

Q3 Public Sector

Quarterly Threat Landscape Scorecard

TLP: CLEAR A-2022-12-07a



Q3 2022 Public Sector Threat Overview

The threat to public sector organizations in Q3 2022 remained broadly consistent with previous quarters, with the ongoing war in Ukraine continuing to shape the cyber threat landscape. ZeroFox Intelligence assesses that the threat to the sector will likely increase in the coming months, underpinned by politically-inspired targeting. There were increases in particular aspects of the social engineering threat, 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 disclosures, particularly in software commonly used by public sector entities, will very likely strain out-of-cycle patch management processes and increase the likelihood 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, with Eastern European public sector bodies in particular likely facing an increased threat from distributed denial-of-service (DDoS) attacks by pro-Russian threat actors. Digital extortion attempts remained below 2021 levels, likely caused in part by difficulty eliciting victims' payments. However, incidents in Q3 2022 highlighted the high threat of attacks against third-party providers that could implicate multiple downstream customers; in coming months, the sector is likely to see an increase in politically-motivated extortion targeting.

Key Cyber Threats to the Public Sector in Q3 2022



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



Vulnerabilities in third-party software used by public sector bodies and the pace of exploitation



State-aligned threat actors conducting cyber espionage against public sector bodies and personnel



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



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



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



Russia-aligned threat actors targeting government and government-linked entities



Ransomware and digital extortion outfits targeting public sector entities

Public 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:

- Public sector organizations likely faced an increased threat of smishing, callback phishing (vishing), and phishing techniques that bypass MFA.
- Vulnerabilities in software commonly used by public sector organizations were added to CISA's Known Exploited Vulnerabilities (KEV) catalog.
- The threat to public sector organizations from IABs increased in Q3 2022
- Most public sector bodies around the world saw a negligible change in the threat from botnets, though Eastern European entities likely faced an increased threat.
- While there were fewer ransomware and digital extortion attempts, threat actors continued to demonstrate a high degree of capability in attacks against critical infrastructure and government functions.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 12:00 PM (EST) on October 10, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

SOCIAL ENGINEERING

The overall threat to the public sector from social engineering remained broadly consistent, although ZeroFox Intelligence has identified categories of increased threat. Public sector organizations should note a likely increased threat from smishing attacks targeting employees, either directly or via enterprise third-party providers, as well as members of the public.[1,2,3] Analysis also indicates an increasing 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 continued to leverage topical lures to entice engagement with malicious emails. Phishing domains impersonating public sector entities remained prevalent, including leveraging tax-related lures.[5,6,7] Impersonating phishing domains and open redirects should be continually monitored and taken down to avoid customers being defrauded or providing an intrusion vector for threat actors. Malware distribution via malicious email attachments and contracting opportunities remained highly prevalent.[8,9] Threat actors have begun leveraging Adversary-in-the-Middle (AiTM) techniques to bypass MFA, including through Phishing-as-a-Service (PhaaS).

Forward Look:

- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.
- Smishing of public sector employees, particularly high profile individuals, and members of the public is likely to continue on an upward trajectory.
- Members of the public are likely to be increasingly targeted with financial-relief scams given the ongoing strain on global economic markets.

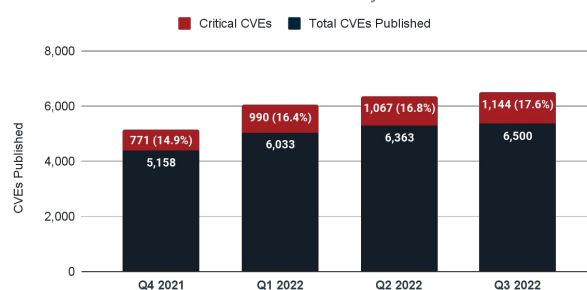
Recommendations:

- 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](https://nvd.nist.gov)

