KROLL

Q4 2022 Threat Landscape Report:

Tech and Manufacturing Targeted as Ransomware Peaks for 2022

Q4 2022 Threat Landscape Report: Tech and Manufacturing Targeted as Ransomware Peaks for 2022

Authors

Laurie Iacono

Keith Wojcieszek

George Glass

In a year where headlines were dominated by the global economic and geopolitical uncertainty around Russia's war on Ukraine, 2022 saw a threat landscape that was both volatile and fragmented, largely due to the war. As the year drew to an end, ransomware hit a peak, primarily due to the rise in attacks impacting the manufacturing, health care, technology and telecommunications industries. This came after a dip in ransomware during the third quarter of 2022, suspected to be due to the disbandment of the Conti ransomware group.

Kroll's research found that several other familiar threats remained highly active throughout 2022, such as a significant increase in phishing and a notable rise in unauthorized access, increasing from 18% of cases in 2021 to 25% in 2022. Notable new initial access methods included an infection method leveraging Google Ads to spread credential-stealing malware and a rise in the use of USB-borne malware as a means to spread infection throughout a network.

Q4 2022 Threat Timeline

Oct 4 **New ProxyNotShell exploit emerges:** ProxyNotShell becomes a new exploit, taking advantage of two vulnerabilities (CVE-2022-41040 and CVE-2022-41082), which gives an attacker visibility of emails on an organization's server and grants them the ability to plant malware on an Exchange server. Microsoft issued mitigation steps to address the vulnerabilities before issuing a patch in the November 8 Patch Tuesday Updates.

Oct 7 **Rclone used in Microsoft 365 to execute email compromise attacks:** Kroll observes the data syncing tool Rclone being used in M365 for network compromises or phishing attacks. Rclone is seen being used to download a large number of files on SharePoint/OneDrive from a Microsoft 365 account in only a little over an hour.

Nov 19 **Google Ads used to distribute Royal ransomware:** Microsoft warns about threat actors using Google Ads to distribute post-compromise payloads, including Royal ransomware.

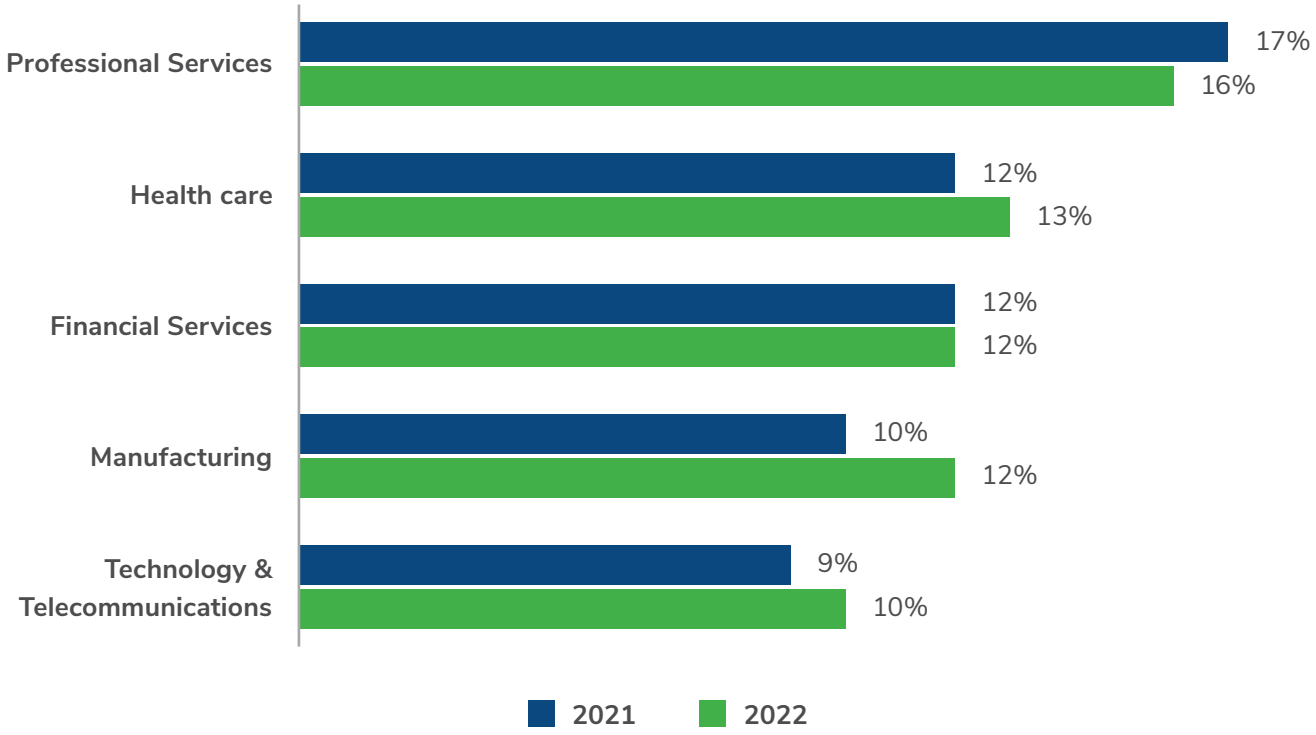
Nov 24 **Qakbot malware used to infiltrate U.S. companies:** The Black Basta ransomware group is found to be using aggressive QakBot malware campaigns that lead to ransomware infections on compromised networks.

