

KROLL

Q2 2022

Threat Landscape:

Ransomware Returns, Healthcare Hit



Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit

Authors



Laurie Iacono



Keith Wojcieszek



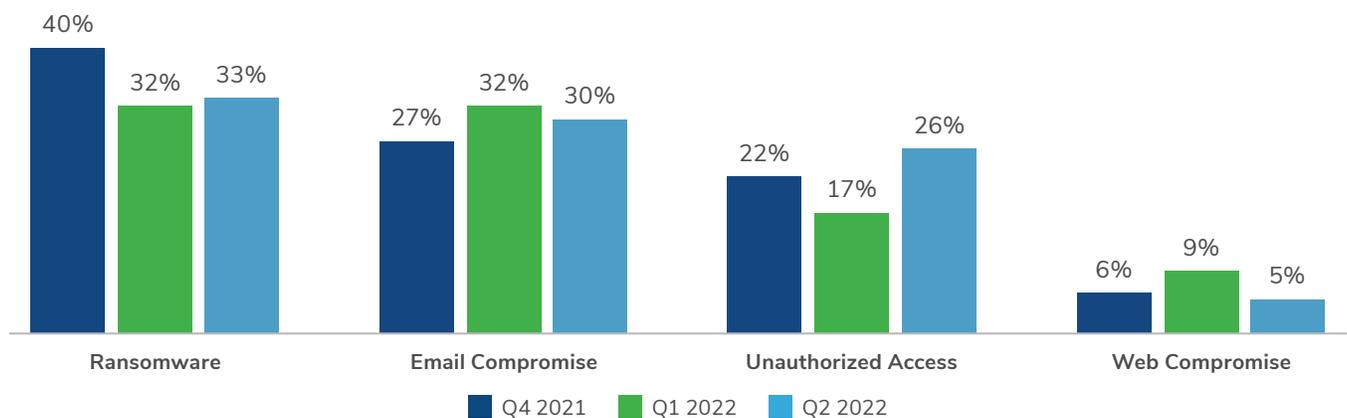
George Glass

In Q2 2022, Kroll observed a 90% increase in the number of healthcare organizations targeted in comparison with Q1 2022, dropping the final nail in the coffin for the “truce” some criminal groups instituted earlier in the COVID pandemic. Ransomware helped to fuel this uptick against healthcare as attacks increased this quarter to once again become the top threat, followed closely by [email compromise](#).

While Kroll continued to see actors exploiting vulnerabilities and phishing schemes to launch ransomware, in Q2 a ransomware incident was most likely to begin via external remote services. Kroll observed an 700% increase in external remote services such as remote desktop protocol (RDP) and virtual private networks (VPN) being used for initial access in the quarter. Of ransomware incidents beginning with phishing, Kroll observed an uptick in the use of [Qakbot malware](#) as a delivery mechanism, particularly for new ransomware groups like Black Basta.

The recent shift to targeting the healthcare industry comes alongside the persistence of ransomware as an incident type and the rise in external remote services being used as an initial access method, giving us an indication of where attackers may focus in coming months. All organizations—especially those in healthcare—would do well to test the resilience of their external remote services and [preparedness for ransomware](#).

