KROLL

Q4 2021 Threat Landscape:

Software Exploits Abound

Q4 2021 Threat Landscape: Software Exploits Abound

Authors

Laurie Iacono

Keith Wojcieszek

George Glass

In Q4 2021, Kroll observed a 356% increase in common vulnerabilities and exposures (CVEs) or zero-day vulnerabilities being exploited for initial access when compared to Q3 2021. With 2021 being a record year for vulnerabilities, this finding may not be surprising, but it underscores the risk to organizations in the wake of high-profile vulnerability notifications - and the speed with which cybercriminals are able to exploit weaknesses in companies' defences.

While significant progress was made during the quarter to disrupt significant cyber groups such as REvil and BlackMatter and multiple dark web markets, cyber threat activity levels did not see a substantial decline. Rather, by the end of December 2021, Kroll observed a spike in new actor-controlled ransomware sites and new ransomware variants as cybercriminals adapted and regrouped in the wake of these disruptions.

This spike of activity post-disruptions highlights the need for organizations to remain vigilant as cybercriminals rapidly evolve tactics to evade detection and mitigate the effects of disruption efforts.

Q4 2021 Threat Timeline

Oct 5 **Ransomware Disclosure Act** - A new U.S. bill from Senator Elizabeth Warren would mandate organizations to report within 48 hours when and how much they have paid to ransomware gangs.

Oct 17 **REvil takedown** - REvil ransomware site goes offline. At the time, actors associated with the variant reported that the gang's domains had been hacked. Subsequent reporting later that week indicated that a coordinated law enforcement operation was responsible for the takedown.

Nov 3 **BlackMatter closing** - The BlackMatter ransomware gang announced it was shutting down due to pressure from authorities.

Nov 8 **Kaseya Attack arrests** - The U.S. Department of Justice announced actions against two affiliates associated with distributing REvil ransomware, including the arrest of an actor alleged to be behind the July 2021 Kaseya supply chain attack.

Nov 15 **Return of Emotet** - After being shut down by law enforcement in January 2021, new Emotet activity is detected with the new Emotet botnets (dubbed Epoch4 & Epoch5) spamming and stealing emails for reply-chain attacks.

Nov 29 **Interpol's Operation HAECHI-II** - The coordinated arrest of over 1,000 individuals as part of a global drive to crack down on cybercrime led to significant intelligence-gathering on new threat trends, including the discovery of a malware-laden mobile app masquerading as a product affiliated with Netflix's "Squid Game".

Dec 2 **Zoho ManageEngine vulnerability warning** - The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory to highlight the cyber threat associated with the active exploitation of a newly identified vulnerability (CVE-2021-44077) in Zoho ManageEngine ServiceDesk Plus.

Dec 10 **Log4J vulnerability breaks the internet** - A critical vulnerability was discovered in the Apache Log4j Java logging library, allowing actors to exfiltrate sensitive information or execute malicious payloads on vulnerable victim application servers, potentially allowing complete access to a target network.

