Quarterly report: Incident Response trends in Summer 2020

blog.talosintelligence.com/2020/06/CTIR-trends-q3-2020.html

By David Liebenberg and Caitlin Huey.

For the fourth quarter in a row, Ryuk dominated the threat landscape in incident response. As we mentioned in last quarter's report, Ryuk has shifted from relying on commodity trojans to using living-off-the-land tools. This has led to a decrease in observations of attacks

leveraging commodity trojans. Email remained the top infection vector, though we observe increased compromises of remote desktop services (RDS) as well as Citrix devices and Pulse VPN. One of the more interesting trends this quarter was the role of the COVID-19 pandemic. Interestingly, we did not observe any engagements in which COVID-19 was used in an attack. However, CTIR has observed the pandemic impacting organizations, affecting their ability to respond and contain cybersecurity incidents.

For additional information, you can also check out our full summary here.

Targeting

A wide variety of verticals were once again targeted, including energy and utilities, financial services, government, health care, industrial distribution, manufacturing, retail, technology, telecommunications, and transportation. The top targeted verticals were health care and technology, a change from last quarter when the top targeted verticals were financial services and government.

Threats

Ransomware continued to comprise the majority of threats CTIR observed. As mentioned above, contrary to previous quarters, CTIR is observing fewer engagements in which Emotet and Trickbot function as the initial dropper for Ryuk. This is one reason why we observed far fewer attacks leveraging commodity trojans this quarter. As mentioned last quarter, Ryuk attacks evolved in other ways as well, leveraging encoded PowerShell commands to download the initial payload, disable security/AV tools, stop backups, and scan the entire network and provide an output of online vs. offline hosts. Ryuk adversaries are using more Windows Management Instrumentation (WMI) and BitsAdmin to deploy the malware in addition to PsExec.

For example, a government organization had thousands of systems encrypted with Ryuk ransomware, affecting nearly 2,000 systems and critical services. There was no evidence of any presence of commodity trojans during the attack. The adversaries compromised a domain administrator account by recovering the password stored in a Group Policy. The adversaries attempted to prevent file restoration by using bcdedit to alter boot configuration data to prevent system recovery, deleted Windows shadow copies, and used vssadmin to remove system restore points. The adversaries then tried to expand the number of affected hosts by granting full permission for all users for all files on all mounted disk drives with icacls.exe. They also sent Wake-On-Lan magic packets to wake shut-down hosts for encryption.

The adversaries used PowerShell to disable real-time monitoring malware protection and a PowerShell cmdlet code “Get-DataInfo.ps1” to scan the network and provide an output of live or dead hosts in text files. The adversaries used the command-line tool BitsAdmin, as well as

WMIC and PsExec with privileged account credentials to copy Ryuk to additional hosts.

In another engagement where CTIR identified a Ryuk infection, the initial compromise was performed with a phishing email that contained an encrypted Microsoft Word document. The malicious code had been embedded in a chess game written in VBA, and once the document was opened, it created a VBS file and executed it through PowerShell. The VBS file downloaded and executed the malicious payload identified as Detplock, a remote access trojan (RAT).

CTIR continued to observe ransomware actors exfiltrating sensitive data as another lever to further compel victims to pay the ransom. This is a continuation of a trend since Winter 2019.

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. CTIR also observed several instances in which adversaries leveraged brute-force attacks against a victim organization's RDS. These types of attacks may be related to the increased threat surface due to remote work stemming from COVID-19 as well as an increase in Phobos ransomware attacks, which typically leverage compromised RDS connections as an initial vector. CTIR also continued to observe multiple compromises of Citrix Application Discovery Controller and Citrix Gateway (CVE-2019-19781) and Pulse Secure VPN (CVE-2019-11510).

COVID-19

Somewhat surprisingly, CTIR has not observed any engagements in which COVID-19 was leveraged, despite the fact that threat actors have been increasingly using COVID-19-related information as lures in phishing and malspam attacks. However, CTIR has observed the pandemic impacting organizations, particularly in the health care industry, affecting their ability to respond and contain cybersecurity incidents since pre-COVID-19 incident response planning did not account for a pandemic occurring along with a parallel cybersecurity incident. Limitations in travel, personnel, and budget all contributed to increased difficulty mitigating incidents, which was observed across multiple incident response engagements in Summer 2020. Additionally, CTIR has observed organizations updating their internal IR and business continuity planning in response to the pandemic. This illustrates the importance of developing a robust incident response plan and maintaining flexibility to make adjustments in response to major global events. Despite a lack of COVID-19-themed campaigns, the pandemic has still increased the threat surface, with an obvious uptick in both RDS and VPN services due to increased remote work. Beyond providing new avenues for adversaries to target, CTIR has also responded by working with victim organizations in identifying the new network "baseline" caused by these changes.