Most Popular Threat Incident Types - Past Three Quarters



Q2 2022 Threat Timeline

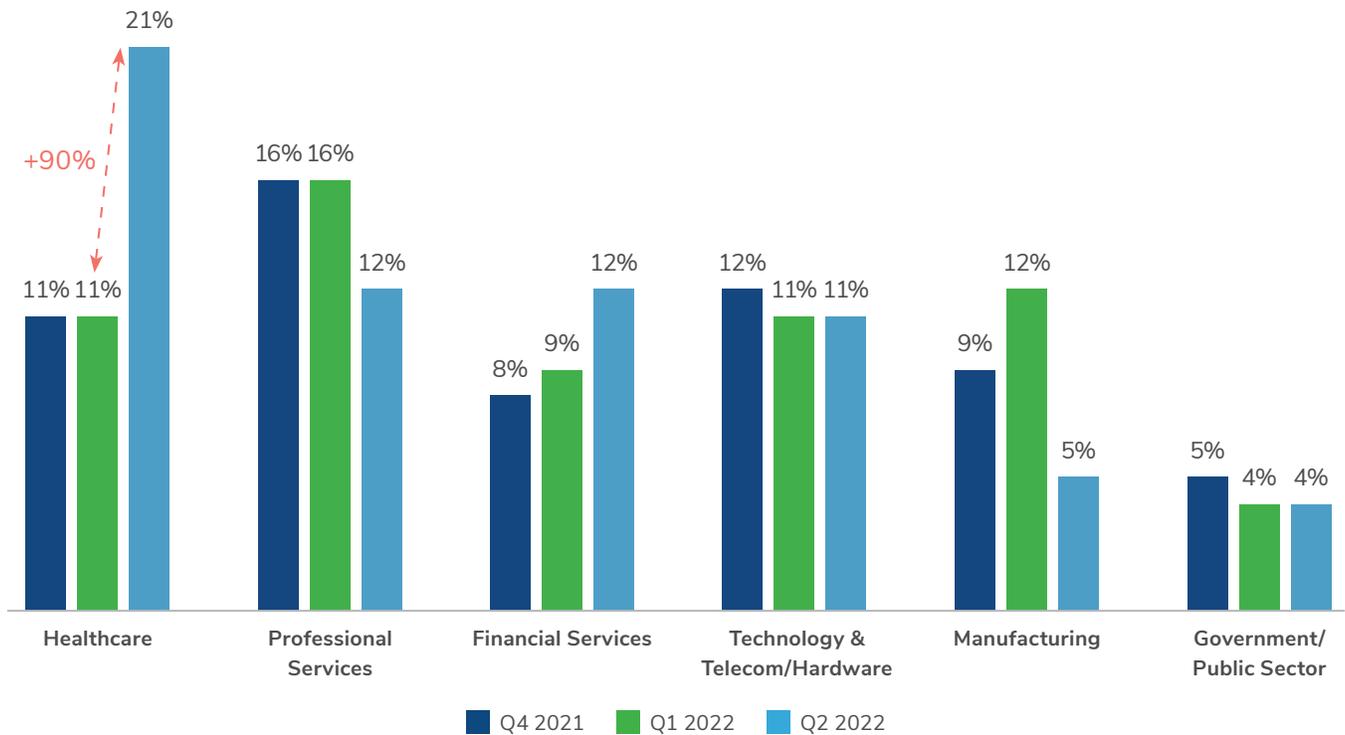
- Apr 22**  **The Changes in Emotet:** The delivery, architecture and operation of Emotet during initial infection changes. The binaries switch from a 32-bit to a 64-bit architecture, developers experiment with password protected email delivery methods with embedded .ZIP files and upon infection, Emotet install Cobalt Strike beacons.
- May 19**  **Conti “Dissolution”:** Conti officially shuts down with its infrastructure and data leak site **now offline**. Members disperse into smaller ransomware operations.
- Jun 2**  **ModPipe POS:** Recent activity targeting payment card information is observed from ModPipe malware by the Kroll Malware Analysis and Reverse Engineering team. Using the JHook hooking module, ModPipe **is able to steal encrypted or decrypted card information** from card processing servers. Along with the JHook module, the hooking targets memcpy and CryptDecrypt have also been seen.
- Jun 3**  **Follina and Atlassian CVEs quickly exploited:** Hacking attempts using the Follina Office Vulnerability are used in a **phishing campaign targeting local U.S. government and European** organizations. The Follina vulnerability, which has not been officially patched at the time of writing, exploits Microsoft Windows Support Diagnostic Tool (MSDT) to get remote access to target systems. The threat actor is currently unknown, but speculated to be a nation-state actor.
- Jun 6**  **BumblebeeLoader:** The **Bumblebee malware strain**, whose operators EXOTIC LILY by TAG have been connected with the Conti ransomware group, found to be operating as a loader. It delivers via phishing emails, deploying additional payloads such as Cobalt Strike.

Sector Analysis: Healthcare Hit

Healthcare overtook professional services as the top targeted sector in Q2, accounting for 21% of all Kroll cases, compared to only 11% in Q1 2022. Common threat incident types impacting the healthcare sector included ransomware (33%), unauthorized access (28%) and email compromise (28%).

Of the ransomware cases, it was common to see a double extortion tactic in which actors exfiltrated data prior to network encryption and then threatened to leak the stolen data as leverage during negotiations. Phishing is a common initial access method for incidents impacting the healthcare sector.

