KROLL

# Q4 2023 Cyber Threat Landscape Report:

## Threat Actors Breach the Outer Limits

# Q4 2023 Cyber Threat Landscape Report: Threat Actors Breach the Outer Limits

**Authors**

Laurie Iacono

George Glass

Keith Wojcieszek

Kroll's Q4 analysis shows ransomware groups increasingly gaining initial access through external remote services. The quarter presented a complex security landscape with a mix of both positive and negative trends: positively, activity associated with larger ransomware-as-a-service (RaaS) operations, like LOCKBIT and BLACKCAT, declined. However, negative patterns continued, like the ongoing focus of threat actors on the professional services industry (continuing a key trend from Q3 and earlier on in 2023).

Interestingly, there was a notable drop in phishing attempts in Q4 in comparison to Q3. However, this was counterbalanced by the continued evolution of these phishing tactics, for example a rise in the use of QR codes. Linked to this, yet another trend we observed following on from Q3 was the ongoing dominance of business email compromise (BEC) attacks.

Kroll observed the renewal of other familiar threats in Q4, such as a rise in ransomware. Even previously terminated malware groups, like the one behind QAKBOT, regrouped and redefined their strategies (with, for example, a reply-chain phishing campaign delivering PIKABOT). These and other trends observed in Q4 2023 point to a testing 2024 for organizations.

## Q4 2023 Threat Timeline

### October

- Multiple vulnerabilities are announced, ranging from those identified in Linux-based mail transfer agent EXIM to issues in application security software F5-BIG-IP.
- By month's end, two vulnerabilities in Cisco IOS XE and Citrix Netscaler products are under widespread exploitation by numerous threat actor groups.

### November

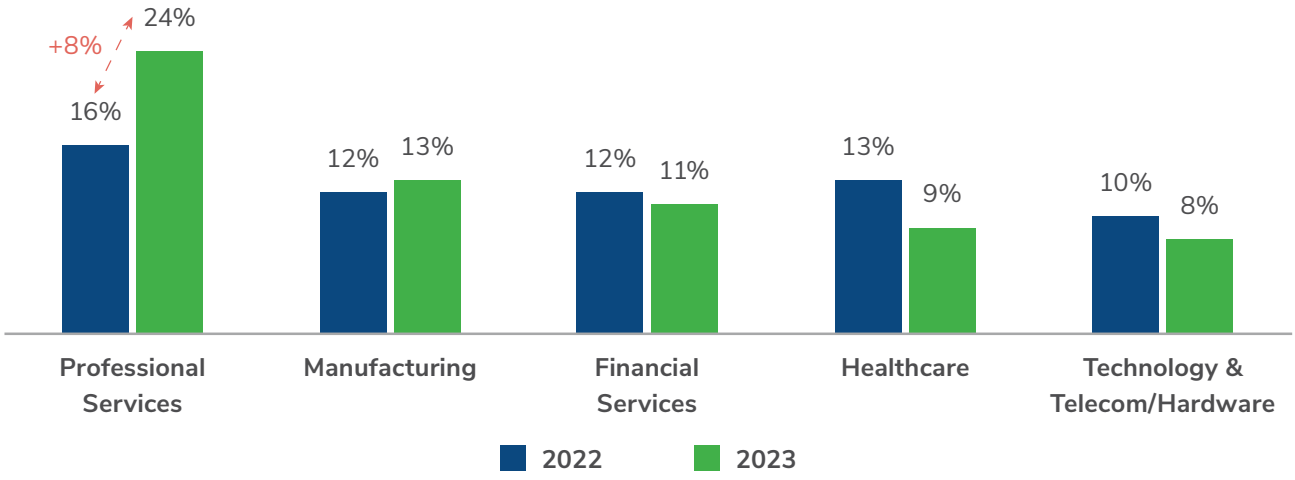
- The actors behind GOOTLOADER campaigns are observed deploying a new tool, GOOTBOT, during post-compromise activities to gain command and control (C2) and lateral movement capabilities.
- DARKGATE and PIKABOT are observed being delivered through phishing, with strong similarities to previous QAKBOT campaigns.
- The information-stealer malware LUMMA, or LUMMAC2, is observed promoting a novel feature that allegedly allows threat actors to revive expired Google session cookies, consequently enabling unauthorized access to Google accounts.

### December

- The threat actor group KTA248 is observed disseminating the ICEDID (BOKBOT) variant, employing a range of techniques to compromise systems and exfiltrate sensitive information.
- CACTUS ransomware is observed being deployed following DANABOT malvertising campaigns, an expansion of the use of CACTUS by threat actors.
- The Windows-based malware DARKGATE is observed using a previously documented TXT DNS record technique to download additional files during a compromise.

