KROLL

Q3 2023 Threat Landscape Report

Social Engineering Takes Center Stage

Q3 2023 Threat Landscape Report: Social Engineering Takes Center Stage

Authors


Laurie Iacono


Keith Wojcieszek


George Glass

Social engineering in its many forms took center stage in Q3 2023. The quarter saw 'human hacking' evolve from a long-standing security challenge to threat actors' method of choice. This was evidenced by our observations of the dramatic escalation of social engineering tactics, with significant increases in phishing, smishing, valid accounts, voice phishing and other tactics – adding up to the highest volume of incidents we have seen in a year.

The increasing volume of social engineering attacks is matched by a broadening range of approaches, whether that is via phone and SMS as the group KTA243 (SCATTERED SPIDER) is known to do, novel email phishing scams, or directly via Microsoft Teams using DARKGATE malware. As part of the rise in social engineering, business email compromise (BEC) continued to grow steadily in popularity, with both established and newer threat actor groups using a range of tactics to access data and in some cases, ransom the information.

In our analysis of all types of cases handled by Kroll, the professional services sector continued to rank first in Q3, with a high concentration of this activity related to legal firms. We also observed nominal rises in the targeting of the construction and manufacturing industries compared with the previous quarter.

Our observations of malware for the quarter highlight some notable trends, including the fact that while the infamous QAKBOT malware has been disrupted, certain indicators suggest that its operators remain active.

Q3 2023 Threat Timeline

July

- Warning published about the possibility of threat actors using tools like TeamsPhisher to launch social engineering attacks via Microsoft Teams.
- Chatter observed on the dark web indicates actors are interested in a malicious version of ChatGPT known as WormGPT.
- New insights gained into the exfiltration methods used by the CLOP gang to steal data during the MOVEit mass exploitation event.

August

- Multiple reports highlight the ever-evolving phishing landscape as reports indicate that nation states are leveraging Microsoft Teams for targeted attacks, a new spam campaign uses Google AMP URLs to bypass email security and yet another phishing campaign uses QR codes to spread malware.
- Critical severities related to Telerik and Citrix NetScaler are observed being used to gain access to networks.