Most Targeted Industry Sectors - Past Three Quarters



Kroll Case Study: Healthcare Organization Hit by Ransomware

An employee at a healthcare organization received a spoofed email from an outside contact purporting to contain a data file that a team member had previously requested. Unknown to the user, the email originated from an IP address associated with the Qakbot Command and Control (C2) and provided a .ZIP file which contained further malicious files, introducing Qakbot into their systems. Once inside the network, the actor deployed Cobalt Strike malware. Threat actors moved within the network for approximately 15 days, making their way into multiple user machines and exfiltrating over 20GB of data before deploying Black Basta ransomware.

Derek Rieck, Associate Managing Director in the Cyber Risk practice at Kroll, comments, “Historically, health care is an attractive target to ransomware groups, as the disruption of critical networks impacting life-saving services may encourage organizations to pay ransom demands. This is intensified by the double extortion tactic, where threatening to publish confidential information, such as protected health information (PHI), can further intimidate victims.”

“Q2 2022 was the first time that we have seen such growth in the volume of attacks against this sector,” Rieck continued “The percentage of incidents almost doubled, whereas we have seen fairly consistent levels previously. This could be linked to the perceived recovery of the health care industry after the impact of COVID-19, perhaps causing some ransomware groups to end their [hiatus against health and medical organizations](#).”



“ Historically, health care is an attractive target to ransomware groups, as the disruption of critical networks impacting life-saving services may encourage organizations to pay ransom demands. ”

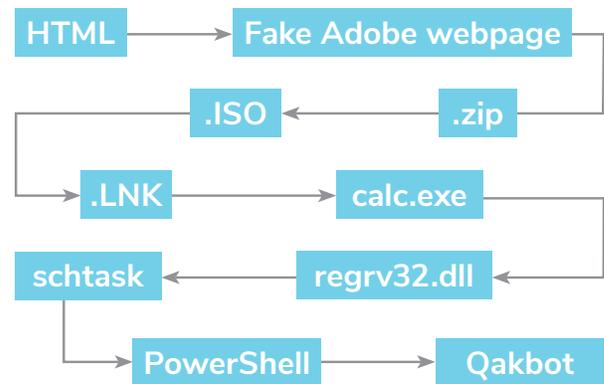
— Derek Rieck, Associate Managing Director,
Cyber Risk, Kroll

Recent Botnet Activity: Qakbot

Phishing attacks continued to evolve in Q2, as Kroll observed threat actors using old and new malware such as Qakbot and Bumblebee. There was an uptick in the use of Qakbot malware as a delivery mechanism for ransomware, particularly from new ransomware groups like Black Basta. Consequently, Qakbot should be treated as a precursor to a ransomware event.

In this quarter, authors of the Qakbot malware added an additional step to the trojan's infection chain, an HTML attachment that negates the need for a fetch of final payload from a command and control server. After arriving as an HTML attachment in a phishing email, the infection chain is as follows:

Example Qakbot infection chain involving repeated engagement from end user



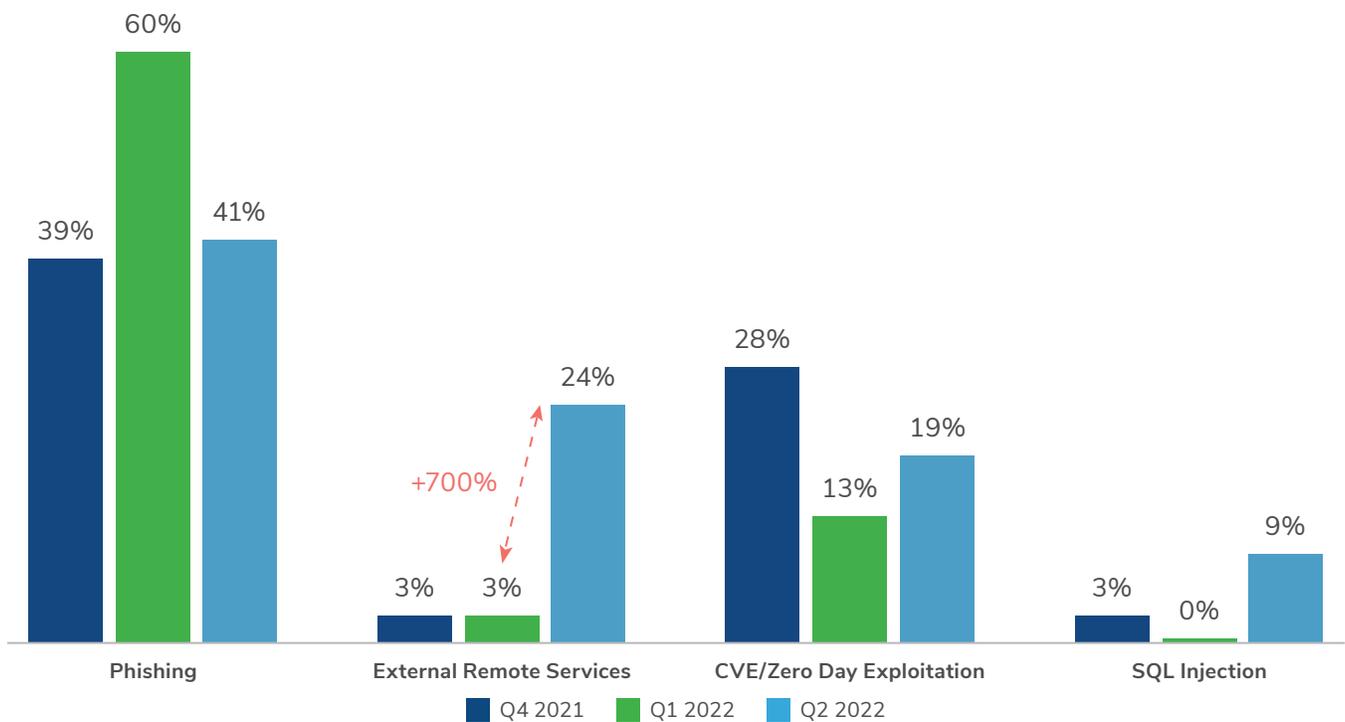
“ As more incidents are stopped by security monitoring tools such as Endpoint Detection and Response (EDR) and anti-virus, threat actors are lengthening attack chains to further evade detection. This highlights the importance of Managed Detection and Response (MDR) solutions that can identify suspicious activity. It also provides a compelling argument as to why MDR should be combined with other security best practices, such as user education. Users should be trained to recognize and avoid such suspicious download processes. ”

— Mark Nicholls, Chief Research Officer,
Cyber Risk, Kroll

Threat Actors Targeting External Remote Services/VPN for Initial Access

While phishing remained the top initial access method across all threat incident types, Kroll observed significant increases in external remote services being compromised and CVEs being exploited for initial access. External remote services were used for initial access 700% more this quarter and CVEs were exploited for initial access 46% more in Q2.

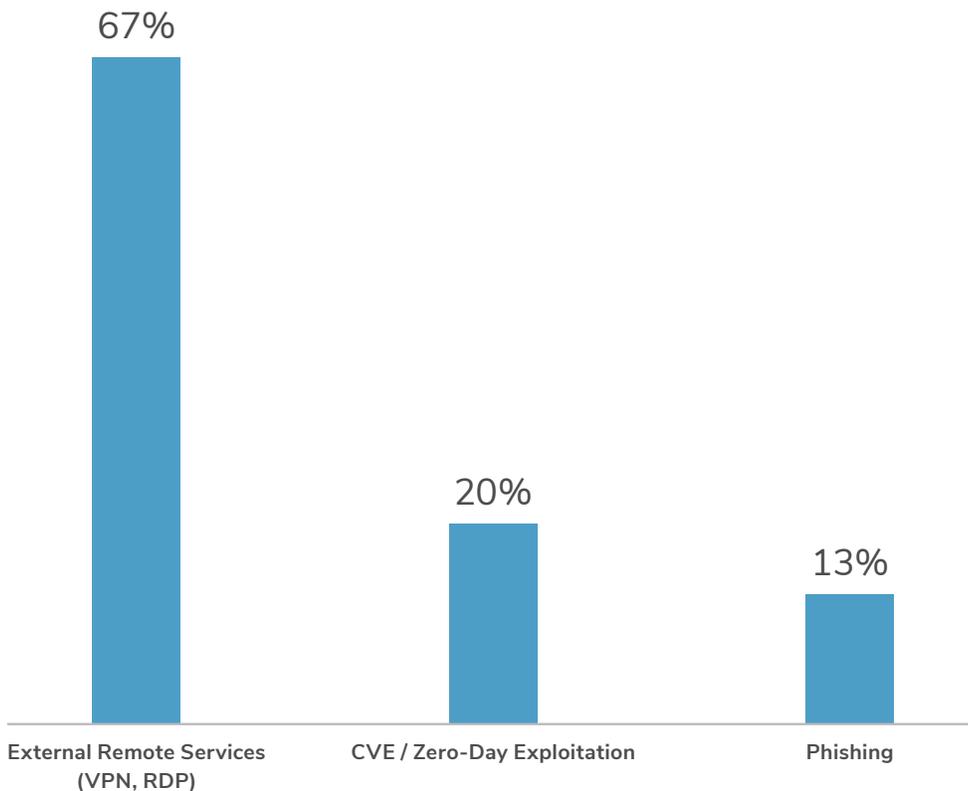
Most Popular Initial Access Methods - Past Three Quarters



