Using a Layered Approach to Improve Ransomware Detection and Response

Employing security analytics to detect the actions before the breach

Introduction

Ransomware is a form of malware designed to render data on an endpoint inaccessible to the user. Ransomware encrypts these files, effectively holding them for ransom. After reviewing the characteristics of four recent ransomware attacks, the Exabeam Security Research Team observed that the indicators of compromise (IoCs) used showed several different methods of gaining access into organizations. However, our analysis of the tactics, techniques, and procedures (TTPs) indicates that once inside, virtually every ransomware attack used the same methods to achieve its goal: credential theft. TTPs are behaviors, and, consequently, to defend against ransomware and credential theft, enterprises need an approach that understands behavior and identifies the TTPs immediately. Once these TTPs are detected, security teams are better prepared to take action and stop a potential attack before it does any damage.

As previously mentioned, a common characteristic of most ransomware attacks is compromised credentials. While it may seem easy to protect the environment against any insider or malicious threat, it gets quite complicated when credential theft occurs and lateral movement happens following an entry point. When legitimate credentials are used, most security tools cannot detect these movements or any abnormal behavior associated with them.

Ransomware's Destructive Effects

In this paper we'll focus on the most common and destructive ransomware in today's environment: encrypting ransomware. This type of ransomware encrypts specific file types or entire drives on a device and holds them hostage until a ransom is paid. This type of attack can be particularly destructive when it affects essential personal or business-critical data.

Following are some alarming statistics about ransomware from Cloudwards and others:

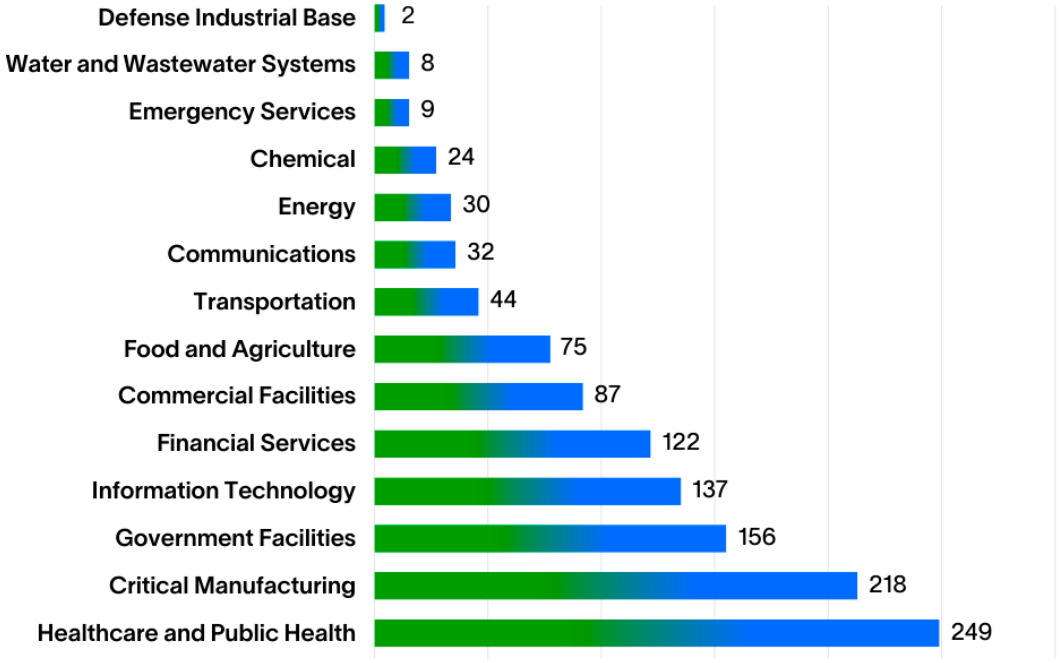
- In the first half of 2023, the rate of ransomware attacks rose 50% year over year, according to the World Economic Forum.
- Over $1 billion in cryptocurrency was paid out to criminals for ransomware in 2023.
- Almost 85% of private-sector organizations say they've lost business or revenue due to a ransomware attack.

