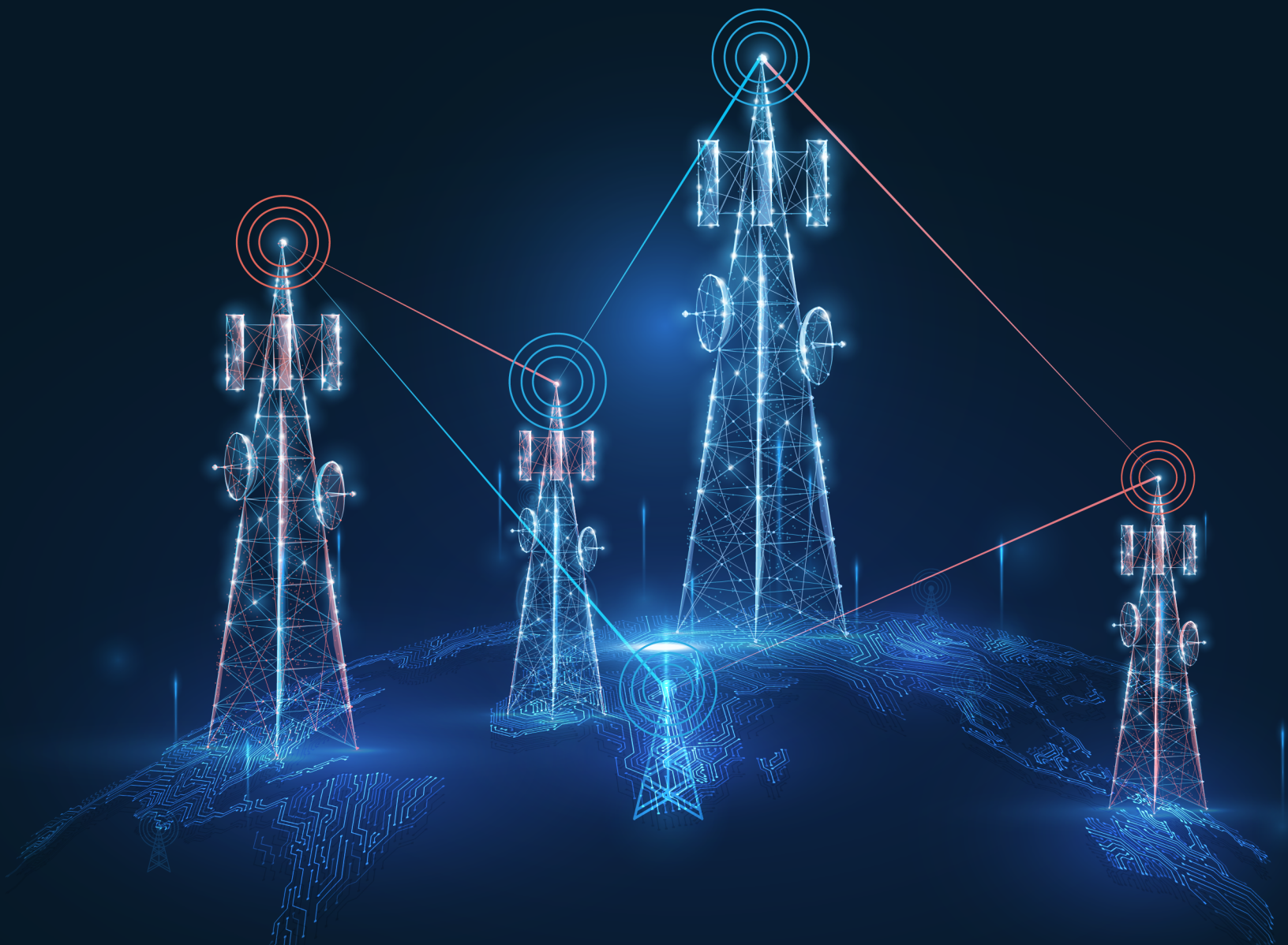
KROLL

Q3 2024 Threat Landscape Report:

Rising Attacks on Tech & Telecoms Reinforce Need for Business Continuity Planning



KROLL

Q3 2024 Threat Landscape Report:

Rising Attacks on Tech and Telecoms Reinforce Need for Business Continuity Planning

Authors

Laurie Iacono

George Glass

Keith Wojcieszek

A notable rise in attacks in Q3 2024 shows that threat actors are increasingly focusing on the tech and telecom sector. This finding aligns with the wider global pattern of attacks against technology companies. Insider threat significantly impacted the sector during the quarter, alongside email compromise and ransomware. The pressure remains on other industries, however, with professional services retaining its status as the sector most targeted by attackers, and four of the five key sectors experiencing an increase in attacks this quarter.

Other reasons to remain vigilant are the rise in nation-state actor activity and the diversification in form and techniques by various ransomware groups. Insider threat and email compromise remain key areas of risk for business, having been the most observed threats in Q3. In a quarter that was defined by the global disruption resulting from the CrowdStrike IT outage, our findings point to a complex and fast-moving threat landscape. Read the report to gain the full picture of the past quarter's security trends, plus recommendations to help your organization stay resilient.

Q3 2024 Threat Timeline

July

- On July 19, 2024, a change is pushed to CrowdStrike Falcon EDR sensor agents, causing crashes and "Blue Screen of Death" (BSOD) on Windows systems sending them into a boot loop as they try to load a faulty driver. The outage impacts critical operations across airports, hospitals, banks, critical national infrastructure and more.
- The PLAY ransomware group expand its tactics by introducing a Linux variant that targets VMWare ESXi environments, which are utilized by businesses to host multiple virtual machines to run and host data. This has the potential to increase victim targets that could lead to more lucrative ransom negotiations.

