KROLL

Q2 2023 Threat Landscape Report:

All Roads Lead to Supply Chain Infiltrations

Q2 2023 Threat Landscape Report: All Roads Lead to Supply Chain Infiltrations

Authors

Laurie Iacono

Keith Wojcieszek

George Glass

Kroll's findings for Q2 2023 reveal a notable shift toward increased supply chain risk, driven not only by the CLOP ransomware gang's exploitation of the MOVEit transfer vulnerability, but by a rise in email compromise attacks. This and other key security trends are shaping a threat landscape in which diverse cyber threats are present.

While CLOP ransomware activity dominated the headlines in Q2, analysis of Kroll engagement data painted a more complex picture of the threat environment. Looking at the numbers, CLOP activity increased by 33% over Q1, with the mass exploitation event also driving up incidences of CVE/exploits for initial access. Even with the volume of cases related to this event, Kroll observed other concerning shifts within the landscape as email compromise engagements rose by 8% and phishing continued to dominate the initial access category. From an industry perspective, attacks on the financial services sector increased by 2%, while attacks on healthcare rose by 2%—a small but modest increase that propelled the sector to the top five most targeted industries for the first time in two quarters.

Our analysis of incidents in Q2 highlights several areas in which actors have evolved their tactics to bypass common security controls (such as multi-factor authentication) and continue to prey on organizations via third-parties and trusted relationships.

Q2 2023 Threat Timeline:

April

- VoIP communications company 3CX confirm that a North Korean hacking group was behind a major supply chain attack it underwent in March 2023. This is attributed to a cluster named UNC4736.
- The FBI seize the domains and infrastructure for stolen credentials market, Genesis, in Operation Cookie Monster—a major blow to the cybercriminal world.
- Microsoft attribute recent attacks on PaperCut servers to the CLOP and LockBit ransomware operations, which used the vulnerabilities to steal corporate data.

May

- Researchers state that a ransomware source code leak has led to the emergence of at least ten imitators of BABUK,a ransomware strain that had its source code leaked online in 2021.
- Kroll Cyber Threat Intelligence analysts indentify CACTUS, a new ransomware strain that has been exploiting flaws in VPN apps to gain access into large commercial entities since March 2023. It is novel in that it requires a key to decrypt the binary for execution, likely to prevent detection via anti-virus software.

