Mandiant In Action

Ransom Insured

The FBI is the lead federal agency for investigating cyber attacks, warning organizations about any potential threats as part of their victim notification program.

Organizations often rely on Mandiant to quickly identify malicious activity and effectively respond.

In this example, a large insurance company activated their Incident Response Retainer after being warned by the FBI about a targeted attack by a known threat actor that deploys ransomware and extorts victims for millions of dollars.

Working directly with the client's security operations center, the Mandiant team was able to stop the attacker before ransomware was deployed and eradicated the threat until it was confirmed there was no evidence of data theft.

For this engagement, the team effectively performed:

- Host Analysis
- Forensic Analysis
- Network Analysis

Problem
Defending against criminals that are increasingly using ransomware to disrupt business operations and extort victims.

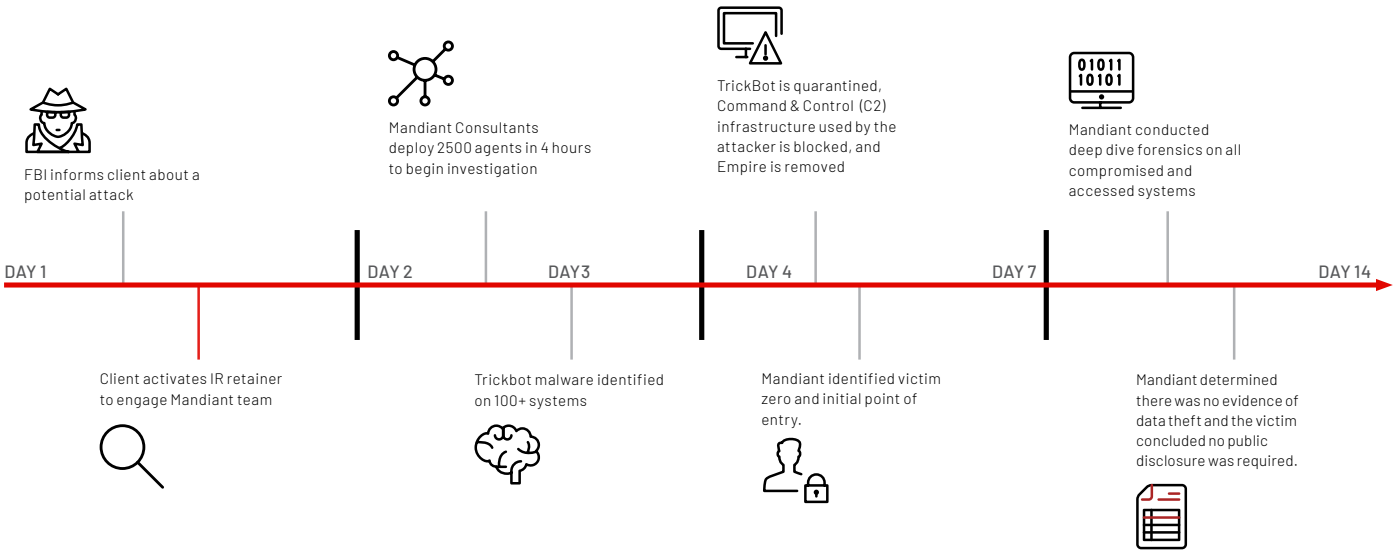
How we did it
Deployed Endpoint agents to effectively identify TrickBot malware, perform forensics on accessed systems that had "hands on keyboard" activity and quickly contain the threat.

How we did it better
In just two weeks, the Mandiant team of experts utilized award winning FireEye Threat Intelligence and technology to identify and contain malware to stop a ransomware attack in flight.

Result
The Mandiant team was able to identify the threat and stop the attacker before ransomware was deployed, helping the client prevent any impact to their customers and avoid damaging their brand.

Eradicating the Threat

Mandiant teams spend about 200,000 hours per year working on the most impactful breaches. Here's a high-level walkthrough of what this two-week engagement looked like:



MANDIANT

The Full Story

The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is serious and continues to grow as attackers become better funded and more sophisticated.

Among the groups the FBI has been tracking is a known threat actor that has been extorting dozens of US companies.

Recently, a FireEye Mandiant client was warned by the FBI as part of their victim notification program. The FBI observed that this attacker had hacked into the client and dumped administration credentials from key computers systems.

The client was informed that the attacker was likely to deploy ransomware in less than one week, or as early as 72 hours. They immediately activated their Incident Response Retainer with FireEye and called for assistance.

Within four hours, Mandiant consultants worked with the client to deploy an agent to 2,500 systems to begin investigating.

The Mandiant incident response team quickly identified Trickbot malware had been deployed on 100+ systems where the attacker was using PowerShell Empire as a backdoor, and ProcDump to dump passwords on multiple systems.

The Mandiant team immediately began working on acontainment plan. On day four, the Mandiant team executed the containment plan, where:

- TrickBot was quarantined,
- Command & Control (C2) infrastructure used by the attacker was blocked,
- Empire was removed.

Mandiant consultants continued to investigate and were able to identify victim zero and the initial point of entry. The team discovered that a vendor the client was using had been previously compromised. The attacker had used the vendor's email account to launch a targeted spear phishing attack using weaponized attachments.

While the ransomware attack was avoided, the insurance company was still concerned about whether there was any data theft and if there were reporting obligations under the breach notification laws.

The Mandiant team performed deep dive forensics on all systems that had been compromised and accessed. Mandiant leveraged the FireEye Labs Advanced Reverse Engineering (FLARE) team to reverse engineer the attacker malware to understand it's capabilities.

Mandiant determined there was no evidence of data theft and the victim concluded no public disclosure was required, The swift response of the Mandiant Services team helped prevent any impact to the clients customers and avoid any damage their brand.

Accomplished over a two-week engagement:

Day 1

The FBI warns the insurance company as part of their victim notification program.

Day 2

The insurance activates IR Retainer with FireEye. Within four hours, Mandiant and the victim deploy an endpoint agent to 2,500 systems and begin the investigation.

Day 3

Trickbot malware is identified on 100+ systems. Mandiant identified the attacker was using PowerShell begins working on containment plan.

Day 4

Execution of the containment plan. TrickBot is quarantined.

Day 7

Mandiant identified victim zero and initial point of entry.

Day 8-14

Mandiant conducted deep dive forensics on all compromised and accessed systems determined there was no evidence of data theft and the victim concluded no public disclosure was required.