External remote services have historically been a common access vector for ransomware groups. At the height of the pandemic in 2020, Kroll reported that open RDP vulnerabilities of popular VPN systems (Citrix NetScaler CVE-2019-19781 and Pulse VPN-CVE-2019-11510) were the **most common precursors to ransomware attacks**.

The majority of incidents in Q2 2022, beginning with access via remote services or CVE exploitation, led to a ransomware attack. This highlights the popularity of compromising external remote services with ransomware threat actor groups and supports the fact that both ransomware and external remote services, as initial attack vectors, increased this quarter.

Most Popular Initial Access Methods for Deploying Ransomware



In previous quarters, out of the most popular initial access methods, external remote services accounted for a much smaller proportion of the overall amount. Several factors may account for the recent rise in Q2 2022 in the use of external remote services, including on-going botnet disruptions, making it harder for ransomware operators to leverage botnets as a method of initial infection. MDR tools are also catching more malware and so external remote services are used as a way to avoid detection. Kroll observed several cases in Q2 where organizations were compromised due to legacy systems or unpatched vulnerabilities.

Kroll Case Study: Log4Shell Vulnerability Exploited for Ransomware and Data Exfiltration

In a BlackCat ransomware situation, Kroll's forensic review identified that actors had scanned the victim's VMware server more than 10 days before returning to access the system via the [Log4Shell vulnerability](#). Once inside the system, actors deployed multiple tools to maintain persistence, including PSTools, ZohoAssist, Total Software Deployment, PDQ Install and Mimikatz to collect credentials. Once credentials were obtained via Mimikatz, the actors used ScreenConnect across hundreds of endpoints to collect and exfiltrate data.

Kroll Case Study: Multi-Ransomware Event

Another event investigated by Kroll began as a singular incident regarding a demand from the SunCrypt ransomware gang. Additional forensic analysis identified the earlier presence of AvosLocker encryption and LockBit 2.0 encryption on their network. Due to anti-detection methods used by various actors once inside the network, evidence was largely destroyed to determine root access. Kroll did observe the threat actor using Domain Admin level credentials while inside the network. A threat actor later communicated that the organization's VPN was vulnerable to an exploit patched in 2018 and that an admin password was of weak security.

Stephen Green, Vice President in the Cyber Risk practice at Kroll, comments, "It is interesting to see the rise in ransomware combined with the rise in external remote services used as an initial access point for attackers. Not always do we have such a clear correlation between an incident and the root cause of how they first got in."

"As many organizations transition to a hybrid style of working," said Green, "identifying the vulnerabilities that external remote services present is critical. Many of the remote systems that we rely on were set up in haste as a reaction to COVID-19 and the widespread work-from-home advice given by governments around the world. Their implementation may have been rushed and less due diligence may have been completed compared to normal circumstances. Now is the time to readdress these environments and build resilience for a longer-term remote strategy."



