

Q3 Healthcare Sector

Quarterly Threat Landscape Scorecard

TLP: CLEAR A-2022-12-07b



Q3 2022 Healthcare Sector Threat Overview

The threat to healthcare sector organizations in Q3 2022 remained broadly consistent with previous quarters, with the ongoing war in Ukraine continuing to shape the cyber threat landscape. In Q3 2022, there were likely increases in particular aspects of the social engineering threat to healthcare organizations, including from smishing, callback phishing, and threat actors leveraging techniques to bypass multi-factor authentication (MFA). ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online v2.0 (FIDO2) and certificate-based authentication. The sustained high pace of vulnerability disclosure, including in internet-connected medical devices and software commonly used by healthcare organizations, will very likely strain out-of-cycle patch management processes and increases the risk of vulnerabilities not being patched in a timely manner. The shift to Initial Access Broker (IAB) market sales being made in private channels rather than advertising in open forums will likely continue and make identifying and mitigating access sales ahead of compromise increasingly challenging. Botnet and malware deployment remained high, including infostealers, trojans, and spyware. Digital extortion attempts against healthcare targets remain below 2021 levels, likely caused in part by difficulty eliciting payments from victims. Incidents in Q3 2022 highlighted the high threat of attacks against third-party providers that could implicate multiple downstream users.

Key Cyber Threats to the Healthcare Sector in Q3 2022



Hackers stealing sensitive patient healthcare information and personally identifiable information



Increased threats from SMS-phishing, callback phishing, and techniques to bypass MFA



Ransomware and digital extortion outfits conducting high-profile attacks against healthcare companies and their third-party partners



Changes to extortion tactics resulting in greater operational downtime, reputational damage, and legal ramifications



Vulnerabilities in third-party software used by healthcare sector organizations and in internet-connected devices



State-aligned threat actors conducting cyber espionage against healthcare bodies



IABs moving towards private means of communication with sellers, making identification and mitigation more difficult



Malware disguised in fake applications targeting employees and members of the public

Healthcare Sector Threats

Categories	Q1 2022	Q2 2022	Q3 2022
Social Engineering			
Vulnerability Exploitation			
Initial Access Brokers			
Botnets			
Malware			
Ransomware			

KEY

Indication of decrease in threat from previous quarter

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter

> Q3 Key Findings:

- Healthcare organizations likely faced an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Vulnerabilities in software commonly used by healthcare organizations were added to CISA's Known Exploited Vulnerabilities (KEV) catalog.
- The threat to healthcare organizations from IABs likely increased in Q3 2022.
- The threat from cyber espionage remained high, with multiple campaigns by threat actors—including state-linked actors—identified in Q3 2022.
- Ransomware and digital extortion attempts against the healthcare sector this quarter highlighted the threat of attacks against third-party providers.

SOCIAL ENGINEERING

ZeroFox Intelligence assesses with low confidence that aspects of the social engineering threat faced by the healthcare sector increased in Q3 2022; attacks against the healthcare sector are very likely underreported. However, it is likely social engineering trends that emerged in campaigns against other sectors in Q3 2022 were also reflected in incidents against the healthcare sector.[1] Multi-industry social engineering campaigns target employees, either directly or via enterprise third-party providers, with increased use of smishing.[2,3]

Analysis indicates an increased threat of callback phishing (vishing), adding legitimacy to malicious emails by impersonating security teams and encouraging victims to return a phone call to authenticate fraudulent activity.[4] Threat actors increasingly leveraged techniques to bypass MFA—including Adversary-in-the-Middle (AiTM), which is now being incorporated into broader Phishing-as-a-Service offerings.[5]

The threat from social engineering campaigns remained evolutionary rather than revolutionary, indicating that exploiting human error remains lucrative for threat actors. Threat actors continued to leverage topical lures to entice engagement with malicious emails, and malware distribution via malicious email attachments remained highly prevalent. Malicious phishing domains and open redirects should be continually monitored and taken down to avoid customers or patients being defrauded or providing an intrusion vector for threat actors. [6,7]

Forward Look:

- Smishing of healthcare organizations' employees and customers is likely to continue on an upward trajectory.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.