## Sector Analysis – Professional Services Remain a Key Focus For Attackers

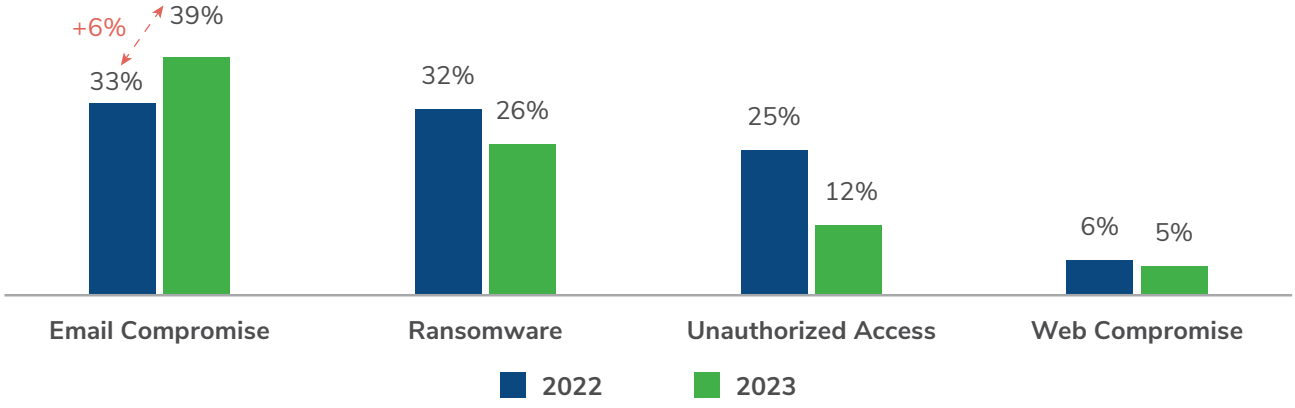
### Top 5 Impacted Sectors: 2022 Vs. 2023 (All Threat Incident Types)




In Q4, Kroll observed that attackers focused heavily on the professional services industry, with slight increases also observed in the health care sector, particularly in respect to ransomware activity. The focus on the professional services industry is the continuation of a trend noted throughout 2023 and follows an sharp increase in cases impacting the sector from 2022 to 2023.

## Threat Incident Types

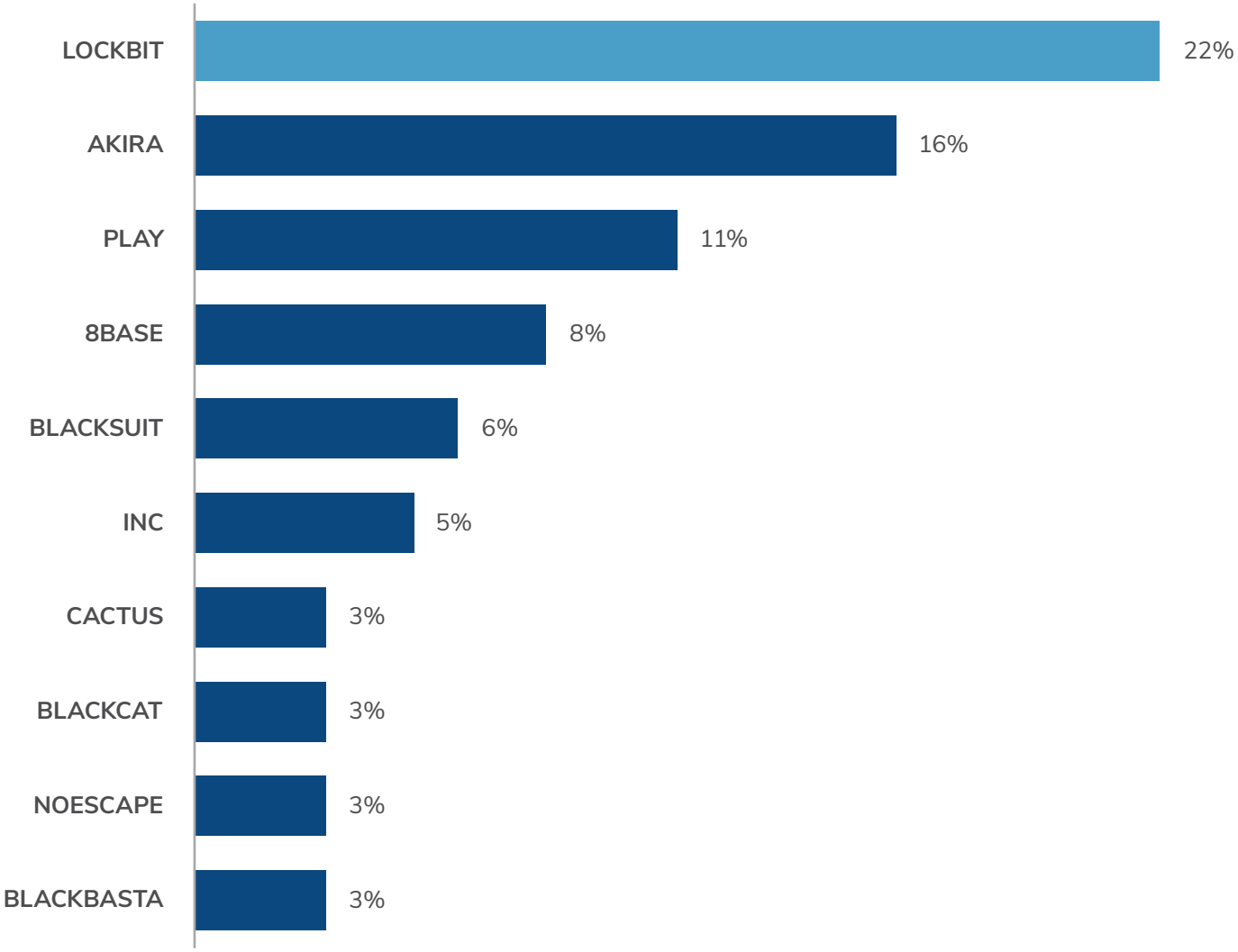
### Year-on-Year Comparison: Most Common Threat Incident Types 2022 Vs. 2023




