Quarterly Report: Incident Response Trends in Q1 2023

By Caitlin Huey

WEDNESDAY, APRIL 26, 2023 08:04

TALOS IR TRENDS

Web shell usage spikes in Q1 compared to previous quarters, correlating with higher instances of exploitation of public-facing applications.

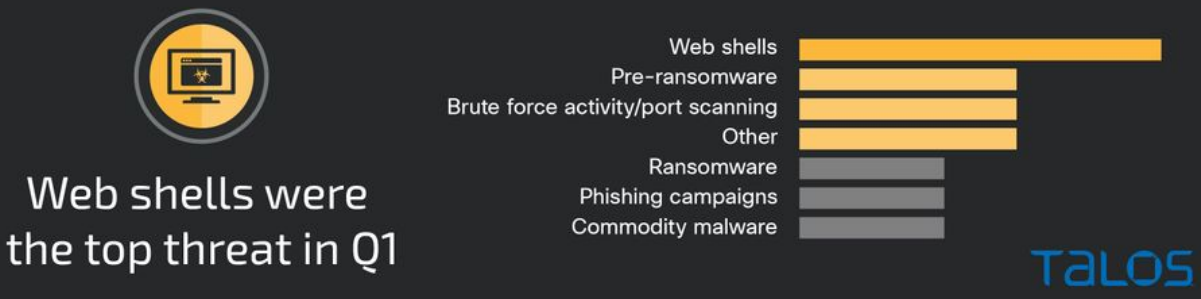
In a novel increase compared to previous quarters, Cisco Talos Incident Response (Talos IR) reports that web shells were the most-observed threat in the first quarter of 2023, comprising nearly a fourth of the incidents Talos IR engaged in. The functionality of these web shells and the specific vulnerabilities and weaknesses in the platforms they targeted varied. Although each web shell had its own sets of basic functions, when there were multiple web shells present in a single engagement, threat actors chained them together to provide a more flexible toolkit for spreading access across the network. This demonstrates the skills actors have in combining multiple means of accesses and tools and increases the liklihood that they will be able to deploy additional malware or obtain sensitive and private information.

Download the one-page overview here

Ransomware made up a smaller portion of threats observed this quarter than in the past, from 20% to around 10%. Given that Talos IR observed a recent surge of ransomware incidents at the end of the quarter that did not close off, this decrease does not necessarily signify a decline in general ransomware activity as much as it is a reflection of activity seen against Talos IR's customer base. However, ransomware and pre-ransomware incidents combined made up more than 20 percent of threats observed. While it can be difficult to determine what constitutes a pre-ransomware attack if ransomware never executes and encryption does not take place, many of the pre-ransomware engagements featured activity associated with prominent ransomware groups, such as Vice Society. We note that in this quarter, particularly in an aforementioned Vice Society engagement, swift action from defenders at victim organizations as well as Talos IR helped mitigate malicious activity before encryption could occur.

This quarter also featured previously seen commodity loaders, such as Qakbot. In engagements this quarter, Qakbot leveraged malicious OneNote documents, consistent with an uptick in various malware distributing weaponized Microsoft Office OneNote attachments. This is evidence of an ongoing trend of threat actors experimenting with file types that do not rely on macros to deliver malicious payloads following Microsoft's move to start disabling macros by default in its applications in July 2022.

In 45 percent of engagements, attackers exploited public-facing applications to establish initial access, a significant increase from 15 percent the previous quarter. In many of these engagements, web shell usage contributed to this uptick where adversaries were attempting to compromise web-based servers exposed to the internet.



Targeting

Health care and public health was the most targeted vertical this quarter, closely followed by the retail and trade, real estate and food services/accommodation sectors, including hospitality.