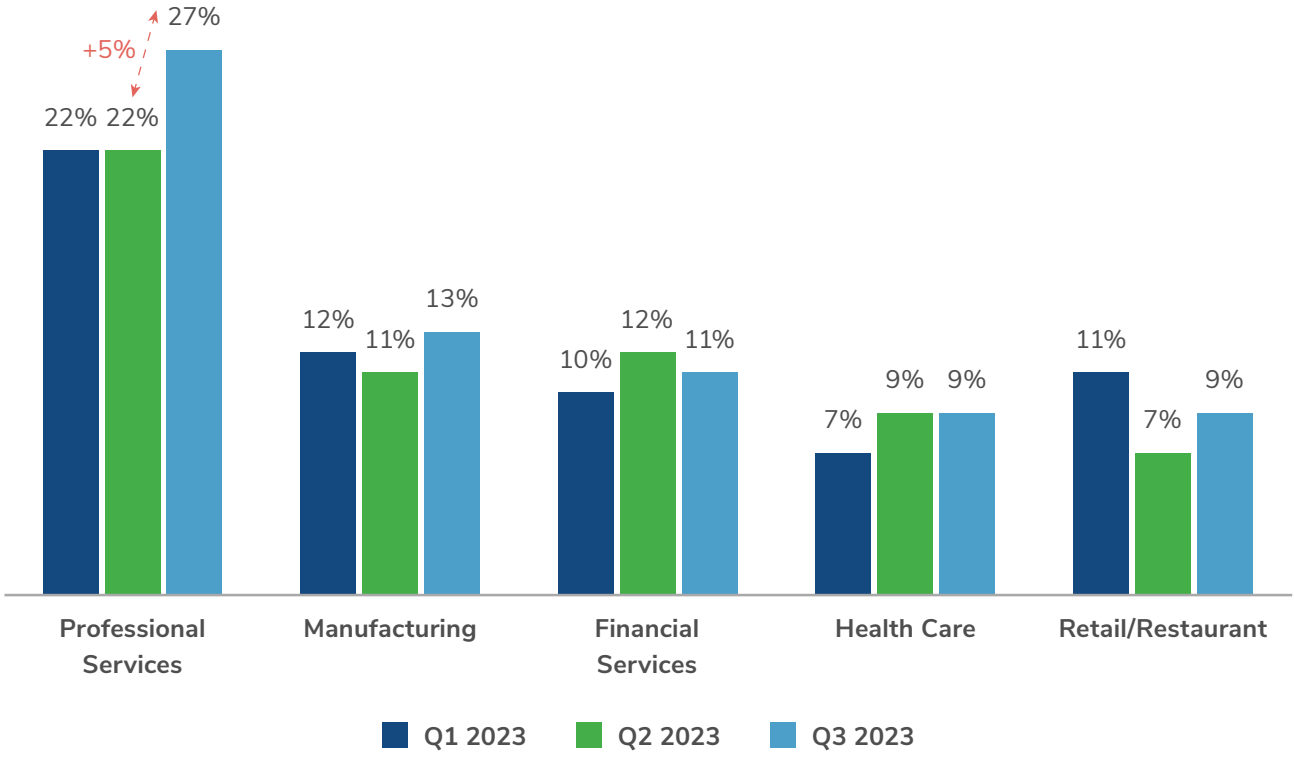
September

- A multinational law enforcement operation announces the disruption of QAKBOT malware. Also known as QBOT, Kroll has tracked activity related to the malware since 2020, frequently observing it as a precursor to ransomware deployment.
- Kroll observes DARKGATE malware being distributed by files shared in Microsoft Teams.
- KTA243 (UNC3944, SCATTER SWINE, SCATTERED SPIDER, 0KTAPUS) uses phone-based social engineering and SMS-based phishing to steal credentials and infiltrate organizations.

Sector Analysis – Professional Services Stay in the Spotlight

In Q3, Kroll continued to see the professional services sector rank first across cases. Similarly to Q1, Kroll saw a high concentration of this activity related to legal firms, fueled by a rise in BEC across all sectors and specific campaigns targeting the legal industry, such as the BLACKCAT ransomware gang.