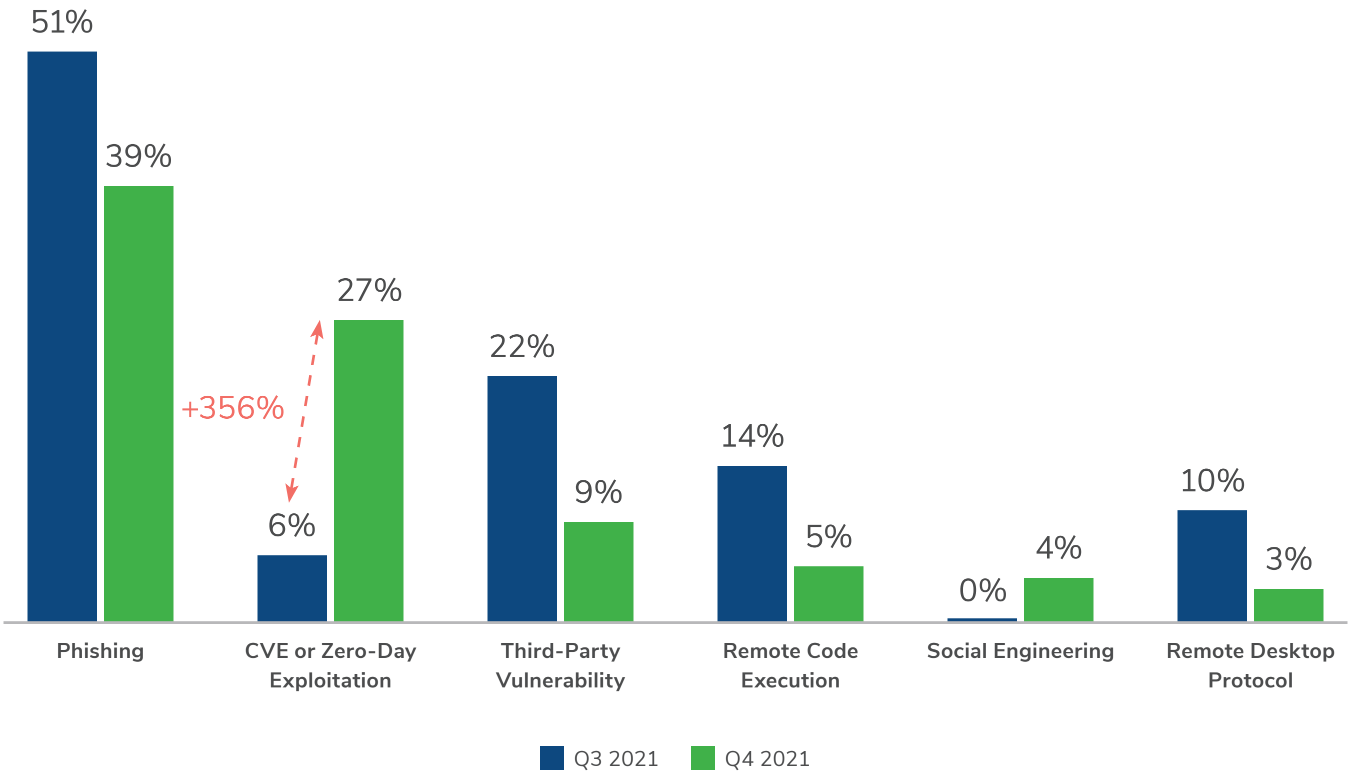
Dec 15 **Emotet attacks faster with Cobalt Strike** - The Emotet malware changes its way of working by directly installing Cobalt Strike beacons to devices already infected by Emotet to give threat actors immediate access to comprised networks.

CVE/Zero-Day Exploitation Hits All Time High

In early December 2021, Kroll's analysis of the National Vulnerability Database (NVD), the Common Vulnerability Database (CVD) repository of the U.S. National Institute of Standards and Technology, revealed that 2021 officially broke the record for common vulnerabilities and exposures (CVEs) logged by researchers.

By the end of December, Kroll observed the impact of this record-breaking year, as CVE/zero-day exploitation accounted for just over a quarter (26.9%) of initial access cases over the Q4 period, driven largely by vulnerabilities in ManageEngine, ProxyShell, VMWare, SonicWall and at the end of the quarter by Log4J. This was a 356% increase compared to the previous quarter.