Kroll continued to see email compromise dominate as an incident type in Q4. As expected after a lull in Q3, ransomware rebounded during the fourth quarter, accounting for 23% of all cases.

## Ransomware 2023

### Top 10 Ransomware Variants – Q4 2023

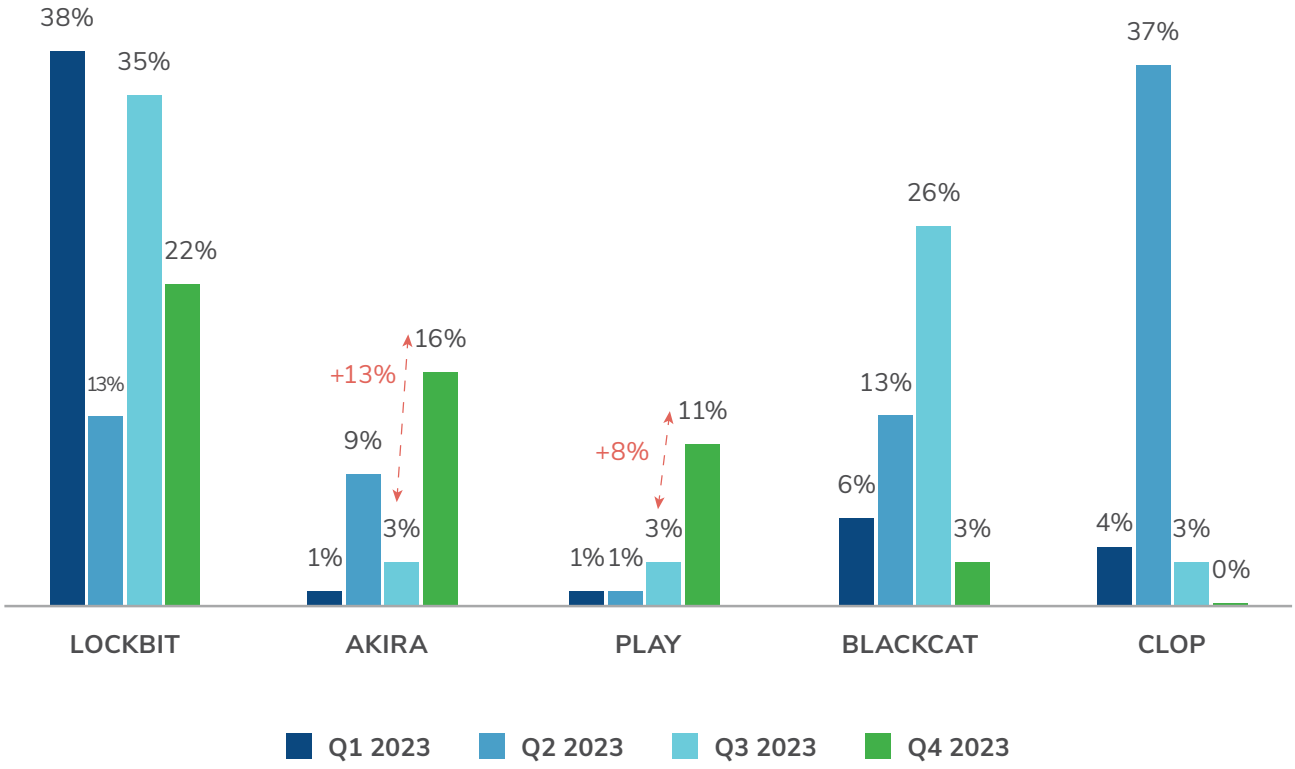



Q4 saw activity from a wide range of ransomware groups, with some key players continuing with campaigns observed earlier in 2023. Kroll observed declines in activity associated with larger ransomware-as-a-service (RaaS) operations such as LOCKBIT and BLACKCAT.