Most Targeted Industry by Sector - Past Three Quarters

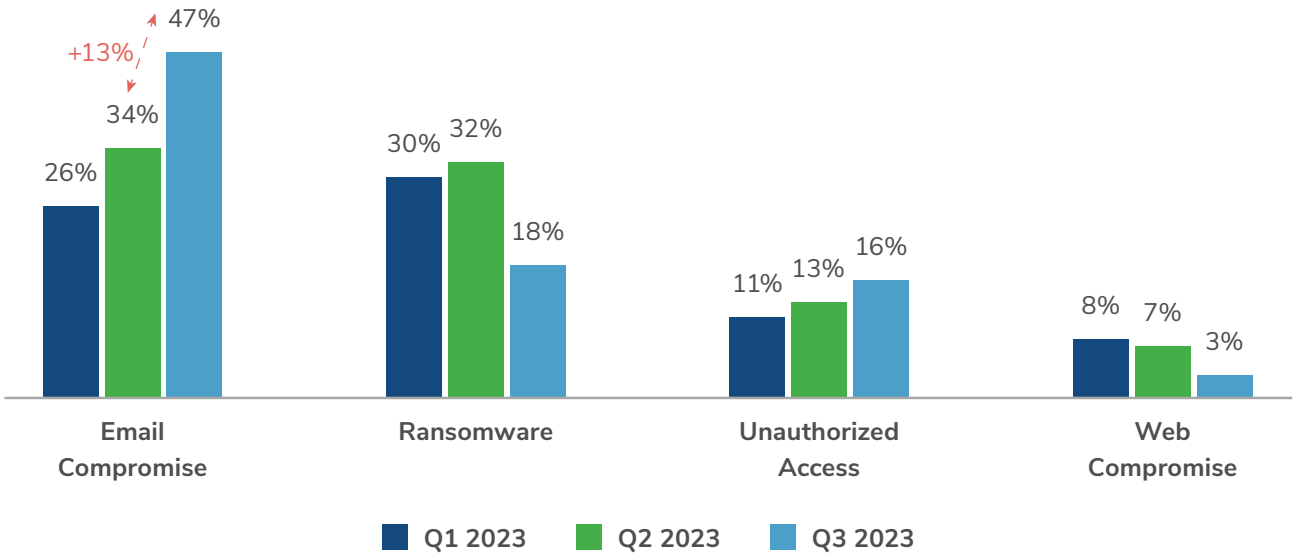


Kroll also observed nominal rises in the targeting of the manufacturing (2%) and construction sectors (1.5%) from the previous quarter. In Kroll's observation, both sectors most frequently experienced BEC in the third quarter. For manufacturing, ransomware was the second most likely threat type to be observed, while insider threat was the second likely threat type for construction. Manufacturing and critical infrastructure are often targeted by cybercriminals due to the potential to execute a catastrophic and high profile attack. The 2021 Colonial Pipeline ransomware attack is a key example of the potential dangers. Historically, the manufacturing sector has been a key focus for criminals as many businesses within the sector did not fully appreciate the size of their attack surface. While the industry is now better prepared to protect itself, the target on its back remains.

Threat Incident Types

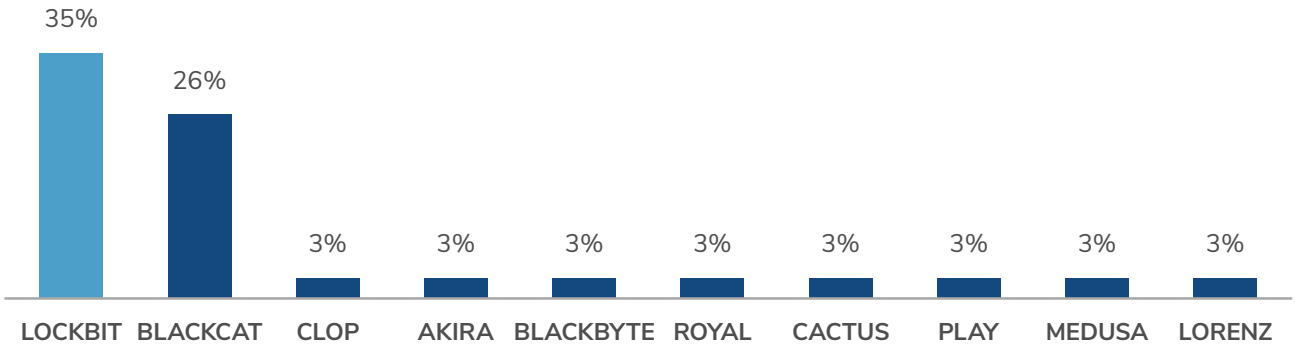
Business email compromise continues to increase steadily in popularity. According to the latest Internet Crime Report from the FBI's Internet Crime Complaint Center (IC3), businesses lost more than $2.7 billion due to BEC. In Q3, Kroll saw an uptick in events related to email compromise, fueling that threat to account for nearly 47% of cases during the quarter.

