WHITE PAPER

Breaking the Ransomware Kill Chain with the Akamai Enterprise Security Suite

Table of Contents

Understanding the ransomware kill chain 4

Initial access 5

Protect internet-facing servers 5

Block phishing URLs 5

Reduce VPN attack surface 6

Command and control 6

Block command and control (C2) servers 6

Discovery 7

Identify network scans 7

Deception against discovery 8

Lateral movement 9

Identify suspicious host indicators 9

Block LAN attacks 10

Restrict management ports 10

Exfiltration 11

Block exfiltration domains 11

Multilayered defense 11

Introduction

Defeat ransomware at various steps of the kill chain using Akamai enterprise security solutions

One of the biggest security threats that organizations face today is ransomware, a form of malware designed to encrypt important files on a device, rendering them unusable. The malware operators then demand a ransom in exchange for a decryption key or software that can restore the files to their original data. In recent years, ransomware crime groups have evolved their tactics and began exfiltrating their victims' data to hold as additional leverage — threatening to leak it publicly or sell it on the dark web.

To be able to defend against this type of attack, it's important for defenders to understand the way that ransomware groups operate to achieve their goals.
This paper will help you do exactly that.

Understanding the ransomware kill chain

Ransomware attacks are complex — breaching the system is just the beginning. To maximize the damage, an attacker must also spread their malicious payload across the network before beginning encryption. If only a single computer is encrypted, the attacker will not have enough leverage to demand a ransom. For the ransomware attack to be successful, the attacker must perform various steps — discover network assets, move laterally, etc. Those steps are often referred to as the ransomware kill chain.

Each step in this chain opens many opportunities for detection and mitigation. Preparing your network beforehand with the Akamai enterprise security suite can reduce your attack surface, and help mitigate and contain any possible damage from ransomware before you're even aware you've been hit. This paper will detail how you can use Akamai Guardicore Segmentation, Enterprise Application Access, and Secure Internet Access to detect and block ransomware activity across the different steps of the kill chain:

Initial access

The first phase of the attack, where attackers breach the internal network from the outside

Discovery

Methods attackers use to identify important assets inside the network

Lateral movement

The phase where attackers spread across the network and compromise additional assets

Command and control

The different ways attackers maintain a communication channel into the network to send information and commands to compromised assets

Exfiltration

Methods used by attackers to exfiltrate sensitive stolen data in a covert manner

Initial access

Every organization has plenty of interfaces with the internet. Attackers will try to abuse each of them to gain access to the network. Akamai allows you to seamlessly protect those interfaces and keep attackers out of your network.

Protect internet-facing servers

Use Secure Internet Access payload analysis capabilities to protect internet-facing servers from exploitation

According to Kaspersky, the most common method attackers use to obtain initial access is exploitation of internet-facing applications — often by abusing one-day vulnerabilities on unpatched systems. Vulnerabilities such as Log4Shell (CVE-2021-44228) and ProxyLogon (CVE-2021-26855) are still being exploited in the wild today to breach networks and deploy ransomware.

Enterprise Threat Protector can be configured to monitor all incoming web traffic to your internet-facing servers; this traffic is then analyzed, and any malicious or anomalous activity can be identified and blocked.

Block phishing URLs

Use Enterprise Threat Protector URL inspection capabilities to detect and block phishing attempts

Phishing is a very common way to breach networks. Attackers will often send emails containing links to malicious attachments or to fake login pages that are designed to steal credentials. Using the Enterprise Threat Protector client on your endpoints will enable you to scan each of the URLs your users click in real time, identifying any malicious or anomalous links and blocking them.

Reduce VPN attack surface

Use Enterprise Application Access to enable secure, application-specific VPN access and reduce external attack surface

In today's hybrid work environment, which often includes remote work, it is becoming more common to allow users to use a VPN to log into the corporate network. Attackers have adapted to this and started exploiting this opportunity to gain access to the internal network. Attackers are often seen attacking employees' personal computers, compromising their VPN credentials and then using them to access the internal network. In some cases, attackers will also target vulnerable servers to leak credentials. In November 2022, attackers abused a vulnerability in Fortinet VPN servers to gain initial access and then proceeded to spread ransomware to the entire network.