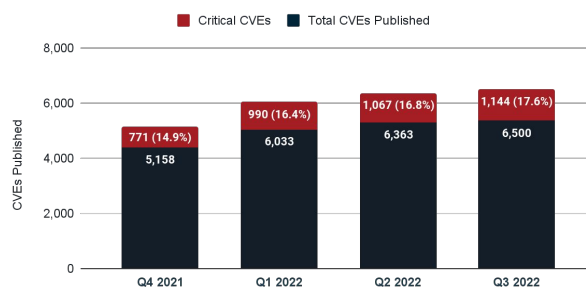
Recommendations:

- Communicate to employees about emerging trends in social engineering scams and how to conduct safe means of authentication.
- Engage ZeroFox Intelligence to conduct an Attack Surface Assessment to understand threats to your organization.

No notable change in threat from previous quarter

Indication of increase in threat from previous quarter

Total CVEs Published by Quarter



Source: hxxps://nvd.nist.gov

VULNERABILITY EXPLOITATION

Reported incidents of vulnerability exploitation against the healthcare sector in Q3 2022 continued to center around commonly-used software modules and Internet-of-things devices. Sustained periods of high vulnerability disclosures place strain on out-of-cycle patch management processes, with vulnerabilities that have long had patches available continuing to be exploited in medical equipment.[8] New disclosures this quarter impacted internet-connected medical devices, as well as Apple operating systems, Atlassian Confluence, Google, Microsoft Windows and Exchange, and WhatsApp.[9,10] Critical vulnerabilities in Zoho ManageEngine and Zimbra email servers were added to CISA's KEV catalog in Q3 2022, of which multiple healthcare organizations are stated to be customers.[11,12]

Forward Look:

- Vulnerabilities in commonly-used software modules and network perimeter infrastructure will likely continue to dominate the exploit landscape.
- Healthcare organizations will likely face an increased threat from threat actors seeking to exploit internet-connected medical devices.

Recommendations:

- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.
- Ensure a thorough understanding of your technology stack and patching schedule, as well as those of operating partners.
- Leverage CISA's KEV catalog to prioritize out-of-cycle vulnerability patching.

FOOTNOTES

[1] hxxps://techmonitor.la/technology/cybersecurity/shatak-hacking-group-healthcare-manufacturing
 [2] hxxps://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations
 [3] hxxps://www.ic3.gov/Media/News/2022/220914-2.pdf
 [4] hxxps://threatpost.com/callback-phishing-security-firms/180182/
 [5] hxxps://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-finance-fraud/
 [6] hxxps://www.bankinfosecurity.com/feds-warn-healthcare-entities-evernote-phishing-scheme-a-19791

[7] hxxps://cyware.com/news/new-seo-poisoning-campaign-spreads-gootloader-malware-ab2a0d7f
 [8] hxxps://www.ic3.gov/Media/News/2022/220912.pdf
 [9] hxxps://thehackernews.com/2022/09/new-vulnerabilities-reported-in-baxters.html
 [10] hxxps://nvd.nist.gov
 [11] hxxps://www.cisa.gov/known-exploited-vulnerabilities-catalog
 [12] hxxps://www.manageengine.com/customers.html

INITIAL ACCESS BROKERS

ZeroFox Intelligence assesses with low confidence that the threat to healthcare organizations from IABs increased slightly in Q3 2022 but remains significantly below 2021 levels. The sustained low numbers of advertised access to healthcare organizations in open forums in Q3 2022 likely reflects an ongoing shift towards brokers preferring private channels to avoid law enforcement scrutiny.[13] Brokers are selling to well-established buyers directly out of an abundance of caution. Brokers are likely increasingly selling access to healthcare organizations to ransomware operators with whom they have established relationships via private channels, underpinning the threat the sector faces from digital extortion.