Most Popular Threat Incident Types - Past Three Quarters



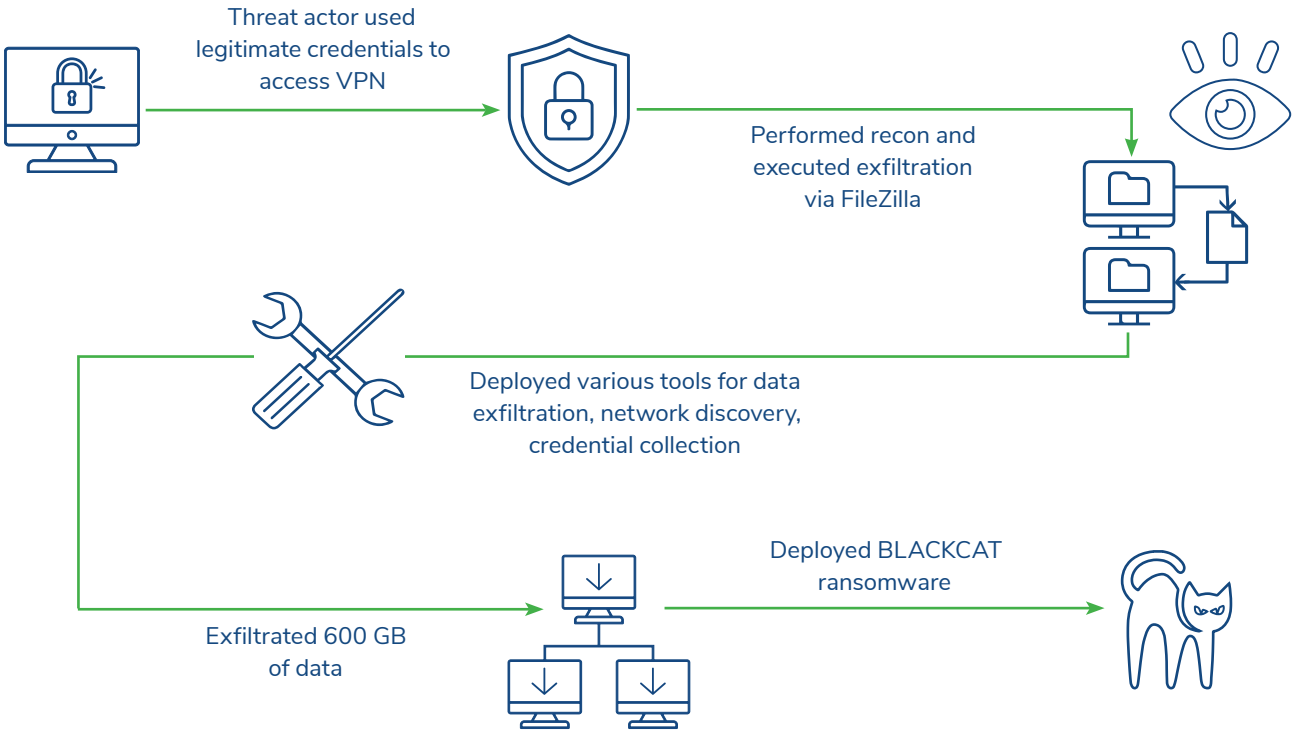
Despite BEC taking center stage, ransomware remains an ever-present threat. While the total percentage of ransomware cases dropped in Q3 (-13.5%), the number of individual ransomware engagements were consistent with previous quarters. The most active groups observed in Q3 were LOCKBIT and BLACKCAT. Kroll also saw increases in activity around newer groups such as CACTUS, RHYSIDA and INC.