Publicly disclosed victims of ransomware in 2023 include:

- Lockbit attacked the Royal Mail in the UK
- VMware ESXI servers globally
- NCR was attacked by the BlackCat ransomware group

Here's a summary from the FBI of infrastructure sector attacks for 2023:

Infrastructure Sectors Affected by Ransomware



Universally, the double whammy of exploitable vulnerabilities and compromised credentials were the two largest, and definitely related, root causes of the attacks. This underscores the importance of good endpoint security combined with visibility into Active Directory/credential management systems as part of any security stack—and the ability to see sequential activity in near-real time as one machine or credential pair is compromised.

And a list of IoC sources isn't enough. You can create a block for every known bad DNS or IP in your network and still fall to a zero day or phishing attack, due to the methodologies used by the many ransomware family strains. The MITRE ATT&CK® framework has multiple tactics and techniques that identify different parts of the ransomware activity, and each TTP can be the important indicator that something in the system is abnormal, when observed.

Tactic	Tactic Name	Technique
T1112	Modify Registry	Defense Evasion
T1012	Query Registry	Discovery
T1082	System Information Discovery	Discovery
T1120	Peripheral Device Discovery	Discovery
T1005	Data from Local System	Collection
T1486	Data Encrypted for Impact	Impact
T1543.003	Create or Modify System Process: Windows Service	Persistence - Privelege Escalation
T1490	Inhibit System Recovery	Impact
T1553.004	Subvert Trust Controls: Install Root Certificate	Defense Evasion
T1078	Valid Accounts	Initial Access - Persistence - Privilege Escalation

Table 1. **With IoCs in the millions, the only predictable ransomware detection is TTPs. This list includes the common ATT&CK techniques detected in most ransomware attacks.**

How Ransomware Works

It only takes one zero-day vulnerability or unpatched device for ransomware to worm its way into a network, and access to a user or service account credential to spread throughout an ecosystem.

After careful analysis of four separate attacks, the Exabeam Security Research Team has determined that while each attack showed different IoCs, meaning malicious actors breached the organization in different ways, once inside, all four intrusions escalated in the same way. The TTPs associated with each intrusion were all the same—the only characteristics all the attacks had in common.

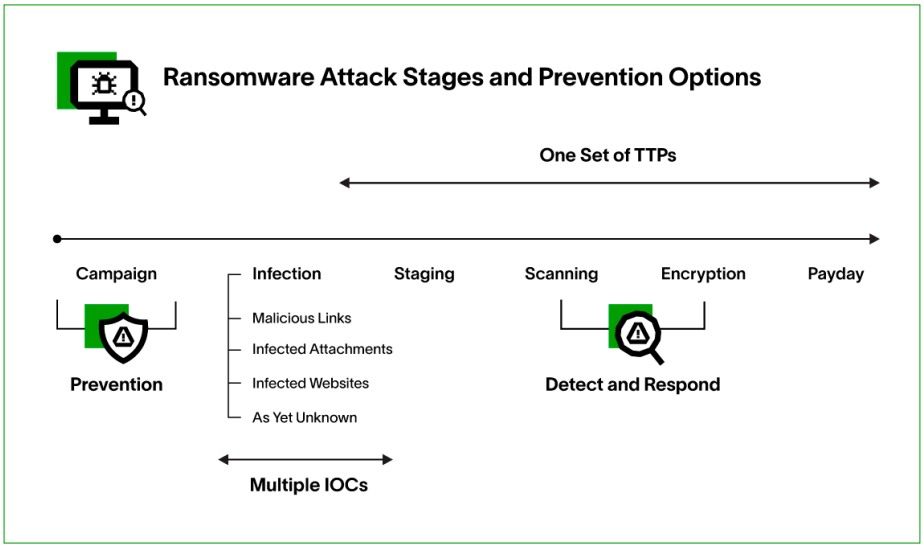


Figure 1. **Ransomware Attack Stages and Prevention Options**

The Standard Six-Stage Ransomware Kill Chain

There is a kill chain associated with ransomware, following seven basic stages. These stages are:

