Incident Response trends Q2 2023: Data theft extortion rises, while healthcare is still most-targeted vertical

blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

Nicole Hoffman July 26, 2023

By Nicole Hoffman

Wednesday, July 26, 2023 08:07

Cisco Talos Incident Response (Talos IR) responded to a growing number of data theft extortion incidents that did not involve encrypting files or deploying ransomware, a 25 percent increase since last quarter and the most-observed threat in the second quarter of 2023.

In this type of attack, threat actors steal victim data and threaten to leak or sell it unless the victim pays varying sums of money, eliminating the need to deploy ransomware or encrypt data. This differs from the double-extortion ransomware method, whereby adversaries exfiltrate and encrypt files and demand payment for victims to receive a decryption key.

Cisco Talos Incident Response Quarterly Report (Q2 2023)

One-page overview of the top threats observed in the field last quarter.

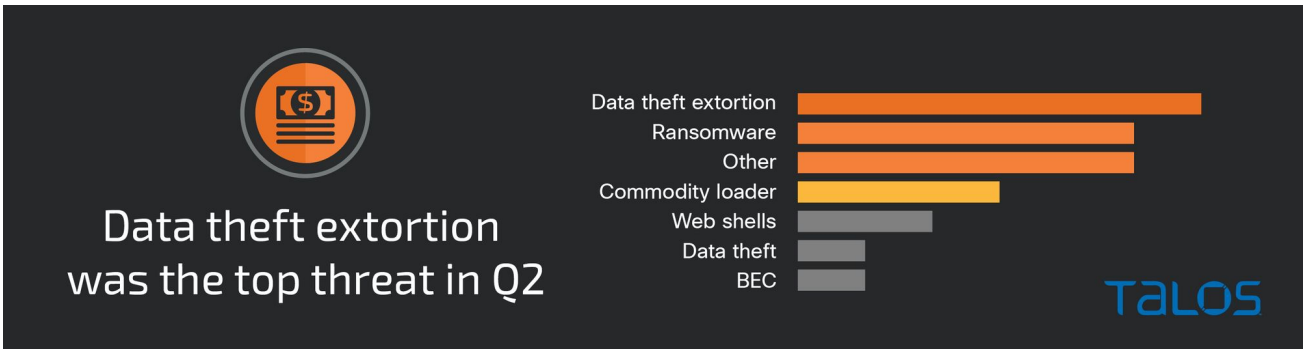
071823 IR Q223 TAR.pdf

172 KB

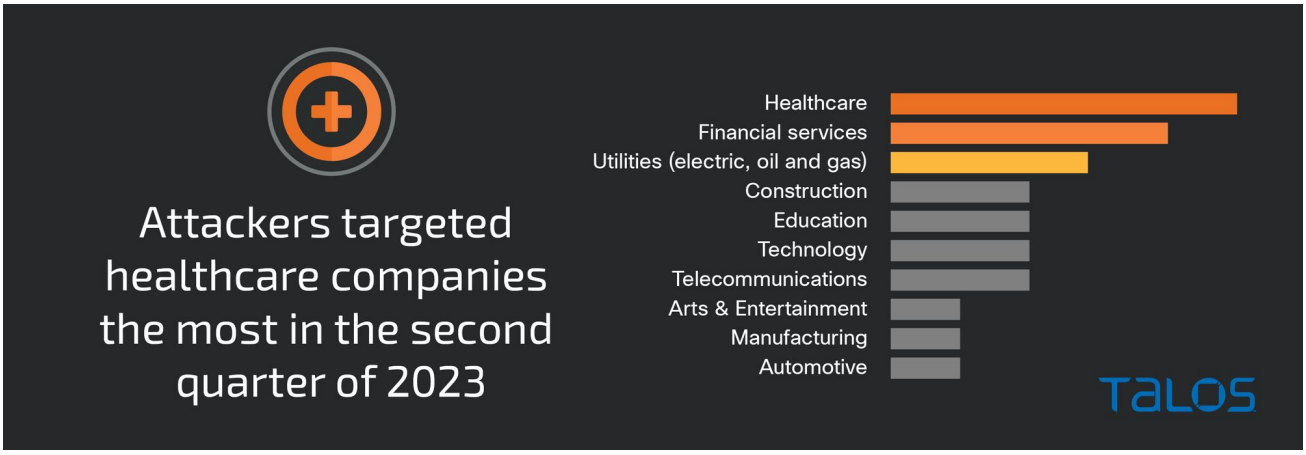
download-circle

Ransomware was the second most-observed threat this quarter, accounting for 17 percent of engagements, a slight increase from last quarter's 10 percent. This quarter featured the LockBit and Royal ransomware families, which Talos IR has observed in previous quarters. Talos IR also observed several ransomware families for the first time, including 8Base and MoneyMessage.