August

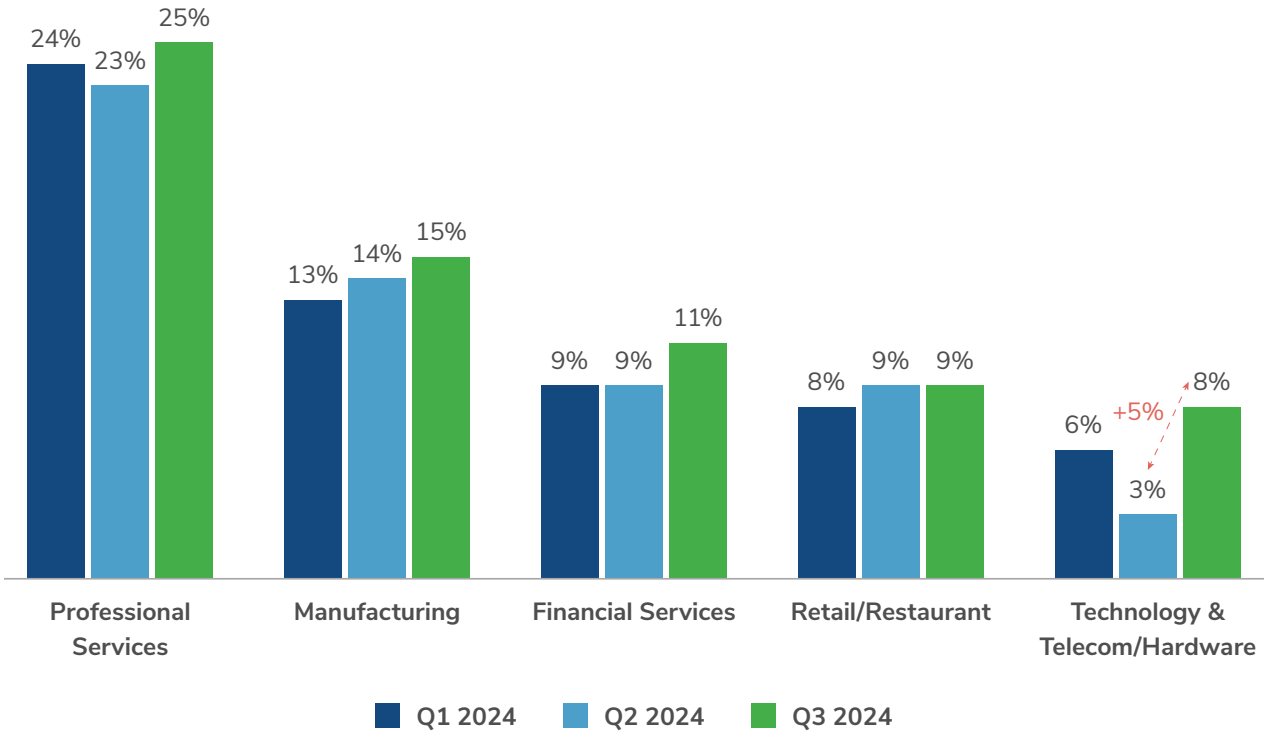
- South Korea's National Cyber Security Center (NCSC) releases a statement detailing that North Korean APT groups Kimsuky (KTA082) and Andariel (KTA116) are attacking organizations in the construction and machinery industries with the aim of stealing trade secrets.
- Microsoft Patch Tuesday addresses 6 Zero-Days, fixing 185 vulnerabilities in August's patch cycle and Microsoft Edge releases.
- A method of downgrading patches on Windows machines dubbed "Windows Downdate" is discovered and presented at BlackHat. Attacks leveraging these techniques may be used to target the Windows kernel or hypervisor. Microsoft acknowledged the vulnerabilities, issuing CVE-2024-21302 and CVE-2024-38202.

September

- On September 3, 2024, the Kroll Cyber Threat Intelligence (CTI) team report on CVE-2024-40755, a critical vulnerability in the SonicWall SonicOS management interface, which could lead to unauthorized access to resources and in certain scenarios, could result in a firewall crash. Kroll observes the CVE being exploited to deliver Akira ransomware.
- AI-generated malware is discovered delivering ASYNCRAT via phishing emails, with HTML smuggling and AES-encrypted attachments used to bypass detection.

Sector Spotlight: Technology and Telecoms Under Attack

Most Targeted Industry by Sector and Over the Past Three Quarters



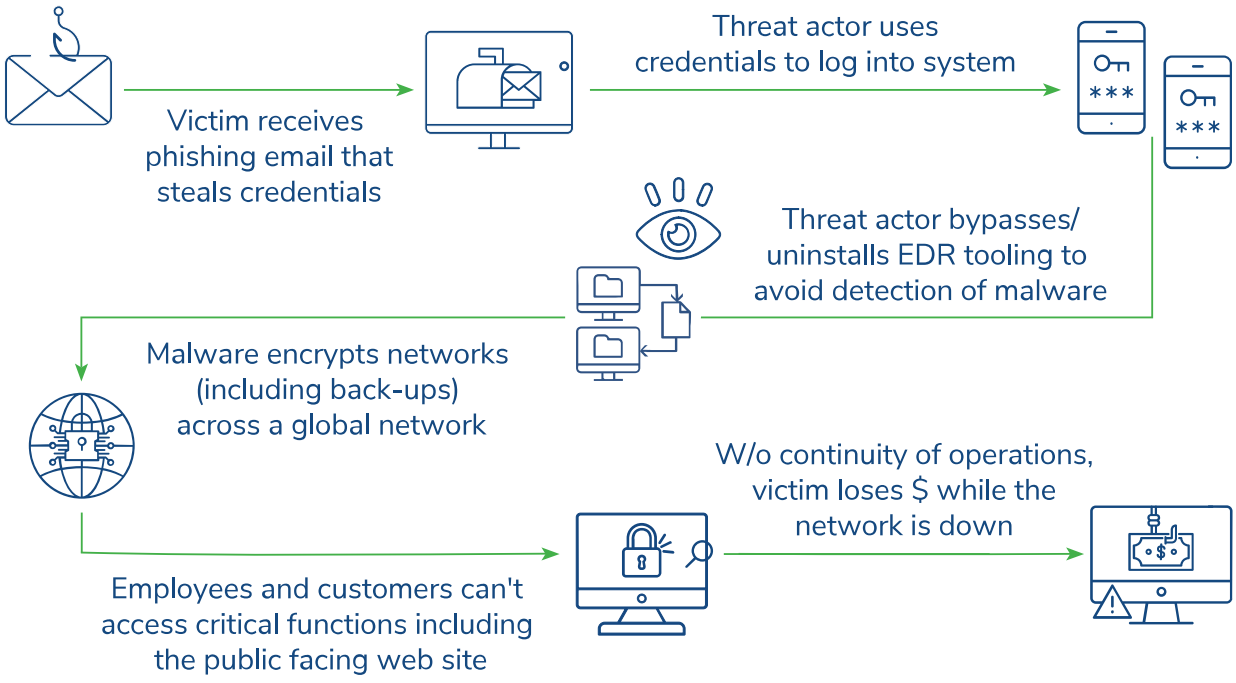
While Q3 2024 saw the professional services sector continue its long run as the industry most targeted by attackers, there was also an increase in attacks on the tech and telecoms sector. A jump of five percentage points compared with the previous quarter is particularly notable in a sector that has experienced relatively low levels of attacks in the past.