Web shell usage spike, featuring activity from FIN13

Since January 2023, Talos IR observed an increase in web shell usage from 6% of all threats last quarter to now comprising nearly 25% of all threats. Web shells are malicious scripts that enable threat actors to compromise web-based servers exposed to the internet. This quarter, Talos observed threat actors using publicly available or modified web shells coded in various languages, including PHP, ASP.NET and Perl. After leveraging web shells to establish a foothold and gain persistent access to a system, adversaries remotely executed arbitrary code or commands, moved laterally within the network, or delivered additional malicious payloads. In many of these web shell incidents, adversaries relied heavily on web shell code sourced from publicly available GitHub repositories. This finding is also in line with a trend observed from Talos IR engagements from July to September 2022 (Q3 2022), where adversaries used a variety of

open-source tools and scripts hosted on GitHub repositories to support operations across multiple stages of the attack lifecycle.

In one cluster of web shell activity, Talos observed targeting patterns and tactics, techniques and procedures (TTPs) potentially associated with the FIN13 cybercriminal threat actor, a significant finding in Talos IR engagements given FIN13's targeted behavior. The web shells with known FIN13 TTPs have varying levels of functionality which include allowing queries to Microsoft SQL (MS-SQL) instances, creating reverse shell connection(s) to external IP addresses, and executing PHP scripts which can be used as a proxy to connect to other services. Consistent with public reporting on FIN13, Talos IR observed a PHP-based web shell ("404.php") that took an IP or DNS entry and a port and attempted to create a proxy connection. The second web shell ("ms3.aspx") was Windows-based and allowed SQL connections to an internal server and, if successful, results would be rendered in the browser. The third was another PHP-based web shell ("re.php") that conducted port scans and created an outbound socket to respond/exfiltrate data to the attacker. This specific web shell contained a hardcoded IP address which resolved to cloud service provider DigitalOcean. The final web shell ("tx.asp") was a Windows-based web shell that used "wscript.shell" and exec() to run commands rendered to the screen via an HTML document. While each web shell on its own had basic functionality, by chaining them together, the actor created a flexible toolkit for spreading their access across the network, while providing a proxy for exfiltrating sensitive data.

While the exact reason for this quarter's increased appearance of web shells is unknown, their recent increased popularity may potentially be related to the ease of obtaining their code through open-source repositories. The availability of and easy access to open-source web shell code, paired with systems that may be publicly exposed or have poorly managed patching, make the use of web shells a lucrative option.

Ransomware

Ransomware made up a much smaller portion of threats this quarter, from 20% of threats to 10%. Looking ahead, there was a recent spike in ransomware engagements which we expect to level out again next quarter. Combined, ransomware and pre-ransomware incidents made up over 20 percent of threats observed.

In a Phobos ransomware engagement, a threat that Talos IR has responded to since 2020, the initial access likely involved remote desktop protocol (RDP). The adversary deployed a file named "mimidrv.sys," which is a signed Windows kernel mode software driver meant to be used with the Mimikatz executable. Talos IR also identified seven startup items that included downloading the ransomware executable, "Fast.exe." This is a common persistence technique that followed activity where the adversary made modifications to the registry on the customer's Amazon Relational Database Service (RDS) server. Upon encryption, attackers encrypted the files, appending them with the ".faust" extension and dropped a ransom note on the targeted systems.

This quarter also featured the Daixin ransomware, a newer ransomware-as-a-service (RaaS) family that Talos IR had never seen before in an engagement. Daixin, which first emerged in June 2022, typically involves affiliates gaining access to victim systems through virtual private networks (VPN) servers or by exploiting unpatched vulnerabilities, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA). In a Daixin ransomware engagement, the affiliate modified registry values, mapped network shares, and ran randomly named BAT files as services on the system. Talos IR also identified the Impacket toolset, a collection of Python classes for working with different network protocols, and a PowerShell script loading a Cobalt Strike payload which subsequently launched a Cobalt Strike shellcode listening on port 4444.

We assess that the recent law enforcement efforts to disrupt ransomware actors will create space for new groups to emerge, consistent with a pattern that has been ongoing for years. In January 2023, the U.S. Department of Justice announced a months-long disruption campaign against the Hive ransomware group. The FBI, along with foreign law enforcement partners, seized Hive servers after entering its networks and capturing keys to decrypt its software, effectively disrupting operations. We have not observed Hive ransomware in Talos IR engagements since August 2022, a likely indication that Hive operations have ceased while former members possibly look to join other groups or rebrand under new names.