Enterprise Application Access allows you to reduce this risk significantly by allowing application-specific, role-based access to your network — it does not grant users full access to the entire network like traditional VPNs, instead only allowing limited access to specified applications. This way, even if an attacker were to compromise the user's credentials and bypass the MFA protection, they will still not gain access to the network, only to a limited set of applications.

Command and control

Block command and control (C2) servers

Use Akamai Secure Internet Access to block known malware command and control servers

Malware in general and ransomware in particular requires communicating with external C2 servers to send commands and retrieve information from infected assets. By analyzing Akamai's extensive communication data, we are able to monitor ransomware and malware C2 domains and to keep track of new and evolving campaigns. The Enterprise Threat Protector client allows us to monitor your entire DNS communication in real time and block communication to malicious domains — preventing the malware from running properly and accomplishing its goals.

Discovery

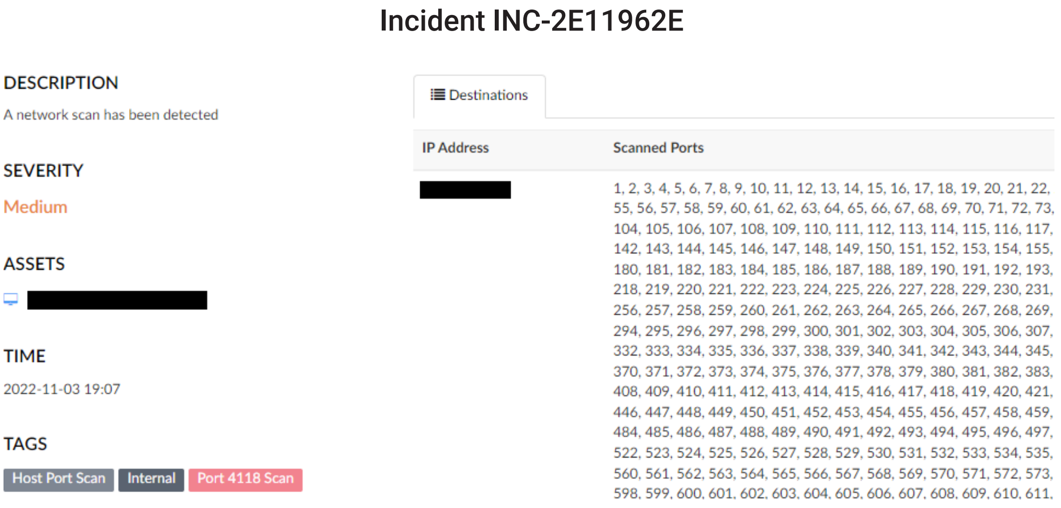
Once attackers breach the network, they will try to identify additional assets to understand the network structure before starting to move laterally. This will often result in internal communication, which can be detected by Akamai Guardicore Segmentation.

Identify network scans

Use Akamai Guardicore Segmentation detectors to identify suspicious network scans

One of the common methods attackers use for network discovery is the usage of port scanning to identify network services — many ransomware groups are seen using open source network scanners. In a recent CISA Advisory regarding the LockBit 3.0 ransomware, the group was shown to be using the "SoftPerfect Network Scanner" to perform port scanning. Another example is the Nokoyawa ransomware group that was observed scanning networks for SQL servers to access sensitive data on them.

Akamai Guardicore Segmentation monitors all the communication in your network and has built-in detectors that will identify and alert on such scans, allowing you to stop the spread of the malware before it starts.



Incident INC-2E11962E

DESCRIPTION

A network scan has been detected

SEVERITY

Medium

ASSETS

[redacted]