Forward Look:

- Illicit access to healthcare organizations will likely increasingly be sold via private or direct communication methods.

Recommendations:

- Employ ZeroFox's Threat Intelligence feeds to get ahead of threat actor activity.
- Proactively monitor for potential network access sales to obtain critical early warnings of impending cyberattacks.

Indication of
increase in threat
from previous
quarter

MALWARE

ZeroFox Intelligence observed no major changes in the threat to the healthcare sector from malware deployment in Q3 2022. The sector remained one of the most frequently impacted by hacks and data breaches and will almost certainly remain so owing to the breadth and sensitivity of the data it holds, as well as large sums transferred in payments. [14,15] App stores remained one of the most prolific means of distributing malware.[16] The threat from cyber espionage remained high, with multiple campaigns by threat actors—including state linked actors—identified in Q3 2022.[17,18] ZeroFox Intelligence assesses with low confidence that the threat from the most popular loaders has increased, with Bumblebee and ChromeLoader now deploying some of the most capable malware strains available.

Forward Look:

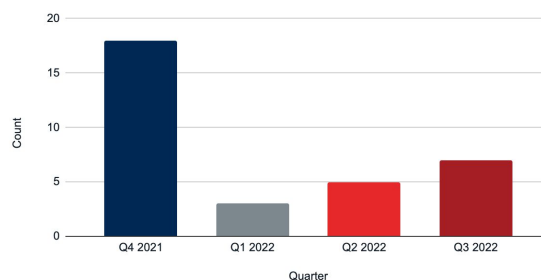
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.
- ZeroFox Intelligence anticipates an increased threat from Russia-linked threat actors targeting healthcare institutions with malware containing destructive components.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise (IOCs) and metadata related to Malware and Ransomware.

No notable
change in
threat from
previous quarter

Advertised IAB Access into Healthcare Organizations by Quarter



Source: ZeroFox Intelligence

BOTNETS

There was no notable change in the threat to healthcare organizations from botnets, which continued to pose a threat via stealing credentials and remotely-controlling infected devices. In Q3 2022, ZeroFox Intelligence ingested almost 45 million credentials harvested by infostealer families commonly deployed by botnets, of which RedLine was most active.[19] Healthcare organizations should be wary of being targeted directly or systems—particularly Internet-of-Things (IoT) devices—being leveraged in politically-motivated Distributed Denial of Service (DDoS) attacks such as those seen against Taiwan and much of Europe.[20,21] Emotet's resurgence continued; it has reportedly infected almost 1.3 million devices since the start of 2022, including healthcare organizations, and is now pushing Quantum and BlackCat ransomware.[22]

Forward Look:

- The threat of healthcare systems being targeted or leveraged in botnet attacks, including by Russia-aligned entities, is likely to increase.
- Emotet is expected to pose an increasing threat to healthcare organizations in the coming months given its resurgence.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate network and infrastructure IOCs of interest, including C2 Domains and Compromised Account Credentials.

No notable
change in
threat from
previous quarter

FOOTNOTES

[13] ZeroFox Intelligence Internal Collections
[14] <https://www.reuters.com/world/china/hacker-offers-sell-data-485-mbn-users-shanghai-covid-app-2022-08-12/>
[15] <https://www.bleepingcomputer.com/news/security/tpi-hackers-steal-millions-from-healthcare-payment-processors/>
[16] <https://www.bleepingcomputer.com/news/security/adware-on-google-play-and-apple-store-installed-13-million-times/>
[17] <https://www.hhs.gov/sites/default/files/evil-corp-threat-profile.pdf>