Most Popular Initial Access Vectors - Q3 and Q4 2021



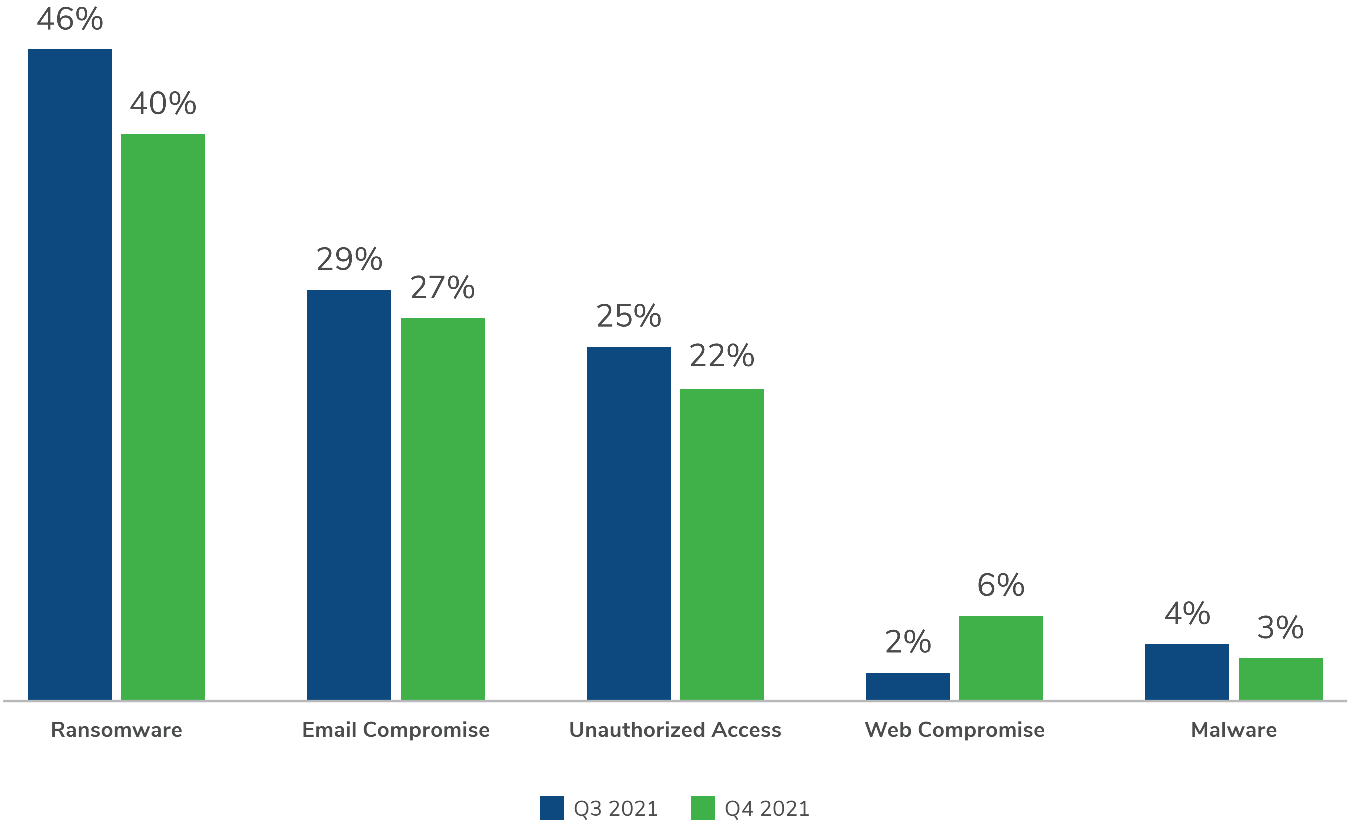
Despite the significant rise in CVE/zero-day exploitation for access, phishing attacks remained the most popular source of infection vector used by adversaries, accounting for 39% of all suspected initial access methods over the final quarter of 2021.

Third-party vulnerability (8.9%) and remote code execution (4.5%), though dropping slightly from Q3, also featured in the top five infection vectors in the quarter. Social engineering made its debut into the top five, also accounting for around 4% of infections.

> **“Phishing continues to be an incredibly effective method of attack. It relies on exploiting people rather than systems, which has led to a consistent number of business email compromise attacks, which are then used to deploy malware or to trick users into entering credentials on fake landing pages. Most of these attacks lead to significant financial and operational loss for victims.**
>
> **Another area at risk from adversaries is the supply chain, where smaller suppliers, who may provide a service to the larger company but generally have less sophisticated IT infrastructure and security systems in place, are attacked in an attempt to reach their end goal: the ‘big fish’.**
>
> **Multi-Factor Authentication (MFA) can be key to protecting against these sorts of attacks, yet it is concerning to see the number of organizations who still haven’t set it up, despite it being incredibly easy to enable on the majority of modern platforms.”**
>
> **— James Thoburn, Incident Response EMEA Team Leader at Kroll**