Dec 5 **New tactics associated with AvosLocker ransomware:** Threat actors associated with the ransomware target Veeam Backup and Replication systems for possible exfiltration. (CVE-2022-26500 and CVE-2022-26501).

Sector Analysis: Tech and Manufacturing Caught in the Crosshairs

In 2022, the top five impacted sectors across Kroll incident response cases were: professional services, health care, financial services, manufacturing, and technology and telecommunications.

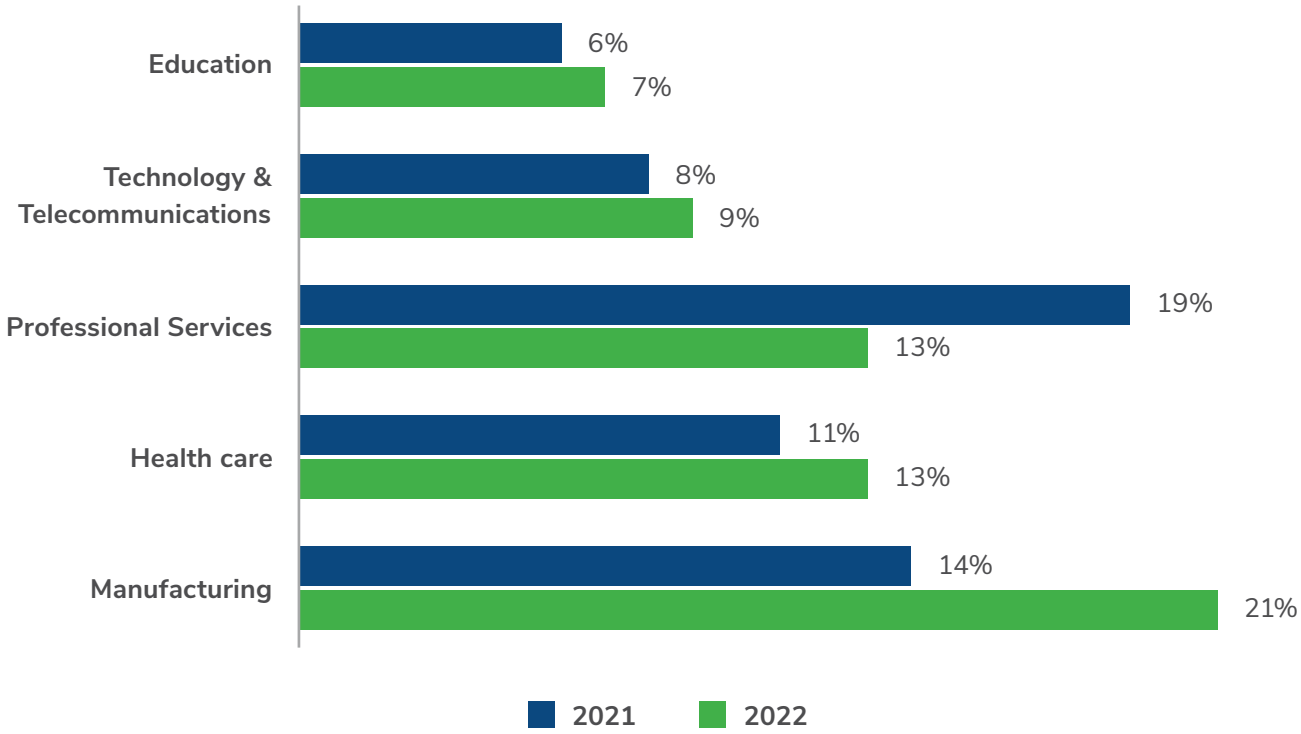
Top Five Impacted Sectors 2022 vs 2021 (All Threat Incident Types)



While the professional services sector has typically been the top targeted sector for Kroll cases, in 2022, Kroll observed a slight decline in those attacks, while other sectors were targeted more, namely manufacturing and technology and telecommunications.

