KROLL

Q1 2023 Threat Landscape Report:

Ransomware Groups Splinter, Swarm Professional Services Sector

Q1 2023 Threat Landscape Report: Ransomware Groups Splinter, Swarm Professional Services Sector

Authors

Laurie Iacono

Keith Wojcieszek

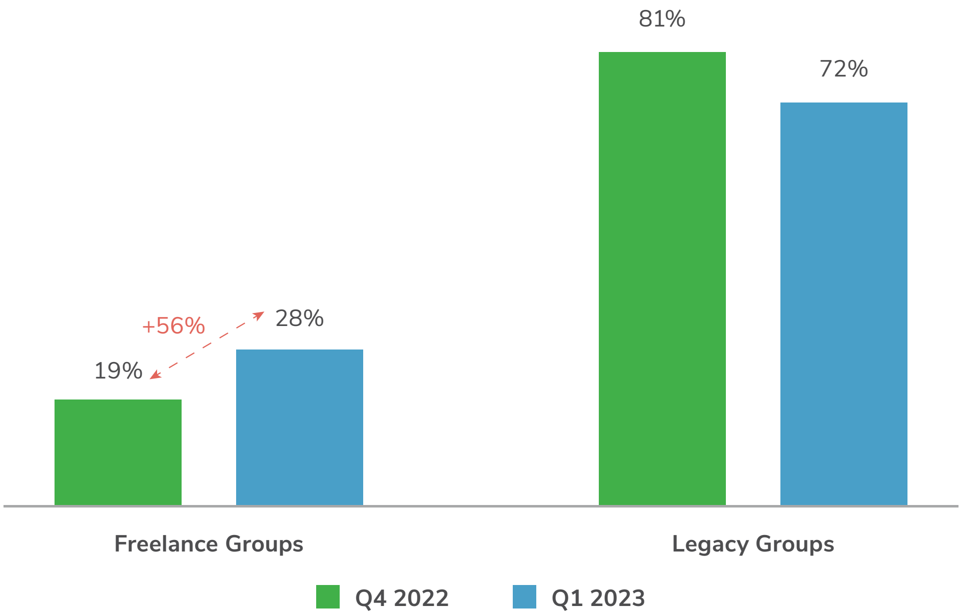
George Glass

Kroll's findings for Q1 2023 highlight fragmented threat actor groups and a continued evolution in attack methods and approaches, which, alongside other key shifts in behavior, have concerning implications for organizations in many sectors.

In Q1 2023, Kroll observed a 57% increase in the overall targeting of the professional services sector from the end of 2022. Ransomware propelled this increase as the sector, particularly legal firms, was the most likely target of extortion and encryption attacks in Q1.

Overall, ransomware accounted for 30% of Q1 cases and 26% of email compromise cases, both remaining closely aligned with the 2022 levels. In Q1, Kroll noted a 56% increase in the number of unique ransomware variants observed. While well-known ransomware-as-a-service (RaaS) operations such as LOCKBIT continue to dominate the ransomware landscape, Kroll observed a number of lesser-known variants during the quarter. Some of these were new but others were established groups that had not been observed for several quarters. The rise in these lesser-known variants, specifically ones such as XORIST, highlights the number of independent attackers conducting ransomware operations outside of the established RaaS groups.

Ransomware Legacy Vs. Freelance Groups - Q1 2023



Phishing continues to lead the pack when it comes to initial access across all cases. Drilling into ransomware cases shows that legacy vulnerabilities such as ProxyShell and Log4j are more likely to be exploited to gain a foothold into the system.

No matter how actors get into a network, data around toolkit deployment during the Kroll Intrusion Lifecycle indicates that actors are using exfiltration tools as standard across a wide variety of threat incident types. As such, enabling organizations to detect actions within a network that denotes staging for exfiltration may help stop attackers in their tracks.

Q1 2023 Threat Timeline:

January 2023

- Europol and the U.S. Department of Justice announce that the HIVE ransomware group's infrastructure had been secretly infiltrated in July 2022. The RaaS gang's Tor payment and data leak sites are seized as part of an international law enforcement operation.
- Law enforcement was able to prevent around $130 million in ransom payments by learning about attacks before they occurred, warning targets, and obtaining and distributing decryption keys to victims.

February 2023

- A ransomware attack targeting VMWare ESXi servers affects over 6,000 vulnerable systems worldwide from February 3 to February 8. ESXi versions before 7.0 U3i appear to be the most heavily impacted, and cloud providers make up most of the affected organizations.
- The ransomware strain is dubbed ESXiArgs due to the ".args" file extension applied on encrypted files. The encryption process specifically targets virtual machine files ".vmdk," ".vmx," ".vmxf," ".vmsd," ".vmsn," ".vswp," ".vmss," ".nvram" and "*.vmem", rendering those virtual machines inoperable.
- CLOP ransomware claims to have stolen data from over 130 organizations by exploiting a zero-day vulnerability in the GoAnywhere MFT secure file transfer tool.
- Security flaw, CVE-2023-066, gives attackers the ability to gain remote code execution on unpatched GoAnywhere MFT instances, with their administrative console exposed to internet access.