The fact that this significant change can occur in just one quarter is a reminder that shifts of this kind have the potential to happen fast in all industries. Four of the five key sectors have experienced an increase this quarter, with one other remaining at the same level as Q2. Although tech and telecoms is in the spotlight this time, overall trends point to the need for all industries to remain vigilant to the impact of evolving attacker tactics.

CASE STUDY
MEDUSA Puts Tech Firm on Pause

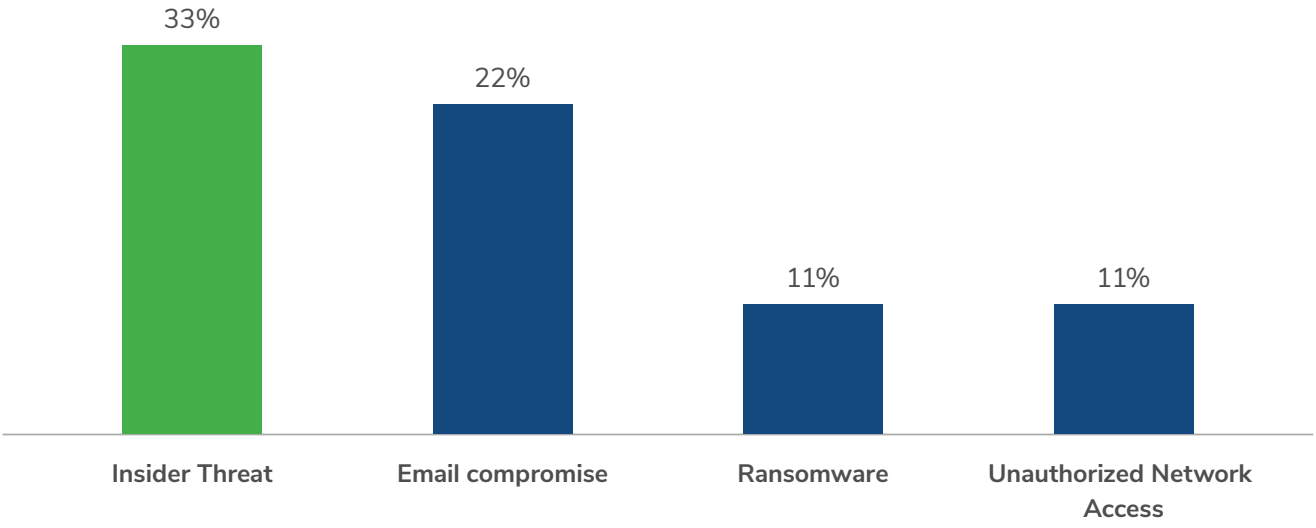
Kroll observed an electronics manufacturing firm hit by MEDUSA ransomware suffer nearly a week of downtime. During this attack, threat actors were observed bypassing at least one of the client's endpoint detection and response tools, which allowed the malware to spread across the network. Lack of visibility across the IT infrastructure also most likely played a role in the extended post-attack downtime and recovery period, highlighting the importance of understanding network infrastructure prior to an attack taking place.

Threat Actors Infiltrate Network Infrastructure



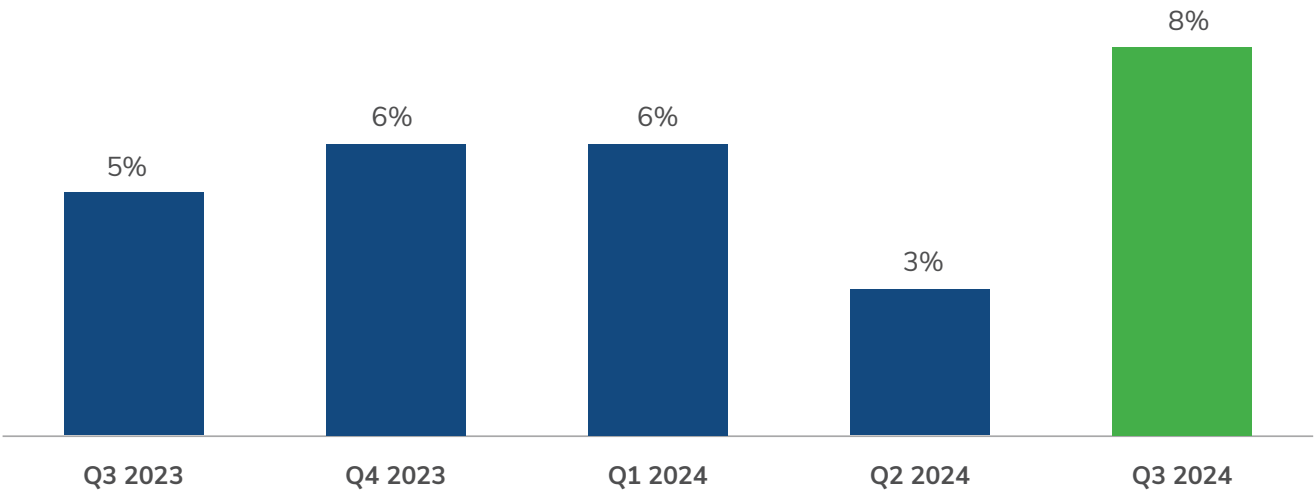
Diverse Threat Types Impacting Tech Sector

Q3 2024 Tech and Telecom Sector – Top 4 Threat Incident Types



Similar to reports from Q1, Kroll observed that insider threat is a significant risk factor for the tech and telecom sector. Email compromise and ransomware are also adding to the security challenges experienced by this industry.