Malicious OneNote documents continue to be leveraged in engagements this quarter

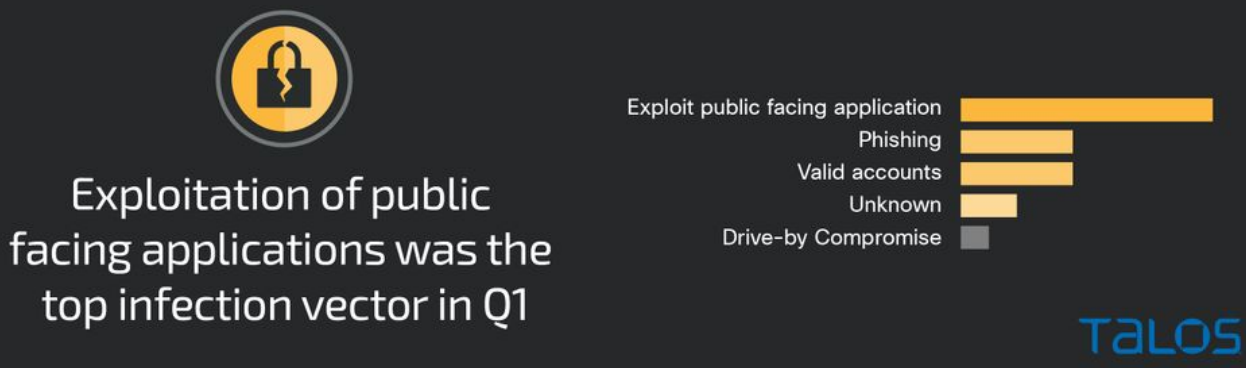
The Qakbot commodity loader was observed across engagements this quarter leveraging ZIP files containing malicious OneNote documents, consistent with endpoint telemetry and public reporting on threats leveraging OneNote documents in phishing emails starting at the end of 2022 and early 2023. In one Qakbot engagement, a ZIP file ("Inv_02_02_#3.zip") was detected as Qakbot and contained a malicious OneNote document which attempted to lure a user to click “open” containing a malicious embedded URL.

While Talos IR did not respond to any Emotet incidents this quarter, Emotet reemerged in March 2023, resuming its spam operations after a months-long hiatus. In a relatively short period, Emotet modified its infection chain several times to maximize the likelihood of successfully infecting victims. By mid-March, Emotet had switched to distributing malicious OneNote documents, highlighting the ways in which threat actors will continue to identify and quickly implement updated delivery methods to infect victims.

Initial vectors

This quarter featured 45 percent of engagements where attackers exploited public-facing applications to establish initial access, a significant increase from 15 percent the previous quarter. In many of these engagements, web shell usage contributed to this uptick where

adversaries were attempting to compromise web-based servers exposed to the internet. Valid accounts and/or accounts with weak passwords or single-factor authentication also helped facilitate initial access where an adversary was leveraging compromised credentials.



Several known vulnerabilities contributed to adversaries gaining initial access via exploiting public-facing applications. In one incident, Talos IR identified activity consistent with exploitation of the WordPress vulnerability, tracked as CVE-2021-24867, in AccessPress Plugin and Theme. As a result, Talos IR identified approximately 20 different web shells and/or website defacements, likely from multiple threat actors identifying and exploiting this older flaw.

In another web shell engagement, Talos IR identified a vulnerable version of Magento (Adobe Commerce) version 2.4.2 that was operating in the Kubernetes deployment at the time of exploitation. Talos IR identified a total of nine known vulnerabilities for this version of the software, not including extensions. Talos IR recommends upgrading all instances of Magento to the latest available version, and routinely checking for vulnerable outdated extension versions that need patching or removed completely to reduce the available attack surface.