March 2023

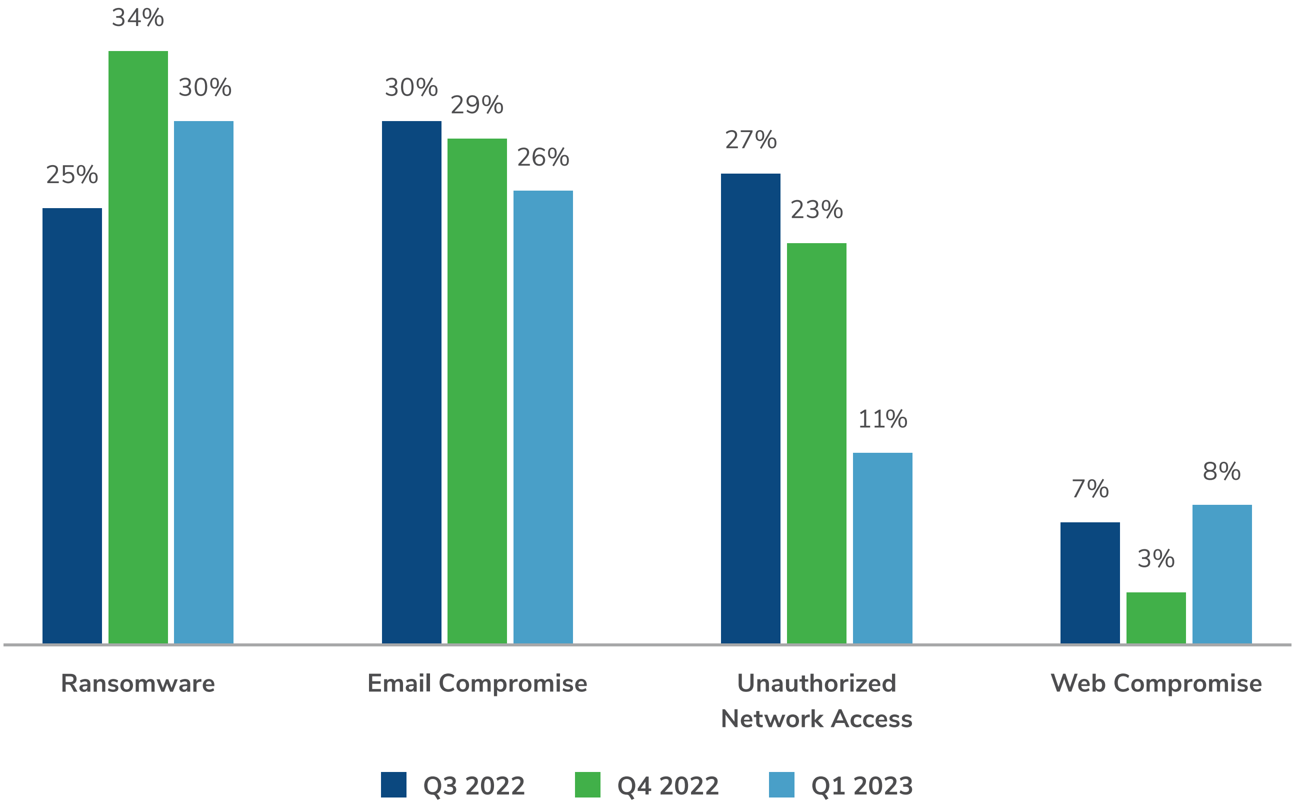
- Kroll identifies a fully featured information stealer and remote access tool (RAT) in the Python Package Index (PyPI) that it calls "COLOURBLIND".
- Analysis of COLOURBLIND demonstrates how the common functionality of malware can easily be written in modern languages such as Python, as well as how the democratization of cybercrime could lead to an intensified threat landscape, as multiple variants can be spawned from code sourced from others.
- Conor Brian Fitzpatrick (aka "Pompompurin") is arrested and charged with a single count of conspiracy to commit access device fraud. Pompompurin was the Breach Forums administrator and an English-language threat actor who had been active since at least October 2020 on English and Russian-language forums.
- Shortly after this arrest, a Telegram message within the "Breach Forums" channels announces they are closing the forum. Breach Forums had become increasingly popular after the seizure of Raid Forums by the U.S. Department of Justice in February 2022.
- With AI chatbots on the rise, cybersecurity concerns increase. All chatbots released publicly to date have either been manipulated to output false information or provide results that appear to be correct but are factually inaccurate.
- Low-level cybercriminals are utilizing chatbots for malicious code development, phishing email creation, scam giveaways and fake landing pages for websites and adversary-in-the-middle attacks.

Threat Incident Types

In Q1 2023, Kroll observed that ransomware and email compromise continue to be the most impactful threats against organizations.

Kroll also noted a rise in web compromise, most typically against the retail sector, highlighting that threat actors attack for financial gain.

Most Popular Threat Incident Types - Past Three Quarters



Malware Threat Trends

In Q1, Kroll observed an increase in all but one of our tracked malware or malicious tool families across our active cases and OSINT collection.

Kroll detected an increase in the use of SLIVER, a cross-platform adversary emulation framework and among one of the growing numbers of public, open-source C2 frameworks, although relatively new to the scene. Due to the public, open-source nature of this tooling, Kroll predicts SLIVER and other similar frameworks will continue to be deployed in more campaigns by threat actors.