Top 10 Ransomware Variants - Q3 2023



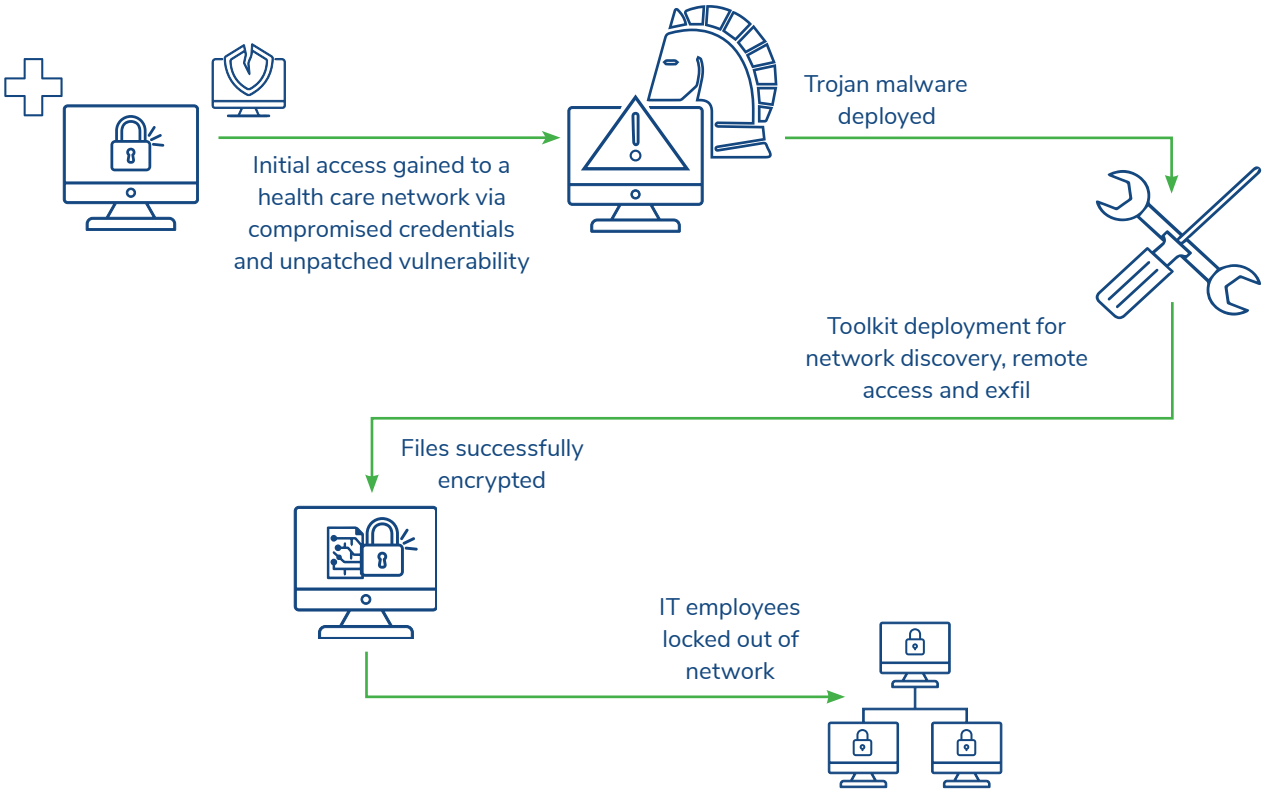
CASE STUDY
BLACKCAT Impacting Manufacturers

In one Kroll case during Q3, threat actors used valid credentials to log into the VPN services of a manufacturing company. In the month following the first unauthorized access, Kroll identified several suspicious logins where actors likely conducted network reconnaissance, at one point executing exfiltration via FileZilla. Nearly six weeks after the first malicious access, actors were observed returning to the system for a period of two days. During that time they used MegaSync to exfiltrate data, as well as tools such as Advanced IP Scanner for network discovery and MimiKatz for credential collection. Ultimately, the actors deployed the BLACKCAT payload as a new service creation. During access, actors exfiltrated nearly 600 GB of data which was later exposed on the threat actor site.