1. **Reconnaissance:** Attackers decide where they want to attack via various internet scraping or mapping programs.
2. **Distribution campaign:** Attackers use techniques like social engineering and weaponized websites to trick or force users to download a dropper which kicks off the infection.
3. **Malicious code infection:** The dropper downloads an executable which installs the ransomware itself.
4. **Malicious payload staging:** The ransomware sets up, embeds itself in a system, and establishes persistence to exist beyond a reboot.
5. **Scanning:** The ransomware searches for content to encrypt, on both the local computer and network accessible resources.
6. **Encryption:** The discovered files are encrypted.
7. **Payday:** A ransom note is generated, shown to the victim, and the hacker waits to collect on the ransom.

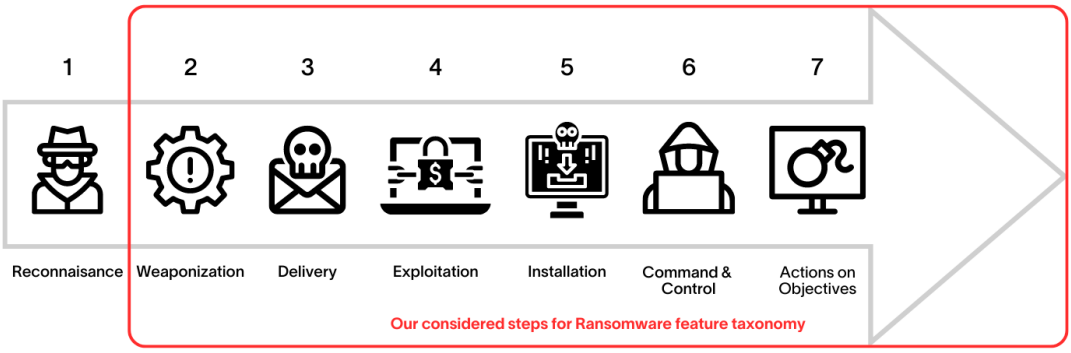


Figure 2. **Ransomware attack stages**

Multiple Means of Entry

As noted above, advanced ransomware exploits gain entry to a system by several different means. Some of the common entry points to a network for ransomware are:

Phishing

Malicious links: Bad actors often use phishing or spearphishing emails with malicious links to deliver their payload. Spearphishing targets the content to the audience, creating realistic-looking emails likely to be clicked based on the interests of targets.

Infected attachments: Likewise, opening attachments in emails or from shares is an effective way to gain access to a network. An unwitting user clicks a link and becomes infected, thereby granting further access.

Drive-by download attacks

Infected websites: Often attackers will inject their ransomware into a website that automatically downloads the ransomware onto a user's machine. Adware and bundleware are also common culprits of drive-by download attacks.

Once a machine is infected, the exploit often uses lsadump or Mimikatz-type tools to enumerate the network and find places to exploit weak passwords or dump credentials to gain access to more accounts to compromise.

Prevention Is Not Enough

Prevention of ransomware's entry into your system is clearly the best scenario, so enterprises should continue to employ tools to prevent entry. Unfortunately, however, no prevention method is guaranteed, as the staggering statistics and increase in ransomware attacks clearly indicate.

Optimal Ransomware Protection

The necessary complement to preventing entry, which can come through multiple attack vectors, is to accept that ransomware may enter at any time and to constantly audit your systems to detect known kill chain behaviors. Once these behaviors are detected, you can act to prevent the lateral movement required to spread the ransomware across your network before it can do any damage. This is an essential part of effective ransomware protection.

Let's consider a more comprehensive, best-practice approach to ransomware protection, which includes not only prevention, but detecting and eradicating ransomware that enters your system.

Prevention

If Benjamin Franklin were alive today, he would probably allow that an ounce of ransomware prevention is worth a pound of remediation. So how do you keep ransomware off your network in the first place? Here are some best practices for prevention.