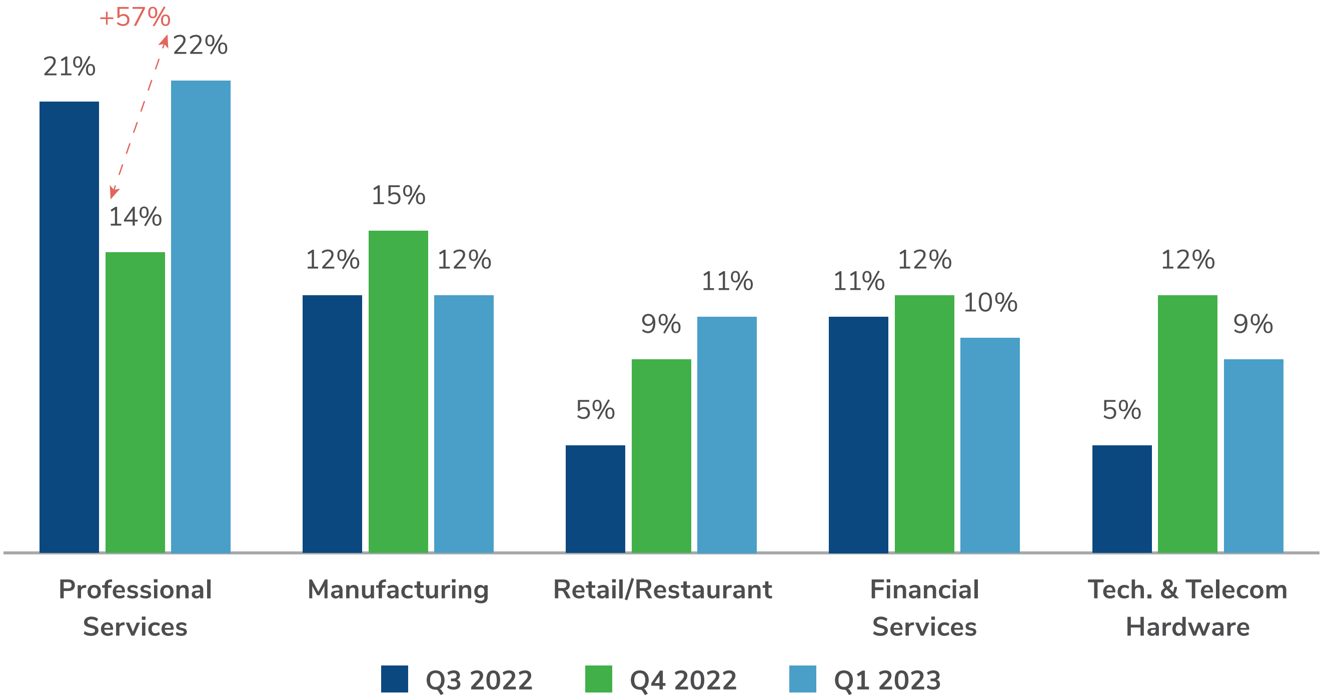
Kroll Top 10

Q1 2023 Trend	Threat Name
↑ 1	SLIVER
↑ 2	EMOTET
↑ 3	REDLINESTEALER
↑ 4	COBALTSTRIKE
↑ 5	GOOTKIT
→ 6	RACCOON
→ 7	PRIVATELOADER
→ 8	QAKBOT
→ 9	URSNIF
↓ 10	VIDAR

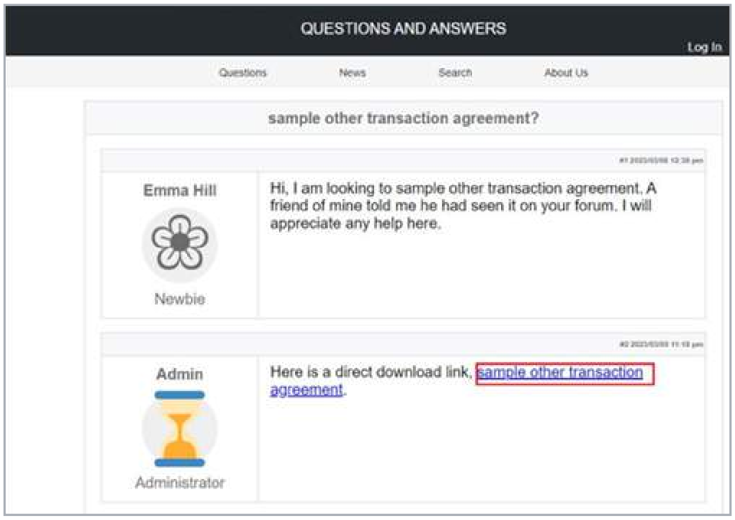
Sector Analysis - Professional Services Swarmed

As observed in Q4 2022, the manufacturing and technology/telecommunications sectors continued to be targeted by ransomware gangs in the first quarter of 2023.

Most Targeted Industry By Sector - Past Three Quarters



However, professional services saw a 57% quarter-over-quarter increase and was the most frequent target of ransomware attacks in Q1. Many attacks against the professional services sector in Q1 impacted legal firms. Similar to the Google Ads abuse tactic leveraged in many late 2022 attacks, Kroll observed an ongoing SEO poisoning campaign by the actors behind GOOTLOADER malware. This involved them targeting legal professionals searching for standard contracts and templates, as shown in the image below.



sample other transaction agreement?