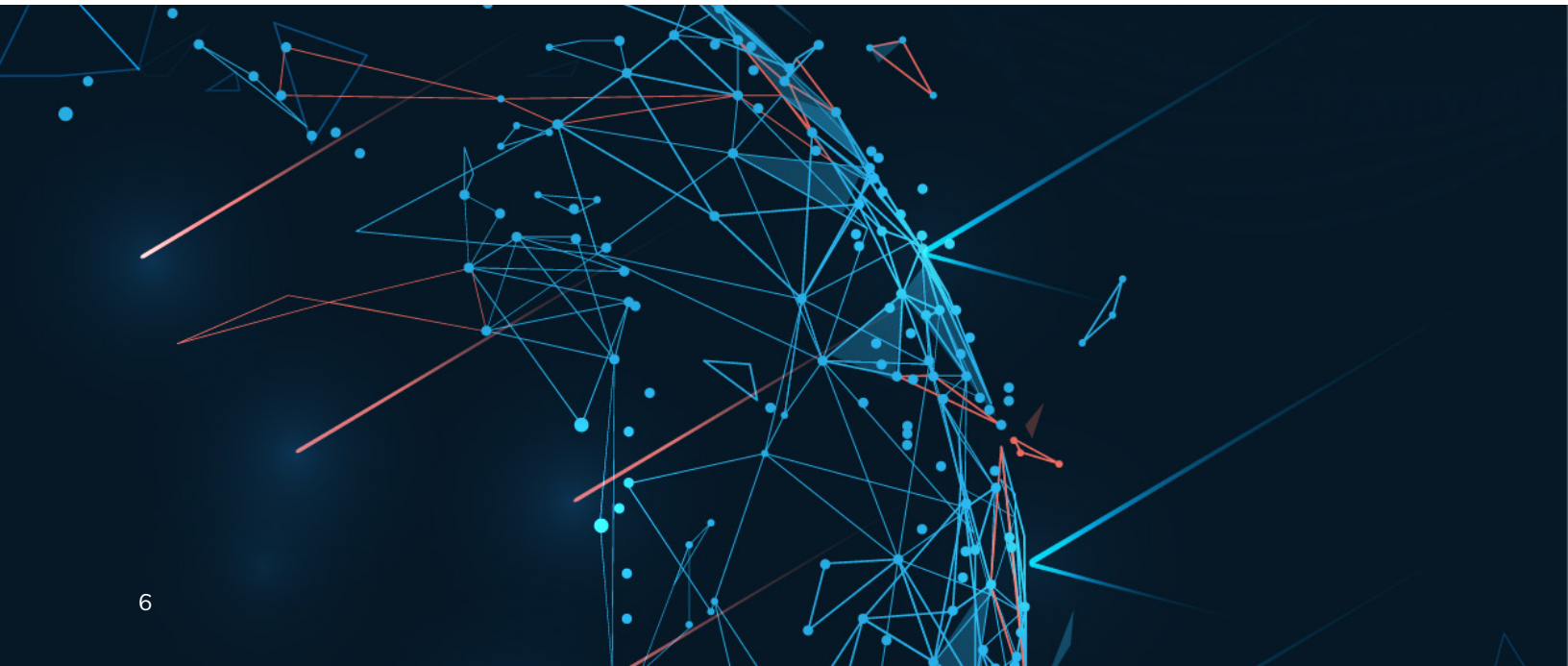
Following an extremely active Q3, BLACKCAT made headlines multiple times during Q4. First, with their move to report a victim company to the Securities and Exchange Commission (SEC) as a new pressure tactic. By the end of the quarter, BLACKCAT found themselves in the crosshairs of international law enforcement as their victim publication site was seized by the Department of Justice on December 19 and then "unseized" by BLACKCAT operators who promptly moved victim notifications to a different site. To date, the "new" BLACKCAT site continues to post victims.

