Quarterly Report: Incident Response trends from Winter 2020-21

blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html

By David Liebenberg and Caitlin Huey.

For the seventh quarter in a row, Cisco Talos Incident Response (CTIR) observed ransomware dominating the threat landscape. The top variants were Ryuk and Vatet, which is notable given the absence of Ryuk last quarter. We also observed variants of Egregor and WastedLocker continuing to target organizations across the globe.

Unlike last quarter, however, these ransomware attacks overwhelmingly relied on phishes delivering commodity trojan maldocs, such as Zloader, BazarLoader and IcedID. Nearly 70 percent of ransomware attacks relied on commodity trojans this quarter. Adversaries also employ commercially available tools such as Cobalt Strike, open-source post-exploitation tools like Bloodhound, and native tools on the victim's system, such as PowerShell. For a broader breakdown of these trends, check out our summary here.

CTIR engaged in several incident response engagements in which organizations unknowingly downloaded trojanized updates to the widely deployed SolarWinds' Orion software. Only one of these engagements involved post-compromise activity.

Looking forward, Microsoft recently announced four vulnerabilities in Exchange Server and revealed that a threat actor named Hafnium had been exploiting these vulnerabilities to drop web shells, targeting an array of organizations. Soon other threat actors began leveraging these exploits as well, ranging from APTs to cryptominer groups, with affected organizations estimated in the tens of thousands. CTIR has been responding to a growing number of incidents involving the Microsoft Exchange vulnerabilities.

Targeting

Actors targeted a broad range of verticals, including business management, construction, education, energy and utilities, entertainment, financial, government, health care, industrial distribution, legal, manufacturing and technology. Adversaries most often targeted health care, as we anticipated last quarter given the spate of ransomware attacks targeting health care organizations. It is worth noting there has been an increase in incidents involving Vatet malware, which has been known to target health care organizations. CTIR identified a potential pattern in which regional hospitals associated with a hospital in a given state is initially attacked and may serve as follow-on targets, particularly if they have active VPN connections to the affected organization. There are many reasons why actors are continuing to target the health care industry, including the COVID-19 pandemic incentivizing victims to pay to restore services as quickly as possible.

Threats

Ransomware continued to comprise the majority of threats CTIR observed. As opposed to last quarter, which marked an absence of commodity trojans, the majority of these attacks relied on commodity trojan maldoc phishes as an infection vector. Adversaries are continuing to use commercially available tools as well: Cobalt Strike was observed in half of all ransomware attacks this quarter. There were also numerous ransomware engagements that leveraged open-source reconnaissance tools such as ADFind, ADRecon and Bloodhound. Windows utilities were common, as well. For example, PowerShell was observed in nearly 65 percent of all ransomware attacks, while PsExec usage was observed in more than 30 percent. Other observed tools included dual-use tools such as TightVNC and CCleaner and compression tools such as 7-Zip and WinRAR.

For example, in an incident response engagement involving an education organization in the U.S., the target was initially infected via a phish containing a commodity trojan. In this case, the phish contained a malicious Microsoft Excel attachment that executed the commodity trojan Zloader when if the user enabled macros (CTIR assessed that this Zloader variant was customized for the target based on the fact that its file hash had not been previously observed). An employee at this organization opened the attachment and forwarded it to a colleague. The adversary then pivoted in the environment, leveraging the Group Policy replication mechanism in Windows Active Directory to distribute Ryuk and using PsExec to move laterally and execute remote commands, in line with previous Ryuk behavior. The adversaries obtained domain administrator (DA) credentials and, besides encrypting systems on the network, also wiped backup indexes. More than 1,000 endpoints were encrypted, causing significant damage to the organization, affecting Active Directory, DHCP, DNS and anti-virus software.