#1 2023/03/08 12:38 pm

Emma Hill

Newbie

Hi, I am looking to sample other transaction agreement. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2023/03/09 11:13 pm

Admin

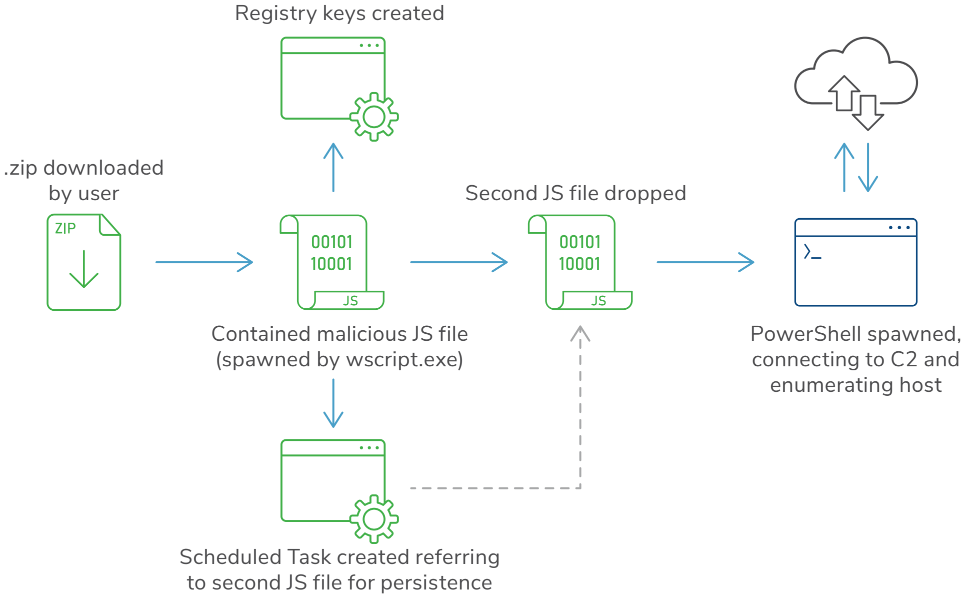
Administrator

Here is a direct download link, sample other transaction agreement.

GOOTLOADER infections typically led to large-scale exfiltration of sensitive data and, in some instances, extortion threats by established threat actor groups.

In cases from March and April 2023, we observed users downloading zip files that contained a malicious JavaScript file identified as GOOTLOADER. This zip file was likely hosted on a compromised website, acting as a watering hole-style attack, with the social engineering theme revolving around business documentation such as contracts or taxes. Once the malicious JavaScript file is executed by the user, a second JavaScript file is dropped into the “Appdata\Roaming\Adobe” directory and is executed by the first script. This second JavaScript file spawns Windows PowerShell (powershell.exe), which we have observed connecting to command-and-control (C2) IPs and domains and performing various host enumeration commands.

GOOTLOADER Attack Chain


Registry keys created
.zip downloaded by user
ZIP
00101
10001
JS
Second JS file dropped
00101
10001
JS
Contained malicious JS file (spawned by wscript.exe)
PowerShell spawned, connecting to C2 and enumerating host
Scheduled Task created referring to second JS file for persistence

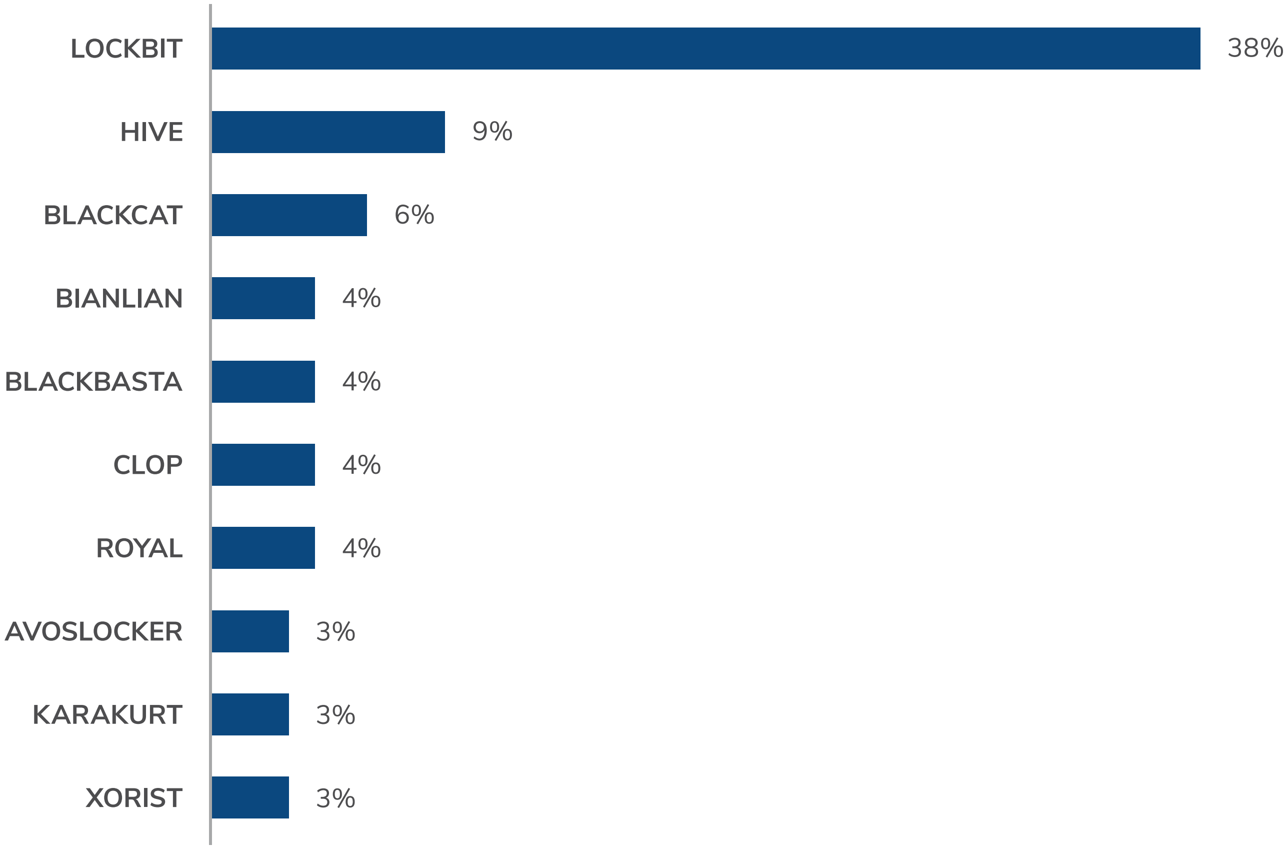
The initial script was also observed creating registry keys and a scheduled task that pointed to the second JavaScript file for persistence. In these cases, further malicious actions were prevented; however, GOOTLOADER has additionally been observed in the wild leading to installations of further payloads including “GOOTKIT,” a sophisticated banking trojan.

