OTORIO Prevents Crippling Cyberattack on a Global Industrial Company

OTORIO's Incident Response (IR) team was called to investigate suspicious activity within the network of one of its customers. The team was able to detect the threat - a Dridex-type ransomware, map all the infected assets and defuse the attack only days before it was set to be executed.

- The Customer: A Leading engineering company with over 30,000 endpoints
- The risk: A Dridex ransomware that infected 99% of the network
- The solution: OTORIO's Incident Response team identified the threat and removed it within 72 hours

THE CHALLENGE: A TICKING TIME BOMB

The attack was first noticed when the customer's IT team discovered a scheduled task on one of its computers, created by a user that was not supposed to be active. When OTORIO's IR team began investigating, it established that the attack was carried out by remote hackers who were continuously monitoring the network. Any attempt to take active measures against it could have resulted in scaring the attackers away, or worse - causing them to execute an irreversible attack. OTORIO's IR team had to work quickly and discreetly as it was evident that the attack can be executed at any time.

OTORIO was tasked with:

- Preventing the ransomware from being executed
- Preventing distribution of the attacker to the client's customers
- Removing the threat from the customer's network
- Minimizing reputational damage to the customer
- Provide root-cause analysis of the attack

Background

The customer is a leading global engineering company, with over 30,000 endpoints distributed globally. The company also maintains remote connections to clients' production sites across over 40 countries worldwide. In the summer of 2019, the company was targeted by sophisticated cyber-attackers, with live operators actively running a multi-stage ransomware attack. By the time OTORIO arrived on the scene, the client's network was 99% compromised, allowing the attackers to deploy a ransomware virus at any moment.

ISOLATING THE THREAT

OTORIO's IR team's first mission was to investigate the suspicious scheduled task, trying to extract any relevant information about its nature or source. After investigating the executable that the task was running, it was determined that the malware was of the Dridex[01] family.
A deeper investigation revealed that hundreds of stations were infected by malware, and that the attackers were using credentials with the highest privileges possible - such as domain administrator - to spread the malware. Time was critical as it was only a matter of days before the hackers could take control of all the stations in the network.

Working closely with the customer's IT and OT teams, OTORIO's IR team scanned the network in order to identify processes that were used throughout the company and flagging possible benign software that were being used maliciously. Together, they located the maliciously installed program used by the attackers. With the guidance and support of OTORIO's IR team, The customer created a situation room and assigned a taskforce to handle the incident consisting of IT employees, domain admins and CISOs from across the globe.

At the same time, OTORIO's Threat Intelligence and Research teams continued to examine the incident. Correlating the data they were able to gather with indicators that linked to previous Dridex attacks, the investigation led to solid connections between IP addresses that were communicating with the customer's network and IP addresses that are known to be used by Dridex.

FINDING PATIENT ZERO

Following the attack footprints, OTORIO's team was able to trace patient zero the first infected computer. This station belonged to one of the customer's employees who unknowingly, browsed a water-holed02 website that had a pop-up message claiming the user must update their browser to continue surfing. Once the employee opened the fake update file, a JavaScript downloader ran and executed the second stage of the attack - the Empire03 framework.

The attacker used both Dridex and the Empire Framework to propagate through the network, actively acquiring higher privilege users until finally getting hold of multiple domain controllers and a variety of different servers and endpoints. At this stage in past Dridex attacks, the group's next step would usually be to install BitPaymer - Dridex's associated ransomware.

TAKING BACK CONTROL

Once the threat was identified, and together with the customer's taskforce, OTORIO's IR team took steps to remove the threat and give the customer back control over its network. These steps included:

- Using the deployed security systems to feed Dridex identifiers into all systems and firewalls in order to block the attacker's communication with the malware.
- Blocking the exploit kit campaign and all its variants using new rules based on indicators that were collected and analyzed during the investigation.
- Creating a specialized cleanup script to remove any remains the attacker may have left behind in the network and initiated a full domain password reset for all users.

In the end, none of the stations on the network were encrypted. The attacker was blocked from the network which was then wiped clean of all traces of malware. Indicators of the attack were collected and implemented into newly-created rules and policies. The customer's security teams were briefed and the investigation and mitigation were concluded. The incident triggered a company-wide security assessment by OTORIO, which now works with the customer on strengthening its network defenses and processes.

[01] Dridex is a malware developed by a cybercrime group dubbed INDRIK SPIDER. Originally, Dridex was used as a banking trojan that would gather credentials in order to steal money from its targets. Over time, Dridex got more sophisticated and shifted its modus operandi towards the world of Ransomware. In its current versions, Dridex utilizes high privilege user credentials they acquire in order to install a custom written Ransomware either to critical assets or domain wide.
www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

[02] A watering hole attack refers to a method in which an attacker compromises a legitimate website in order to infect unsuspecting victims who browse the website. This watering hole attack was created with a known exploit kit that drops malware as a service for malware creators.

[03] Empire is an open source post-exploitation framework that offers secure communications between attacker and target. It allows the attacker to run different commands on the victim's network to gather information or perform actions without being detected.