CASE STUDY
RHYSIDA Goes After Health Care Sector

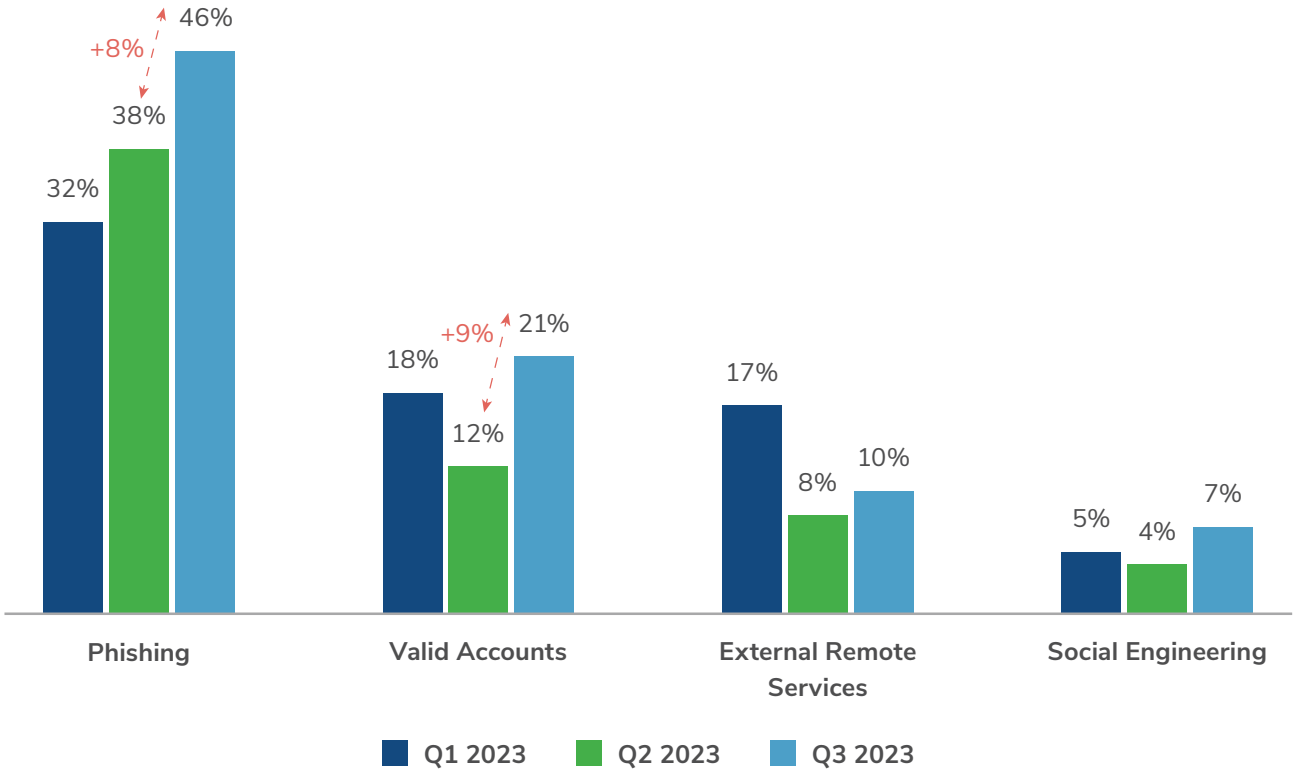
Warnings issued in early August by multiple government agencies indicated that a new ransomware group, RHYSIDA, was targeting the health care sector. Changing trends in Kroll engagements mirrored this report in the third quarter. In one case impacting a large health care organization, actors accessed the system using compromised credentials (also known as valid accounts) coupled with a vulnerability in the client's Citrix NetScaler environment. Shortly after access, the threat actors deployed SYSTEMBC, a Trojan malware that helps hide connections to a threat actor's command and control (C2) infrastructure. The actors used multiple tools during the incident, including Advanced Port Scanner for network discovery, AnyDesk for remote access and MegaSync for exfiltration. After files were successfully encrypted, the actors changed passwords to the system so that IT employees could not access the network.



Social Engineering Yields Initial Access

Social engineering, or what many refer to as "hacking humans," is a leading cause of network breaches and unauthorized access to remote systems. Kroll saw social engineering tactics increase dramatically in the third quarter, with significant increases in phishing (8%), valid accounts (9%) and voice phishing (vishing), as well as other tactics (3%).