“ As many organizations transition to a hybrid style of working, identifying the vulnerabilities that external remote services present is critical. ”

— Stephen Green, Vice President,
Cyber Risk, Kroll

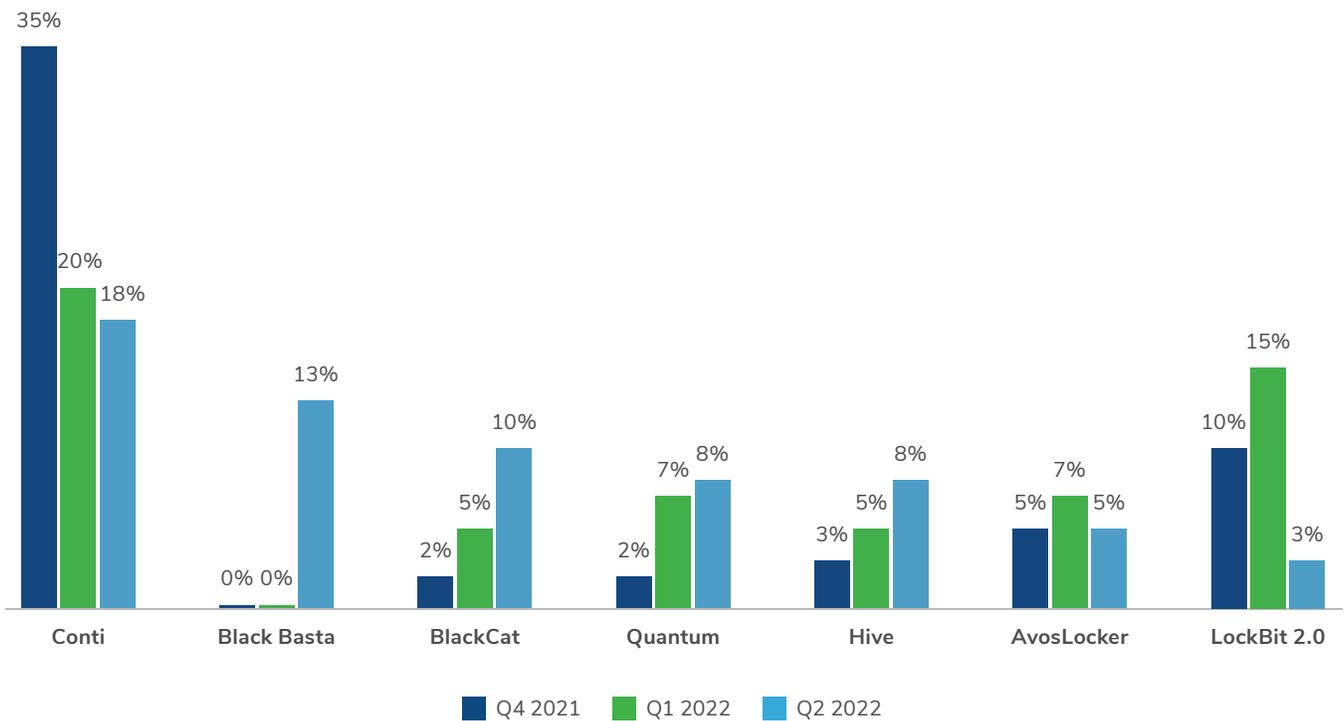
Ransomware Variants

After a series of high-profile leaks, Conti ransomware’s actor-controlled site and chat negotiations page went dark on June 23. Kroll data mirrored this decline in Conti activity with associated ransomware cases accounting for only 18% in Q2 compared with 20% in Q1 and 35% in Q4. Likewise, Kroll saw a drop in LockBit 2.0 activity during the quarter.

Variants on the rise included the previously mentioned Black Basta ransomware gang. Observed by Kroll as leveraging Qakbot malware for access, Black Basta’s first post on underground forums referenced their willingness to buy access into corporate networks, likely recruiting **initial access brokers** to support their activities. Other groups that increased their activity during Q2 included BlackCat, QuantumLocker and Hive.

Supporting Kroll’s findings that the healthcare sector is being targeted by ransomware groups, the U.S. Health Sector Cybersecurity Coordination Center (HC3) issued an analyst note in April indicating that the Hive ransomware group was aggressively targeting the healthcare sector. The Hive ransomware group is known to leverage remote services for access.

Most Popular Ransomware Variants - Past Three Quarters



Best Practices: A Focus on Remote Services

Across the board, ransomware groups continue to use tried and tested techniques to compromise their victim's environments, taking advantage of security weaknesses to gain footholds into systems and launch malicious payloads. This makes maintaining and building cyber resilience a priority to avoid being compromised by a ransomware attack.