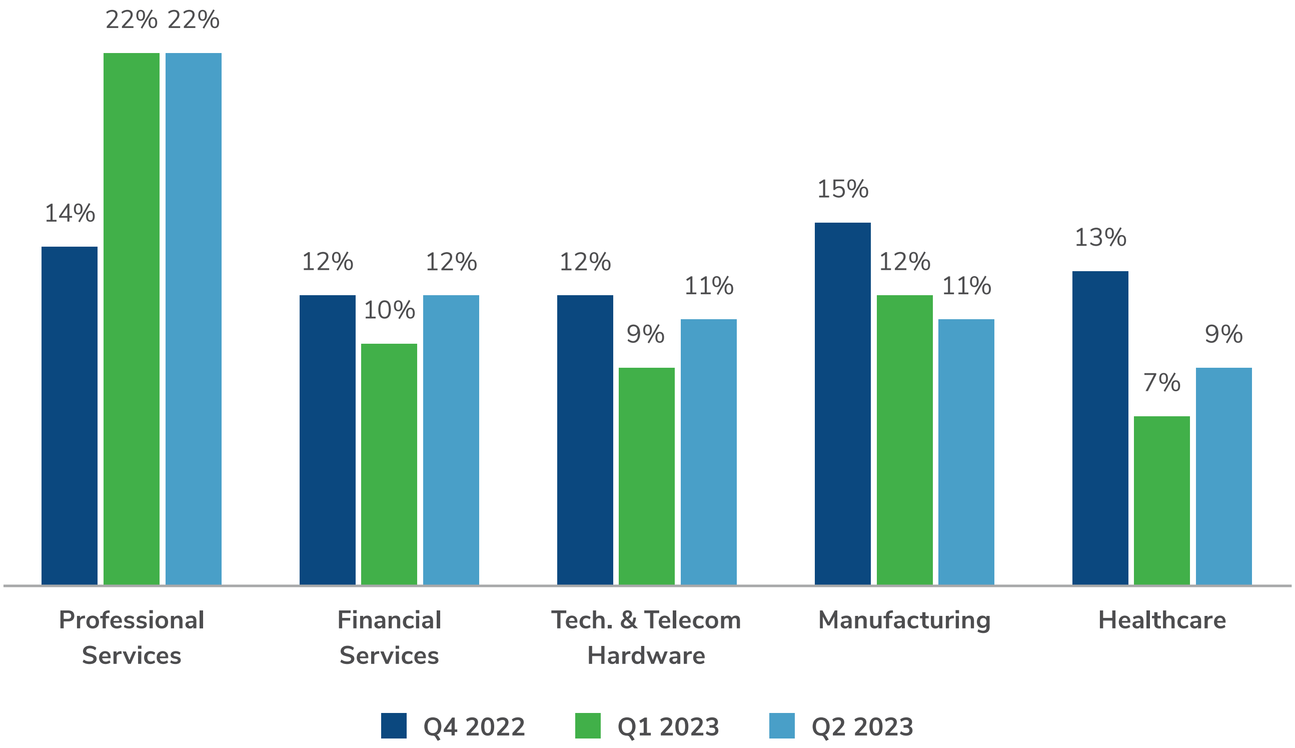
June

- The CLOP ransomware group exploit a serious zero-day vulnerability, CVE-2023-34362, affecting the MOVEit file transfer tool.
- Researchers find that threat actors can leverage "AI package hallucinations" to create ChatGPT-recommended, malicious code packages that developers could inadvertently download when using the chatbot, building them into software that is then used widely, presenting a significant risk for the software supply chain.

Sector Analysis - Health and Wealth Under Attack

In Q2, Kroll observed increases in attacks targeting the financial services, health care and technology and telecommunications sectors. A review of financial services cases identified that the most observed threat incident type was email compromise.

Most Targeted Industry By Sector - Past Three Quarters



In addition, while the financial services sector is not typically targeted by ransomware, the CLOP group's ransomware activity impacted small- to mid-sized regional banks. Kroll also observed a number of cases in which financial institutions were affected by the CLOP exploitation when a third party they worked with was posted to a CLOP victim publication site, exposing data related to their customers. This type of activity and its impact underscores the fragility of organizational interdependence and its potential role in supply chain attacks.

