CERT-EU

Memo

10/04/2019 - TLP:WHITE

A Cryptojacking campaign had disruptive impact

Reference: Memo [190410-1] - Version: 1.0
Keywords: Disruption, cryptojacking
Sources: publicly available information

Key Points

- The systems of a Japanese company were shutdown following a first-stage attack suspected to precede a cryptojacking campaign.
- This incident highlights the disruptive nature of cryptojacking attacks and their ability to affect victims' operations.
- In 2018, several cases of disruption caused by cryptojacking attacks were reported.

Summary

On April 6, Japanese media reported that Japanese eyeglass lens maker Hoya Corp was hit by a cyberattack at its key production base in Thailand in late February, leading to a partial shutdown of its factory lines for three days.

About 100 computers were infected with a credential harvesting malware, which the company believes was a first-stage attack in a suspected cryptojacking campaign.

Hoya was able to block the attackers' cryptojacking attempt after the credential-stealing malware put an abnormal load on a network server, which led to the quick discovery of the attack. Although the second stage infection was reportedly repelled, the initial attack slowed a key server down, hitting production and back-office processes. Workers were no longer able to use software to manage orders and production, with output slumping to around 40% of normal levels at two facilities. In addition to affecting the plant in Thailand, Hoya says the malware also affected its Japanese offices and invoice distribution. Even though Hoya still hadn't recovered from the attack by the end of March, it said in an official statement that the attack will have "little impact" on its long-term operations.

Comments

Cryptocurrency mining is a resource-intensive process of authenticating transactions in return for a cryptocurrency reward. While mining itself is legal, fraudulently compromising systems to do the work (aka cryptojacking) is not.

This incident highlights the potential disruptive nature of cryptojacking attacks and their ability to affect victims' operations, even if depicted as covert threats operating unbeknownst to their targets.

While cryptocurrency mining has typically been viewed as a nuisance, experts have recently seen several cases where mining has affected business operations, rendering some companies unable to operate for days and even weeks at a time. The tools employed for such nefarious activities have caused system and application crashes due to high CPU usage.

In early 2018, CrowdStrike cyber-security firm reported on sophisticated capabilities built into a cryptomining worm dubbed WannaMine. This tool leverages persistence mechanisms and propagation techniques similar to those used by nation-state actors. WannaMine employs "living off the land" techniques such as Windows Management Instrumentation (WMI) permanent event subscriptions as a persistence mechanism. It also propagates via the infamous EternalBlue exploit leveraged by WannaCry. In one case, a victim informed CrowdStrike that nearly 100 percent of its environment was rendered unusable due to CPU overutilization.

In November 2018, the Canada-based St Francis Xavier University also suffered major disruption from a crypto-mining campaign. The university purposefully disabled all network systems to halt the automated coin mining attack. The university stated they "had no choice but to deprive these hijackers further access by shutting down systems to understand the scope of the issue."

CERT-EU has observed continued attempts to install cryptojacking malware on the infrastructure of EU institutions, bodies and agencies since at least the first half of 2017. To our knowledge, none of them had had disruptive effects.

To avoid detection, actors performing cryptojacking activities will usually try to limit the CPU usage of the mining software on compromised hosts. However in order to maximize the potential gain of such activities, miners will work collaboratively, leaving footprints at the network level since they need to communicate with a mining pool, making them easier to detect using the right network monitoring strategies and technologies, as applied by CERT-EU.