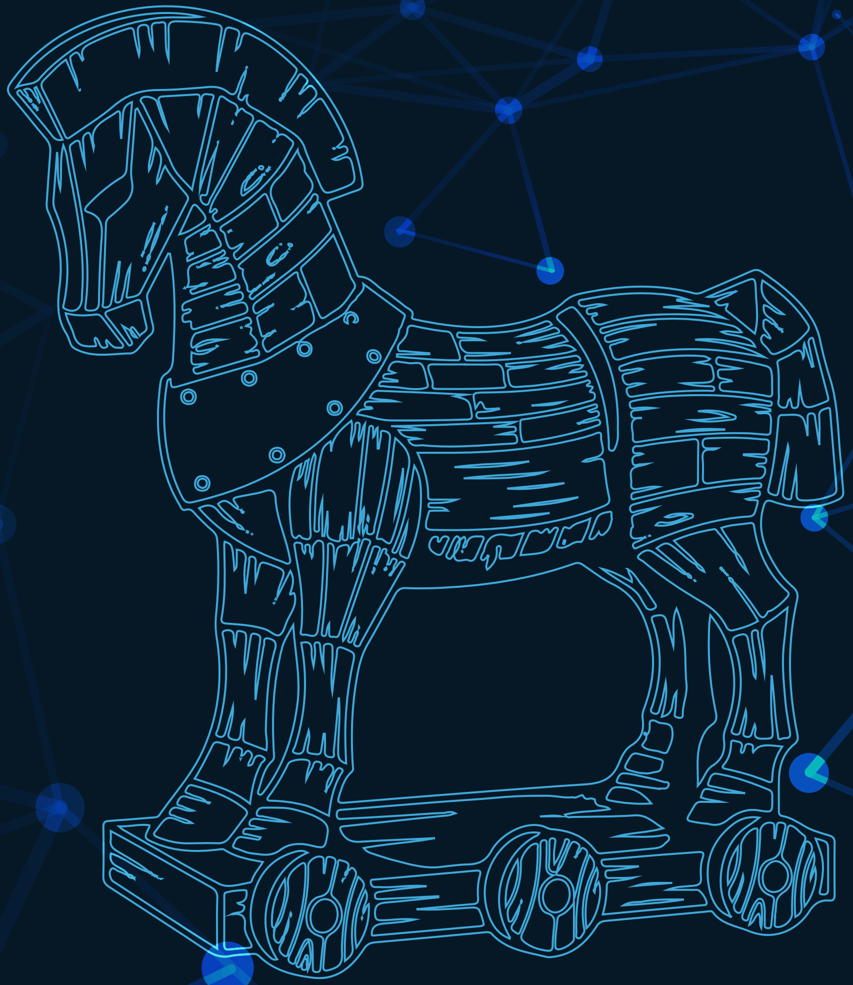
KROLL

Q3 2022 Threat Landscape:

Insider Threat, The Trojan Horse of 2022



Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022

Authors

Laurie Iacono

Keith Wojcieszek

George Glass

In Q3 2022, Kroll saw insider threat peak to its highest quarterly level to date, accounting for nearly 35% of all unauthorized access threat incidents. Kroll also observed a number of malware infections via USB this quarter, potentially pointing to wider external factors that may encourage insider threat, such as an increasingly fluid labor market and economic turbulence.

Kroll also saw an increase in general malware as a threat incident type, fueled by the proliferation of information stealing malware such as URSA, Vidar and Raccoon, among others.

With the widespread use of info-stealer malware, it may come as no surprise that Kroll continues to see valid accounts used to gain an initial foothold into a network. This shows that, in many cases, threat actors are using legitimate credentials to access and authenticate into systems.

Q3 2022 Threat Timeline

Jul 8

LockBit 3.0 Unveiled: LockBit 3.0, the first ransomware bug bounty program, is released. Many new extortion tactics are added to its repertoire, and bounty payments for improvements or vulnerabilities are advertised.

Jul 28

New MFA Bypass Phishing Method: A new phishing tactic that exploits the Microsoft Edge WebView2 control is released. Threat actors exploit WebView2 in order to steal cookies and credentials after a user has successfully logged in, bypassing MFA and gaining full access.

Aug 2

Increase in Vishing and Smishing Attacks: An increase in phishing attacks was observed, specifically vishing and smishing attacks in which threat actors attempt to gain valuable personal information for financial gain through phone calls, voice altering software, text messages and other tools.

