the same. Briefly put, security teams could find benefits in automating the following:

- Intel-based detection deployment across various toolsets
- Detection actions and reactions, based on severity, criticality, and system
- Response playbooks that automate low-level actions, allowing analysts to free up and deal with the problems that matter

Believe it or not, your ability to automate may be closer than you realize. You should look at the automations available within your current controls and platforms or reach out and inquire about what actions may be available to add to the controls you already have in place. As discussed in the introduction, adversaries and defenders both gain benefits from technology advancements.

[3] "Exchange Exploit Leads to Domain Wide Ransomware," https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/

[4] "From Zero to Domain Admins," https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/

Ransomware Defenses

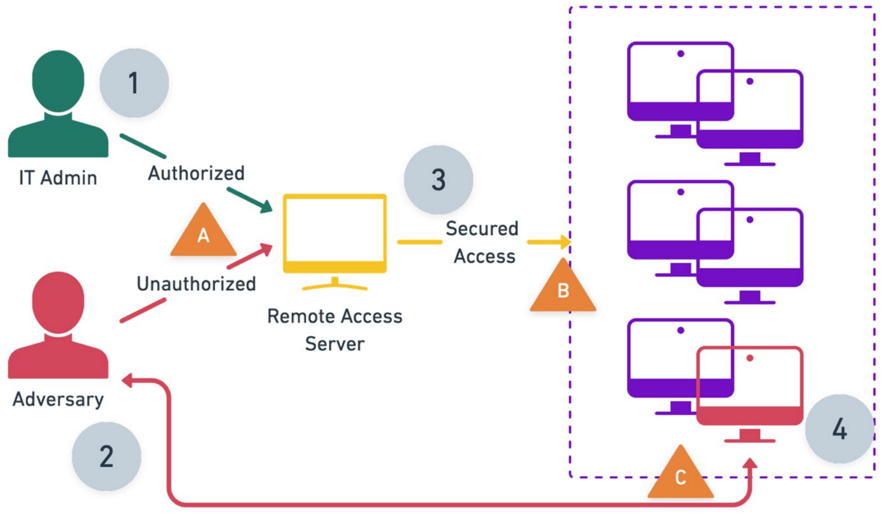
Of course, just because we're seeing a change in ransomware tactics and techniques does not mean organizations have no chance of defending against these types of attacks. Quite the contrary: The noisier the ransomware adversaries are, the more opportunities that exist for detection. In fact, the noisier they are, the easier it is to detect them early. The following case studies describe some sample defenses and countermeasures and how they can defend against ransomware attacks or help mitigate ransomware risk.

Remote Access Abuse

Our first case study looks at one of the most popular entry vectors abused by ransomware threat actors—open remote access tools and solutions. Remote access into an environment is not an inherently a bad thing; many organizations legitimately use remote access to provide administrative functionality to an environment. This is often necessary for remote branches or with remote employees (which have recently surged).

What becomes a concern is when an organization deploys remote access with minimal to no security configuration, default or easily guessed credentials, or single-factor authentication. Even worse, if a remote access solution becomes vulnerable and easily exploited, adversaries can utilize that to take control of a legitimate install, even with correct security implementations.

The easiest way to mitigate remote access abuse is to simply remove it all together. However, if an organization determines that the business requires it, or that it is necessary for operations, the next best step is to wrap protections around it to prevent adversaries from using it as an entry vector into the organization. Figure 1 outlines a remote access deployment that organizations can use to mitigate ransomware attacker trends.



Adversary Path

1. A legitimate, authorized user accesses the environment via single-factor credentials.
2. An adversary obtains the same credentials and, with little resistance, logs into the environment.
3. Once the adversary is in, they can move between perimeter and internal systems with ease following the same routes.
4. With remote access, successful C2 communications, the adversary can easily deploy ransomware and hold the environment hostage.

Ransomware Mitigation

A. The perimeter is not always the easiest to secure—sometimes we must leave services accessible, even if we want to close them. Instead, consider:

   a. Multi-factor authentication

   b. VPN or zero trust architecture to secure user access

B. The hop between the perimeter and internal networks deserves its own layer of protection. Defense-in-depth strategies can help secure unauthorized access to these segments.

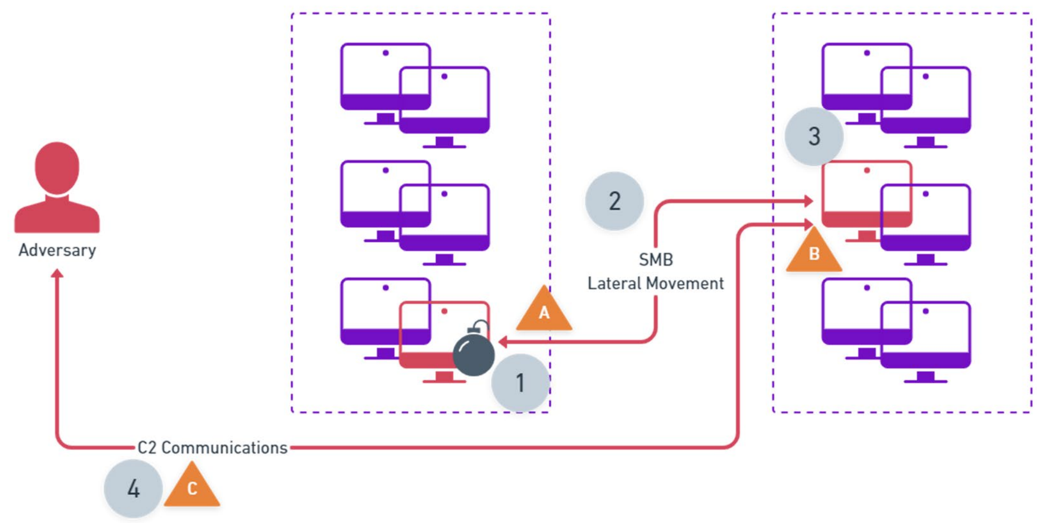
C. Network and endpoint prevention, detection, and response can help mitigate or eliminate the ability to install malware, establish outbound C2 communications, and deploy ransomware.