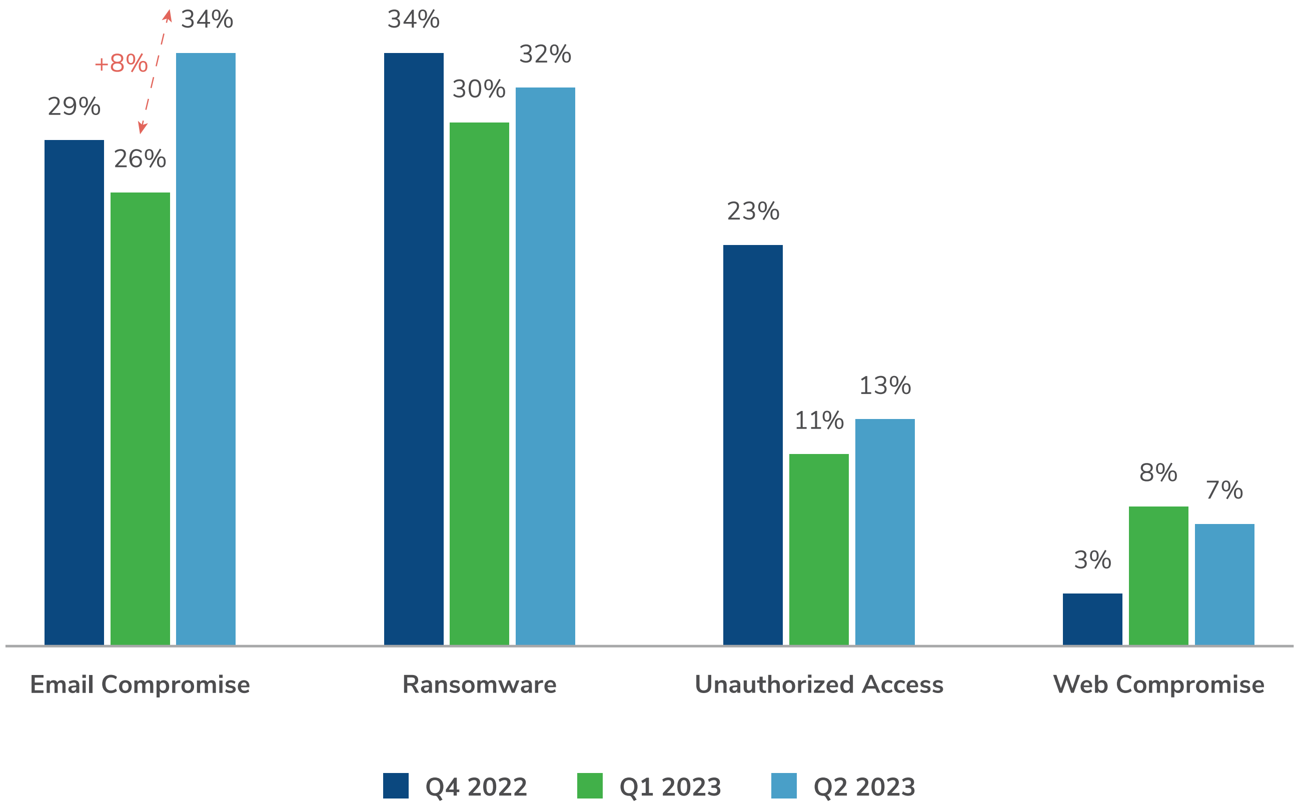
The rise in attacks on health care aligns with our findings outlined in our Data Breach Report that it was the most breached industry of 2022.

Threat Incident Types

Spotlight: Email Compromise Evolves and Evades

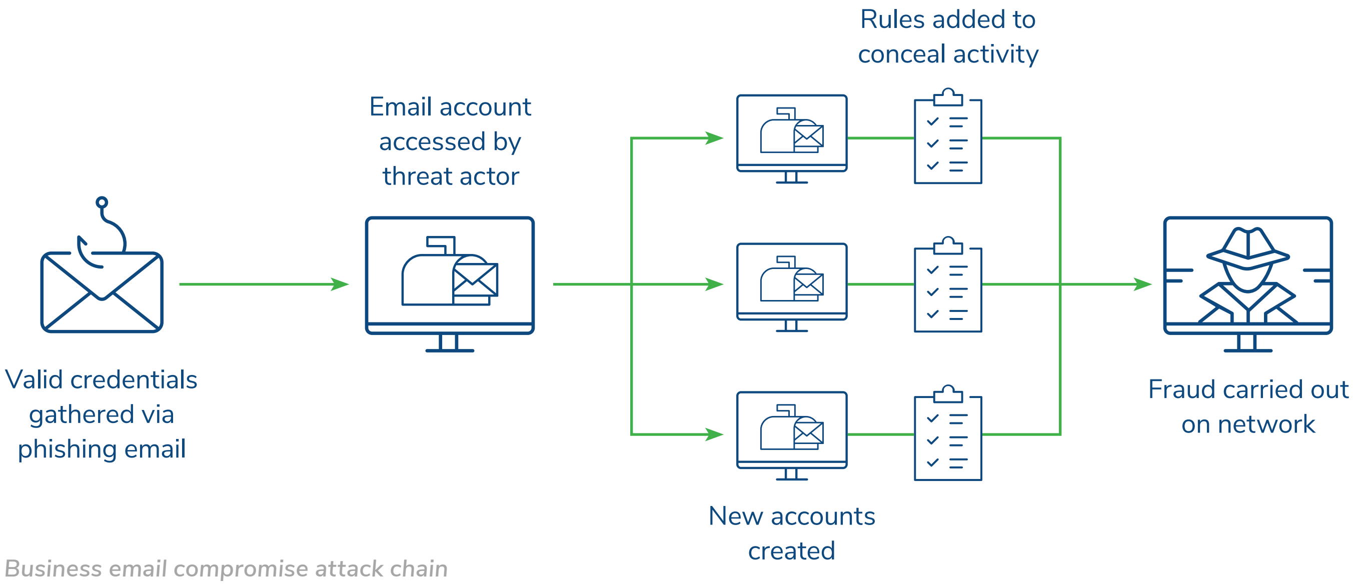
Incidences of email compromise increased by 8% in the second quarter of 2023. Kroll defines an email compromise event as one where email accounts are accessed maliciously by a third party, a phishing email or spam campaign is identified or an organization's email is used or compromised in a fraud scheme (such as business email compromise).