Ransomware Activity – Independent Attackers Taking a Leaf Out of the Established RaaS Playbooks

Although large RaaS operations such as LOCKBIT dominated the ransomware landscape in Q1, Kroll also observed a 56% increase in unique variants from the previous quarter. This rise in unique variants included new variants such as CACTUS, DARKSKY and NOKOYAWA, and others familiar, but not observed in several quarters, such as XORIST and RANSRECOVERY.

Kroll has identified an increase in "one-off" ransomware variants that tend to use well-known builders. While these incidents do not typically include data exfiltration and do not extort through the threat of data release, it is likely that a server will be encrypted. A ransom note is created which details a contact email address, an amount of cryptocurrency required for decryption and an extremely short deadline for a response. Kroll has observed a number of XORIST-based encryptors that enable the threat actor to create a unique file extension. This builder, along with video tutorials, is available online. Initial entry is normally provided by an exposed remote service or a common vulnerability. It is likely that the increase of these incidents is in part due to several of the RaaS groups being dismantled and the ease of entry to conduct encryption. As access is not provided by a RaaS group, typically the threat actor does not explore the network as widely as a traditional ransomware actor and may only encrypt the server where they landed.

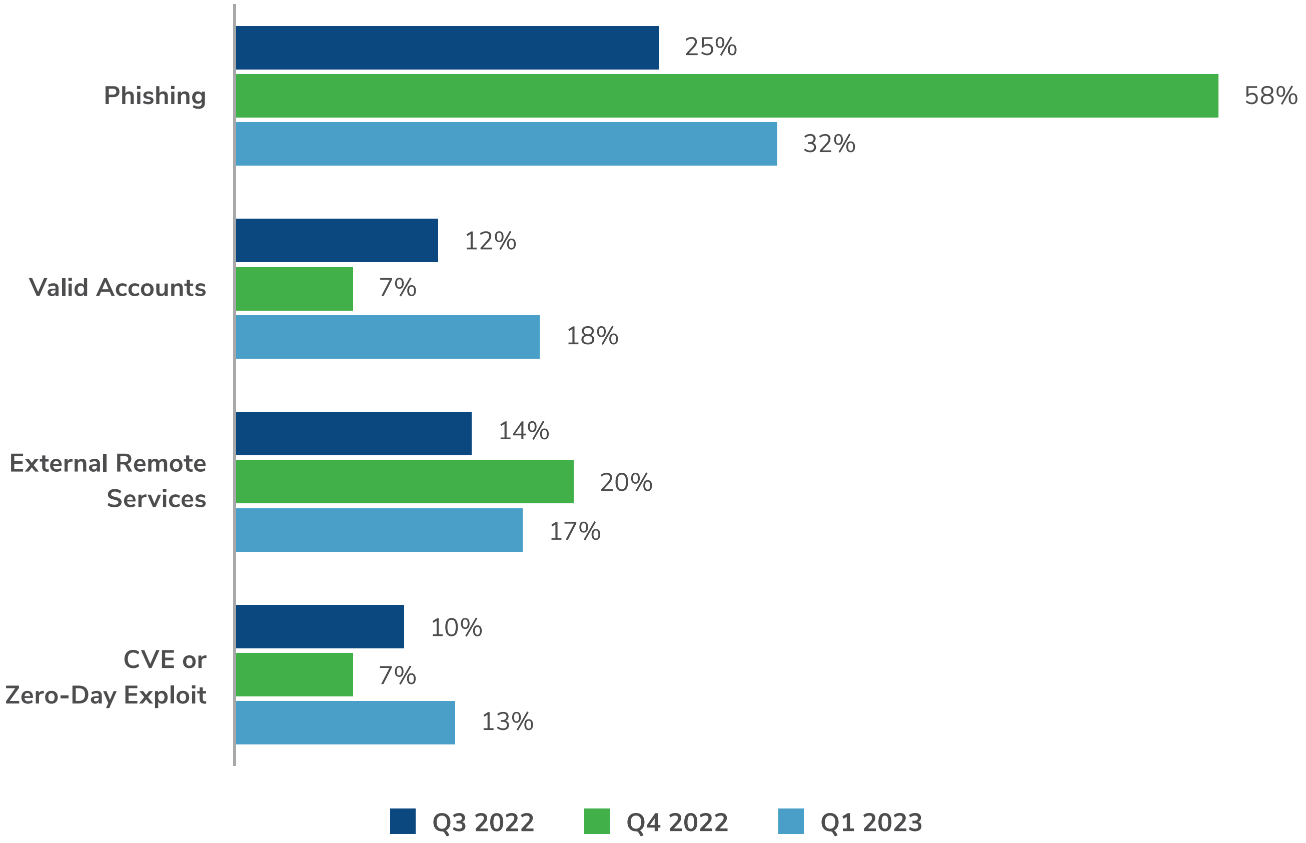
Top 10 Ransomware Variants - Q1 2023



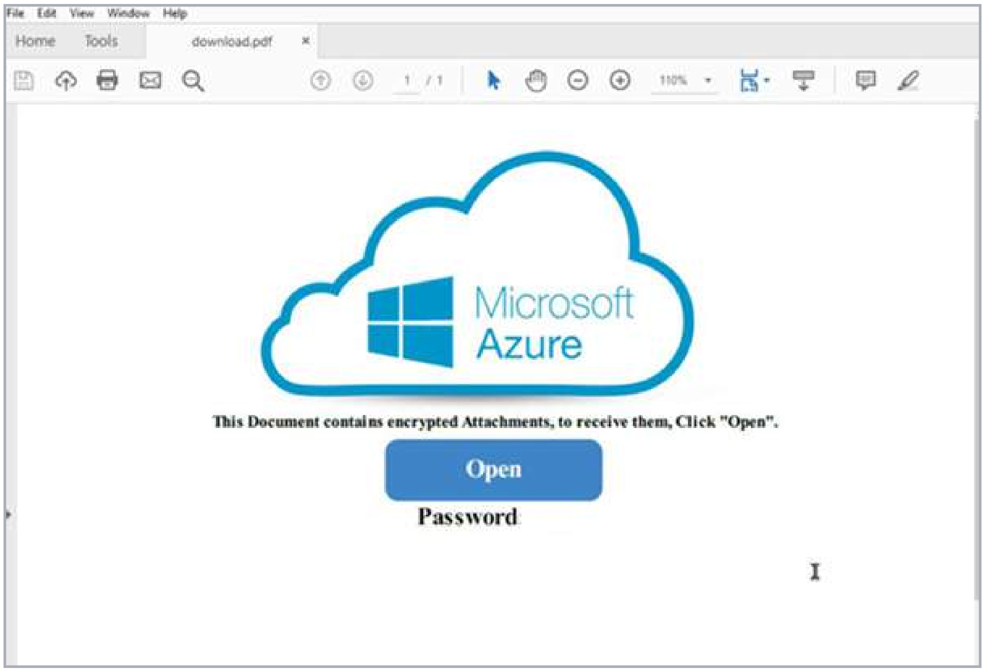
Kroll Intrusion Lifecycle Initial Exploit - Phishing Opens the Door for Threat Actors