Aug 24

WordPress Sites Hacked: Hacked WordPress sites are changed to display fake Cloudflare DDoS protection pages.

Sep 6

Vice Society Ransomware Attacks on School Districts: U.S. school districts are increasingly targeted by the Vice Society ransomware group. The FBI, CISA and the MS-ISAC advise that attacks against the education sector could potentially increase during the 2022 to 2023 school year.

Sep 30

Microsoft ProxyNotShell Vulnerability: At the end of Q3, a new exploit now known as ProxyNotShell is released based on two vulnerabilities, CVE-2022-41040 and CVE-2022-41082. The new exploit uses a similar chained attack to that in the 2021 ProxyShell exploit, which we covered in the Q4 Quarterly Threat Landscape Report 2021 and Q1 Quarterly Threat Landscape Report 2022 and continue to see used in attacks.

Insider Threats and Rapidly Evolving Market Conditions

Dubbed the “great resignation” by many media outlets, 2021 and early 2022 saw the rise of employees seeking new opportunities in the wake of the COVID-19 pandemic and the shift to remote work. This has been encouraged by the growth in supply of potential employment, with the Organization for Economic Co-operation and Development (OECD) registering an overall net gain of more than 9 million jobs in June 2022 for OECD countries, compared to pre-pandemic levels.

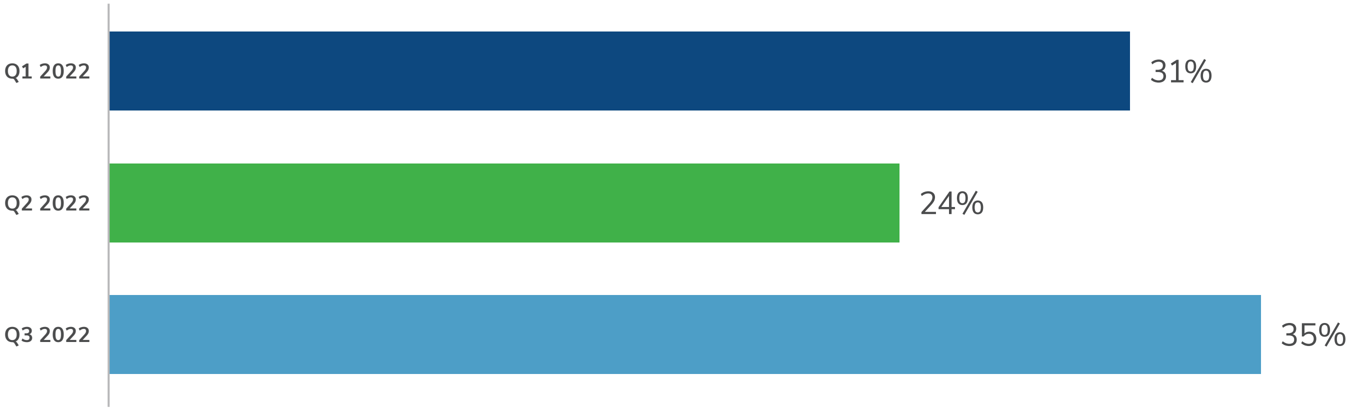
While always a challenge, the risk of insider threat is particularly high during the employee termination process. Disgruntled employees may seek to steal data or company secrets to publicly undermine an organization, while other employees may seek to move over data–such as contacts lists and other proprietary documents–that they can leverage at their new organizations.

Case Study: In the Firing Line for Data Theft

Many of the cases Kroll observed in Q3 coincided with the employee termination process. In one example, an employee attempted to steal gigabytes worth of data by copying it over to cloud storage networks. In this instance, the company followed a standard protocol that included disabling the user’s accounts and deleting data from cloud storage accounts accessible to them. Months after the employee left for a competitor, the organization began to suspect that the individual was using company data at their new position in order to enhance sales efforts. A review of the individual’s personal laptop identified that they had created copies of company data on multiple cloud storage accounts and personal data storage devices when they still had access to the corporate network. A review of the individual’s web browser history also identified multiple searches related to personal cloud storage and deleting log files.

Through forensic analysis, Kroll was able to create a timeline of activity showing the movement of confidential files across multiple personal emails, cloud storage accounts and physical devices. Activity largely coincided with suspicious search terms, such as deleting log files, indicating that the user knew the activity was wrong and made a deliberate effort to cover their tracks.