[18] <https://www.hhs.gov/sites/default/files/ap41-recent-activity.pdf>
[19] ZeroFox Intelligence Internal Collections
[20] <https://www.reuters.com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-ami-d-china-tensions-2022-08-04/>
[21] <https://nsm.no/aktuelt/malware-tjenestenektangrep-mot-norske-nettsteder>
[22] <https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022>

RANSOMWARE

The ransomware and digital extortion threat to healthcare organizations in Q3 2022 remained broadly consistent with previous quarters, with the sector remaining as one of the most heavily-impacted by ransomware attacks.[23,24] Extortion attempts remained below 2021 levels, likely caused in part by difficulty eliciting payments from victims.[25] Incidents this quarter highlight the high threat of attacks against third-party providers that could impact downstream healthcare customers.[26,27,28] Healthcare service providers face a high threat, with threat actors very likely believing that the pressure from downstream dependents will make targets more susceptible to paying ransoms. The healthcare supply chain threat is compounded by developments in extortion tactics, with ALPHV/BlackCat—one of the most prolific targeters of the healthcare sector—providing leaked victim data in a searchable format.[29] While not a novel tactic, LockBit announced a move into conducting DDoS attacks against victims as a pressure tactic, which may see other groups adopt similar methods.[30] The updating of exfiltration tool Exmattter with data corruption functionality indicates a possible move towards ransomware gangs destroying data rather than encrypting it, using the exfiltrated copies as the means of recovering data.[31]

LockBit remained the sector's primary digital extortion threat, and Black Basta, which was flagged in Q2 2022 as an emerging actor, continued on an upward trajectory. Healthcare organizations should also note the threat from state-backed groups.[32,33] Security teams should be wary of updated versions of strains that frequently target the sector and their associated IOCs, including Hive and BlackCat, as well as the unusually high number of new strains identified this quarter.[34] In coming months, the industry may see an increased extortion threat from Karakurt, which saw a significant increase in targeting towards the healthcare sector and is linked to the former Conti operation.[35]

> Forward Look:

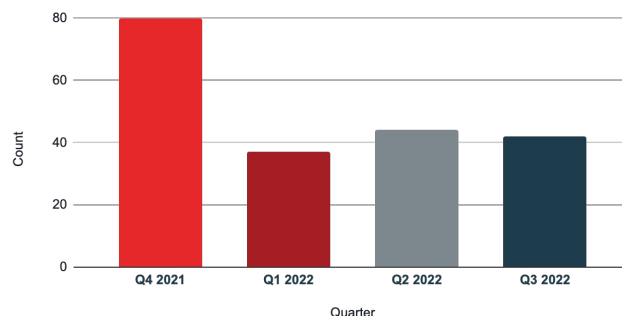
- ZeroFox Intelligence anticipates the threat of digital extortion to healthcare organizations will most likely increase.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational damage, and legal ramifications.

> Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search interface to investigate IOCs and metadata related to Malware and Ransomware.
- Should an organization be impacted by a ransomware event, engage ZeroFox Intelligence for support.

No notable
change in
threat from
previous quarter

Total Healthcare Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

QUARTERLY SPOTLIGHT

Organizations must adapt their approach to security as threat actors pivot to circumvent or intercept MFA. Weak MFA methods, such as SMS verification codes, have long been exploited by threat actors to compromise enterprise systems. However, analysis indicates an increase in recent months of threat actors leveraging phishing techniques where traditionally-strong MFA gives little or no protection. These techniques include AITM phishing, MFA fatigue or spamming—as encouraged by Lapsus\$—and OAuth Consent phishing attempts, which are all techniques that are included in widely-distributed phishing kits.

Phishing-resistant MFA attempts to limit a corporation's risk of social engineering attacks and should be implemented in conjunction with a broader Zero Trust initiative.

ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online v2.0 (FIDO2) and certificate-based authentication.[36] FIDO2 aims to maximize security with minimal impact on user experience. It supports passwordless, two-factor, and multi-factor user authentication with embedded or external authenticators. All FIDO protocols are based on Public Key Infrastructure.