Most Popular Threat Incident Types - Past Three Quarters



While it is a well-recognized security concern, email compromise is sometimes overlooked in the mass media in comparison to more headline-grabbing threats such as ransomware. Despite this, it remains a viable threat to organizations and was associated with more than $2.4 billion in total losses in 2021, according to the Internet Crimes Complaint Center (IC3) annual report. Financial losses from business email compromises have grown ten-fold since the agency first started reporting them in 2015.

A review of Kroll cases associated with business email compromise indicate a familiar pattern of activity, as shown below.

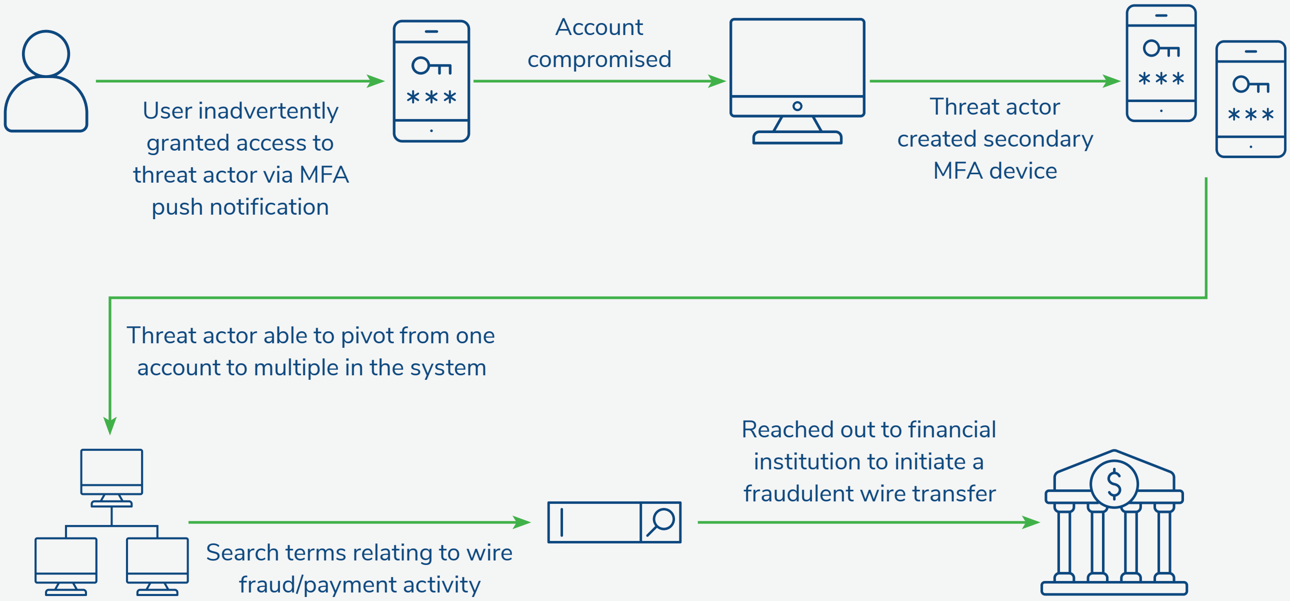

Rules added to conceal activity
Email account accessed by threat actor
Valid credentials gathered via phishing email
Fraud carried out on network
New accounts created

