Quarterly Report: Incident Response trends from Fall 2020

blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html

By David Liebenberg and Caitlin Huey.

For the sixth quarter in a row, Cisco Talos Incident Response (CTIR) observed ransomware dominating the threat landscape. However, for the first quarter since we began compiling these reports, no engagements that were closed out involved the ransomware Ryuk (though there were engagements that were kicked off this quarter involving Ryuk, but have yet to close). The top ransomware families observed were Maze and Sodinokibi, though barely more than any others, continuing a trend of "democratization" for ransomware families observed in last quarter's report, in which no one family was dominant. With Maze adversaries' recent announcement of retirement, the possibility remains that more ransomware groups will step up to fill the void, accelerating this trend.

Besides the drop in Ryuk, we saw a continuing decline in commodity trojans such as Trickbot and Emotet, as ransomware adversaries rely more on open-source tools, the Cobalt Strike framework, and a combination of various living-off-the-land tools and utilities, or "LoLBins."

The lack of Ryuk is somewhat surprising given recent reports from the U.S. government that indicate adversaries are looking to target health care organizations with Ryuk. Part of this could be related to the timing of these incidents, which occurred toward the end of Q3 2020. We do note that there were several Ryuk cases opened toward the end of the quarter which have yet to close, including one affecting a health care company. CTIR also observed a general increase in engagements involving attacks against health care organizations toward the end of the quarter, though they mostly involved other malware families, such as the Vatet loader, which is known to target this industry. For more information, you can check out the full report summary here.

Targeting

Actors targeted a broad range of verticals, including agriculture, food and beverage, health care, education, energy and utilities, industrial distribution, law enforcement, local government, manufacturing, and technology. The top targeted vertical was manufacturing, a continuation of last quarter. However, as mentioned above, there was a spike in attacks against health care organizations, and some of these engagements have yet to close out. In counting both engagements that were opened and closed out this quarter, health care and manufacturing sectors were tied as being the most affected sectors this quarter. Looking ahead, it appears that adversaries will continue to target the health care industry with ransomware and other types of attacks given their security postures and incentives to pay, especially given the situation with the COVID-19 pandemic, which threat actors have been more than willing to capitalize on.

Threats

Ransomware continued to comprise the majority of threats CTIR observed. In a continuation from last quarter, no one ransomware family was dominant. Furthermore, there were no engagements that closed out involving Ryuk (though there was one engagement which opened this quarter in which Ryuk is suspected). In the past, Ryuk was much more prominent. In a continuation from the last several quarters, the majority of ransomware attacks were not observed in conjunction with commodity trojan infections, instead relying on open source tools, Cobalt Strike, and living-off-the-land utilities.

For example, a U.S. manufacturing company was targeted with a phishing email that contained a malicious ZIP file. Once downloaded and opened, an adversary carried out multiple malicious actions, including connection to a malicious IP address, account enumeration, and execution of encoded PowerShell. The adversary attempted to deploy a malicious ransomware file called “hnt.dll,” which CTIR identified as a Maze ransomware variant, although the mutexes were slightly different from previous Maze mutexes which could have indicated a new strain. The customer had Cisco AMP for Endpoints running which successfully quarantined the malicious DLL. The adversary used several commercially available and open source tools for malicious means, including PowerShell to execute encoded commands; Cobalt Strike, including executing "Invoke-DACheck", an Aggressor script that checks to see if the current user is a domain administrator and "Norton Power Eraser," a scanning tool that irreversibly removes forensic artifacts vital to the investigation from systems. CTIR investigated possible indicators of data exfiltration from six hosts to a malicious C2 IP address, including large amounts of packets exchanged over the observed time period. However, they found no evidence of data staging or any specific indicators that data was exfiltrated from the environment.

It is worth highlighting that the Maze ransomware group announced they have officially closed down their ransomware operation and claimed they will no longer be leaking new company data on their site. While the validity of Maze's claim is still unknown at this time, it is possible that lower-tiered ransomware groups may attempt to compete within this threat landscape now that a very high-profile group has announced its departure.