Ransomware Remains the Dominant Threat to Organizations

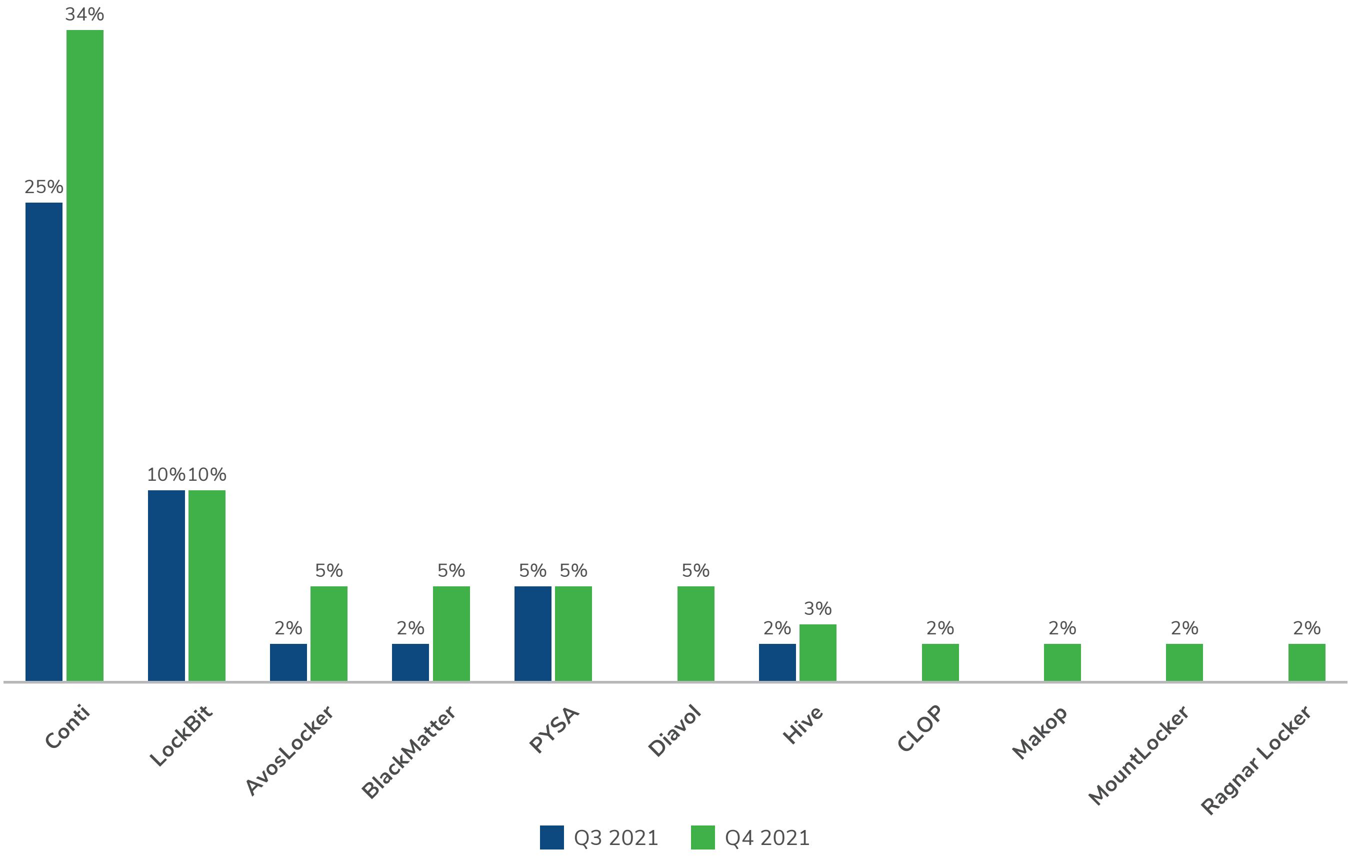
Most Popular Threat Incident Types - Q3 and Q4 2021



Ransomware (39.9%) was once again the most prominent threat type in Q4 despite a small decrease from the previous quarter. Email compromise (27.0%) and unauthorized access (21.7%) also remain popular methods of attack for adversaries in Q4, with the latter seeing activity double since Q1 2021. Web compromise also started to see an uptick in activity towards the end of Q4, rising in prevalence by almost 4% on the previous quarter.

Conti and LockBit were the top ransomware variants, with the Conti variant being by far the most active in Q4, accounting for more than a third of all incidents (33.9%). AvosLocker, BlackMatter, PYSA and the newcomer Diavol were close behind.

Most Popular Ransomware Variants - Q3 and Q4 2021



Emotet Comes Back to Life

The infrastructure of well-known banking Trojan malware Emotet was disrupted by law enforcement efforts in the first half of 2021. Unfortunately, in November 2021, Emotet returned to the spam scene, updated and refreshed with new capabilities.

While Emotet's initial attack method did not appear to change significantly, small alterations in the command and control (C2) protocol from RC4 to base64 and XOR encoding were identified, while the number of commands changed from four to seven, and dozens of new infections were identified in the first 24 hours alone. A month later, it became an even more serious threat as it started deploying Cobalt Strike beacons directly, giving immediate network access to threat actors and making ransomware attacks imminent and giving defenders less time to react to intrusions.