Looking across all threat incident types in Q1, phishing remained the number one initial exploit method. Of cases that started with a phishing lure, malicious links were the most likely path to infection. During Q1, Kroll observed phishing attachments continuing to evolve following the Mark-of-the-Web changes to Microsoft. While the latter half of 2022 saw actors turn to container files (.lnk or .iso) for phishing lures, early 2023 marked the rise of Microsoft OneNote (.xml) files being used to deliver malware. In February 2023, Kroll identified several instances of clients downloading malicious OneNote attachments as part of an ongoing QAKBOT campaign dubbed "QakNote." QAKBOT itself was originally used as a banking trojan but has evolved over the years to include a variety of techniques, such as the ability to move laterally within the environment, use of C2 servers and, in the event of being unnoticed by the user, lead to ransomware (such as BLACKBASTA or ROYAL).

Top 5 Initial Access Methods - Past Three Quarters



Towards the latter half of Q1, Kroll directly observed an increase in infections following QAKBOT campaigns that leveraged PDF lures. The name of the PDF varies, with references to invoices, complaints and management information. Once opened, the PDF usually contains an image of a logo of a productivity suite application or cloud-based document storage service. The image is commonly followed by a piece of social engineering text encouraging the user to click a button labeled “open.” In some cases, the button is followed by a password.



This Document contains encrypted Attachments, to receive them, Click "Open".