## AKIRA and PLAY Emerge as Top RAAS Groups

### The Most Prolific Ransomware Variants of 2023

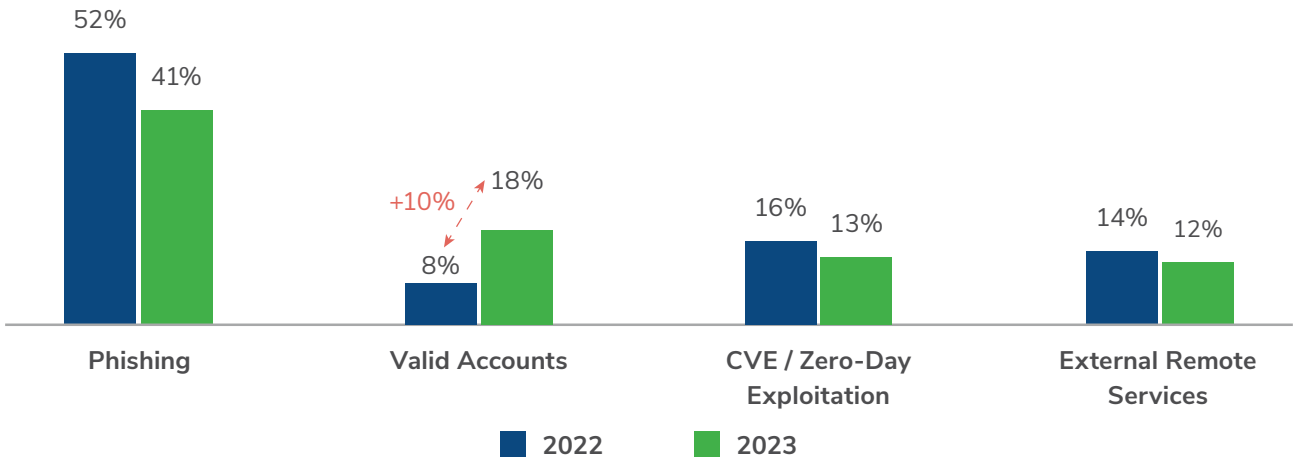



Kroll also observed upticks in activity by several variants, including AKIRA, PLAY, INC and CACTUS during Q4. Looking at ransomware cases, the most likely initial access method was external remote services, presenting another key area of concern for organizations.



## External Remote Services Yields Initial Access

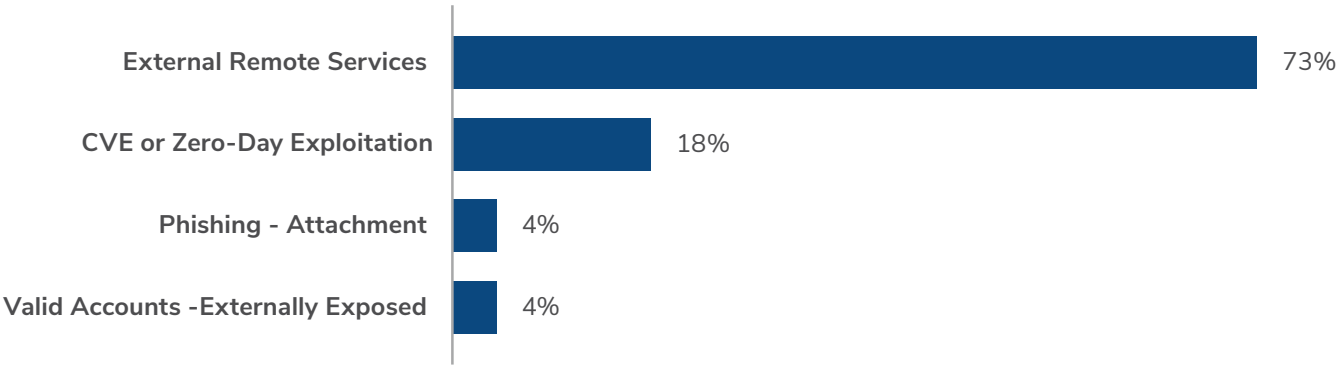
### Year-on-Year Comparison: Most Common Initial Access Methods 2022 Vs. 2023




Although lower in volume than in Q3, phishing continued to be the most likely initial access vector for Kroll engagements. Similar to 2022, phishing continues to evolve as threat actors try new and more sophisticated ways to tempt users into clicking on their malicious links. In Q4, Kroll analysts reported on a rise in the use of QR codes in phishing campaigns. Such tactics make defense more challenging as users may be less likely to perceive these codes as being suspicious, increasing the possibility of them accessing the links via personal devices, which are outside of corporate security monitoring.