In relation to the trends Kroll is seeing around initial access methods, organizations would be wise to pay close attention to the security around remote services. **Implementing multi-factor authentication** on these systems and keeping remote services inaccessible from the internet is advisable. Furthermore, maintaining a **regular patching, testing and vulnerability scanning schedule**, particularly for vulnerabilities in VPNs and RDP services.

Security efforts should be prioritized in the healthcare sector. Checking that backups are available and recovery capabilities are tested, as well as having manual alternatives for electronic tasks (that can maintain continuity of critical functions in the wake of a network attack or outage) is essential.

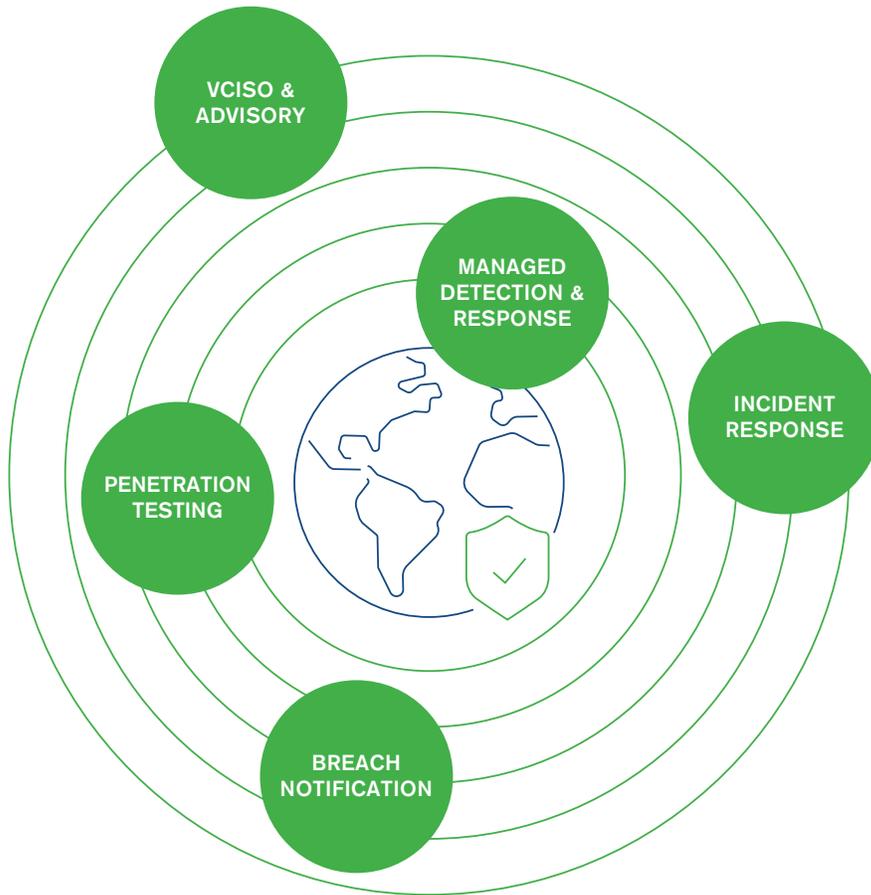
Healthcare Becomes a Target as Ransomware Uses Remote Services as a Route In

It is concerning to see healthcare rise so dramatically up the most targeted industry list, especially at a time when services are undoubtedly under pressure, recovering from the strained environment caused by COVID-19. Though always disruptive, ransomware's ability to grind company operations to a halt, becomes more devastating in an environment where business continuity means saving lives.

Kroll saw an increase in threat actors targeting remote services for initial access into networks in Q2. There were also longer, more evasive attack chains led by actors aiming to launch malware such as Qakbot, and Kroll continued to see activity around high-profile vulnerabilities such as Log4J.

The key takeaway from Q2 2022 was not to neglect remote services in your cyber strategy. With many offices approaching a new hybrid working environment, systems that were hastily deployed at the start of the pandemic may now need readdressing to avoid them becoming a security vulnerability and initial access point for cyberattacks.

Seamless Cyber Risk Solutions



See more at kroll.com/cyber

Additional Resources



New MFA Bypass Phishing Method Uses WebView2 Applications with Hidden Keylogger



A CISO's Guide to Container Security: Understanding Vulnerabilities & Best Practices



The Rise of Vishing and Smishing Attacks – The Monitor, Issue 21



Kroll Responder Managed Detection and Response



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

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 over 6,000 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 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.