Based on previous trends, Emotet is likely to target multiple different sectors as we head into 2022.

Case Study: Email Thread Hijacking

Kroll observed a new email thread hijacking campaign in Q4, this one targeting victims via the ProxyShell vulnerability to retrieve and send spam emails via a victim's Microsoft Exchange API. We have observed this new tactic impacting multiple victims in multiple different sectors, with the spam campaigns attempting to deliver the SquirrelWaffle payload.

Kroll has previously reported on email thread hijacking campaigns propagated by Qakbot malware. Such campaigns send out emails that are responding to legacy email threads, increasing the legitimacy of such emails to evade email spam filters and to deceive the recipients into clicking on subsequent links or malicious attachments.

In one of the Kroll cases leveraging this tactic in Q4, Kroll's client indicated that one of its customers was reporting an influx of malicious emails coming from the client's domain address. Initial forensic review identifying the attack was difficult because this type of attack leveraged the Exchange API in a way Kroll had never observed before in the wild.

Ultimately, Kroll examiners identified several different logs within the client environment showing that the attacker was leveraging the Exchange API to retrieve and send the emails. Commands being issued by the adversaries such as "ResolveNames", "SearchMailbox", "FindItem", "GetItem", and "CreateItem" were types that would normally be seen as part of daily business activity. Yet, in this case, the adversaries were manipulating the Exchange API to access and download email data.

A forensic review later identified that the adversaries had been scanning the system for Exchange vulnerabilities for weeks leading up to the attack and initiated the attack less than 24 hours after the client upgraded an Exchange version that had the software vulnerability. In turn, the client was unable to identify that their business email had been compromised, as the new system had not been fully patched, and the hijack was invisible on their side.

“With the constant evolution of cyber threats, all firms should look into the real possibility that they will be targeted and weigh the risks involved in defending their assets.

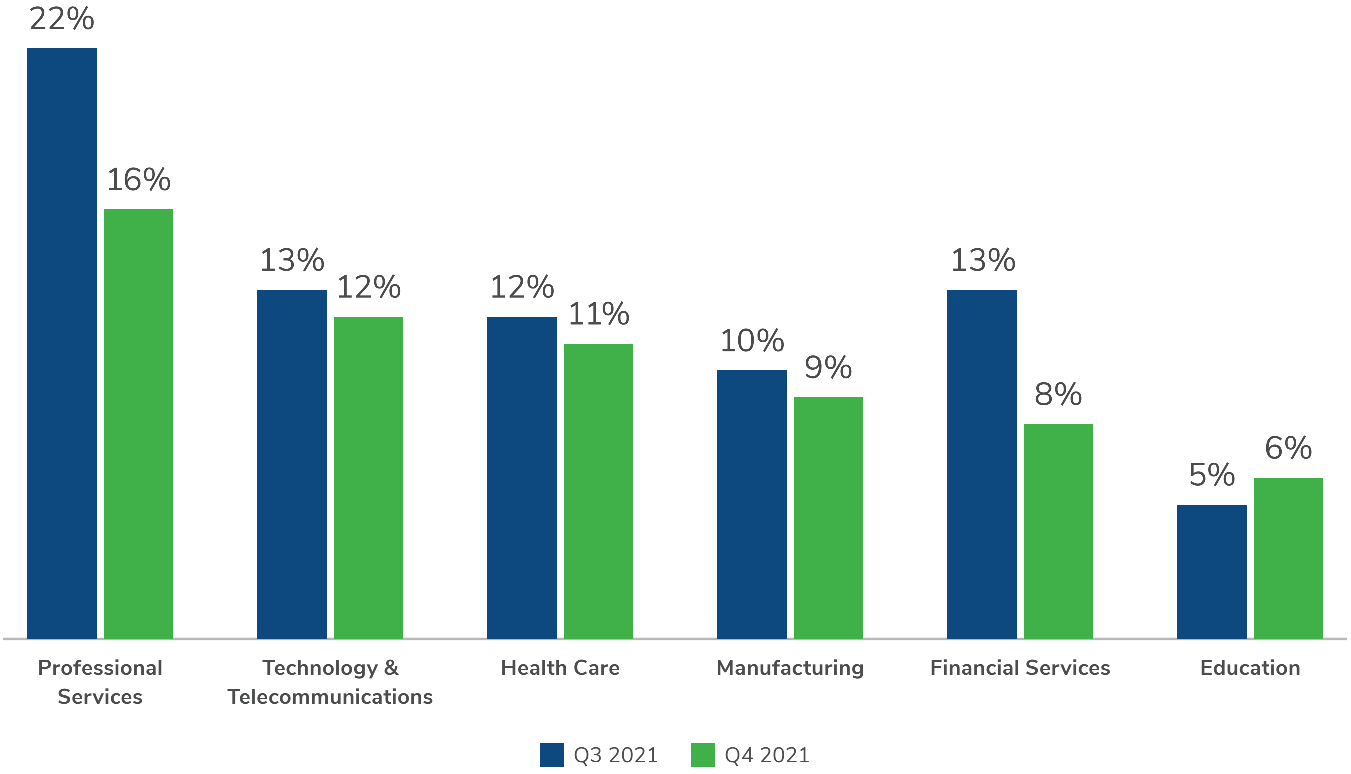
With this particular method of intrusion, a way for companies to ensure they are prepared is to shorten their patch testing windows, especially given the rise in zero-day vulnerabilities. When a patch is issued, some firms will test that patch for up to six months until they are comfortable to deploy, yet we are seeing cases where vulnerabilities were exploited on the same day a patch comes out. Depending on the asset, this window needs to be shorter; companies need to do a better job of understanding their assets and applying the proper risk tolerance.