Incident Response Cases in the Tech and Telecom Sector Over the Past Five Quarters



Kroll's observations of the continued targeting of the technology sector dovetails with other widely reported attacks on such firms in Q3. For instance, AT&T announced a data breach in early July that impacted phone records of nearly all customers, including phone numbers, text records and location-related data.

Global Headwinds Impacting Technology Sector

CrowdStrike IT Outage Causes Chaos

Although not a cyber attack, a July 19 outage involving CrowdStrike Falcon produced the "Blue Screen of Death" across thousands of organizations, grounding flights worldwide at one point. The incident, caused by a faulty software update, was remediated, but not before highlighting the global chaos that unfolds when a widely used technology tool is unavailable. The event, now often referred to as the "largest IT outage in history" underscores the importance of business continuity planning.

Nation-State Actors Escalate Their Efforts

Nation-state actors ramped up their activities in Q3. Email security firm KnowBe4 revealed that it had been targeted by North Korean actors in July. The scheme, similar to one reported by Kroll in Q1, revolved around a remote employee impersonating a U.S. IT worker in an attempt to infiltrate the organization.

In September, reports emerged that a campaign involving a China-based threat actor group had gained access to multiple US telecommunications firms and internet service providers (ISP). It is interesting to note the level of focus on tech firms in this context, a pattern that again aligns with trends observed by Kroll.

Historical Targeting of Technology Firms

The recent activity against technology firms calls to mind previous widespread attacks targeting technology firms:

February 2020—Microsoft Exchange "ProxyLogon" vulnerabilities exploited: Long-standing ProxyShell vulnerabilities in certain Microsoft Exchange Server versions are found to have been exploited by threat actors in August 2021. Learn more.

December 2020—Solarwinds supply chain attack impacts hundreds: IT system management software maker Solarwinds is attacked by threat actors who insert malicious code into a software update. Once victims apply the impacted update, a custom malware monitors their systems to identify the target and drop additional malware as needed. Learn more.

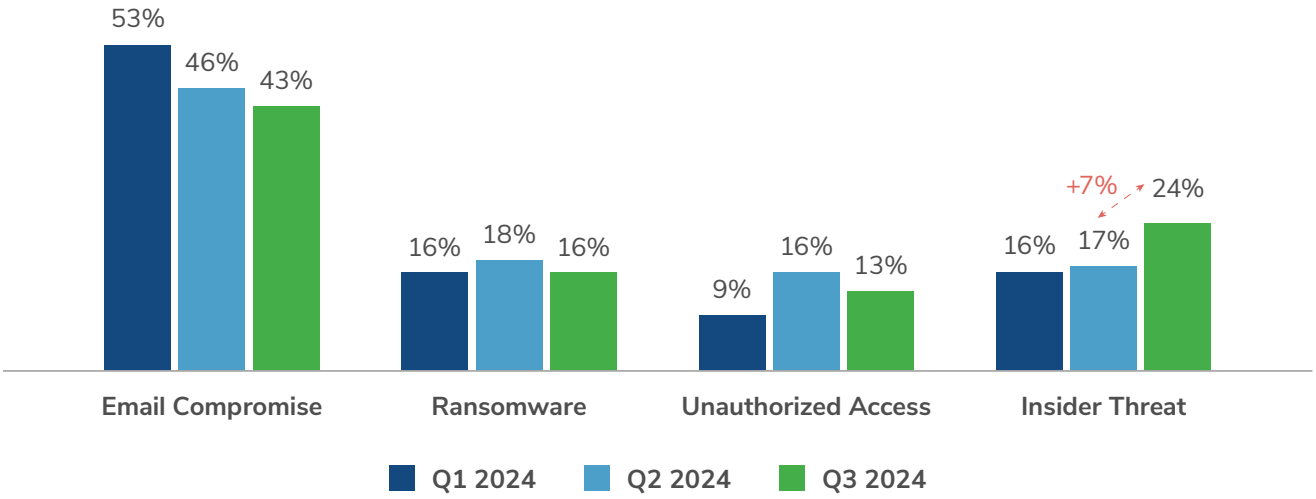
July 2021—REvil attacks Kaseya: IT and security management company Kaseya reports that it has been impacted by a ransomware attack affecting its Virtual System Administrator (VSA) product. The supply chain attack, which affected about 60 managed services providers (MSPs) and up to 1,500 client organizations, leveraged a zero-day vulnerability (CVE-2021-30116). Learn more.

January 2022—Lapsus$ group targets technology firms for data theft: Threat actor group Lapsus$ targets numerous technology firms in early 2022 including Samsung, Nvidia, Okta and Microsoft. Lapsus$ uses a variety of social engineering techniques to access their victims then steal sensitive data such as source code once inside the network. Learn more.

May 2023—MOVEit software zero day exploited: A zero-day vulnerability in MOVEit Transfer is actively exploited to gain access to MOVEit servers to upload a web shell, exfiltrate data and initiate intrusion lifecycles, and potentially also enable a threat actor to move laterally to other areas of the network. Learn more.