Unauthorized Access Cases Related to Insider Threat (% of total)



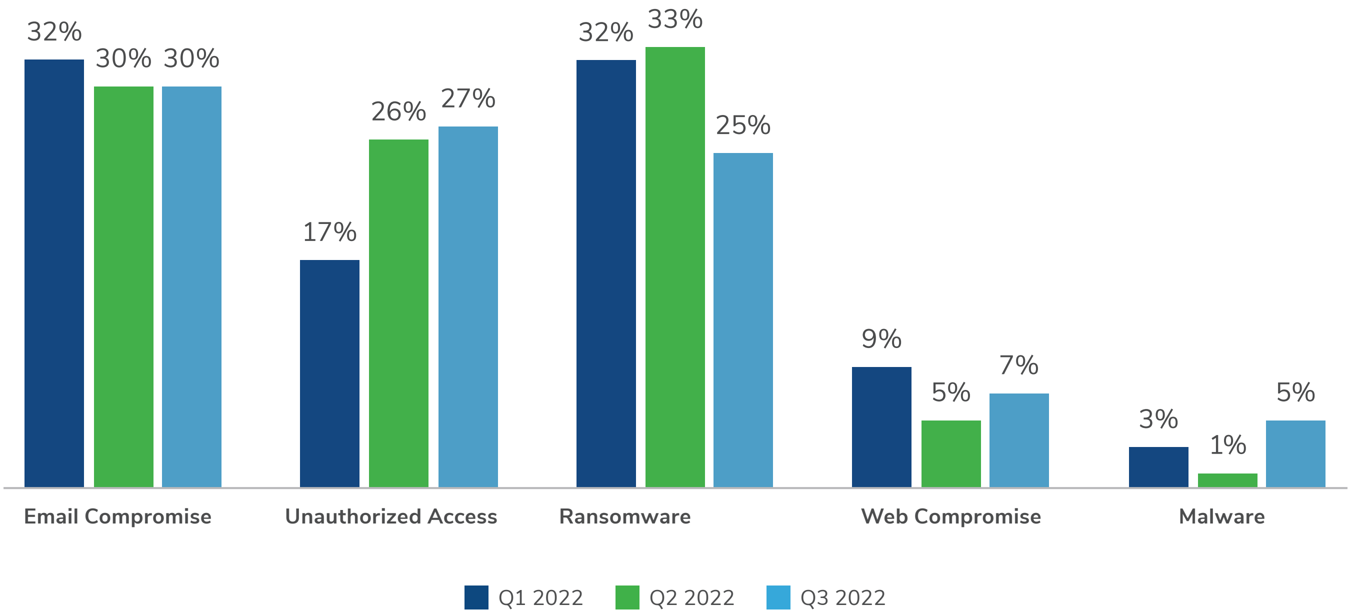
> “Insider threat is a unique problem in cybersecurity, Unlike the usual circumstances in cyber security, where you are defending the network from (at least in the initial attack stage) external attackers, in an insider threat situation, you are defending the business from someone on the inside. This can be particularly difficult, as the user often won’t raise any red flags and could have a high level of permissions and access rights.
>
> The only way you may be able to identify the threat in flight is through suspicious behavior, such as detecting mass downloads or uploads. This therefore makes file and folder access auditing—in addition to logging on-file transfer services—particularly important for tracking, especially within regulated industries or with servers containing sensitive data. Failure to monitor closely could mean that the real damage has already been done by the time you recognize an incident has occurred.”

— **Jaycee Roth**, Associate Managing Director,
Cyber Risk, Kroll

Threat Incidents: Malware Jumps, Insider Threat Soars

With email compromise plateauing at 30% and the ratio of overall ransomware attacks declining in the third quarter, Kroll observed modest increases in other threat incident types, such as unauthorized access (27%), web compromise (7%) and malware (5%).