Business email compromise attack chain

- Valid credentials for a user's inbox are gathered via a phishing email.
- The account is accessed by a threat actor, who then uses that access to take over additional email accounts.
- During their time in the network, the threat actor is frequently observed creating inbox rules to conceal their activity.
- Once actors are embedded into accounts, they begin to carry out some type of fraud. This may take the form of:
  - Using the access to contact a known third-party—such as the victim's financial institution—to authorize a fraudulent wire fraud transfer
  - Sending emails from the unauthorized accounts to other users inside or outside the organization, directing them to change or update bank account information or issue a wire fraud transfer

Case Study: MFA Fatigue Leads to Attempted Fraud

As previously stated, the most common vector for business email compromise is valid credentials harvested from a phishing email. Kroll has previously reported on the ways in which attackers bypass multi-factor authentication methods. We continue to see actors using such tactics to gain access to systems.


User inadvertently granted access to threat actor via MFA push notification
Account compromised
Threat actor created secondary MFA device
Threat actor able to pivot from one account to multiple in the system
Search terms relating to wire fraud/payment activity
Reached out to financial institution to initiate a fraudulent wire transfer

How attackers bypass multi-factor authentication methods

In one Kroll case during Q2, a user inadvertently granted access via an MFA push notification when a threat actor initially logged into the webmail version of their inbox. Once inside the network, the threat actor leveraged this access to add a secondary MFA device to the email account.

The threat actor was able to pivot access from this one account to multiple ones in the system. Once inside these accounts, analysis revealed that the actor commonly searched for terms related to wire fraud or payment activity to identify additional internal and external accounts of interest.

The threat actor created rules once inside the inbox to conceal their activity. This included rules that archived messages from certain senders or that moved messages with a certain document type into an RSS folder, marking them as read.

In this case, log analysis revealed that the actors were able to obtain and view a number of documents with sensitive data while they were in the system.

Ultimately, the actors reached out to the victim's financial institution to initiate a fraudulent wire transfer. In this case, the financial institution identified the requests as suspicious and reported them to the victim organization, helping them to identify the activity and avoid financial losses.

Case Study: MFA Fatigue Leads to Attempted Fraud

Commonly Observed Threat Actor Search Terms	
ACH Payment	Wire instructions
ACH Change Vendor	Ach
ACH Tellus	Aging
Wire	Receivable
ACH Bank Change	Remittance
Banking info	Banking Info verification
Invoice	

Email Compromise and Current Phishing Tactics

During Q2, Kroll has been tracking an uptick in activity pertaining to global spam campaigns designed to harvest user credentials that leverage open redirects.