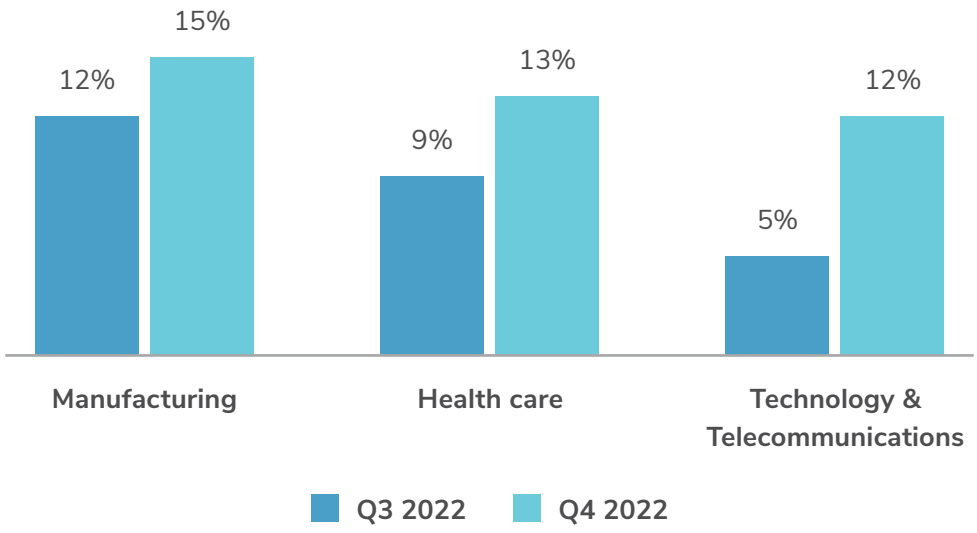
This differs from the industry spread of data breaches Kroll saw in 2022. In Kroll's Data Breach Outlook report, health care overtook finance as the most breached industry of the year, accounting for 22% of all breaches, compared to 16% in 2021. Delving further into this data, Kroll received most engagement from consumers whose data had been breached in the financial services sector, and this concern seems to be increasing as call volumes increased 127% year on year in 2022.

Percentage of Ransomware Incidents Across the Five Most Impacted Sectors in 2022



Ransomware was evident in the majority of attacks impacting manufacturing, health care, technology and telecommunications. Its prevalence in these sectors spiked in the fourth quarter.

Quarter-Over-Quarter Increase in Ransomware Attacks in Q4 2022



There were some other notable cases Kroll observed in the manufacturing, technology and telecommunications industries that point to wider trends.

Case Study: The Technology and Telecommunications Industry Becomes a Route to Managed Service Providers

In the technology industry, Kroll has seen many attacks on managed service providers (MSPs). In one case, threat actors had set up Google Ads for the search term "common IT management software." This software is widely used by MSPs, and it is likely that IT administrators and MSPs were the target of these adverts. The ads provided the legitimate software packaged with a Batloader installer that, when executed, provided a backdoor with elevated privileges to the network. This then allowed the threat actor to quickly scout the internal network for sensitive files and high-value systems before disabling security software.

The threat actor traversed several file servers and extracted data from each before exfiltrating the data to cloud data storage via Rclone. Once the exfiltration was completed, the Black Basta ransomware binary was executed. The impact of this activity had many complications as data was removed, which may have contained client data, as well as the encryption of vital servers, likely affected the MSP's daily operations to its clients, thus increasing the pressure to pay the ransom.

"MSPs are a prime target for cybercriminals," says Vice President at Kroll, Stephen Green. "The nature of an MSP's business means that the demands of the supply chain will often provide greater pressure to pay any ransom. The access granted to an MSP also provides opportunities to conduct further attacks against its clients for additional payments. This may be a reason Kroll has observed threat activity increasingly targeting the technology sector and is supported by a number of industry warnings about supply chain risk, including from the Five Eyes (FVEY) intelligence alliance and the UK's National Cyber Security Centre (NCSC)."