Most Popular Threat Incident Types



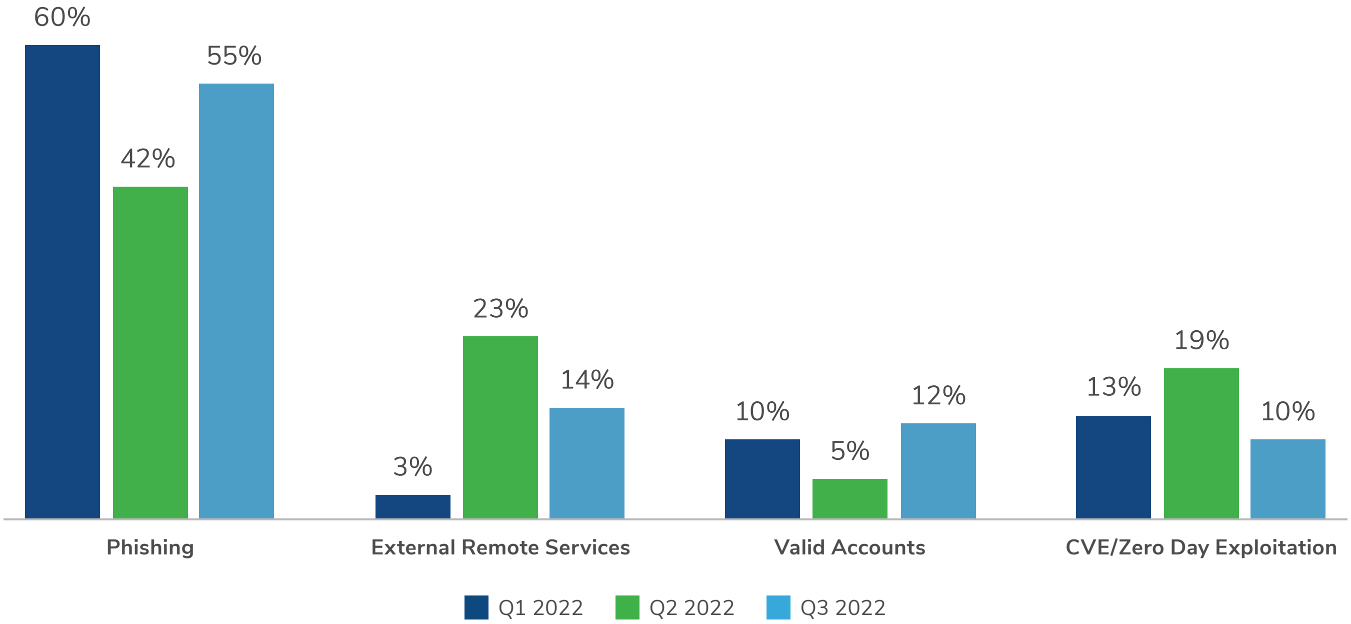
After declining in Q2, web compromise saw a small uptick in Q3. Kroll's experts note that web compromises impacting small- to medium-sized e-commerce websites have been on the rise since the onset of the COVID-19 pandemic, when many brick-and-mortar stores had to either partially or completely move their sales efforts to e-commerce platforms. In many of these instances, cyber security may have taken a backseat as merchants worked to maintain sales amid lockdowns. Although there is not one singular vulnerability related to this activity, Kroll has frequently observed actors taking advantage of e-commerce sites which have little to no capability to identify malicious activity and a lack of robust back-ups or patch management systems. In extreme cases where the actor has been on the system for a long time, many businesses are having to rebuild their sites from scratch to ensure security mechanisms and proper logging are in place.

Malware (excluding ransomware) saw a jump from 1% in Q2 to 5% of cases in Q3. This increase is likely linked to the proliferation of information stealing malware such as Redline, Raccoon, Vidar and URSA. These types of malware, also known as "info-stealers," are typically spread through phishing campaigns. Once a victim's machine is infected, the malware is able to target and steal a variety of data, including browser histories, device fingerprints, login credentials and financial data. Information from this malware is often sold on credential markets where a user may buy a listing that gives them access from a compromised computer from which they can then log an attack. It is also widely believed that information gained through this type of malware helps to fuel the activities of initial access brokers operating in the ransomware ecosphere by providing legitimate credentials for access into corporate networks.

Threat Actors Targeting Credentials for Initial Access

In Q3, Kroll observed an uptick in phishing and the use of valid accounts as a vector for initial access. Kroll saw a rise in phishing lures being sent via text message—known as "smishing"—where threat actors sent the malicious payload via a container file instead of an Office document (e.g., .ISO instead of .docx or .word) and instances where, in lieu of a link, cybercriminals used social engineering to dupe victims into calling a phone number from which a fraudulent call center would walk them through the installation of malware of a remote management tool.