## Ransomware Cases in Initial Access Methods

### Percentage of Ransomware Cases in Initial Access Methods Throughout 2023

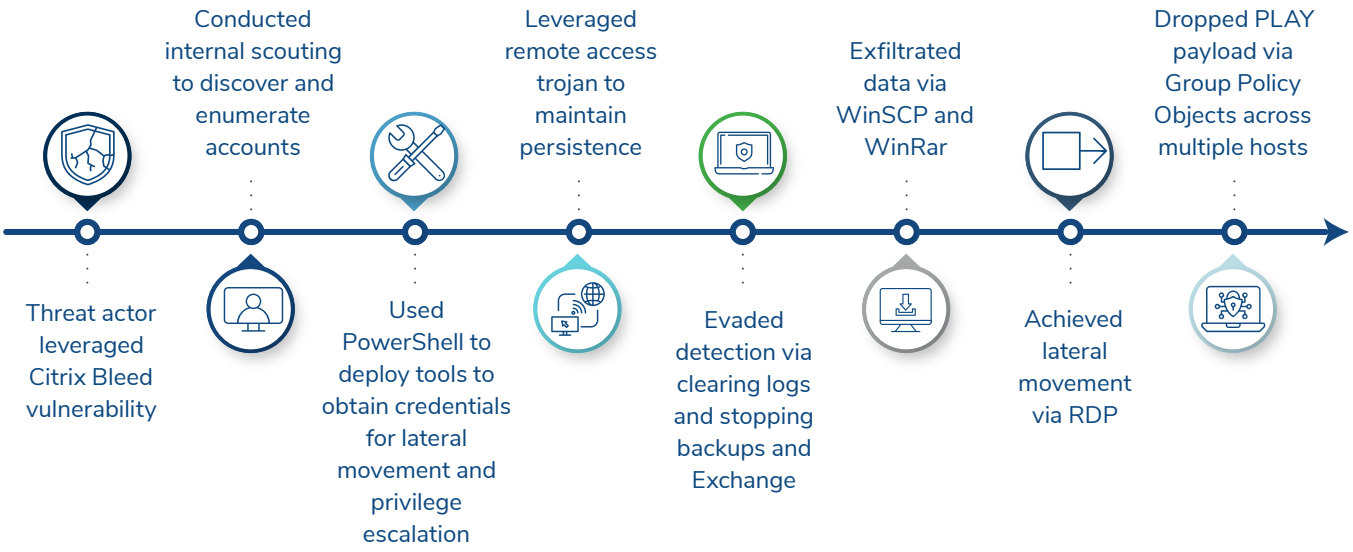



Kroll also observed an increase in external remote services used for initial access, particularly by ransomware actors. Looking at these cases, Kroll identified that in most cases, actors are either exploiting a known vulnerability, such as CitrixBleed (CVE-2023-4966), or accessing a VPN that lacks multi-factor authentication (MFA) through valid credentials or brute-force attacks. As will be discussed later in the report, valid credentials may be obtained in a variety of ways, such as through dark web markets that sell data harvested from information-stealing malware.

# CASE STUDY
## PLAY Ransomware Exploits Citrix Bleed Vulnerability

A threat actor leveraged the CitrixBleed vulnerability to gain access to a professional services firm. Once inside the network, they conducted internal scouting to discover and enumerate domain accounts, trusted domains, permission groups and remote systems. The actor then used Powershell to deploy tools, including Mimikatz, to obtain credentials for lateral movement and privilege escalation. They maintained their persistence in the network via a remote access trojan and used several tactics to evade detection (e.g., clearing logs and stopping services such as back-ups and Exchange). Data was exfiltrated from the system via WinSCP and compressed using WinRar. Lateral movement was achieved via remote desktop protocol (RDP) and the ultimate execution of the PLAY ransomware payload was delivered via Group Policy Objects across multiple hosts.

### PLAY Ransomware Payload Delivery Process




KROLL

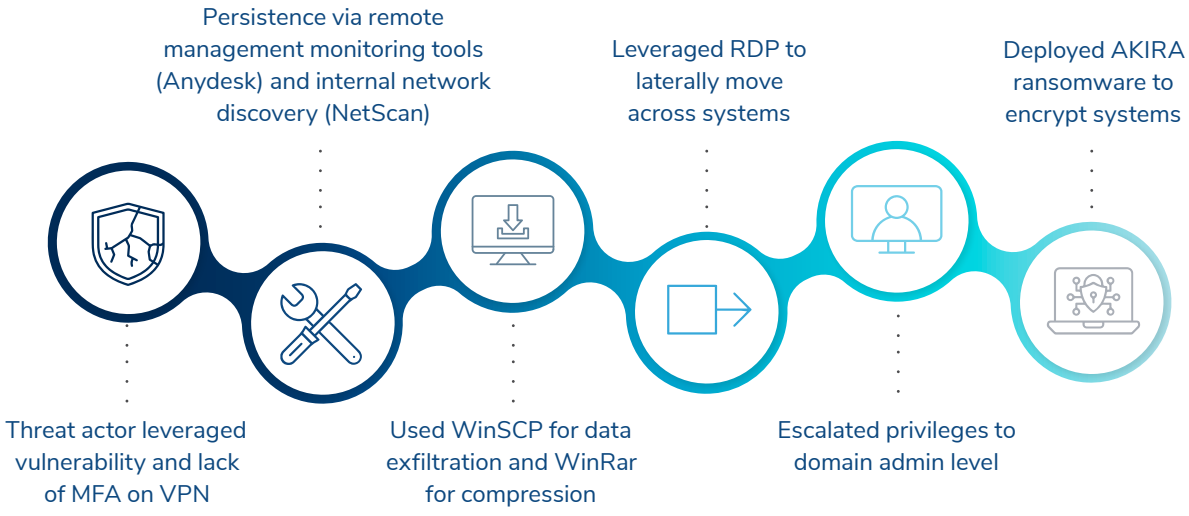
## CASE STUDY
## AKIRA Ransomware Leverages Vulnerability & Lack of MFA on VPN