Figure 1. Remote Access Deployment for Mitigating Ransomware

Fileless Malware

Our second case study examines an adversary who leaves little to no evidence on disk. Via the use of fileless malware, in-memory scripts, and native system binaries, they fly under the radar while conducting damaging and impactful ransomware breaches. These techniques create a tough spot for security teams who rely on legacy or file-based detections to detect malware.

One key issue with fileless malware or abuse of native system binaries is the ease with which adversaries can hide in plain sight. Native system binaries run all the time. In fact, it's not inherently irregular for a system to run its own executables. After all, they are necessary for runtime. Adversaries just do something different from what the binary was intended (such as using BITSAdmin to download a file from a malicious remote resource).



Adversary Path (Final State)

1. Infiltration into the environment can begin with a spear phish, drive-by download, or some other event to establish initial compromise. This can be a method that utilizes native system binaries and scripts, leaving little malware on the system.
2. Lateral movement can also be achieved automatically via scripts and native tools, with malicious traffic blending into normal environment traffic.
3. Moving from one system to another is not hard—native protocols, shared passwords and admin accounts, and open ports in trusted networks allow for adversaries to easily move from one to many.
4. With established communications, adversaries can maintain connectivity into an environment.

Ransomware Mitigation

A. The first mitigation comes from using endpoint and network detection and response tools to detect malicious use of native system files. System files have very distinct behavior—controls should look for anomalies to the expectations. User behavioral analytics can also help discover these anomalies.

B. Lateral movement to another system allows an adversary to scale their operation and achieve their objectives—it also creates more opportunities for detection.

C. Finally, adversary C2 communications often have a distinct pattern. Despite blending into normal outbound traffic, they display traits that can be used to detect and prevent adversaries from maintaining a necessary bidirectional channel.

Figure 2. Prevention/Detection of Fileless Malware

Mitigating these TTPs is also significantly harder because we cannot prevent a system from running its own binaries. Instead, we must look to in-memory or behavioral analysis to determine when a runtime is good or irregular (and potentially malicious). Figure 2 shows a common situation involving prevention or detection of fileless malware.

New and Emerging Technologies

We must also consider the future of information security defenses to understand how newer technologies can help prevent and mitigate ransomware attacks. Key solutions to examine include:

- **Encrypted Traffic Analysis (ETA)—**Adversaries might encrypt their network traffic to evade detection mechanisms. However, encrypted traffic does not render metadata unavailable. Rather, we can look for key metadata signatures and patterns that can provide insight and intent of encrypted traffic.
- **Moving Target Defense (MTD)—**This prevention mechanism relies on morphing or dynamically altering code to dodge exploitation attempts. Adversaries rely on static code or binaries to exploit vulnerabilities; MTD prevents exploitation by removing the ability to exploit.
- **AI event aggregation, correlation, and intrusion prevention—**Looking far ahead in technical capabilities, AI detection and prevention mechanisms can be used to correlate and detect events that lead to an intrusion, ultimately stopping them before an adversary has a chance to gain a foothold into an organization.

Closing Thoughts

Unfortunately, 2020 and 2021 laid the foundation for ransomware actors to establish notoriety and build big businesses from the digital suffering of others. Although ransomware is not a new threat, adversaries will continue to change their TTPs to maximize their chance for success and to evade detection. This creates both a challenge and an opportunity for security teams, even as it may shift where they need to prioritize their detection and prevention efforts.

This whitepaper described where organizations need to prioritize by examining some of the current ransomware trends and by identifying things organizations should watch for in 2022. Whether it's a shift in tactics and detections, use of a tried-and-true technique, or simply a behavioral shift in demands and extortion, ransomware actors will certainly be around for a very long time (as long as they can make money), and we can expect this ever-looming threat on the horizon.

Additionally, although this whitepaper focused heavily on ransomware, security teams must remember that adversaries often share TTPs, regardless of their final goal. Key attack steps such as credential harvesting and lateral movement are not unique to ransomware. Therefore, by using ransomware as a catalyst for increasing prevention, detection, and response capabilities, an organization can bolster itself against multiple types of attacks and adversaries.

This paper also covered adversary and defensive trends at a certain point in time. However, we'll be the first to say that what your environment may need, other environments may want. Conversely, a posture and strategy that works over here might not work over there. The only consistency is that adversaries don't care. They have just one final goal in mind, and we can use that to our advantage. We encourage every security team to consider the intricate and unique needs of their own environment and deploy ransomware defenses and countermeasures appropriately.

Sponsor

SANS would like to thank this paper's sponsor:

Gigamon®