Compromised credentials or valid accounts were the top observed means of gaining initial access this quarter, accounting for nearly 40 percent of total engagements. It was challenging to identify how the credentials were compromised considering they were obtained from devices outside the company's visibility, such as saved credentials on an employee's personal device.



Continuing the trend from last quarter, healthcare was the most targeted vertical this quarter, making up 22 percent of the total number of incident response engagements, closely followed by financial services.



Data theft extortion on the rise, featuring Clop, Karakurt and RansomHouse

Data theft extortion was the top observed threat this quarter, accounting for 30 percent of threats Talos IR responded to, a 25 percent increase in data theft extortion incidents compared to last quarter. The rise in data theft extortion incidents compared to previous quarters is consistent with public reporting on a growing number of ransomware groups stealing data and extorting victims without encrypting files and deploying ransomware.

Data theft extortion is not a new phenomenon, but the number of incidents this quarter suggests that financially motivated threat actors are increasingly seeing this as a viable means of receiving a final payout. Carrying out ransomware attacks is likely becoming more challenging due to global law enforcement and industry disruption efforts, as well as the implementation of defenses such as increased behavioral detection capabilities and endpoint detection and response (EDR) solutions.

This quarter featured activity from the RansomHouse and Karakurt extortion groups for the first time in Talos IR engagements. Active since 2021, Karakurt typically gains access to environments via valid accounts, phishing, or exploiting vulnerabilities. In one observed Karakurt data theft extortion engagement, the attackers hijacked a remote desktop protocol

(RDP) account, enumerated domain trusts using the network administration command-line tool nltest, executed PowerShell scripts to recover passwords, and modified domain policies.

RansomHouse has been active since late 2021 and is known for gaining access to corporate environments by exploiting vulnerabilities. In a RansomHouse engagement, the adversaries used non-interactive sessions to bypass multi-factor authentication (MFA), carried out a DCSync attack to collect credentials from a domain controller, and abused remote services such as secure shell (SSH) and RDP to move laterally. A DCSync attack occurs when attackers use various commands in Microsoft Directory Replication Service (DRS) Remote Protocol to masquerade as a domain controller to acquire user credentials from another domain controller. An attacker first needs to compromise a user account with domain replication privileges, which are typically domain admins.

Some ransomware groups, such as BianLian and Clop, are reportedly shifting away from using encryption, favoring data theft extortion in recent attacks, according to public reporting. Although Talos IR did not respond to any BianLian incidents this quarter, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on May 16 with the FBI and the Australian Cyber Security Centre (ACSC) confirming that as of January, the BianLian group stopped conducting ransomware operations in favor of performing exfiltration-based data theft extortion. BianLian group's shift from deploying ransomware may also be due to the release of a free decrypter for BianLian ransomware in January 2023, possibly prompting them to pursue alternate methods. It is possible BianLian determined they could be successful without the use of data encryption in their operations.

Active since February 2019, the Clop group started as a ransomware-as-a-service (RaaS) operation with an affiliate program that relied on the double extortion technique involving stealing and encrypting data. With the rise in data theft extortion incidents this quarter, it is possible the trend will continue, with other groups who primarily deploy ransomware shifting to data theft extortion as a primary means of receiving a payout.