When reviewing an organization’s patch management process, the risks to consider include the likelihood that a bad actor can identify the vulnerability, the severity of the vulnerability, and whether any compensating controls exist. When shortening the patch cycle isn’t feasible, look to disable the impacted services, implement rules at your perimeter to prevent communication with the service, and implement monitoring of the impacted service to enable you to act quickly to mitigate the potential exposure to your business.”

— Dan Ryan, Associate Managing Director at Kroll

Professional Services Sector Remains Top Target, Attacks on Education Increase

Most Targeted Sectors - Q3 and Q4 2021



The professional services sector once again remained the most targeted sector overall in Q4, accounting for 16% of cases, despite a slight dip of almost 6% on last quarter's figures.

Overall, the top five targeted sectors (professional services, technology/ telecommunications, health care, manufacturing and financial services), were unchanged from Q3 to Q4. Phishing continued to be the top threat for four of the top five sectors, apart from tech firms, where the main threat was CVE/zero-day exploitation. CVE/zero-day exploitation was also the top reported Initial Access Method for the government/public sector in Q4.

Across the board, an increase in attacks was seen in the education (6% of attacks), pharmaceutical (5%), construction (4%), and food and agriculture (4%) sectors, even though they each accounted for a relatively small amount of the incidents. Ransomware was the most significant threat to all of these sectors except education, where unauthorized access was primarily used to infiltrate systems. This is likely due to the more open IT infrastructures that we see in the education sector and because the fourth quarter in particular coincides with the new academic year in North America and Europe, making access to systems a key target at this time for threat actors.

Wrapping Up Another Tough Year in Cyber

In Q4 2021, cybercriminals demonstrated how quickly they can adapt and evolve to overcome disruption efforts and develop new ways and methods to exploit published vulnerabilities and inflict damage on unpatched devices at ever-increasing speeds.

CVE/zero-day exploitation gained significant ground as an initial access method over the last quarter of the year, and the volume of incidents using this tactic is likely to increase in 2022 as threat actors use more sophisticated methods to spread malware and evade detection.