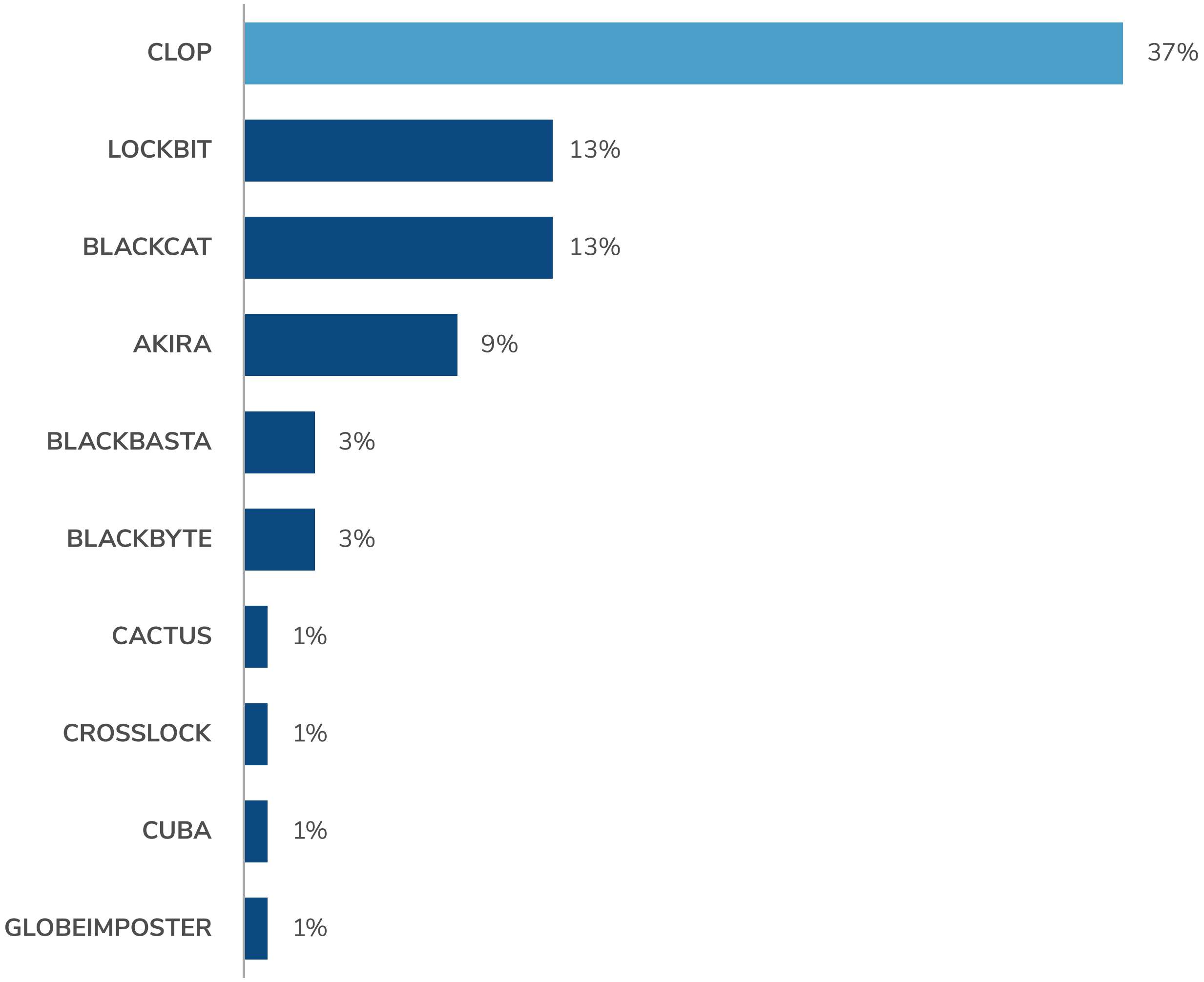
Open redirects are vulnerabilities that occur when a website accepts user-supplied input as part of a URL parameter in a redirect link, without proper validation or sanitization. This vulnerability can be exploited by an attacker to craft a malicious URL that appears legitimate but redirects the user to a different, potentially harmful website designed to capture credentials in order to access a victim's network.

Alongside this, threat actors are leveraging phishing kits that can alter the phishing landing page on the fly based on arguments passed from the redirect links, making the websites appear more trustworthy to the victim.

Spotlight: MOVEIt Transfer Flaw Exploited

On May 31, Kroll began receiving reports that a zero-day vulnerability in MOVEit transfer was being actively exploited to gain access to MOVEit servers. The vulnerability, assigned CVE-2023-34362, allowed unauthenticated attackers to gain access to the MOVEit database and manipulate its contents. Upon initial notification, Kroll observed threat actors using the vulnerability to upload a web shell and exfiltrate data.