Threat Incident Type: Ransomware Activity Becomes More Volatile

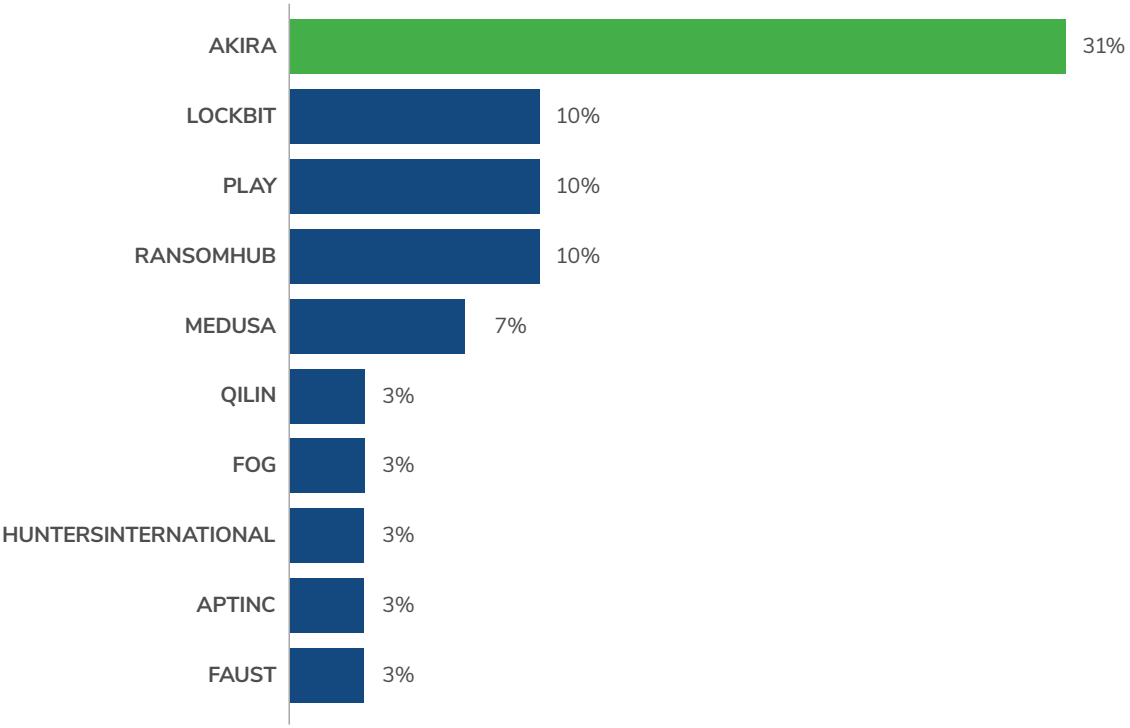
Most Popular Threat Incident Types Over the Past Three Quarters



While insider threat and email compromise were the most observed threats in Q3, Kroll also noted the emergence of several new ransomware variants, highlighting possible rebrands and spin offs following earlier law enforcement disruptions of LOCKBIT and the public exit of BLACKCAT/ALPHV earlier this year.

Ransomware Persists as a Prominent Threat

Top 10 Ransomware Variants—Q2 2024



In Q3, Kroll observed a spike in activity related to the AKIRA ransomware gang. The majority of those cases targeted organizations with a vulnerable SonicWall VPN.

Kroll also observed the emergence of new ransomware gangs such as VANIR, MAD LIBERATOR, LYNX and CICADA.

Kroll analysts identified a leak site for VANIR ransomware group appearing in July 2024. In September, the group's operation was disrupted by the State Bureau of Investigation Baden-Württemberg. A press release from German law enforcement announced the seizure of the ransomware group's data leak site and stated that the investigation into the identity of the threat actor(s) behind it is still ongoing.

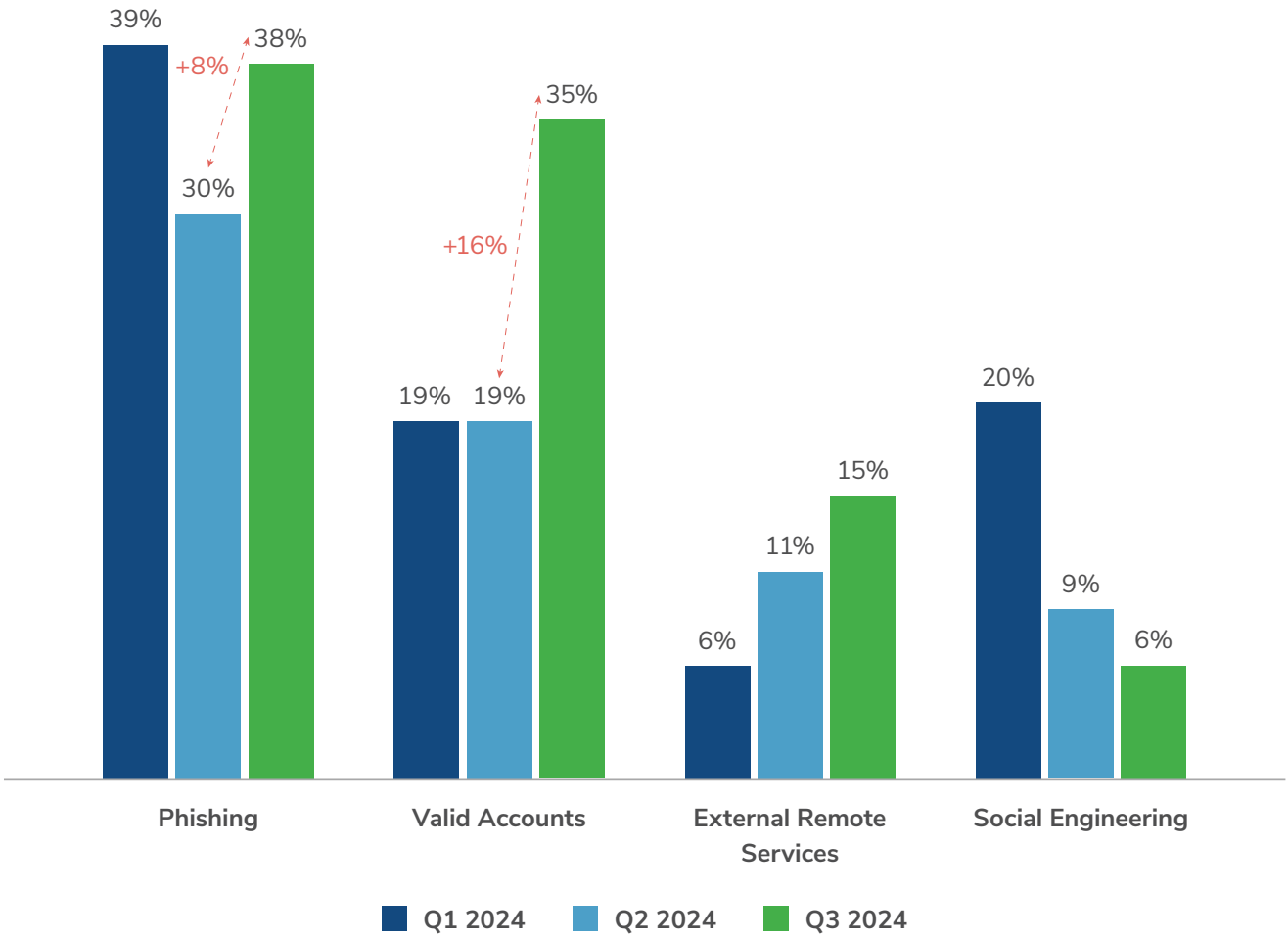
MAD LIBERATOR was also identified in July 2024 by the creation of their data leak site. The groups state they are "comprised of hackers all over the world and do their best to help companies fix their security issues and recover their files." MAD LIBERATOR encrypts files using the AES/RSA algorithm and is not an affiliate group.