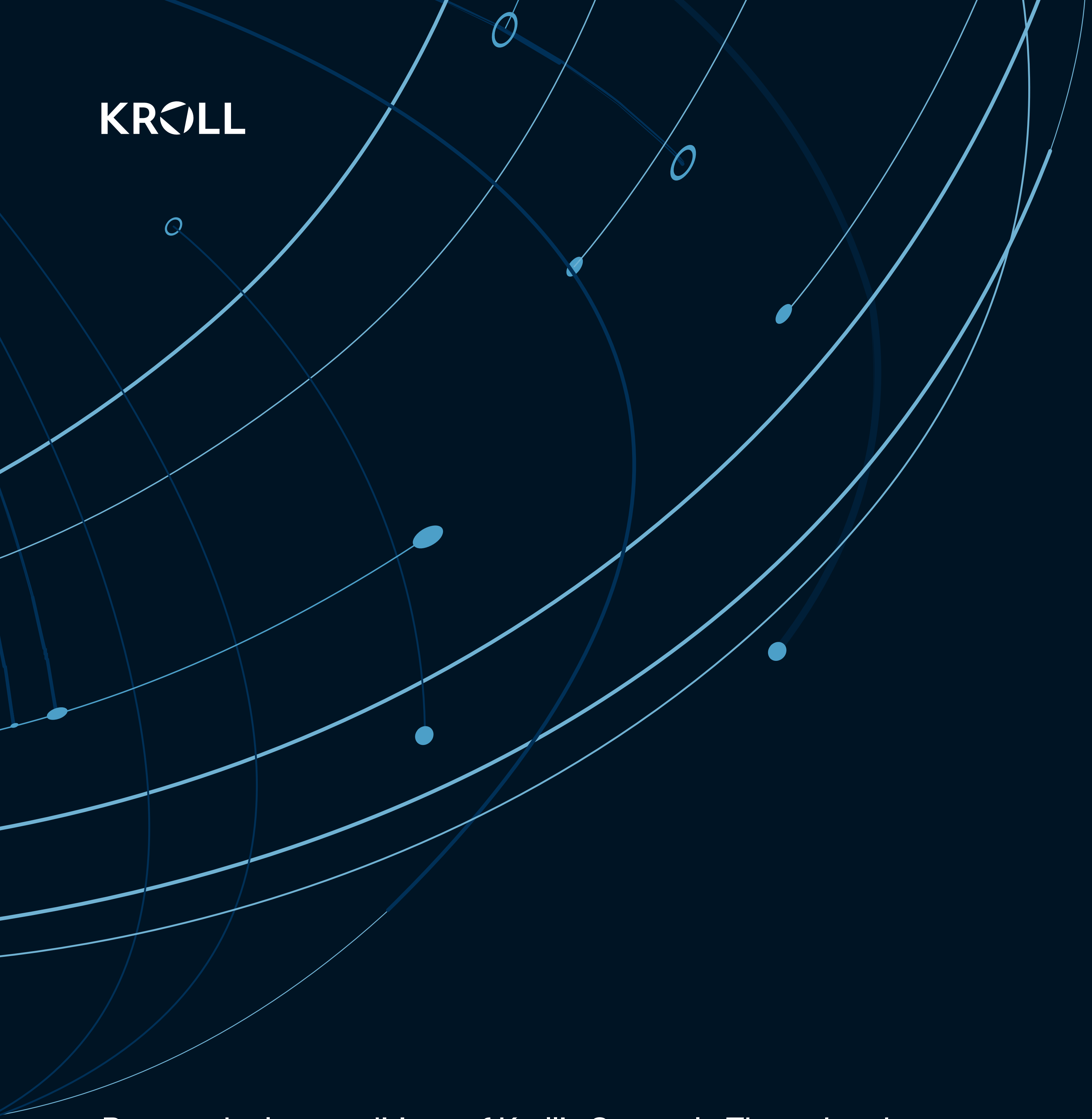
Previously unseen methods of email thread hijacking using ProxyShell to propagate malspam via the Exchange API were also identified in Q4 2021, further highlighting the evolving levels of sophistication and efficacy that adversaries are reaching. Similar attacks are likely to be witnessed in 2022 and beyond.

Like any other quarter, unrelenting cybercriminal attacks highlight the need for all organizations to improve their security posture, particularly around Essential Cyber Security Controls such as multifactor authentication, security culture training and email hygiene.

Trends around CVE/zero-day exploitation and active email thread hijacking campaigns underscore the need for organizations to implement the following:

- A robust vulnerability management plan to prioritize and install patching updates
- Regular user education and phishing assessments
- A series of proactive measures, such as penetration tests and red teaming, to check for vulnerabilities that threat actors could exploit
- Endpoint detection and response (EDR) technologies to look for suspicious behavior within an organization's IT environments
- Thoroughly prepared and tested plans for a fast and effective response to security incidents

The events in Q4 2021 highlighted the rapid evolution of adversaries, not just in terms of the actors themselves, but also in the vulnerabilities they exploit. Businesses must use actionable threat intelligence to guide the management and prioritization of these vulnerabilities and ensure they have a strong managed detection and response program in place. In the event of attackers managing to breach an organization's systems, such a program brings great benefits, including allowing for fast validation, containment of the threat and support with post-incident recovery.



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

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.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 Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India