Top 10 Ransomware Variants - Q1 2023



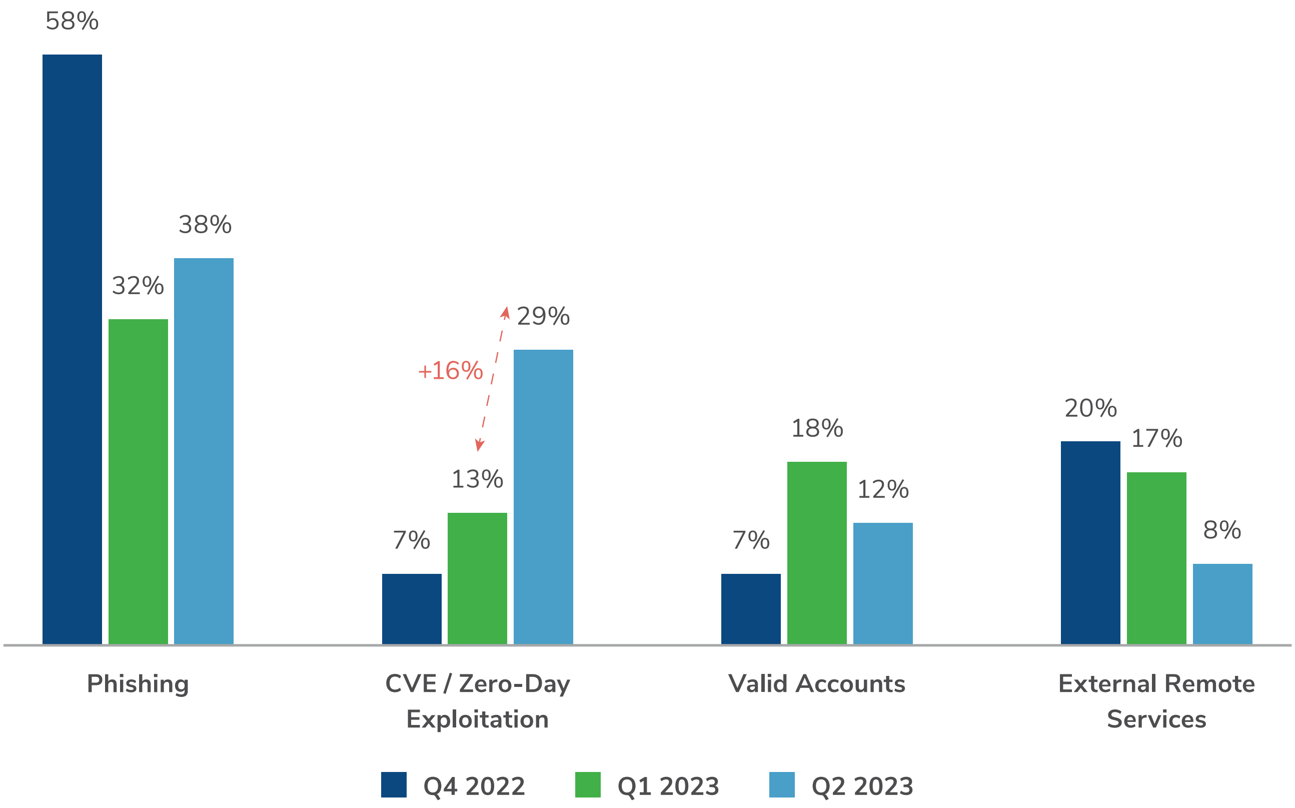
Within days of the vulnerability being published, the CLOP ransomware gang took public credit as the actors behind the attack, indicating that they would begin sending ransom demands to impacted companies on June 14.

Initial Kroll analysis of the MOVEit cases across their client base identified that similar activity targeting MOVEit servers had been observed as far back as 2021, suggesting that the CLOP ransomware group had likely identified the zero-day years earlier and had spent some time creating automated tools to aid them in conducting the mass-exploitation event.

Initial Access

With respect to initial access, Kroll saw the most quarter-over-quarter increases associated with CVE/exploit, most of that driven by the CLOP ransomware exploitation of MOVEit transfer software. Phishing remained the top initial access vector most typically associated with email compromise.

Top 5 Initial Access Methods - Past Three Quarters



Kroll also continues to track a cluster of LockBit 3.0 attacks leveraging victim's VPN for initial access (External Remote Services).

Kroll observed clear evidence of a password spray attack occurring in some cases where logging was available. In nearly all these cases, Kroll observed an overlap of indicators of compromise related to the threat actor IP range and threat actor host name. A notable point is that several of the cases observed in this trend had multi-factor authentication associated with VPN access. However, a lack of knowledge about default settings and misconfigurations allowed for the MFA bypass.

In several cases investigated by Kroll, access was successfully gained using generic and easily guessable usernames and passwords such as "intern" and "payroll." or terms that were more unique and specific to the victims' network usernames that were likely found on paste sites or via attacker reconnaissance.