— **Stephen Green**, Vice President, Cyber Risk, Kroll

Case Study: Cybercriminals Tap into Business Continuity Concerns in the Manufacturing Sector

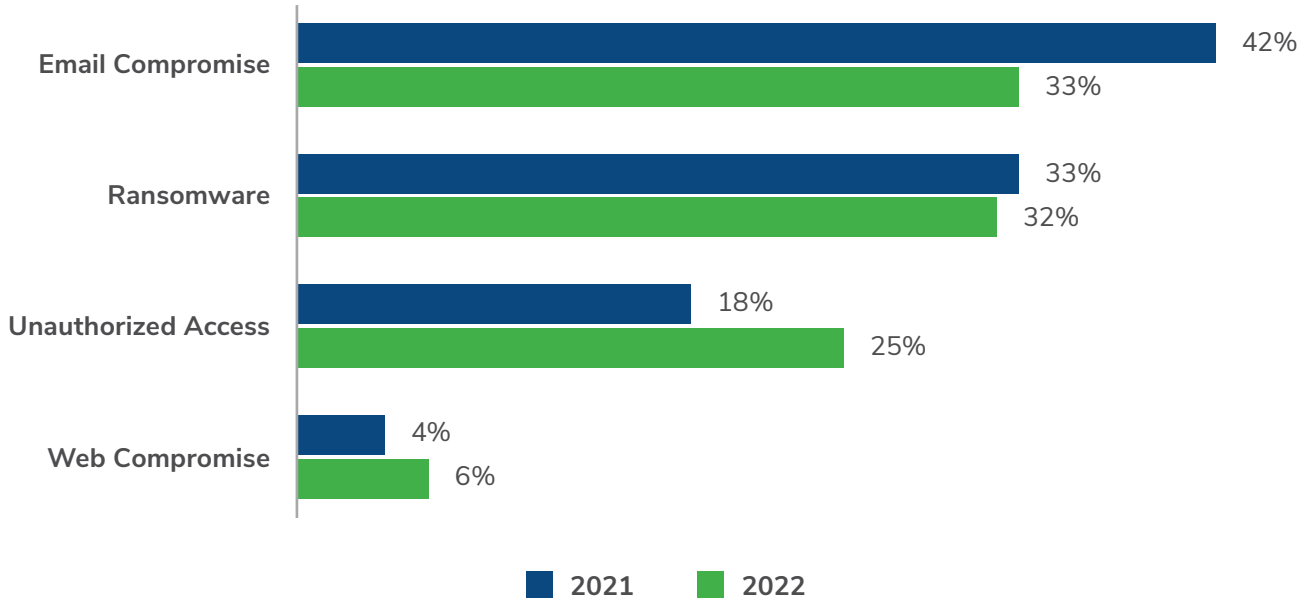
In a representative incident in the manufacturing sector, Kroll observed the deployment of Vice Society ransomware. Initial access was obtained through a botnet infection that helped attackers conduct an initial exploration of the network. Once the attackers had gained a foothold in the system, they maintained persistence using a variety of remote access tools. After moving into a domain admin account, they exfiltrated hundreds of gigabytes of data for a series of days and then encrypted the network. The attackers locked IT staff out of the company's systems. This meant that all critical operating systems, including production, were halted.

50% **annual increase in ransomware cases targetting the manufacturing sector in 2022**

> **"The manufacturing sector is an attractive target for ransomware gangs due to the level of business disruption it can cause," says Kroll Managing Director, Walmir Freitas. "Often these sectors hadn't typically seen themselves as targets for cybercriminals because they held limited sensitive information. But the growth in ransomware has changed the game; manufacturing organizations may be more willing to pay a ransom when their ability to operate is hanging in the balance."**
>
> — **Walmir Freitas**, Managing Director, Cyber Risk, Kroll

