Quarterly Report: Incident Response trends in Summer 2020

By Jonathan Munshaw

Published: 2020-09-01 · Archived: 2026-04-05 23:04:51 UTC

Quarterly Report: Incident Response trends in Summer 2020

Tuesday, September 1, 2020 11:00

By David Liebenberg and Caitlin Huey.

For the fifth quarter in a row, Cisco Talos Incident Response (CTIR) observed ransomware dominating the threat landscape. Infections involved a wide variety of malware families including Ryuk, Maze, LockBit, and Netwalker, among others. In a continuation of trends observed in last quarter's report, these ransomware attacks have relied much less on commodity trojans such as Emotet and Trickbot. Interestingly, 66 percent of all ransomware attacks this quarter involved red-teaming framework Cobalt Strike, suggesting that ransomware actors are increasingly relying on the tool as they abandon commodity trojans. We continued to see ransomware actors engage in data exfiltration and even observed the new cartel formed by Maze and other ransomware operations in action.

For a more complete breakdown with more information, you can check out the full report summary here.

Targeting

Actors targeted a broad range of verticals, including manufacturing, education, construction, facility services, food and beverage, energy and utilities, financial services, healthcare, industrial distribution, real estate, technology, and telecommunications. The top targeted vertical was manufacturing, a change from last quarter when the top targeted industries were health care and technology.

Threats

Ransomware continued to comprise the majority of threats CTIR observed. In a break from previous quarters, no one ransomware family was dominant this quarter. In the past, Ryuk was much more prominent. In a continuation from last quarter, the majority of ransomware attacks were not observed in conjunction with commodity trojan infections. Part of the reason for this could be an increase in the use of Cobalt Strike. Sixty-six percent of ransomware engagements this quarter involved the use of Cobalt Strike.

For example, an engineering company was infected with LockBit ransomware. The adversaries used Cobalt Strike for command and control (C2) purposes, with CTIR observing traffic to a Cobalt Strike C2 every six minutes. The adversaries also used an open source post-compromise tool called “CrackMapExecWin,” which is designed to automate assessments of large Active Directory networks. This tool was executed on different network ranges in the victim environment to have all the systems on those networks perform a forced Group Policy update. The Group Policy included an XML file which set up a service that executed the ransomware from a client's compromised server. The adversaries created user accounts on compromised hosts and established remote desktop connections to targeted servers using their accounts. They also cleared event logs as a means of evasion. The adversaries also deployed TeamViewer, frequently used by actors to exfiltrate information.

Interestingly, data from this attack was posted on a site Maze uses to publish their stolen data, reflecting the fact that LockBit, along with other ransomware operations engaging in these ransomware/data theft hybrid attacks, have joined together to share resources and data.

There were also Remote Access Trojans (RATs), such as a financial services organization that received a targeted phishing attempt with a maldoc containing a JavaScript RAT submitted via the organization’s ticket-handling system and web shells, including a manufacturing organization that had their Telerik server exploited, after which the adversary then deployed APSX .NET web shells.

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 an increase in actors exploiting servers running the Telerik UI framework. The latest vulnerability (CVE-2019-18935) allows for remote code execution. It is particularly dangerous because there are many ASP.NET applications that may run older versions of Telerik UI that leaves victims exposed, even if the applications are patched themselves. In one instance, an adversary targeted a tech company via a server running Telerik UI. The adversary then ran “cmd.exe” and executed malicious commands culminating in a ransomware attack.

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

- Phishes with malicious attachments were the top infection vector.
- Several open-source tools, such as Mimikatz; Windows utilities, such as PsExec; and red-team tools such as Cobalt Strike were commonly observed this quarter.
- Encoded PowerShell commands account for several execution techniques seen, illustrating the need for policies to limit unprivileged users from using PowerShell or CMD applications.
- Remote Desktop Protocol (RDP) was a key technique used for lateral movement. This is a continuation of a trend seen last quarter around attacks against victim organization’s remote desktop services (RDS), possibly related to the increased threat surface due to remote work stemming from COVID-19.

ATT&CK techniques

- **T1566.001 Phishing: Spear-phishing Attachment** — Maldoc downloads Qakbot after macros are enabled.
- **T1053 Scheduled Task/Job** — Executables create scheduled tasks on the system to run as the user account.
- **T1059.001 Command and Scripting Interpreter: PowerShell** — Executes PowerShell code to retrieve information about the client's Active Directory environment.
- **T1021.001 Remote Desktop Protocol** — Adversary connects to the system using RDP with valid credentials.
- **T1070 Indicator Removal on Host** — Remove files and artifacts from the infected machines.
- **T1132.001 Data Encoding: Standard Encoding** — Use base64 to encode C2 communications.
- **T1486 Data Encrypted for Impact** — Deploy Netwalker ransomware.
- **Software: Cobalt Strike** — Qakbot associated IP addresses in "CLOSE_WAIT" status to a known Cobalt Strike beacon IP.