Inside the PDFs, the button is a hyperlink to a zip file, which, once clicked on, will be downloaded. The zip file is often password-protected, with the password displayed to the user in the PDF, providing false reassurance to the victim. This also serves as a detection evasion measure because antivirus products cannot open the zip to inspect the files. The zip contains either a Windows Script, .wsf file, or a JavaScript, .js file. When these scripts are executed, they will spawn the Windows Script (wscript.exe) that, in turn, spawns PowerShell to download the next stage.

Although requiring several stages in user interaction, this phishing social engineering technique for initial access remains successful for threat actors in 2023, with QAKBOT, in particular, being observed.

Valid accounts and external remote services continue to be the top methods for attackers to gain a foothold into systems, highlighting the ongoing popularity of info-stealer malware and threat actor exploitation of open remote desktop instances.

Drilling into ransomware cases only, Kroll observed that CVE/Exploit and remote services are the top vectors for access. Legacy vulnerabilities such as Log4j and ProxyShell continue to be leveraged by ransomware actors attempting to exploit systems.

Kroll Intrusion Lifecycle – Toolkit Deployment Tees Up Exfiltration

Once threat actors are on systems, tools helping them to exfiltrate data are frequently observed as a common attack technique. Kroll frequently observes data exfiltration across threat incident types. While some of these attacks ultimately lead to encryption, Kroll also saw a number of cases this quarter in which exfiltration followed by an extortion attempt was the main mission execution by the threat actor.

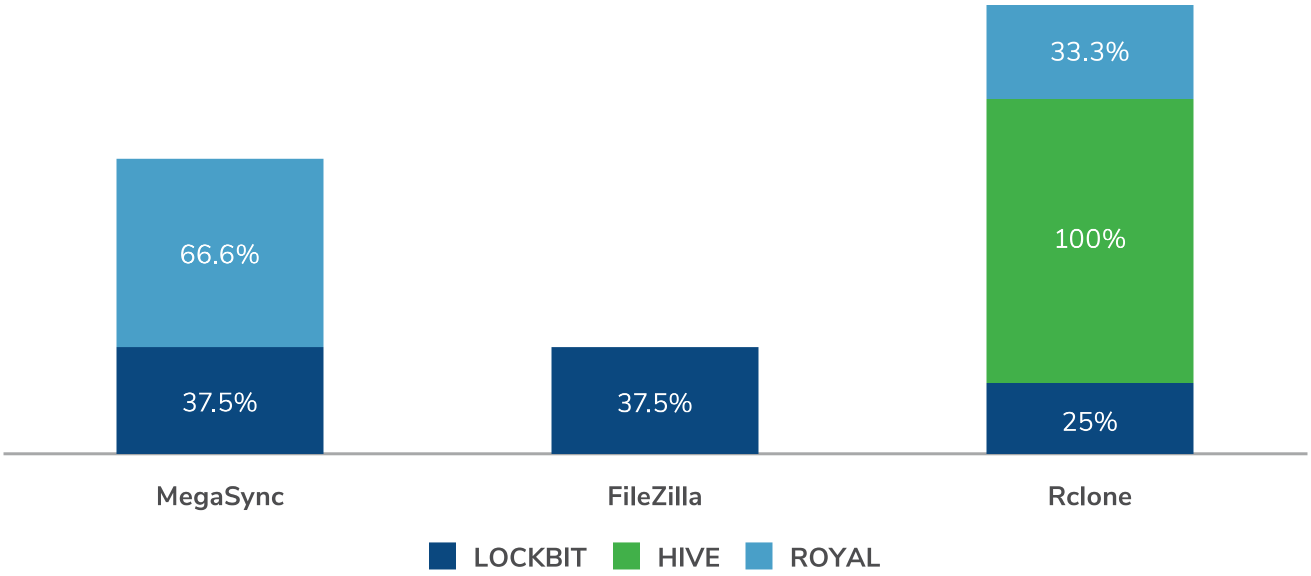
Groups such as LUNAMOTH were observed using this tactic via a callback phishing scheme, prompting users to call a customer service number to avoid a renewal fee for an unwanted service. Once the user is connected with the fraudulent number, they are prompted to accept a remote access management tool that allows the threat actor to exfiltrate data from their system. They are then subsequently extorted to pay a fee or risk publication of the stolen data.

After an extended hiatus, CLOP ransomware group reactivated during this past quarter. Following its claim to have attacked over 130 companies via a zero-day exploit in the Go Anywhere file transfer system, Kroll observed a 380% increase in victim postings to their actor-controlled site, with nearly 100 companies posted in March. In Kroll's review, such attacks only focused on data exfiltration and extortion.

Other groups took advantage of the extortionary landscape, launching mass campaigns claiming to have exfiltrated files and requesting payment through an email message. Such messages signed by various groups (MIDNIGHTGROUP, SILENTRANSOMGROUP, etc.) were sent to thousands of recipients at hundreds of companies throughout March 2023. In Kroll's observation, such claims were the act of opportunistic, financially motivated actors and did not indicate that unauthorized access onto the network had occurred.

Large-scale RaaS groups, such as BLACKBASTA, include exfiltration as a standard operating procedure, highlighting that detecting the first signs of exfiltration is an important step in preventing an incoming cyberattack.