While phishing-resistant MFA will not protect against all attacks, ZeroFox Intelligence has yet to observe threat actors on the deep and dark web publishing or brokering exploits related to phishing-resistant MFA.[37]

FOOTNOTES

- [23] <https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/>
- [24] <https://www.securityweek.com/new-york-emergency-services-provider-says-patient-data-stolen-ransomware-attack>
- [25] ZeroFox Intelligence Internal Collections
- [26] <https://www.databreaches.net/associated-eye-care-partners-llc-discloses-vendor-breach-can-you-guess-which-vendor/>
- [27] <https://www.bankinfosecurity.com/ransomware-attack-caused-nhs-outage-says-vendor-a-18779>
- [28] <https://www.epomagazine.com/cyber-security/identity-management-firm-entrust-suffers-a-security-breach-ransomware-gang-obtains-files/>
- [29] <https://blog.cyble.com/2022/07/06/alphv-ransomware-expands-its-arsenal-of-extortion-techniques/>

- [30] <https://www.itworldcanada.com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301>
- [31] <https://securityaffairs.io/wordpress/36226/cyber-crime/exmattter-tool-shift-extortion-tactics.html>
- [32] <https://blog.reversinglabs.com/blog/gwainlocker-ransomware-targets-south-korean-industrial-and-pharmaceutical-c>
- [33] <https://www.cisa.gov/uscert/ncas/alerts/aa22-187a>
- [34] Updated strains of ransomware identified this quarter include Liith, Cheers, Yanluowang, Omega, RedAlert, BianLian, Royal, Monster, Agenda, and PlayCrypt.
- [35] <https://www.cisa.gov/uscert/ncas/alerts/aa22-152a>
- [36] <https://fidoalliance.org/specifications/>
- [37] ZeroFox Intelligence identified an academic paper that describes a potential weakness in FIDO UAF that could allow threat actors to bypass verification if they have a malware implant.

OUTLOOK

The cyber threat to the healthcare sector is unlikely to change significantly in the near term. However, a swift resolution to Russia's war in Ukraine or a rapid downturn in global economic conditions could catalyze changes to the nature of the threat.

Social engineering scams will almost certainly remain evolutionary rather than revolutionary, with a high prevalence of campaigns impersonating healthcare providers targeting members of the public. Healthcare organizations should expect to be increasingly targeted via third-party providers, particularly those afforded trusted access within a network. Threat actors will very likely increasingly seek to bypass MFA to compromise corporate environments, including targeting authentication providers. ZeroFox Intelligence anticipates an increasing threat of malicious actors exploiting vulnerabilities in internet-connected medical devices, although vulnerabilities in commonly-used software modules will likely continue to dominate the exploit landscape.

As a critical sector, healthcare supply chains, particularly those across Europe, will likely become an increasingly attractive target for Russia-aligned threat actors. There is an even chance ransomware and digital extortion attacks against the healthcare sector will increase in Q4 2022. As the Northern Hemisphere enters winter and healthcare services face greater strain, threat actors will likely increasingly seek to target healthcare organizations, perceiving that disruption to providers' operations during the winter period may make them more likely to pay extortion demands.

ZeroFox Intelligence anticipates a continued increase in IABs leveraging private means of communication to sell access, as well as leveraging trusted relationships with specific buyers. There is no indication the threat will decrease, with buyers still seeking to obtain access via brokers. However, the ability to identify and mitigate access sales ahead of compromise will very likely become increasingly challenging, amplifying the importance of partnerships with third-party security vendors that have access to private channels.


ZEROFOX INTELLIGENCE

December 7, 2022

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use **TLP: RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share **TLP: RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use **TLP: AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share **TLP: AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use **TLP: GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use **TLP: CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share **TLP: CLEAR** information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform.

With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready to See for Yourself?

> Request a Demo:

Sign up on zerofox.com/request-a-demo

> Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400