Kroll observed cases involving LYNX ransomware, another group emerging around July 2024 with rumors of the group using INC source code. LYNX claims that it's "core motivation" is to gain financial incentives and that it has a strict policy against targeting hospitals, government institutions and non-profit organizations since they play an important role in society.

Another new variant observed during the quarter was CICADA/CICADA3301 which carries out double-extortion tactics and operates a data leak site to use as a part of its campaign. Researchers have discovered overlaps in CICADA3301 and ALPHV/BLACKCAT, which could possibly indicate a rebrand or affiliates of the previous group working for this new ransomware operation. Researchers have also discovered that CICADA3301 may uitlize or work with the Brutus botnet for initial access to corporate networks.

Initial Access Spotlight: External Remote Services and Valid Accounts

Top 4 Initial Access Methods—Past Three Quarters



In Q3 2024, external remote services and valid accounts were the methods most likely to be used by ransomware actors to get into networks. A report in August highlighted the nation-state aspect of the ransomware ecosphere, as the U.S.'s Cybersecurity and Infrastructure Security Agency and FBI reported that Iranian actors were targeting industries, particularly information technology, with exploits related to VPN structure to gain access. These actors sometimes use this type of access for persistence and data exfiltration. They have also been observed selling initial access online.

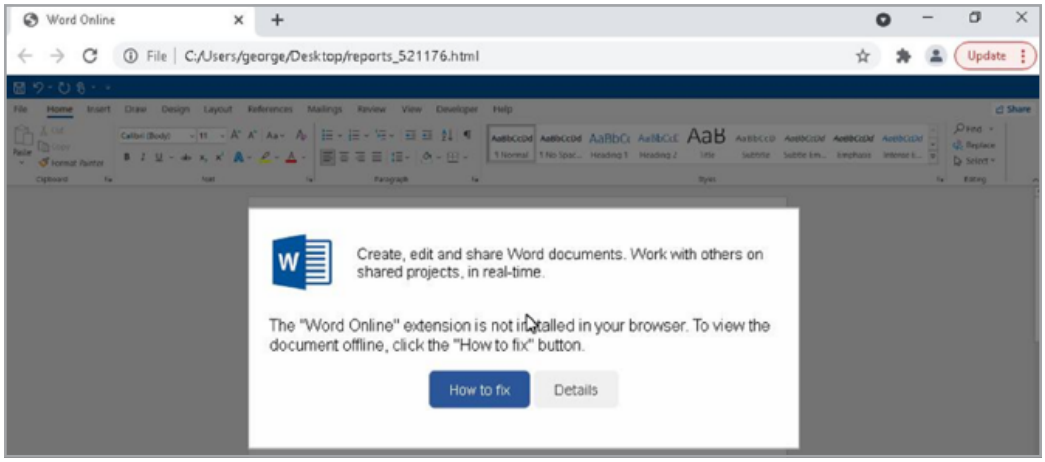
Malware Spotlight – LUMMASTEALER / IDATLOADER

Top 10 Malware Strains—Q3 2024

Q3 2024 Trend	Threat Name
↑ 1	LUMMASTEALER (NEW)
↑ 2	STEALC
↑ 3	AGENTTESLA
↑ 4	REMCOS (NEW)
↑ 5	REDLINESTEALER
↓ 6	COBALTSTRIKE
↓ 7	METASPLOIT
↑ 8	AMADEY
↑ 9	SLIVER
↑ 10	XWORM (NEW)

