Infocyte

CASE STUDY / BIOTECHNOLOGY

Infocyte HUNT

Infocyte Partner uses HUNT to identify new malware variant, masked behind Ryuk ransomware; works with Infocyte threat hunters to close attack entry vector.

THE CUSTOMER

A top 5 global security software provider, leading incident response efforts for a ransomware attack at the U.S. offices of an international biotechnology firm with heavily guarded IP.

ASSET DISCOVERY + THREAT HUNTING + VULNERABILITIES + INCIDENT RESPONSE

BACKGROUND

In Q3 of 2018, law enforcement officials responded to a Ryuk ransomware attack at a US-based biotechnology firm with global operations and high-value intellectual property — not to mention valuable customer and financial data. Due to the severe nature of the ransomware attack, the FBI was called to assist in investigating the source of the attacks.

The biotech firm requested incident response assistance from a top-tier cybersecurity software company — an Infocyte HUNT partner — contracted to conduct a thorough compromise assessment of the biotech firm's network and hunt for evidence of other attack vectors or backdoors.

THE CHALLENGE

The defensive security technology deployed on the biotech firm's newtork included next-gen firewalls with IPS, network appliances, monitoring tools, and a leading endpoint protection platform (EPP). Our partner's incident response team (reinforced with Infocyte threat hunters) needed an easy-to-deploy and quick assessment tool, capable of efficiently collecting, analyzing, and prioritizing forensics data.

Additionally, the IR team needed to hunt for other IOCs and the mysterious patient zero, or entry vector and backdoor into the biotech firm's network.

THE SOLUTION

Infocyte HUNT's threat hunting platform was selected to inspect and assist in guided IR efforts. HUNT was selected for its ability to:

- Quickly and effectively perform forensic triage simultaneously on all hosts in the environment
- Detect file-less malware in memory (Ryuk malware is known to sometimes use file-less techniques)
- Ability to analyze historical execution artifacts
- Deploy in an agentless model, bypassing the need to go through change management processes for endpoint software installations

THE DISCOVERY

Infocyte HUNT was instrumental in helping uncover new malware variants and new attack techniques being used by this Ryuk ransomware campaign, including confirming the presence of the Trickbot trojans and Mimikatz credential dumper.

Results from our IR and threat hunting efforts, along with analysis and recommendations are included on the following page.

Infocyte HUNT Results

SUMMARY

- **Scope:** All high-value assets and workstations
- **Term of engagement:** Ongoing
- **Date of engagement:** August 2018
- **Resources to deploy:** 1 security analyst
- **Scan type:** Critical assets and endpoints
- **First results in less than 15 minutes**

KEY FINDINGS

- Ryuk ransomware
- 20 systems with memory-injected Trikbot trojans
- Mimikatz credential dumper
- 70+ execution artifacts

ANCILLARY FINDINGS

- Stolen credentials
- New malware variants
- In-memory remote access

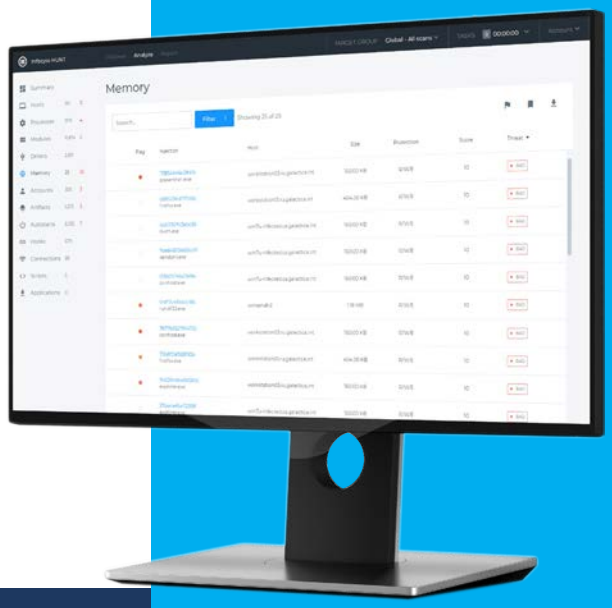
Details of this attack are still under active investigation. Indicators, samples, and other technical intelligence data related to Ryuk ransomware have been released to the community via our partners and law enforcement agencies.

ANALYSIS

The discovery of Trickbot trojan variants — a type of in-memory remote access malware historically used for long-term collection in the financial industry, and mimikatz — suggests the Ryuk malware variant used in this campaign may be part of a long-term targeted collection campaign (a "pseudo ransomware" tactic common to the Lazerous Group and their Hermes malware).

The stolen credentials and trickbot trojan, in this case, can be used as the initial entry vector for a targeted attack or as a "leave-behind" after the ransom is paid and satisfied to give the attackers long term access to the network.

The hidden remote access could also be leveraged to ensure a more effective attack across all critical services/data or repeating ransoms in the future.



THE RESULTS

Infocyte HUNT was deployed and within 15 minutes inspected the first 300 systems suspected to be compromised. Almost immediately, HUNT flagged 20 systems with active memory-injected Trickbot trojans, a system with a mimikatz credential dumper, and over 70 related execution artifacts.

Using HUNT, the Incident Response (IR) team was able to develop a timeline of the attack, based on timestamps from the historical artifacts, enabling them to rapidly identify patient zero and the entry vector for the coordinated Ryuk ransomware attack.

Infocyte threat huning platform, HUNT, provided the IR team with the rapid ability to scope the incident, collect samples of the various malware components — found both in-memory and on-disk — and identify patient zero. Additionally, Infocyte's team assisted our Partner in successfully closing the attacker's entry vector.

"[...] We immediately identified a wicked Mimikatz trickbot trojan infection, masked behind Ryuk ransomware—and more. Infocyte was amazing and saved us a bunch of time."

- Lead Incident Responder
Check Point Software

CONCLUSION & RECOMMENDATIONS

Attacks like this demonstrate a clear need to be proactive and hunt for threats in an environment. Historically, the only defense against ransomware was front-line protection (to prevent it from executing).

Unfortunately, this has changed. The steady rise in silent cryptocurrency miners replacing in-your-face ransoms and the use of pseudo-ransomware to mask the real intent of long-term access, suggests that organizations need to actively look for these cyber threats.

This is especially true immediately following an attacks, which may appare to be a commodity malware infection but may actually turn out to be something bigger and far more destructive to companies.

CONCLUSION & RECOMMENDATIONS (CONT'D)

We continue to see a rise in ransomware attacks leveraging administrative credential theft and dropping secondary payloads, like Trickbot, as hidden "leave-behinds" in order to retain access to the ransomed network following remediation.

Some targeted ransomware attacks will use these tools to scout the network for a future ransom or destructive attack like what was seen in the Saudi Aramco attack.

ADDITIONAL READING

https://www.scmagazineuk.com/does-ryuk-herald-return-ransomware-threat/article/1491072?sf91971320=1

https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

https://securingtomorrow.mcafee.com/mcafee-labs/taiwan-bank-heist-role-pseudo-ransomware/

https://twitter.com/malwrhunterteam/status/1030529747174998016

Infocyte™

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com