Most Popular Initial Access Methods - Past Three Quarters



Valid accounts for initial access was another area in which Kroll observed growth from Q2 to Q3, which is where legitimate credentials are used to access an account. Cybercriminals using this method may take over an account in several different ways, such as purchasing credentials from information-stealing malware or credential-stuffing attacks.

Case Study: Credential Stealing Malware via Email

In one case observed by Kroll, a victim received a phishing email prompting the recipient to download banking software from what appeared to be a well-known financial institution. In reality, the user was downloading the banking portal module feature of URSA malware.

Once downloaded, the banking portal module is configured to display fake windows any time users attempt to connect to one of the legitimate financial organizations that the malware targets for credential-stealing. To the end-user, the portals appear to be legitimate. Users are prompted to enter information, such as credentials and MFA tokens, which is then stolen by the threat actors and used to access the legitimate banking site. In this instance, while the user interacted with the actor-controlled banking module, threat actors used the credentials to attempt two large transactions, one of which was successfully executed for upward of $100,000.

> **“The combination of fake windows, portals and credential-stealing malware makes for a difficult scam for users to identify. Once they’ve fallen victim to the initial phishing attack, the process looks incredibly similar to the legitimate website, and consequently many will enter their credentials as usual. While it goes without saying that being vigilant to potential phishing attacks will reduce the chances of this type of attack being successful, it’s also important to pay close attention to your accounts so that you can urgently advise your bank of transactions you don’t recognize.”**
>
> — **Mark Johnson**, Senior Vice President,
> Cyber Risk, Kroll

A Rise in Attacks via USB

In recent months, Kroll has observed an increase in USB-based malware cases targeting clients. Over the past two years, due to the pandemic, the hybrid work model has increased in use among many organizations. This change resulted in many employees starting to utilize their own devices to carry out their day-to-day tasks, using USBs to transfer data from one device to another. In Q3 2022, threat actors and cybercriminal groups were observed sending and dropping USB drives to victims' offices with the intention of operators gaining access to their devices after the USB drives were plugged in.

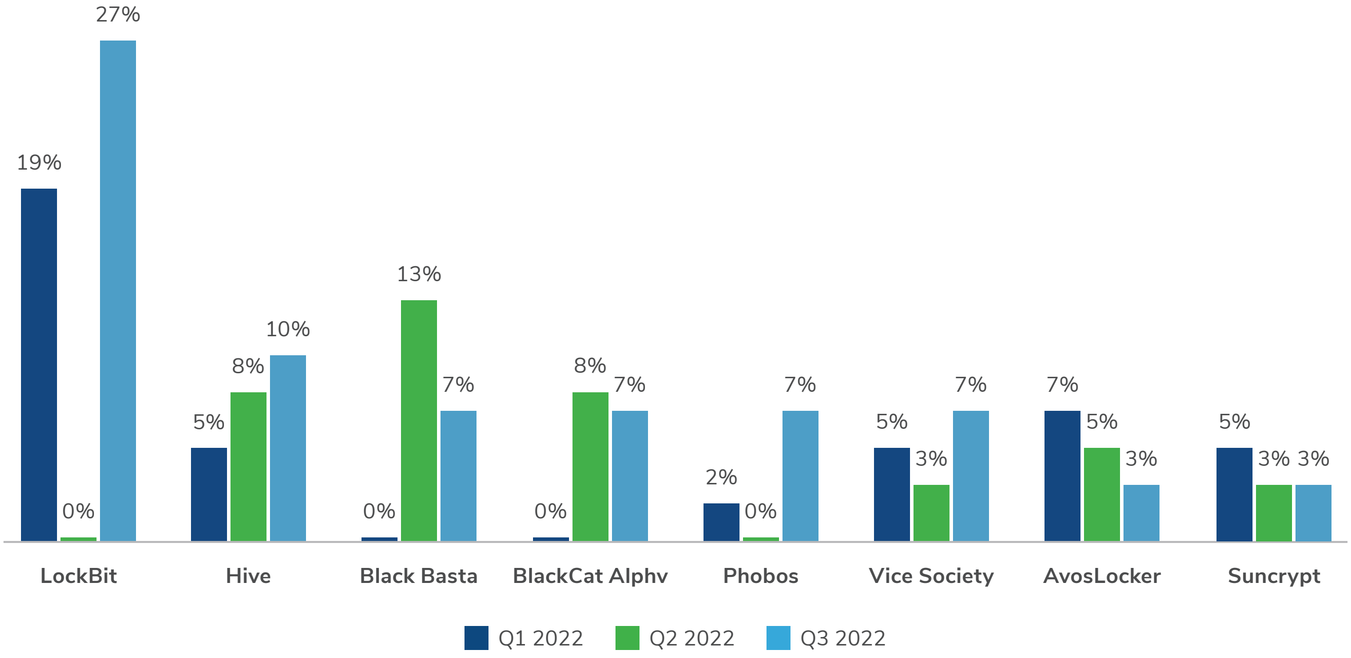
Kroll has worked on a number of cases where a USB device was found to be the initial access vector. In one case, an infected USB device contained multiple malware strains which ultimately attempted to install a cryptominer on the user's system. Fortunately, the endpoint detection and response tool was able to identify the suspicious activity before it could be installed.