Patch software and operating systems: In the absence of a zero-day exploit, there is likely a patch to prevent attackers from deploying malware on your system. Patching can be bothersome and cause problems from time to time, but they pale in comparison to getting your network ransomed.

Uninstall legacy and unsupported applications: Many ransomware attacks attempt to take advantage of old and vulnerable software to create an entry vector to your network. Managing applications on endpoints prevents this in most cases.

Teach your staff security hygiene: Well-informed employees are often the best line of defense against the attack techniques used by the purveyors or ransomware.

Backup frequently: Backing up frequently prevents the need to pay the ransom in the first place. Storage is relatively cheap these days, so follow established organizational backup procedures to keep good backups, and maybe even backups of your backups.

Detecting Ransomware in Operation

As noted above, in the best case, you will keep ransomware from getting into your system. But if it does, all is not necessarily lost if you can catch and remediate the ransomware quickly.

Ransomware wants to strike as fast as possible, with most phases in the attack lasting only minutes. The table below shows there are only a few phases where an organization can disrupt an active ransomware attack.

Campaign	N/A	N/A
Infection	Seconds	IOC usually doesn't exist
Staging	Seconds	IOC usually doesn't exist
Scan	Minutes to hours	Behavioral modeling
Encrypt	Minutes to hours	Behavioral modeling
Payday	N/A	Too late

With ransomware, time is of the essence. Detecting the ransomware during the early phases of the attack such as "Infection" and "Staging" would require an IoC; however those IoCs usually only exist after attacks have been effective and reported back to security vendors at least once. Worse, the most effective ransomware attacks use zero-day or freshly released vulnerabilities.

Endpoint detection and response/anti-virus (EDR/AV) vendors can efficiently disrupt the ransomware at the encrypt stage, but unfortunately, they can only do this for known ransomware strains for which they have developed deterministic signatures. For new ransomware, EDR/AV vendors usually err on the side of caution. Disrupting zero-day ransomware would typically require endpoint security vendors to also disrupt regular users from normal endpoint operations, such as preventing any suspicious process to open or save and/or delete files.

Exabeam research suggests the defender's greatest opportunity to detect is when the ransomware is out in the open, as it spreads on the network during the "scan" phase. This is when the ransomware is:

- Scanning the network for files and locations to encrypt
- Verifying the endpoint's capabilities to encrypt the files and to delete the cleartext versions of these files
- Checking for the endpoint's ability to communicate to a command-and-control center

This behavior can be detected by user and entity behavior analytics (UEBA) tools using advanced analytics behavioral modeling. Because these tools ingest telemetry from across the broader security stack, they are uniquely capable of understanding what is normal and what is not. Once a behavioral model is triggered, these tools can then surface relevant insights to an analyst and/or automate the next right action. It is almost impossible to write effective correlation rules for unknown behaviors, because doing so would require too many rules and generate too many false positives. But UEBA solves this problem. It detects the behavioral deviations and spots malicious activity without the need for signatures—one behavioral model can literally cover the detection scope of millions of rules.