Most Common Cyber Threats of 2022 vs. 2021

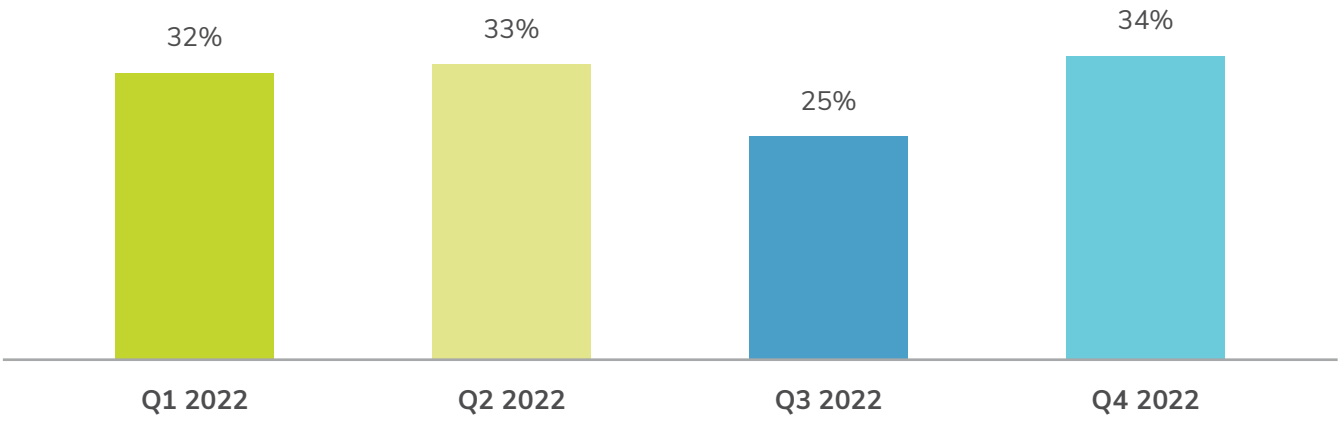
Year-on-Year Comparison: Most Common Threat Incident Types in 2021 and 2022



Several notable trends shone through in our analysis:

- Email compromise saw a decline from its 42% peak in 2021, likely due to widespread patching for the Microsoft Exchange ProxyLogon vulnerabilities that threat actors continued to attempt to use to exploit email servers in 2022.
- Unauthorized access saw a large year-over-year increase in 2022. As discussed in the *Q3 Threat Landscape report*, insider threat accounted for the majority of this activity in 2022.
- Although the total number of ransomware incidents in 2022 decreased slightly from 2021, ransomware still accounted for nearly a third of Kroll incident response cases.

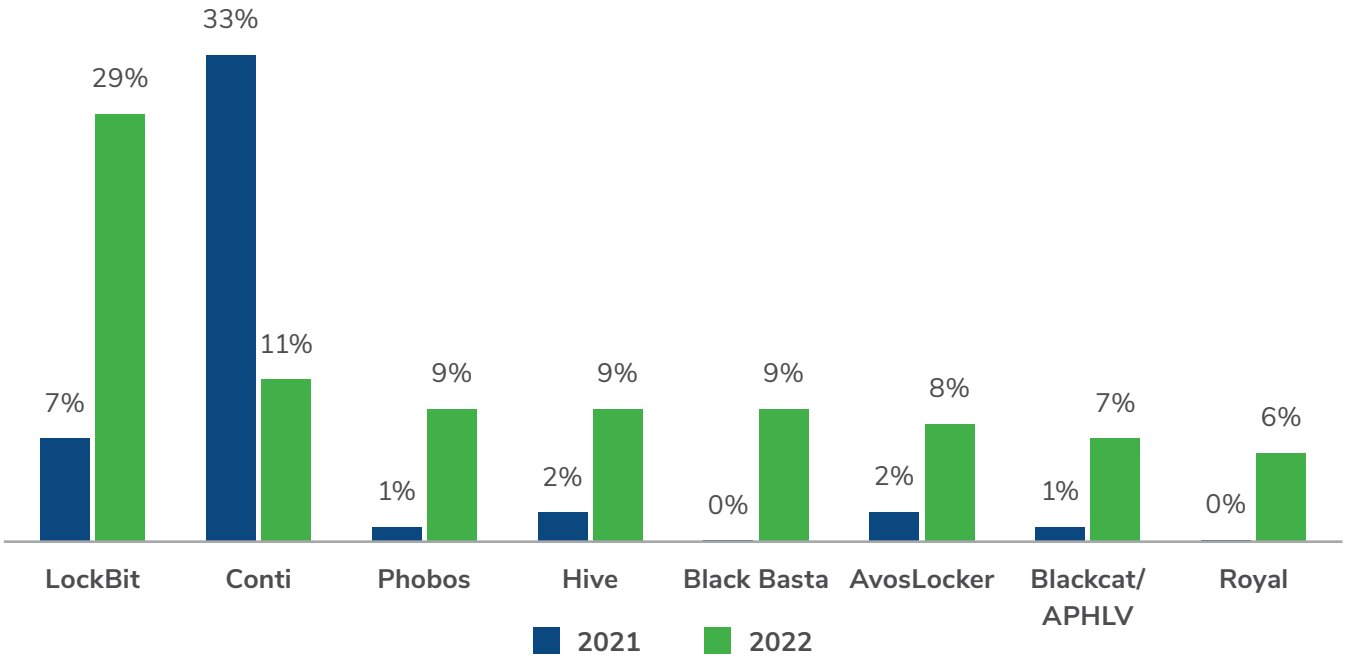
Percentage of Ransomware Incidents in Kroll Cases Throughout 2022