In December 2020, Cisco Talos became aware of a sophisticated supply-chain attack in which adversaries gained access to victims' networks via trojanized updates to SolarWinds' Orion software. This attack targeted numerous large enterprises and U.S. government agencies. CTIR engaged in several incident responses in which organizations had unknowingly installed the compromised update. Only one of these engagements involved post-compromise activity, such as malicious PowerUP PowerShell execution. PowerUP appears to be part of PowerSploit, and is a collection of PowerShell modules that are used to assist red teaming activities. While the PowerUP-like PowerShell script did not execute anything at this time, it appeared to be set up as a wrapper or utility, possibly for additional code to be funneled into. CTIR continues to monitor for activity related to the SolarWinds compromise.

Beginning in March, CTIR has been responding to a growing number of incidents involving the Microsoft Exchange vulnerabilities. In one engagement, a customer in the payment processor/technology sector saw no indication that CVE-2021-26855 was exploited. They did, however, observe scanning behavior from a known IP address linked to these attacks, which sent packets to a particular Exchange server beginning February 28. In another engagement, a customer in the healthcare sector saw a CVE-2021-26855 exploit, though we have yet to determine if the activity was just limited to scanning at this time. In one incident response engagement affecting an organization in Germany, we saw a slight deviation from the post-exploitation activity in the aforementioned engagements. The activity started in much the same way, with the adversary installing web shells on the victim environment. However, prior to the deployment of web shells, the customer saw the Domain Admin account password was reset via the presence of the "Password last set" attribute in Active Directory (AD).

Initial vectors

It was difficult to identify an initial infection vector in many engagements last quarter 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 seventh quarter in a row. The vast majority of these were comprised of maldoc phishes as mentioned above. However, there were also engagements involving business email compromise, such as when an employee at an entertainment company received a phish with a spoofed Microsoft Online login page, after which the adversary attempted to authenticate to their Office 365 account from multiple locations. The adversary successfully authenticated and bypassed MFA through use of a legacy application, highlighting the need to disable legacy protocols.

CTIR encourages all organizations to save their logs to make any potential incident response engagements more efficient and effective.

Other notable initial vectors included exploitation of public-facing applications, such as an education organization that had their F5 Load Balancer exploited via CVE-2020-5902 — a remote code execution vulnerability in f5 — in the course of a DDoS attack. There were also several instances of exploitation of a vulnerability in Telerik UI, tracked as CVE-2019-18935. Talos first saw an increase in actors exploiting Telerik UI in summer 2020 — a trend that continues today.

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:

- Phishing with malicious attachments and links accounted for a larger number of the initial access techniques this quarter compared to the previous quarter.
- We observed a variety of execution methods using native Windows utilities, such as "rundll32.exe" and "msiexec.exe". The use of these utilities may avoid triggering security tools due to them being commonly used in daily operations.
- Engagements involving cryptocurrency mining malware continue to be very low. However, the number of ransomware engagements nearly doubled this quarter.
- Leveraging valid accounts is the most observed lateral movement technique this quarter. RDP usage and remote access services, such as TightVNC, for lateral movement, increased this quarter.

- **Initial Access (TA0027) — T1078 Valid Accounts:** Credentials for a compromised account were leveraged by the adversary
- **Persistence (TA0028) — T1053 Scheduled Task/Job:** Adversaries create a scheduled task to run malicious executable every hour
- **Execution (TA0041) — T1204.002 User Execution:** Malicious File: Adversary sent phishing emails that contained a malware attachment when clicked, would deploy additional tools to harvest credentials
- **Discovery (TA0007) — T1482 Domain Trust Discovery:** Use AdFind (“adfind.bat”) to query for all users, computers, groups, and trusts
- **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:** 7-Zip used to compress a file containing dumped LSASS credentials
- **Defense Evasion (TA0030) — T1070 Indicator Removal on Host:** Remove files and artifacts from the 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:** Exfiltrated data was located on a file sharing site
- **Impact (TA0034) — T1486 Data Encrypted for Impact:** Deploy Ryuk ransomware