SYGNIA

CASE STUDY:
SYGNIA MDR IN ACTION

Sygnia MDR detected and contained malicious activity attempting to deploy Lumma Stealer malware.

Timeline of Events

7:00:37 PM
A user accessed a legitimate website, which had been compromised at the time. The compromised website was infected with a fake reCAPTCHA prompt.

7:03:03 PM
The fake reCAPTCHA prompted the user to execute a series of steps, including opening the 'Run' Windows utility, pasting a PowerShell command that had been copied to the user's clipboard from the fake reCAPTCHA, and executing it."

7:04:43 PM
PowerShell attempted to download a malicious zip file containing Lumma Stealer malware. The initial PowerShell command, which was copied, accessed another PowerShell script from a different URL. This second PowerShell script attempted to download a malicious zip file containing Lumma Stealer malware.

The download was blocked by a sinkhole. If the download had not been blocked, the malicious zip file would have downloaded, extracted and executed Lumma Stealer.

8:36 PM
The relevant PowerShell logs were received into Sygnia's Velocity Threat Detection, Investigation and Response (TDIR) platform. Sygnia MDR runs on the Velocity platform.

8:48 PM
Velocity generated an alert about a suspicious PowerShell download, associated with a malicious URL that is base64 coded. After a thorough investigation, it was discovered that the activity originated from a compromised domain with a fake reCAPTCHA page. It is notable that no other security vendors raised an alert on this activity.

8:54 PM
Client was notified with initial investigation insights and remediation recommendations.

9:10 PM
Host contained, user disabled and passwords reset.

What is Lumma Stealer malware?

Lumma Stealer (also known as LummaC2 or Lumma Stealer v4) is a sophisticated information-stealing malware (infostealer) that has become increasingly active and dangerous since its emergence around 2022. It's part of a broader trend of "stealers-as-a-service" (SaaS) offerings on the cybercrime underground, where threat actors can subscribe to use the malware and access a control panel to manage stolen data. It is used to extract sensitive material from infected systems, including browsing history, saved logins, and cookies from browsers including Google Chrome, Microsoft Edge and Opera.

Why is it difficult to detect?

Lumma Stealer malware is particularly difficult to detect because it is designed to evade traditional and even advanced security solutions. Creating effective detection rules for Lumma Stealer is difficult because of the high volume of false positives such rules tend to generate.

How Sygnia detected this

Sygnia MDR detection engineers and security analysts work in close collaboration with both Sygnia Incident Response and Red Team, which allows them to create and utilize Indicators of Compromise (IoCs) based on the latest attacker activities. This enables Sygnia to create high efficacy, low-noise detection rules that catch what others miss.

This particular detection came from a Sygnia custom developed detection rule, not from the client's security technology, demonstrating the value of Sygnia's custom detection rules, which go beyond standard out of the box capabilities.

Within ten minutes of the alert being triggered, Sygnia notified the client and provided remediation actions. Using the Pathfinder agent collection capabilities, Sygnia reconstructed a full timeline of the attack. Sygnia provided the client with all investigation insights and clear remediation actions, without needing to perform any additional investigation on their end.

> Pathfinder is Sygnia's proprietary, lightweight agent that collects binary data from servers and workstations.

In the client's words

"We had a security event last night, maybe the closet we've been to a true breach since 2020. We are still investigating but it seems that the (Sygnia) MDR team and Velocity have saved the day for us. Wanted to express my gratitude and let you know that the MDR service has really paid off for us"

Vice President, Information Technology