Ransomware Analysis: 2022 – A Year of Regrouping, with Rising Activity in Q4

Ransomware continues to be a top threat impacting organizations, and during the past year, Kroll has seen many ransomware groups evolve their tactics to reach more victims.

Most Common Ransomware Variants – 2022 to 2021 Comparison



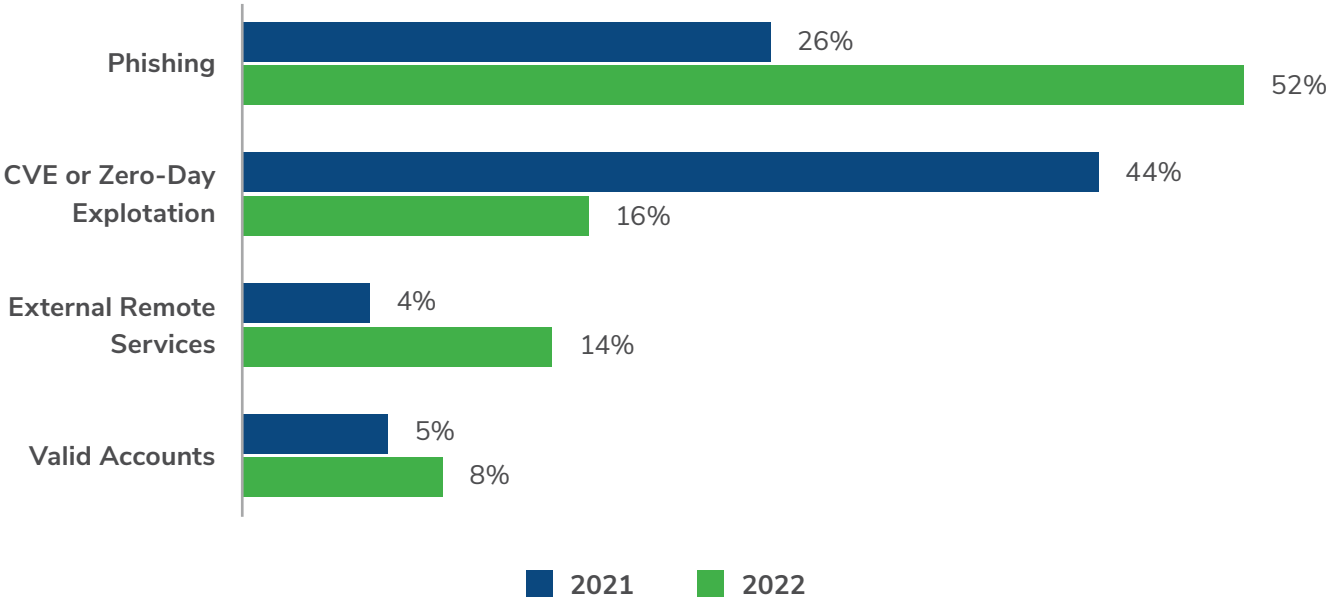
As security controls got better at stopping certain ransomware attacks, affiliates were forced to switch to different variants during the same access period. This observation highlights that affiliates distributing ransomware are often doing so on behalf of more than one cybercriminal group. In 2022, Kroll observed increased activity from familiar groups such as Hive, AvosLocker and Vice Society. After Conti disbanded in June 2022, LockBit became the most commonly observed ransomware across Kroll engagements. Other newcomers such as BlackBasta and Royal were also active during the year.