TIME

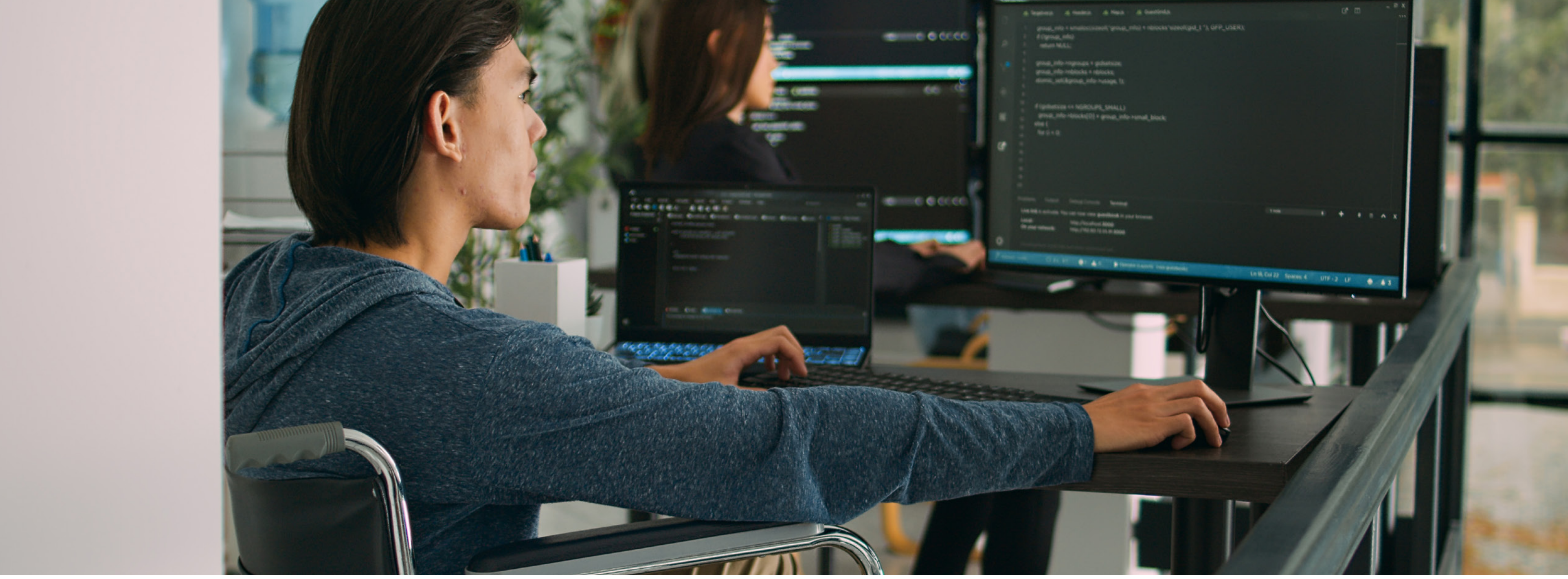
2022-11-03 19:07

TAGS

Host Port Scan · Internal · Port 4118 Scan

IP Address	Scanned Ports
[redacted]	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611,

Fig. 1: Network scan incidents in Akamai Guardicore Segmentation



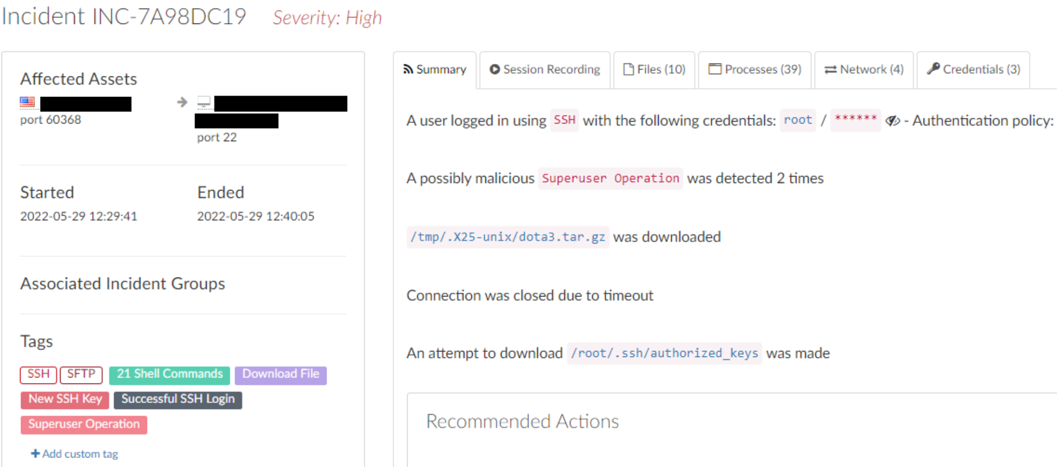
Deception against discovery

Use Akamai Guardicore Segmentation to identify discovery attempts

When attackers breach a network, they don't have prior knowledge of its structure and of the different assets in it. To overcome this gap, they will have to "probe in the dark" and try to find their way manually. Akamai Guardicore Segmentation allows you to take advantage of this using the deception service — luring attackers into honeypot servers, monitoring their activities, and alerting you once anomalies are detected.