In October 2023, Kroll identified an uptick in engagements involving AKIRA ransomware, a trend that has continued into early 2024. Kroll observed that in the majority of cases, initial activity could be tracked back to a Cisco ASA VPN service. It is likely that this activity reflected previous reporting that affiliates distributing AKIRA were targeting VPNs failing to enforce MFA and exploiting a zero-day vulnerability in Cisco ASA and Firepower Threat Defense (FTD) services. CVE-2023-20269 allows unauthenticated users to run a brute-force attack to identify valid credentials and establish a clientless SSL VPN session. Cisco updated their advisory in October to include a patch, available via software upgrade.

Intrusion activity following access included persistence via remote management monitoring tools, such as AnyDesk, and internal network discovery via tools, such as Advanced IP Scanner and NetScan. During this time, the actor used WinSCP for exfiltration and WinRar for compression. They then leveraged RDP or remote services creation to laterally move across systems before escalating privileges into a domain admin-level account within two days of network access. Shortly after privilege escalation, AKIRA ransomware was deployed to encrypt systems.

Looking at these cases side-by-side highlights the similarities in activity we see between ransomware variants. While this presents a challenge for clustering activity for attribution, it also provides opportunities for defenders to protect themselves against a number of different attackers by setting up overarching rules capable of detecting and defeating this type of activity.

### AKIRA Ransomware Attack Chain



## Malware Trends and Analysis

Kroll actively tracks malware C2 infrastructure, submissions to public sandboxes and active IR and MDR case data to generate lists of the most active malware strains for comparison.

### Kroll Top 10 Malware Strains – Q4 2023

| Q4 2023 Trend | Threat Name |
|---|---|
| ↑ 1 | PIKABOT |
| ↓ 2 | COBALTSTRIKE |
| ↑ 3 | ASYNCRAT |
| ↑ 4 | QAKBOT |
| → 5 | ICEDID |
| ↓ 6 | NJRAT |
| ↑ 7 | LUMMASTEALER |
| ↓ 8 | REDLINESTEALER |
| ↑ 9 | STEALC |
| ↓ 10 | AGENTTESLA |

## Malware and Ransomware Steal the Limelight

Like Q3, Q4 saw some dramatic changes to the malware and ransomware landscape, with many being a direct result of law enforcement activity to disrupt and degrade the infrastructure of some of the most prolific types. In August, the QAKBOT botnet was heavily disrupted, leading to infrastructure changes and a significant drop in QAKBOT infections in Q3. However, the attempts of threat actors to rebuild the botnet put it firmly back in the top 10 list in Q4. In yet another twist to the tale, although QAKBOT is featured high up on our quarterly trend list, we did not observe any successful infections.

Notably, the threat actor tracked by Kroll as KTA248 (TA577, TR), as well as one of the actors operating huge QAKBOT campaigns, began deploying new malware strains to gain

initial access into corporate environments. This meant that while in Q3 we saw significant increases in DARKGATE, PIKABOT tops our list for Q4. Both malware strains are operated by KTA248 as a potential successor to QAKBOT. Kroll observed a significant overlap between PIKABOT and QAKBOT infrastructure from early- to mid-2023. In November, Kroll noted a reply-chain phishing campaign delivering PIKABOT.

Infostealers also make up more of the quarterly top 10 in Q4, with LUMMASTEALER (LUMMAC2) and STEALC seeing significant upticks. Throughout 2023, and especially in Q4, Kroll witnessed significant increases in infostealer activity, the development of capabilities and new entrants to the market.

## Underground Usage of Infostealer Malware on the Rise

Q4 2023 saw the strengthening of the trend in which infostealer malware has become its own ecosystem in the cybercriminal underground. Infostealer logs are a significant factor in the initial access broker market: threat actors who specialize in selling access they have gained to corporate environments to ransomware operators who then complete the attack chain and extort the victim.