Although the group associated with Royal ransomware has been active since January 2022, Kroll first observed a case in November 2022, and in Q4, Royal ransomware accounted for nearly 14% of ransomware activity. Royal appears to be a collective of threat actors from other well-known malware groups such as Roy/Zeon, Conti and TrickBot, working together as a private ransomware group. Royal ransomware has been connected with many different initial access techniques, including callback phishing attacks, brokered access and Google Ads abuse.

Other variants that Kroll observed on the rise in Q4 were Phobos, Dharma and AvosLocker.

Top Initial Access Methods in 2022

Year-on-Year Comparison: Most Common Initial Access Methods in 2021 and 2022



2022 saw a significant shift in the top initial access methods for threat actors. While CVEs and zero-day exploitations were responsible for 44% of initial access methods in 2021, phishing was responsible for 52% in 2022. In 2021, a high percentage of Kroll's email compromise cases were associated with the Exchange ProxyLogon CVE and a significant volume of exploited vulnerabilities.

In Q4, Kroll noted another rise in the use of external remote services, which continues to be a favorite access method for ransomware groups. Kroll also reported on a novel access method leveraging Google Ads to infect users with credential-stealing malware such as VIDAR.

Beyond VIDAR, which has been around since at least 2018 and has benefitted from several improvements over the years, the increase of SocGholish usage for initial access in 2022 is worth highlighting. SocGholish is commonly delivered via search engine optimization hijacking, ad impersonation and drive-by-download. In 2022, SocGholish worked with cybercriminal partners to increase its infection efficacy by increasing the number of websites serving malware and the reputation of the sites that redirect to them, helping to improve their search engine rankings. Defenders should treat detections of either VIDAR or SocGholish as a high-severity threat.

2022 Into 2023: Turbulence Continues

Activity observed by Kroll in Q4 aligned with the trend that defined 2022 as a whole: not only have many familiar threats not gone away, but they continue to evolve and adapt. This was evidenced by the prominence of ransomware throughout 2022, hitting health care in Q2, then education in Q3, before a significant spike in focus on technology and manufacturing in Q4.

While the specific types of threats may not have changed much from 2021 to 2022, the central story of 2022 is cybercriminals' ability to quickly evolve and regroup in the face of advancing security controls, law enforcement activity and geopolitical disruption. The near-seamless transition from Office maldocs to container files in phishing attacks and new access tactics like Google Ads abuse illustrate the constant evolution of techniques to which organizations must pay attention in order to improve their defenses. However, they also need to ensure they are prepared to meet the challenges presented by newly emerging threats.

The Year Ahead: Threats Likely to Evolve in Form and Focus

As threat actor activity is often shaped by fluctuations in economic conditions, there is little doubt that the variability of behaviors observed in 2022 will endure in 2023. Due to the continued market volatility across the globe and the ongoing war on Ukraine, it is likely that the unstable circumstances in which attackers thrive will persist in 2023. The continued democratization of cybercrime through technology such as ChatGPT could also drive further developments in threat activity.

2023 is likely to see threat actors honing their tactics to move faster and more nimbly, with more techniques to circumvent defense tools. This makes swift detection of suspicious activity even more critical for organizations. As suggested by activity observed in Q4, it is also highly probable that ransomware will continue to evolve in complexity and impact in the year ahead.

With the value of cryptocurrency going down and the average ransomware profits declining in 2022, 2023 could well see ransomware-as-a-service groups looking to maximize their revenue streams and ransomware actors as a whole becoming more destructive.

Following on from the technology sector being a major target of ransomware in Q4 2022, large IT providers are likely to be a target in 2023, as threat actors attempt to use them as a route to compromise end clients via supply chain attacks. An increase in attacks against Operational Technology (OT) environments is also highly probable, as is the use of techniques similar to those used in 2022.

Key Steps to Stay Resilient in a Volatile Security Landscape

With so many sectors targeted by attackers throughout 2022, no industry or market segment can afford to be complacent as it relates to ongoing monitoring of their internal infrastructure. Actionable threat intelligence and a robust managed detection and response program will play a vital role in enabling businesses to respond effectively to the many and varied threats likely to arise in 2023. Apart from working with trusted partners to achieve this, businesses can implement specific changes themselves. These include enforcing multi-factor authentication, using remote desktop protocol (RDP), creating multiple backups and having effective access control. By taking proactive steps now, organizations can ensure they are better prepared to respond to the global headwinds likely in 2023 and beyond.

To learn more, view the Kroll guide, *10 Essential Cybersecurity Controls for Increased Resilience*.

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.