For example, an attacker breaches the network and tries to brute-force the SSH credentials of a Linux server. Akamai Guardicore Segmentation will identify this anomaly and forward the attacker to a dynamically generated honeypot. Once inside the honeypot, all the attacker's actions are logged, and an alert is generated.

The following is an example of one such alert:



Incident INC-7A98DC19 *Severity: High*

Affected Assets

[redacted] port 60368 → [redacted] port 22

Started 2022-05-29 12:29:41

Ended 2022-05-29 12:40:05

Associated Incident Groups

Tags

SSH SFTP 21 Shell Commands Download File New SSH Key Successful SSH Login Superuser Operation

A user logged in using `SSH` with the following credentials: `root` / `******` - Authentication policy:

A possibly malicious `Superuser Operation` was detected 2 times

`/tmp/.X25-unix/dota3.tar.gz` was downloaded

Connection was closed due to timeout

An attempt to download `/root/.ssh/authorized_keys` was made

Recommended Actions

Fig. 2: Deception incident in Akamai Guardicore Segmentation

Lateral movement

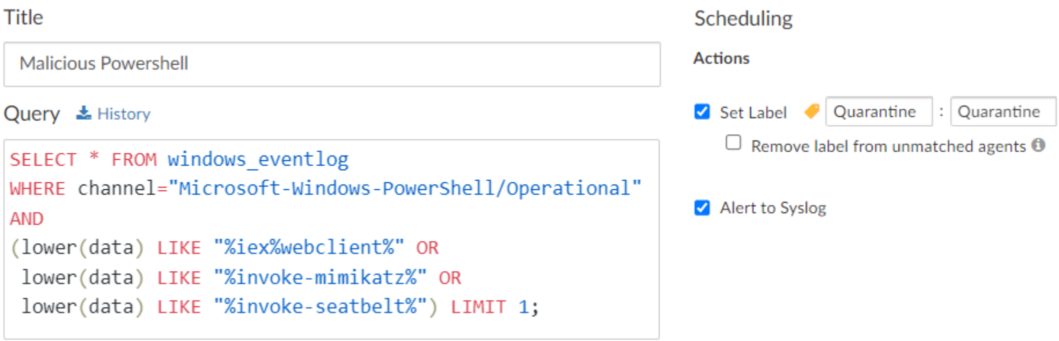
After an attacker gains access to the network and familiarity with its topology, they would want to use it to move laterally. Modern ransomware groups will breach a network and then move laterally to compromise as many assets as possible — encrypting all of them. Akamai enterprise security products allow you to limit the possibilities of lateral movement and to minimize the breach scope.

Identify suspicious host indicators

> Use Akamai Guardicore Segmentation Insight module to identify suspicious host indicators in various ways

Attackers use PowerShell tools to achieve a variety of goals — one of them is to perform lateral movement. PowerShell droppers are very common, and attackers often use them as the first piece of code they execute on a compromised asset. Recent infections of the Quantum ransomware were shown to be doing exactly that — running PowerShell code over Windows Management Instrumentation (WMI).

Using the Insight module of Akamai Guardicore Segmentation, you can run scheduled queries to scan the PowerShell event log on all of your assets, labeling assets with malicious indicators and quarantining them.



Title

Malicious Powershell

Query History

```
SELECT * FROM windows_eventlog
WHERE channel="Microsoft-Windows-PowerShell/Operational"
AND
(lower(data) LIKE "%iex%webclient%" OR
 lower(data) LIKE "%invoke-mimikatz%" OR
 lower(data) LIKE "%invoke-seatbelt%") LIMIT 1;
```

Scheduling

Actions

☑ Set Label Quarantine : Quarantine

□ Remove label from unmatched agents

☑ Alert to Syslog

Fig 3: Creating a scheduled Insight query to detect malicious PowerShell

But PowerShell is only one example. Insight can be leveraged to scan a wide variety of lateral movement indicators, using any of the existing osquery tables, for example:

- Use the File table to detect malware files based on names or hashes
- Use the Startup Items table to detect suspicious autorun entries on your assets
- Use the Yara table to scan files on your assets using yara rules to detect malware strains

Block LAN attacks

Use Akamai Guardicore Segmentation to block and detect attacks on local network protocols

After breaching patient zero in the network, attackers abuse vulnerabilities in LAN protocols such as ARP to compromise other assets. Using a traditional firewall, those attacks can easily go under the radar, as they are performed in Layer 2 — and this type of communication doesn't reach the firewall.