**(New) highlights the strain's debut in the Kroll top 10*

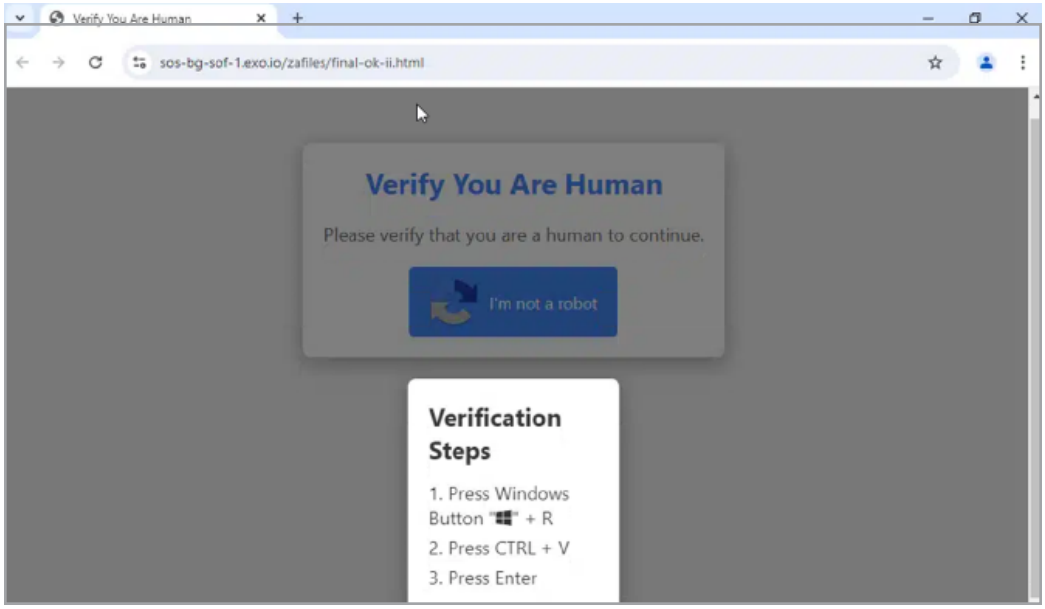
Q3 marked a significant increase in information stealer attacks. Kroll has tracked highly effective social engineering techniques throughout Q2 and Q3. We previously detailed this technique in our Q2 report as part of an ongoing CLEARFAKE campaign, which socially engineers the user into entering malicious commands into a PowerShell or Command Prompt window. Kroll believes this technique was made popular in a DARKGATE distribution campaign that started in May, and was conducted by KTA248 (TA577, Tramp). This campaign used phishing to deliver an HTML attachment designed to look like a Microsoft Word window.



Example of HTML Lure Rendered in Browser (Source: Kroll + VirusTotal)

This technique has evolved over the course of Q2 and Q3, with CLEARFAKE campaigns using it as part of a fake browser update lure. A methodology referred to as 'ClickFix' has seen similar lures like fake browser updates or errors through social engineering which similarly sees the user tricked into executing malicious commands.

Kroll observed that the latest style of social engineering that tricks users into executing malicious commands was highly effective. This is because the newest methods are designed to look like security tools such as CAPTCHAs, which are not typically covered in cybersecurity awareness training.



Example of CAPTCHA Lure Rendered in Browser (Source: Kroll)

Kroll has seen this form of social engineering become highly effective at luring victims into installing information-stealing malware, specifically LUMMASTEALER which was being dropped by IDATLOADER. In Q3, LUMMASTEALER was the most common malware observed by the Kroll Responder service. This corroborates open-source reporting that information stealers continue to be a significant driver of the cybercrime underground market.

Achieving Cyber Resilience: Key Recommendations

The Pace of Attack Increases: Trends observed by Kroll in Q3 2024 demonstrate the speed at which threat actors can advance their tactics and areas of focus. The sudden rise in attacks on tech and telecom in just one quarter demonstrates how quickly threat actors can evolve, leaving organizations struggling to keep up.

Disruption Is Interconnected: The wave of disruption that the global CrowdStrike IT outage created around the world in Q3 2024 demonstrates the impact of such events on organizations. In an increasingly interconnected and cloud-dependent world, this large-scale domino effect is highly unlikely to be a one-off. The only question is how prepared organizations will be when the next such incident occurs.

One-hit Approaches Are Inadequate: The growing efforts of nation-state actors and the continued volatility of ransomware groups point to a landscape in which it is increasingly risky to rely on reactive, one-off approaches to security. With so many threat types and conflicting security requirements, it is imperative that companies fully embrace business continuity and incident response planning.

Risk Grows Increasingly Complex: As the nature of security risk becomes more complex and variable, organizations must ensure that they view business continuity from a broad-ranging perspective. Mitigating risks requires significant collaboration and effort beyond cyber and technology teams to include business resilience and third-party/outsourcing functions. Despite this, many organizations still lack robust and sustainable solutions that will enable them to manage the associated risks.

AI Generates Fresh Threats: With AI-generated malware found to be delivering ASYNCRAT via phishing emails this quarter, it is clear that the technology continues its rise as yet another weapon in threat actors' armories. The growing use of these types of tools again highlights the risks of relying on traditional security approaches alone.

With so many varying factors in play in Q3 2024 and likely to affect security in the months ahead, the Kroll CTI team makes the following recommendations:

- Ensure that your organization prioritizes **incident response** planning. A well-structured plan will safeguard your employees, protect your data and ensure business function is maintained.
- Support incident response planning with **regular testing and assessments** to validate that processes are in place during an emergency. Regular testing can help you identify, monitor and analyze vulnerabilities in your information security systems. It can also enable you to identify potential data privacy and security compliance issues that may have been previously overlooked.
- Complete regular, customized **incident response tabletop exercises** led by seasoned experts. This will give the members of your incident response team a valuable opportunity

to clarify and rehearse their roles and boost their confidence in carrying out their assigned duties in the event of an incident. Tabletop exercises will also highlight where guidance or information needs to be updated.

- Put in place a **cyber risk retainer** capable of enabling swift and strategic response in the event of an incident. As well as being fully configurable to your environment, this should be customizable to a level that enables you to access the type of proactive response and notification services required to fulfill your evolving security situation and business goals.
- Ensure your organization has **key controls** in place and that each capability and control implemented includes a combination of people, process and technologies to be fully effective. These controls also require good governance and metrics to provide ongoing assurance that they are working properly and delivering return on investment—and to identify when they are not.
- Gain an **expert external review** of your existing business continuity plans to ensure alignment with evolving industry best practices and business needs. This is best achieved by working with a cyber security partner with the breadth of experience and offerings to enable you to achieve comprehensive cyber resilience.