Security weaknesses

The lack of multi-factor authentication (MFA) remains one of the biggest impediments for enterprise security. Nearly 30 percent of engagements involved organizations that either had no MFA or only had it enabled on a handful of accounts and critical services. Talos IR frequently observes ransomware and phishing incidents that could have been prevented if MFA had been properly enabled on critical services, such as endpoint detection response (EDR) solutions or VPNs. To help minimize initial access vectors, Talos IR recommends disabling VPN access for all accounts that are not using MFA.

The increase in web shell engagements highlights the need for more vigilance in helping to prevent web shells. Talos provides the following recommendations:

- Routinely update and patch all software and operating systems to identify and remediate vulnerabilities or misconfigurations in web applications and web servers.
- In addition to patching, perform general system hardening, including removing services or protocols where they are unnecessary and being aware of all systems exposed directly to the internet.
- Disable unnecessary php functions in your “php.ini”, such as eval(), exec(), peopen(), proc_open() and passthru().
- Frequently audit and review logs from web servers for unusual or anomalous activity.

Top-observed MITRE ATT&CK techniques

The table below represents the MITRE ATT&CK techniques observed in this quarter’s Talos IR engagements. Given that some techniques can fall under multiple tactics, we grouped them under the most relevant tactic in which they were leveraged. Please note, this is not an exhaustive list.

Key findings from the MITRE ATT&CK framework include:

- Exploitation of public-facing applications was the top observed initial access technique, with the increased web shell activity likely contributing to this significant observation.
- PowerShell is routinely used by adversaries to support a multitude of threats. We continued to observe high usage of PowerShell, in addition to a number of other scripting languages, including Python, Unix shell, and Windows command shell, which enabled web shell execution.
- The open source red-teaming security toolkit Mimikatz was used to support nearly 60 percent of ransomware and pre-ransomware engagements this quarter. Consistently observed across previous quarters, Mimikatz is a widely used post-exploitation tool used to steal login IDs, passwords, and authentication tokens from compromised Windows systems.

Tactic	Technique	Example
Initial Access (TA0001)	T1190 Exploit Public-Facing Application	Attackers successfully exploited a vulnerable application that was publicly exposed to the internet
Reconnaissance (TA0043)	T1592 Gather Victim Host Information	Text file contains details about host
Persistence (TA0003)	T1505.003 Server Software Component: Web Shell	Adversaries deployed web shells against web-based servers

Execution (TA0002)	T1059.001 Command and Scripting Interpreter: PowerShell	Executes PowerShell code to retrieve information about the client's Active Directory environment
Discovery (TA0007)	T1046 Network Service Scanning	Use a network or port scanner utility
Credential Access (TA0006)	T1003 OS Credential Dumping	Deploy Mimikatz and publicly available password lookup utilities
Privilege Escalation (TA0004)	1484 Domain Policy Modification	Modify GPOs to execute malicious files
Lateral Movement (TA0008)	T1021.001 Remote Desktop Protocol	Adversary made attempts to move laterally using Windows Remote Desktop
Defense Evasion (TA0005)	T1027 Obfuscated Files or Information	Use base64-encoded PowerShell scripts
Command and Control (TA0011)	T1105 Ingress Tool Transfer	Adversaries transfer/download tools from an external system
Impact (TA0040)	T1486 Data Encrypted for Impact	Deploy Hive ransomware and encrypt critical systems
Exfiltration (TA0010)	T1567 Exfiltration Over Web Service	Use legitimate external web service to system information
Collection (TA0009)	T1560.001 Archive Collected Data	Adversary leveraged xcopy on Windows to copy files
Software/Tool	S0002 Mimikatz	Use Mimikatz to obtain account logins and passwords

RELATED CONTENT

Quarterly Report: Incident Response Trends in Q4 2022

JANUARY 26, 2023 04:01

Ransomware continued to be a top threat Cisco Talos Incident Response (Talos IR) responded to this quarter, with appearances from both previously seen and newly observed ransomware families.