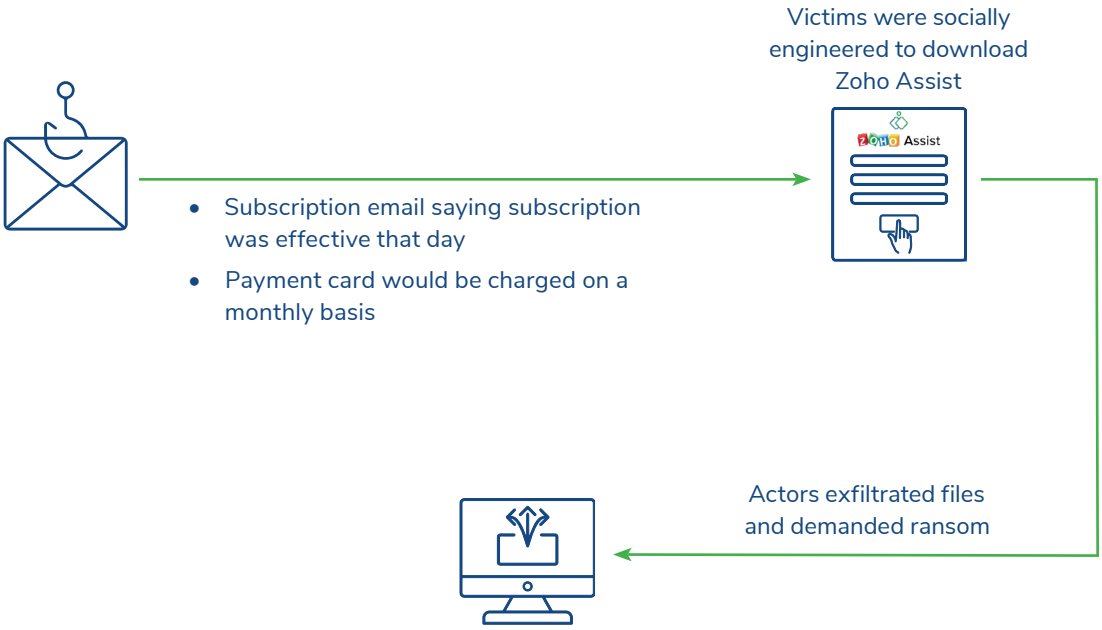
Top 4 Initial Access Methods - Past Three Quarters



This rise in social engineering activity aligns with multiple open source reports warning about these types of attacks via Microsoft Teams, and the rise of activity by the group KTA243 (SCATTERED SPIDER), which uses phone and SMS-based social engineering tactics to lure users into exposing their credentials.

CASE STUDY
Fitness Subscription Phishing Putting People in a Spin

In Q3, Kroll observed a number of cases where individuals from professional services firms received a fake email stating that their subscription for a popular fitness membership service was starting, effective that day, and that their payment card would be charged automatically on a monthly basis. In several cases, recipients responded to these prompts either by email or phone to indicate that they did not order such a subscription. From there, recipients were socially engineered to download Zoho Assist – a remote support software session. Once access was granted, actors exfiltrated files, then demanded a financial ransom to avoid data publication.



Malware Trends & Analysis

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.

Kroll Top 10 Malware Strains - Q3 2023

Q3 2023 Trend	Threat Name
↑ 1	COBALTSTRIKE
↑ 2	DARKGATE
↑ 3	NJRAT
↓ 4	REDLINESTEALER
→ 5	AGENTTESLA
↑ 6	ICEDID
↑ 7	PIKABOT
↑ 8	ASYNCRAT
↓ 9	RACCOON
↓ 10	AMADEY

A marked difference from the findings shared in our Q2 threat landscape report is the absence of QAKBOT in the top 10 malware list. This is because the FBI disrupted the infamous botnet in August. Kroll has been tracking QAKBOT for many years. Also known as QBOT, PINKSLIPBOT and QUAKBOT, it is typically delivered via malspam and has been observed using reply-chain thread-hijacking attacks for some time, in order to increase clickthrough rates. After consistent updates and new modules, QAKBOT was used as an initial entry vector for many ransomware groups, including CONTI, PROLOCK, EGREGOR, REVIL, MEGACORTEX and Black Basta. It is estimated that the botnet had infected 700,000 machines worldwide.

QAKBOT distributors, notably KTA248 (TA577), often took breaks throughout the year, and distribution of the malware dropped markedly from mid-June. The FBI disruption essentially cut communication with the command and control infrastructure layers of the botnet and issued an uninstall command to infected devices.