Infostealers are most commonly deployed via phishing, malvertising and fake or misleading posts on social media. This means there is often little specific targeting of individuals or organizations, although this is possible. Threat actors hope to infect as many individuals as possible to collect as many credentials as they can. However, this often presents an unseen risk to corporate environments as employees' personal machines can become infected. These might contain credentials that provide access to corporate credentials or present a threat from their reuse, enabling threat actors to test them against edge services such as VPN, email platforms or application gateways.

One of the most common varieties of infostealer we currently encounter is REDLINESTEALER.

## REDLINESTEALER

REDLINESTEALER, or simply REDLINE, is available on underground forums through a monthly subscription service that gives an attacker access to the REDLINE panel and the ability to pack the malware and collect the logs of stolen information. Its main functionality is to steal data such as passwords, credit card information, usernames, locations, cookies and hardware configuration from infected systems. REDLINE collects this data from a number of sources, including installed browsers, such as SQLite databases, VPN credentials and cryptocurrency wallets, such as files containing *.wallet.

If REDLINE is found to have been executed on a device, it is safe to consider that any credentials stored locally on that device have been compromised. REDLINE can also download files, making it likely that further payloads could be deployed to a victim device should a threat actor require more functionality depending on their objectives (e.g., high bandwidth data exfiltration or ransomware).

In Q4, Kroll investigated a surge in cases in which users downloaded a file associated with REDLINE. In this instance, the lure was a PDF converter software, where it was likely that the users were searching for a legitimate copy of a tool or, as in some cases, victims were searching for innocuous phrases such as “printable calendars” or “business models.” However, the malicious “pdfconvertercompare[.]com” site was presented early in the search results. This site is still active and serving malware as of January 2024.

### Free Exfiltration Mechanisms Scale up the Infostealer Threat

Because infostealer malware is commonly sold as part of a service, threat actors running the services will often look to free services as a scalable solution to control the malware and use it as a method of exfiltration. Infostealers are sold directly on Telegram and use the same service to control and host extracted victim data. Similarly, VIDAR has used Steam usernames to host C2 information and many infostealers will use services such as Discord for storage of exfiltrated data. For these reasons, Kroll recommends blocking Steam, Telegram and Discord domains if they are not used for business activities.

## Defending Against the Perimeter Threat: Key Recommendations

To defend against ransomware, Kroll recommends that organizations:

- Enforce MFA for VPN access - All MFA is not created equal. Phishing-resistant MFA such as FIDO is essential to prevent phishing attacks. SMS and Email OTP codes as well as TOTP app or hard tokens are easily phishable with open source tools. Push notification applications are vulnerable to MFA fatigue attacks, where the attacker repeatedly triggers MFA push notification until the user accepts to make the notifications stop. FIDO security keys or authenticators are the only devices that are effective at preventing phishing attacks.
- Prioritize patching for vulnerabilities impacting VPN appliances.
- Enable risk profiling or conditional access policies for remote access. This can deny access to a user attempting to log in under suspicious circumstances, and can also be configured to only allow limited access if the user's authentication context has elevated risk criteria.
- Enable role-based access control to enforce the principle of least privilege; only users requiring remote access to a resource should have it. Regularly audit access control policies to ensure only required access is provisioned.
- Ensure user accounts are not vulnerable to credential stuffing and password spraying by enforcing a banned password policy. The policy should ban passwords that are known to be weak and that contain company or organizational words or passwords discovered in previous breaches.
- Undertake regular attack simulations to detect weaknesses in edge appliances and validate security controls and detection capabilities.

### A Complex Quarter Points to a Challenging Year Ahead

Q4's rise in the use of external remote services as a ransomware attack vector sets the tone for what is already looking to be a demanding year ahead. With the popularity of remote or hybrid working, organizations must be vigilant in ensuring they have strong defenses in place both centrally and at perimeter level.

Our analysis for Q4 shows a mix of positive and negative trends, very much setting a pattern of "two steps forward, three steps back" in terms of progress for organizations seeking to strengthen their security posture amid a shifting threat landscape.

To counter the continued volatility underlined by our findings for Q4, organizations can benefit by adopting a consistent approach to advancing their security. Achieving this involves working strategically with a trusted long-term security partner capable of aligning closely with their particular security concerns and the changing threat climate. This requires the capacity to support organizations' efforts in preparing for known threats as well as emerging ones, such as the potential for more sophisticated voice-related phishing and other types of social engineering.

The increased use of external remote services by ransomware groups and the advance of other types of threats, such as infostealer malware, highlights that there is no area of security about which organizations can afford to be complacent. Those taking action now will be more likely to achieve the level of cyber maturity required to meet the security challenges of 2024.

KROLL

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.