KROLL

Why Kroll?

✓ Fueled by intelligence from 1000s of M&A, IR and Regulatory Response engagements:

As the world's largest IR provider, Kroll integrates real-world intelligence from 1000s of incident response, M&A due diligence, and regulatory compliance engagements a year to deliver relevant threat models and assessments.

✓ Integrated Advisory and Technical Expertise:

Our globally recognized professionals combine strategic advisory with in-depth technical assessments, providing support for all aspects of your transactions.

✓ End-to-End Support Throughout the Transaction Lifecycle:

From initial due diligence to post-merger integration, Kroll ensures accurate and informed cyber risk management across the entire transaction lifecycle.

✓ Minimal Disruptions to Business Operations:

We utilize remote technologies for our assessments, minimizing disruptions to business operations and eliminating the need for agent deployment, allowing for seamless and efficient due diligence.

Kroll has a dedicated insurance team for insurance and legal channels, with extensive relationships with 85+ cyber insurance carriers and exclusive benefits to insureds.

INDUSTRY RECOGNITION

CREST | PEN TEST | CSIR | SOC

CREST has accredited Kroll in Penetration Testing, Incident Response, and SOC services

CISA CISM

ISC2 Certified professionals in Information Security Auditing and Information Security Management

Gartner

Recognized Kroll as representative vendor for Digital Forensics and Incident Response, Managed Detection and Response, and Third-Party Risk Management Solutions

IDC

Kroll named 'Major Player' in the IDC MarketScape: Worldwide Cybersecurity Consulting Services in 2024

TALK TO A KROLL EXPERT TODAY

North America
T: 877 300 6816

UK
T: 808 101 2168

Hong Kong
T: 800 908 015

Additional hotlines at:
kroll.com/hotlines

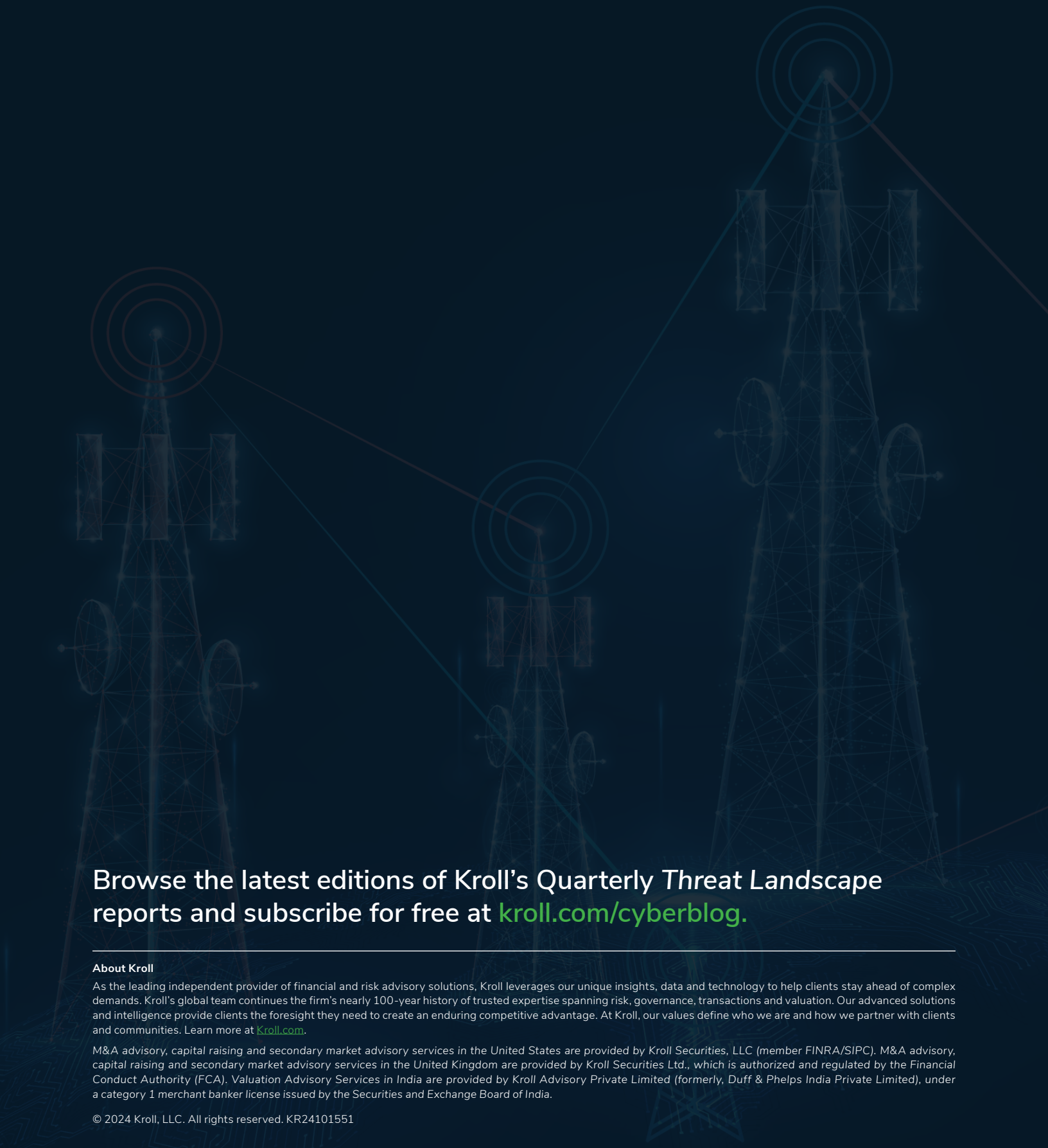
Singapore
T: 800 101 3633

Australia
T: 1800 870 399

Brazil
T: 0800 761 2318

Or via email:
CyberResponse@kroll.com

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 financial and risk 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.