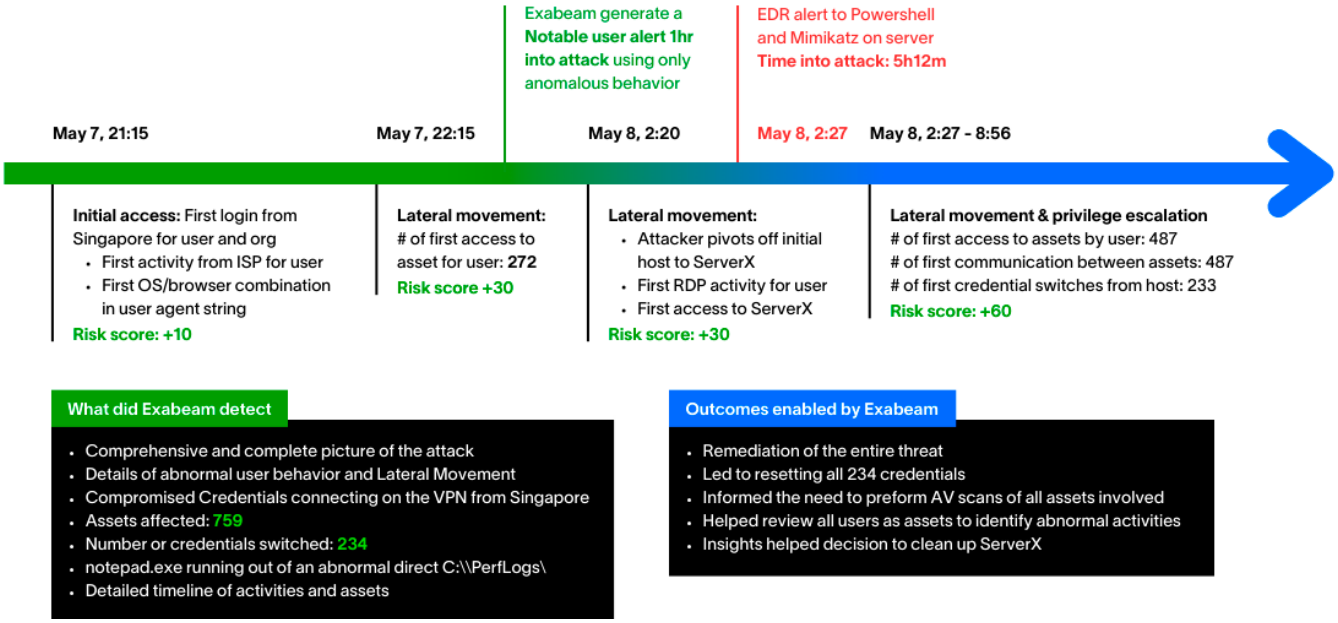


Figure 3. **Exabeam gives a comprehensive picture of compromised insider activities.**

Summary

Ransomware is here to stay, and organizations large and small need to revisit their risk management priorities for this attack vector. The ransomware defender's window of opportunity is small and demands a layered approach to detection and response that includes advanced analytics to find new ransomware strains and their variants. This can be done by analyzing the behavior of the ransomware executable and its interactions with the host and the network.

How Exabeam Can Help

Exabeam Security Analytics detect and alert on ransomware by looking for unique signatures of ransomware activity. While the ransomware use case has only fact-based models, there are hundreds of potential behavior models that can trigger, which, in sequence, can indicate early ransomware activity. Exabeam can help identify currently known types of ransomware behavior, including Conti, LockBit, WannaCry, and NotPetya with all their variants. The rules are derived from forensic analysis of how the malware is installed and deployed, providing early detection of the ransomware.

Exabeam also looks for indications of journal or backup deletion. There are very few individuals in an organization who should be permitted to delete backups. The backup policy assigned for an organization is not designed to be tampered with by non-administrators. Activity involving the deletion of shadow copies and system journals may not always be related to ransomware, but it is always worth investigating if an anomalous rule trigger occurs for a user. Exabeam also provides detection of system utilities that are utilized by attackers in ransomware attacks. And it looks for specific command arguments that are known to be used by attackers to deploy ransomware.

Exabeam provides an additional measure of coverage through its built-in Threat Intelligence Service. The Threat Intelligence Service pulls down IPs, domains, and extensions known to be associated with ransomware attacks, and adds the identifiers to the pertinent context table. These context tables are then used in rule logic to trigger alerts when events breaking the rules occur on the network. If the source or destination IP is a known ransomware IP, the rule will trigger—likewise for known ransomware domains. Ransomware often renames files to demonstrate to the affected user that the files are now encrypted. When these extensions are detected, a rule will fire.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam

Learn more at
www.exabeam.com →

Exabeam, the Exabeam logo, New-Scale SIEM, Detect. Defend. Defeat., Exabeam Fusion, Smart Timelines, Security Operations Platform, and XDR Alliance are service marks, trademarks, or registered marks of Exabeam, Inc. in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.
©abeam, Inc. All rights reserved.