Since the QAKBOT disruption, Kroll has observed a rise in relatively unseen malware strains, such as DARKGATE and PIKABOT, while other open-source stealer malware trends remain consistent. This indicates that QAKBOT operators are looking for a new initial access malware to deploy.

Kroll recently observed cases of DARKGATE malware being delivered to several organizations in the transportation and hospitality sectors through Microsoft Teams messages. This activity has also been highlighted throughout open-source reporting, sharing a number of key indicators with Kroll observations, such as common filenames, adversary infrastructure and similar domain name convention to host the initial download.

Defending Against the Social Engineering Threat: Key Recommendations

With social engineering on the rise in Q3, it is critical that businesses take proactive steps to ensure that they have adequate defenses in place. As this type of threat continues to diversify, organizations need to be vigilant about identifying and addressing all potential areas of attack. This starts with applying a number of key security controls to improve overall security posture. Businesses should also consider the following steps:

Phishing and Unauthorized Access

- Provide regular training and awareness sessions for all users
- Ensure detection with URL rewriting via email protection
- Apply user behavior analytics, message trace logs, audit trace logs etc.
- Implement phishing-resistant authentication methods, such as devices enrolled in FIDO (Fast IDentity Online), especially for privileged users
- Review and update IT helpdesk policies and exception handling procedures to address social engineering attacks aimed at enrolling or disabling multi-factor authentication (MFA) and unauthorized devices
- Use creative Conditional Access control (CAC) policies to reduce your attack surface. For example:
  - If your corporate device policy only includes Windows for desktop and iOS mobile devices, block Android and MacBooks from authenticating
  - Disable or limit the scope of allowed MFA methods, such as SMS and voice approval, or unused MFA application types
  - Consider blocking or flagging authentication attempts and enrollment from geographies outside the scope of your organization's footprint
  - Limit the number of allowed MFA devices per user and require extra authentication factors when authorizing MFA devices
  - Review and reduce session token lifetimes and implement continuous access evaluation features (CAE) where available

Illicit Consent Grant

- Manage app consent policies
- Limit the apps users can consent to (or disable altogether). Any previously consented application will still have consent after making changes

Detection

- Use Microsoft 365 Defender portal (if licensed)
- Remove all Oauth consent grants
- Get AzureADPSPermissions.ps1

Familiar Threats Present Fresh Security Challenges

Our findings over the past two quarters highlight the fact that long-standing and sometimes more overlooked threats can quickly change in form and focus to become pressing security issues. While supply chain threats evolved in Q2 to become a key concern, social engineering followed a similar pattern in Q3. 'Human hacking' has proven to be threat actors' approach of choice over the past few months, adding further complexity to an already turbulent threat landscape. With diverse forms of social engineering now being leveraged, businesses must ensure that they have the up-to-date capabilities required to defend against them.

A look back at Q3 2022 illustrates how dramatically security conditions can change. The situation has shifted from a decline in ransomware attacks in 2022 to the current climate in which ransomware groups both new and old are adopting fresh tactics. Similarly, while email compromise plateaued in Q3 last year, it is rising across all sectors one year on. Another critical change from 2022 to 2023 is that global socio-economic conditions have increased in volatility, with the potential to impact on the cybersecurity status of businesses in many industries. Indeed, our findings from Q1 and Q2 2023 pointed to a continuation of fraught security conditions, due to the splintering of large ransomware groups and other shifts. This has been borne out by the trends we observed in Q3 and shows no sign of abating in the final quarter of 2023 and beyond.

The challenge is not just external. As shown in other recent Kroll analysis, organizations are not only at risk from evolving threats but also from their own perception of their readiness to address those threats. By working with a trusted and field-proven security partner, businesses can ensure they are prepared to respond effectively to the challenges that lie ahead. Working toward true cyber maturity will ensure that organizations are better equipped to defend both against novel security challenges and the resurgence and reinvention of familiar threats.

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.