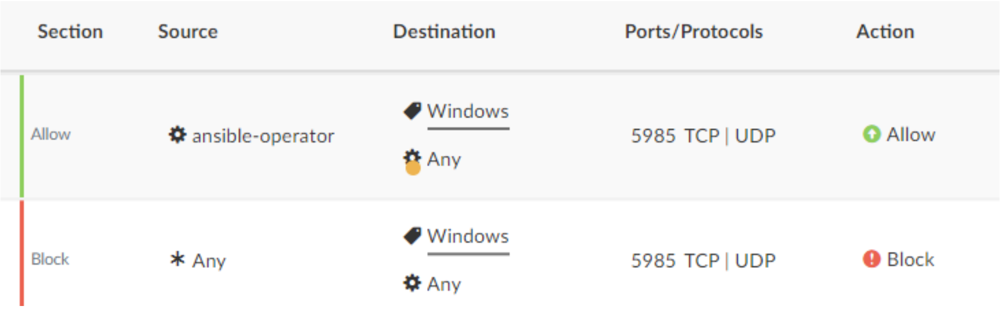
Akamai Guardicore Segmentation's software-based approach allows you to monitor and block all the traffic that goes into or out of an asset, even the local traffic that would normally not reach the enforcing firewall.

Restrict management ports

Use Akamai Guardicore Segmentation to create process-level policy to reduce the attack surface over sensitive ports

Once inside the network, attackers will usually perform privilege escalation on compromised assets with the purpose of stealing credentials. Once credentials are obtained, attackers will often use management protocols such as RDP, RPC, SMB, and WinRM to execute a ransomware payload on all of the assets in the network. However, blocking these ports entirely is often not a viable option as administrators require them for regular operations.

Akamai Guardicore Segmentation allows you to apply policy on the process level, enabling you to determine which processes should be communicating over sensitive management ports. Let's examine WinRM — it is used by many administration programs, including Ansible. However, it is also often abused by attackers using tools such as Evil-WinRM to perform lateral movement. Using Akamai Guardicore Segmentation, we can create a policy to allow incoming WinRM connections only from Ansible processes, blocking other processes over the same port:



<table>
<tr><th>Section</th><th>Source</th><th>Destination</th><th>Ports/Protocols</th><th>Action</th></tr>
<tr><td>Allow</td><td>ansible-operator</td><td>Windows
Any</td><td>5985 TCP | UDP</td><td>Allow</td></tr>
<tr><td>Block</td><td>Any</td><td>Windows
Any</td><td>5985 TCP | UDP</td><td>Block</td></tr>
</table>

Fig. 4: Example of Akamai Guardicore Segmentation policy to limit WinRM communication

Exfiltration

In recent years, attackers adapted their extortion tactics and began leaking sensitive files from their victims to be used as additional leverage. Attackers will try to blend in with the network noise as they exfiltrate the data from the organization, but they can often still be detected and blocked during this phase.

Block exfiltration domains

Use Akamai Guardicore Segmentation to limit access to services that can be abused for data exfiltration

Attackers often use public tools to leak data from the network, a very common option being public hosting services such as MEGA, Dropbox, and Google Drive. The challenge in monitoring these domains is that they are commonly used legitimately inside the network. For example, accessing the MEGA domain through a browser could be considered legitimate, but doing so using the rclone utility — which is being actively used by several attack groups to exfiltrate data — would be considered malicious.

Using Akamai Guardicore Segmentation, we can minimize the risk from such tools by blocking their domains from all endpoints that do not require access to them, and only allowing access through approved applications such as browsers.

Multilayered defense

To achieve their most desired goal, attackers have to go through several different attack phases. Each step provides a chance for defenders to block and detect the associated malicious activity. Using the different Akamai security products, defenders can employ mitigations at each step of a ransomware kill chain — stopping attackers in their tracks and detecting any anomalous behavior.

For more information about Akamai Guardicore Segmentation, or to request a personalized product demo, visit akamai.com/guardicore

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn. Published 09/23.