Exfiltration Tools Most Commonly Used by Ransomware Operators



Case Study: QAKBOT Exfiltrates to BLACKBASTA Encryption in Record Time

Kroll has continued to monitor BLACKBASTA actors leveraging QAKBOT to provide an initial foothold within the network. Interestingly, the use of QAKBOT has evolved since previous reporting and is now being used to install Cobalt Strike, directly reducing the dwell time of the threat actor to within one to two days. Typically, QAKBOT is delivered by a phishing email containing a hypertext markup language (HTML) attachment, which itself downloads a zip file once opened. In Q1, Kroll also observed instances where QAKBOT was delivered via customer support software, harkening back to a tactic Kroll reported on in 2021, where actors leverage live chat applications to deliver malware.

This zip file will contain a .lnk file that masquerades as a document. This contains a command to download a JavaScript file that downloads the QAKBOT dynamic link library (dll) before injecting it into a legitimate Windows process, “wermgr.exe”. A standard set of initial reconnaissance commands are executed and sent back to the command and control (C2) server, which include “net share” and “ipconfig /all”.

BLACKBASTA actors then gain hands-on control via Cobalt Strike and attempt to Kerberoast credentials and “pass-the-hash” to move laterally via the “getmac.exe” injected process. Once the threat actor has identified files of interest for exfiltration, Rclone is used to automate the extraction to cloud storage. After the actor has completed the previous steps, a BLACKBASTA encryptor is downloaded, which is typically named after the victim. Once executed, files are appended with an extension “.basta”, a ransom note is placed within each directory named “instructions_read_me.txt” and the desktop wallpaper is changed. If the victim does not respond to the demands, their name is then listed on the group’s “shaming” site before copies of exfiltrated documents are released.

Detecting Data Exfiltration

Detecting exfiltration of data and responding quickly to a true positive can make the difference between the loss of megabytes and gigabytes of data. It also serves as one of the last detection opportunities before ransomware deployment.

Network monitoring can be used to detect large amounts of data leaving the corporate network, but there are many methods for threat actors to avoid detection by network monitoring tools. This is also compounded by the distributed nature of remote work and thus pure network monitoring may not suit all organizations. Threat actors may adopt a "low and slow" approach to exfiltration whereby data is sent in smaller pieces over a longer period of time to blend in with daily flows of data. Prior to exfiltration, threat actors may also encrypt data to avoid detection via advanced network monitoring, which identifies the type of data moving across the network.

On the endpoint: Kroll consistently observes the Rclone tool used by ransomware actors to sync data to remote file storage locations. It is imperative that the deployment and behavior of this tool is detected, and its unauthorized use should be considered an imminent threat of ransomware deployment to be acted upon immediately. Similarly, Kroll has observed the "Caldera" adversary simulation tool used to send files to remote servers. Detection of this technique can be achieved by investigating the system pagefile, system resource usage monitor (SRUM) and the UsnJrnl ($J).

We also provide a high-level Sigma rule for detection of Rclone deployment and execution.

Detecting compression of large files can also be an indicator that a threat actor will soon begin exfiltrating data, commonly done with tooling such as 7zip, WinRAR or zlib. But simply detecting the usage of these tools can lead to high numbers of false positive detections, and thus this should be combined with detections for other behaviors.

Preventative Measures

Network administrators can prevent access to common file-sharing sites that are used by ransomware operators such as MEGA. Consider blocking the following domains.

- *.mega.co.nz
- mega.nz
- file.io
- uploaded.net
- 4shared.com
- anonfiles.com
- anonymfiles.com
- send.exploit.in
- ufile.io
- sendspace.com
- rapidgator.net

Ensure that network segmentation effectively separates areas of the network either logically or physically, especially those that handle backup data.

Monitoring of Cloud Environments

To best protect cloud environments, organizations should implement foundational network security practices, such as limiting the number of public IP addresses that provide access to cloud resources. They can shrink the attack surface further by blocking unauthorized traffic with a Web Application Firewall.

A Climate of Reinvention Demands Continued Vigilance

While the dismantling of certain types of threat actor groups would at first seem to be positive news for organizations, our findings for Q1 2023 show that the story is more complicated. Power shifts among RaaS groups have led to the emergence of lone "splinter" actors that, despite not yet possessing the scope or scale of established groups, are certainly capable of inflicting extensive damage in order to achieve their aims. Although the professional services sector was the key focus for independent ransomware threat actors in Q1 2023, it is quite possible that other sectors will be targeted in the months to come. With attackers of many types adapting both themselves and their tools, and previously dormant groups reactivating, reinvention very much characterizes the current state of the threat landscape.

At a time of ongoing global economic turbulence and increasingly democratized cybercrime, the security environment is likely to be defined by more new variants of methods and attackers in the near future. Faced with this prospect, organizations cannot afford to be complacent, especially as recent Kroll research highlights overconfidence around cyber preparedness can come at a high cost. To counter these risks, organizations need to be ready to continually review and adapt their stance to cybersecurity. Ensuring that key controls are in place is an important starting point but being effectively equipped in the current fragmented and ever-diversifying threat landscape demands much more than this. Organizations will benefit from continued vigilance, supported by the insight and expertise of a trusted security partner who is able to advise, act and adapt alongside them in response to fast-changing conditions. Doing so will stand businesses in good stead in what is likely to continue to be a turbulent year for cybersecurity.

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.