Password spraying targets the use of commonly used passwords, especially frequently seen default passwords such as the season and year(for example, “Summer2023.”) In one instance, Kroll observed successful access through the victim’s VPN, harnessing usernames associated with former employees who had never been removed as authorized users from the network. This event highlights the importance of scheduled user audits in helping to prevent unauthorized access via accounts that are no longer needed or used within the environment.

During Kroll’s investigation into this cluster of events, it was noted that in some cases the victims had established multi-factor authentication (MFA) protection for the VPNs that were eventually breached by threat actors. In both instances, the victims had relied on their DUO MFA application default setting which allowed for unenrolled users to gain access, meaning that a dormant account was allowed to authenticate via DUO MFA—gaining access through the VPN to the network. In another instance, the victim misconfigured their setting, essentially not requiring MFA to access the VPN for certain users. Recommendations for avoiding these types of security breaches include the enforcement of MFA for all users and understanding settings before implementation to avoid a re-enrollment scenario.

Malware Trends & Analysis

Q2 2023 Trend	Threat Name
↑ 1	QAKBOT
↑ 2	COBALTSTRIKE
→ 3	REDLINESTEALER
↑ 4	AMADEY
↑ 5	AGENTTESLA
↑ 6	PRIVATELOADER
↓ 7	RACCOON
↓ 8	SLIVER
→ 9	URSNIF
↑ 10	ICEDID

Kroll actively tracks malware command and control infrastructure, submissions to public sandboxes and active incident response (IR) and managed detection and response (MDR) case data to generate lists of the most active malware strains for comparison.

This quarter, Kroll observed a significant uptick in QAKBOT activity in both casework and from uploads to public sandboxes, matching our knowledge that sizeable malspam campaigns delivering QAKBOT occurred in Q2. It is important to remember that QAKBOT is commonly delivered via reply chain email attacks and can therefore spread easily from one organization to another, as victims are far more likely to open a malicious attachment from a known third party than a cold email. Kroll also observed increases in AMADEY and AGENTTESLA.

Notably, REDLINESTEALER stays in the top three malware strains detected in both open-source uploads and in Kroll's own casework.

Third-Party Risk Emerges as a Notable Threat Amid Continued Volatility

Our findings for Q2 2023 reflect continued instability in the threat landscape. The activity of the CLOP ransomware group and the increase in email compromise attacks add up to supply chain risk becoming a notable threat. Often less prioritized as a security issue by organizations, third-party risk is now presenting as a key area of concern due to shifting threat actor behaviors and priorities.

In Q1 2023, we highlighted the trend of reinvention among threat actors, and Q2 is no different. Attackers continue to successfully transform and adapt, with our findings highlighting the importance of leveraging continuously updated and reviewed security approaches. Just one example of this type of evolution in Q2 is the use of open redirect abuse in phishing attacks. It is important to note that these types of pivots aren't only being made in relation to tactics and techniques. They are also being undertaken on an industry level, as seen in the impact of CLOP ransomware activity on regional banks, even though the financial services sector is not usually targeted by ransomware. That's not to say that the use of established attack techniques has stalled;threat actors also continue to achieve their goals through the use of tried-and-tested approaches such as phishing. In response, organizations should ensure that they have a comprehensive cybersecurity strategy, whether that's for the cloud or on-premises.

While some sectors were more targeted than others in Q2—notably health care, making it one of the top five targeted industries for the first time in two quarters—all sectors need to prepare to respond to entrenched and emerging security threats.

The key underlying security trend of this quarter also requires organizations to look closer to home in order to address their cyber risk. The rise in supply chain risk calls for businesses to confirm the strength and security of their relationships with their business partners and suppliers. Alongside this, they should ensure that they have robust and proactive support from a trusted security partner. Doing so will mean that they are better positioned to weather the variable conditions in the threat and economic landscape in the months ahead.

Browse the latest editions of Kroll's Quarterly *Threat Landscape* reports and subscribe for free at kroll.com/cyberblog.

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.