In a Clop data theft extortion engagement this quarter, the adversaries gained initial access by exploiting a zero-day remote code execution (RCE) vulnerability in the Forta GoAnywhere managed file transfer (MFT) application, tracked as CVE-2023-0669. Notably, the affiliate did not deploy ransomware and only conducted data theft extortion upon exfiltrating victim information. The Clop ransomware group has a history of mass exploitation of zero-day vulnerabilities in campaigns targeting file transfer applications, affecting hundreds of companies globally. This includes several zero-day vulnerabilities in the Kiteworks, formerly Accellion, file transfer application (FTA), tracked as CVE-2021-27101, CVE-2021-27102, CVE-2021-207103, and CVE-2021-27104, and a SQL injection vulnerability in the Progress Software's MFT application known as MOVEit Transfer, tracked

as CVE-2023-34362. U.S. law enforcement has taken notice and increased pressure on the group, offering a $10 million dollar reward for information on the identification or location of Clop members.

It is highly unusual for a ransomware group to consistently exploit zero-day vulnerabilities, given the resources required to develop such exploits, possibly suggesting that the Clop ransomware group possesses a level of sophistication and funding matched only by advanced persistent threats (APTs). Given the group's incorporation of zero-days in MFT applications in recent attacks, and the group's perceived success in affecting hundreds of organizations, Clop is likely to target MFT applications in the future.

Ransomware

Ransomware accounted for 17 percent of the total number of engagements responded to in Q2 2023 (April - June), a slight increase compared to 10 percent last quarter. 8Base and MoneyMessage ransomware operations were observed for the first time this quarter, in addition to the previously seen ransomware operations LockBit and Royal.

First discovered in March 2022, 8Base is a ransomware group/operation that uses a customized version of Phobos ransomware and steals data prior to encryption. Although the group has been around for over a year, it started gaining increasing popularity in June 2023 after a significant spike in activity.

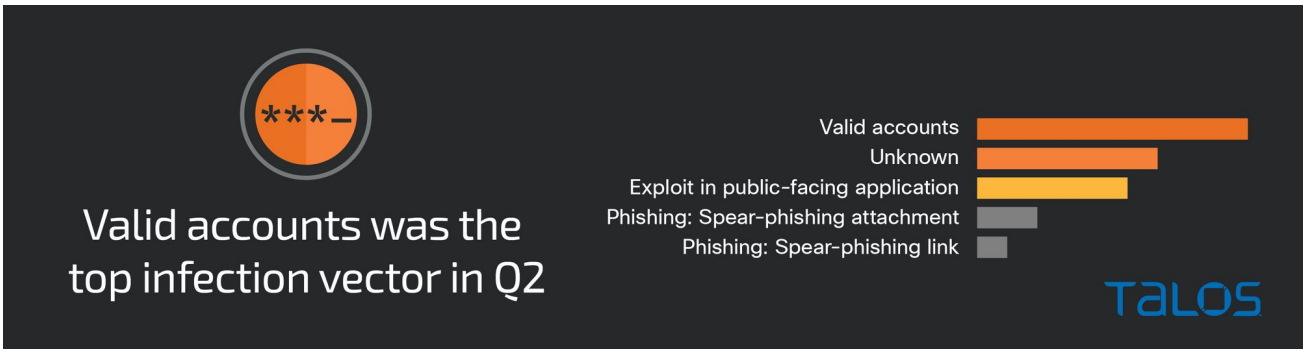
In an 8Base ransomware engagement, the legitimate remote desktop application AnyDesk was installed in the Performance Logs (Perflogs) directory, potentially as a way to evade detection. The Perflogs folder is a system-generated folder that stores information about the performance of the device. The attackers were also observed dumping credentials from the Local Security Authority Subsystem Service (LSASS) memory, creating new processes with an existing user token to bypass access controls, escalating privileges using the runas command, and using the Windows command shell to execute PowerShell scripts.

MoneyMessage is a fairly new ransomware operation that was first discovered in March 2023. Similar to 8Base, the MoneyMessage ransomware group operates under the double-extortion model. MoneyMessage is a ransomware family written in the C++ programming language and uses the Elliptic Curve Diffie-Hellman (ECDH) key exchange and ChaCha stream cipher algorithm for encryption, both of which are commonly used by ransomware families.

Talos IR responded to a MoneyMessage ransomware attack where the MoneyMessage encryptor was dropped in the Netlogon directory allowing for the deployment of the ransomware to multiple hosts. Prior to executing ransomware, the attackers also uninstalled various security tools, such as EDR solutions, via PowerShell scripts to impair defenses.