Kroll also identified infections from USB devices containing .LNK files which, when clicked, run an MSI installer process to fetch and install RaspberryRobin, a malware strain typically distributed via USB drive.

Ransomware Activity: Variable but Impactful

With Conti officially shutting down their actor-controlled site on June 23, the official release of LockBit 3.0 dominated the ransomware headlines in the first part of Q3. Against this backdrop, Kroll saw its incidence of LockBit cases increase dramatically during the quarter.

Most Popular Ransomware Variants - Past Three Quarters



By the end of Q3, LockBit, which once recruited insiders to help them launch malware, found themselves dealing with their own insider leak as the builder for LockBit 3.0 was leaked on GitHub. Likely to have been leaked by a former member dissatisfied with financial proceeds, researchers identified attacks leveraging the builder within two to three days of the leak.

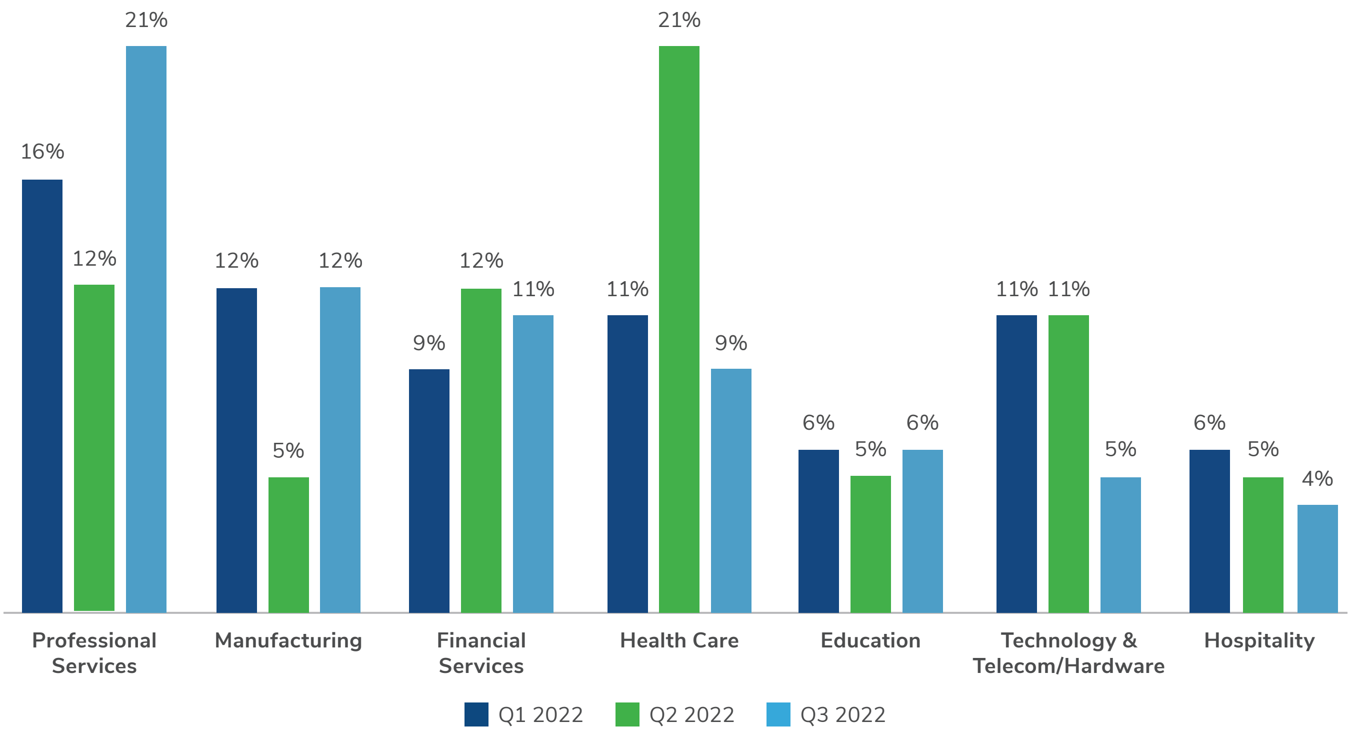
Meanwhile, as students across the globe transitioned back to classes, multiple ransomware groups, including Hive and Vice Society, targeted the education sector with high-profile ransomware attacks. In Q3, the education sector accounted for nearly 10% of all ransomware attacks, second only to manufacturing (12%). Similar to last quarter, CVE/Zero-Day Exploitation (33%) and External Remote Services (22%) were the most likely initial access methods for ransomware attacks.