CTIR has observed a spike in Vatet loader/ransomware engagements this quarter affecting health care entities. Vatet is known to be used by adversary groups to specifically target health care organizations. In one open incident response engagement involving a U.S. medical center infected with Vatet, CTIR identified the likely infection vector as an IcedID phishing email with a ZIP attachment that used steganography for loading commands to the Vatet loader itself. From there, IcedID downloaded and ran Vatet, which started Cobalt Strike activity and eventually launched and executed the Defray777 ransomware.

Other observed threats this quarter included business email compromise (BEC), cryptocurrency mining, web shells, brute-force attacks, exploit attempts and information stealers.

Initial vectors

For the majority of engagements, definitively identifying an initial vector was difficult due to shortfalls in logging. However, in engagements in which the initial vector could be identified, or reasonably assumed, phishing remained the top infection vector for the sixth quarter in a row. Besides email, other initial vectors that CTIR has observed this quarter include drive-by downloads, RDP brute-force attacks, and exploitation of various vulnerabilities, including Microsoft Exchange (CVE-2020-0688), SaltStack Salt (CVE-2020-116511 and CVE-2020-11652), and Oracle WebLogic (CVE-2020-14882).

Top-observed MITRE ATT&CK techniques

Below is a list of the most common MITRE ATT&CK techniques observed in this quarter's IR engagements. Given that some techniques can fall under multiple categories, we grouped them under the most relevant category in which they were leveraged. This represents what CTIR observed most frequently and is not intended to be exhaustive.

Key Findings:

- The usage of Cobalt Strike decreased by half. However, we do note that there are many open engagements that rely on Cobalt Strike for post-exploitation.
- We observed a robust combination of various living-off-the-land tools and utilities, or “LoLBins.” This is a continuation of a trend seen in late 2019 where actors combine fileless malware and legitimate cloud services to improve chances of staying undetected.
- Encoded PowerShell commands account for several execution techniques, illustrating the need for policies to limit unprivileged users from using PowerShell or CMD applications.
- Leveraging valid accounts is the most observed technique used for lateral movement this quarter. RDP usage for lateral movement decreased this quarter. However, we did see brute-force attacks almost double this quarter.

ATT&CK techniques

- **Initial Access (TA0027), T1078 Valid Accounts:** Use valid compromised credentials in BEC scam.
- **Persistence (TA0028), T1543 Create or Modify System Process:** Install a cryptomining application service on the system to maintain persistence on the server.
- **Execution (TA0041), T1059.001 Command and Scripting Interpreter: PowerShell:** Executes PowerShell code to retrieve information about the client's Active Directory environment.
- **Discovery (TA0007), T1082 System Information Discovery:** Used Process Hacker to identify infected machine’s OS information.
- **Credential Access (TA0006), T1003 OS Credential Dumping:** Use tools such as Mimikatz to compromise credentials in the environment.
- **Privilege Escalation (TA0029), T1484 Group Policy Modification:** Force group policy update that creates service to execute ransomware.
- **Lateral Movement (TA0008), T1021.001 Remote Desktop Protocol:** Adversary connects to the system using RDP with valid credentials.
- **Collection (TA0035), T1560.001 Archive Collected Data:** Archive via Utility: One binary was capable of extracting system information and files that are subsequently placed within a tar archive, which is compressed with bzip2.
- **Defense Evasion (TA0030), T1070 Indicator Removal on Host:** Remove files and artifacts from an infected machine.
- **Command and control (TA0011), T1132.001 Data Encoding: Standard Encoding:** Use Base64 to encode C2 communication.
- **Exfiltration (TA0010), T1567 Exfiltration Over Web Service:** Data exfiltration was performed with the usage of FirefoxSend.
- **Impact (TA0034), T1486 Data Encrypted for Impact:** Deploy Maze ransomware.

- **Software, Cobalt Strike:** Execution of “Invoke-DACheck," a Cobalt Strike Aggressor Script to check if the current user is a domain administrator.