Initial vectors

In the majority of the engagements Talos IR responded to this quarter, adversaries gained initial access by abusing compromised credentials to access valid accounts. The use of valid accounts was observed in nearly 40 percent of the total engagements, a 22 percent increase from Q1 2023.



It is difficult to say how adversaries obtained the compromised credentials used to access valid accounts. There are a number of ways credentials can become compromised, such as third-party data breaches, information-stealing malware such as Redline, and phishing campaigns. This is especially true if employees reuse credentials across multiple accounts, highlighting the importance of using strong password policies and enabling MFA across critical servers.

Security weaknesses

A lack of MFA or improper MFA implementation across critical services played a part in over 40 percent of the engagements Talos IR responded to this quarter. Talos IR frequently observes attacks that could have been prevented if MFA was enabled on critical services, such as VPNs. In nearly 40 percent of engagements, attackers were able to abuse compromised credentials to access valid accounts, 90 percent of which did not have MFA enabled. In some engagements, adversaries were able to bypass MFA with MFA exhaustion/fatigue attacks.

MFA exhaustion attacks occur when an attacker attempts to repeatedly authenticate to a user account with valid credentials to overwhelm victims with MFA push notifications, hoping they will eventually accept, allowing the attacker to successfully authenticate into the account. Identification and user education are key parts of countering MFA bypass techniques. Organizations should ensure employees are aware of who to contact in these situations to determine if the event was a technical issue or malicious in nature.

Talos IR recommends disabling VPN access for all accounts that do not have MFA enabled. Additionally, Talos IR recommends expanding MFA for all user accounts (e.g., employees, contractors, business partners, etc.). Talos IR has repeatedly seen attackers targeting vendor and contractor accounts (VCAs), which typically have expanded privileges and

access. VCAs are often overlooked during account audits due to trust placed in the third party, making them an easy target for attackers. Talos IR recommends disabling VCAs when they are not needed, implementing least privilege access, and validating that logging and security monitoring are enabled for VCA accounts.

Talos IR also recommends organizations perform a password audit across all user and service accounts to ensure complexity and strength are aligned with the industry best practices per account type (e.g., privilege, service, user, etc.) to prevent password enumeration techniques, such as password spraying.

Top-observed MITRE ATT&CK techniques

The table below represents the MITRE ATT&CK techniques observed in this quarter's IR engagements, which includes relevant examples and the amount Talos IR saw in 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:

- The use of valid accounts was the top observed initial access technique, accounting for nearly 40 percent of the total number of engagements.
- Observed in over 50 percent of engagements this quarter, PowerShell is a dynamic command line utility that continues to be a popular utility of choice for adversaries likely for a number of reasons including stealth, convenience and vast IT administration capabilities.
- In 26 percent of engagements this quarter, Talos IR observed attackers abusing remote services, such as RDP and SSH, to facilitate lateral movement.
- The top persistence mechanism observed this quarter was the abuse of Windows Task Scheduler to create scheduled tasks, allowing adversaries to execute programs or commands at scheduled times or at system startup.

Tactic	Technique	Example
Initial Access (TA0001)	T1078 Valid Accounts	Adversary leveraged stolen or compromised credentials.
Execution (TA0002)	T1059.001 Command and Scripting Interpreter: PowerShell	Executes PowerShell code to retrieve information about the client's Active Directory environment.

Persistence (TA0003)	T1053.005 Scheduled Task/Job: Scheduled Task	Scheduled tasks were created on a compromised server to execute malware during startup.
Defense Evasion (TA0005)	T1562.001 Impair Defenses: Disable or Modify Tools	Uninstall security tools to evade detection.
Credential Access (TA0006)	T1003.006 OS Credential Dumping: DCSync	Use DCSync attack to gather credentials for privilege escalation routines.
Lateral Movement (TA0008)	T1563.002 Remote Services Session: RDP Hijacking	Adversary compromised an existing user's Remote Desktop Protocol session.
Impact (TA0040)	T1486 Data Encrypted for Impact	Deploy ransomware and encrypt critical systems.
Software/Tool	S0359 Nltest	Enumerate remote domain controllers with Nltest.