Sector Analysis: Professional Services Sees Sharp Rise in Attacks

Professional services overtook health care as the most targeted sector overall in Q3, accounting for 21% of all Kroll cases, compared with just 12% in Q2. Common threat incident types impacting professional services included email compromise (40%), unauthorized access (27%) and ransomware (10%).

It is positive to see a reduction in attacks on a number of sectors such as technology and telecoms, hospitality and financial services in comparison with the previous quarter. However, the speed and volume of the changes in attack levels observed quarter to quarter throughout 2022 highlight that organizations in all sectors must ensure they are taking appropriate steps to maintain a robust security posture.

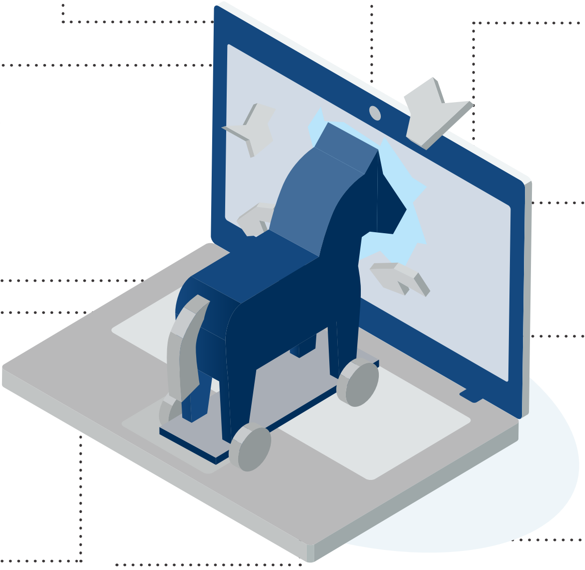
Most Targeted Industry Sectors - Past Three Quarters



Best Practices for Defending Against Insider and Physical Threats

To protect against and detect insider threats, our experts recommend users to:

- Deploy, manage and monitor Endpoint Detection & Response (EDR) sensors to all endpoints within the network
- Communicate with physical security operations centers and/or investigation teams to collaborate and share data
- Conduct robust logging and random auditing of active directory or other privileged access credentials
- Disable USBs and other external peripheral devices from company-owned devices



- Use canary or honey tokens throughout corporate infrastructure
- Integrate checks of cyber security program elements into your internal audit and compliance programs to assure that they are working as intended
- Require employees to use only company-approved devices and systems
- Restrict physical and electronic access immediately for any departing employees
- Maintain restrictions for using social networking sites and non-corporate email on company devices
- Employ digital risk protection solutions such as Kroll’s CyberDetectER® DarkWeb that continuously monitors at-risk data
- Watch for early warning indicators that include remote access during off-hours, unexplained exporting of large amounts of data and never taking a vacation

Recognizing the Threat Within

The number of positive trends in Q3, such as a plateau in email compromise and a decline in ransomware attacks, have been overshadowed by the significant rise in insider threats. Impacts from the pandemic are still being felt as a more fluid labor market and continued high levels of remote or hybrid working influences the threat landscape. Organizations are under greater pressure than ever to assess their potential security threats from multiple perspectives, including both external threats and those hidden within the organization.

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.