VULNERABILITY EXPLOITATION

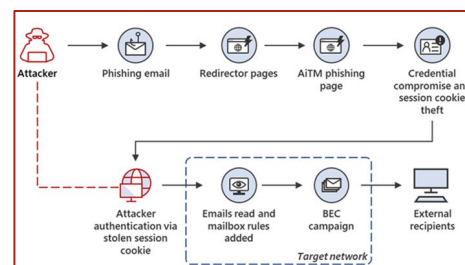
The most widely-reported examples of vulnerability exploitation in Q3 2022 remained in commonly-used software modules and network perimeter infrastructure. Sustained periods of high vulnerability disclosures place strain on out-of-cycle patch management processes, with new disclosures in Q3 2022 impacting Apple operating systems, Atlassian Confluence, Google, Microsoft Windows and Exchange, and Whatsapp.[10] Critical vulnerabilities in Zoho ManageEngine and Zimbra email servers were added to CISA's Known Exploited Vulnerabilities (KEV) catalog in Q3 2022, of which multiple public sector entities are stated to be customers.[11]

Forward Look:

- Vulnerabilities in commonly-used software modules and network perimeter infrastructure will likely continue to dominate the exploit landscape.

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.



AiTM Phishing Campaign Overview
Source: [hXXps://www.microsoft.com](https://www.microsoft.com)

FOOTNOTES

[1] [hXXps://www.securityweek.com/european-central-bank-head-targeted-hacking-attempt/](https://www.securityweek.com/european-central-bank-head-targeted-hacking-attempt/)
 [2] [hXXps://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations/](https://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations/)
 [3] [hXXps://www.kentucky.com/news/local/crime/article264967969.html](https://www.kentucky.com/news/local/crime/article264967969.html)
 [4] [hXXps://threatpost.com/callback-phishing-security-firms/180182/](https://threatpost.com/callback-phishing-security-firms/180182/)
 [5] [hXXps://www.bittimes.com/cyber-security-hackers-target-national-portal-india-via-unprecedented-phishing-technique-850189](https://www.bittimes.com/cyber-security-hackers-target-national-portal-india-via-unprecedented-phishing-technique-850189)
 [6] [hXXps://blog.jcyble.com/2022/09/14/phishing-campaign-targets-greek-banking-users/](https://blog.jcyble.com/2022/09/14/phishing-campaign-targets-greek-banking-users/)

[7] [hXXps://blog.jcyble.com/2022/09/13/phishing-campaign-targets-japanese-tax-payers/](https://blog.jcyble.com/2022/09/13/phishing-campaign-targets-japanese-tax-payers/)
 [8] [hXXps://thehacknews.com/2022/07/researchers-uncover-new-attempts-by.html](https://thehacknews.com/2022/07/researchers-uncover-new-attempts-by.html)
 [9] [hXXps://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-impersonate-us-govt-agencies/](https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-impersonate-us-govt-agencies/)
 [10] [hXXps://nvd.nist.gov](https://nvd.nist.gov)
 [11] [hXXps://www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

INITIAL ACCESS BROKERS

ZeroFox Intelligence assesses with low confidence that the threat to public sector organizations from IABs increased in Q3 2022 but remains below 2021 levels. The sustained low numbers of advertised access to public sector organizations in open forums in Q3 2022 likely reflects an ongoing shift towards brokers preferring private channels to avoid law enforcement scrutiny.[12] According to threat actor chatter observed by ZeroFox Intelligence, brokers are selling to well-established buyers directly out of an abundance of caution. Brokers are likely increasingly selling access to high-profile public sector entities to ransomware operators with whom they have established relationships via private channels, underpinning the threat the sector has faced from digital extortion.

Forward Look:

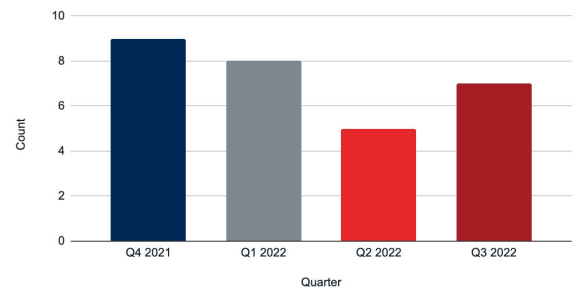
- Illicit access to public sector entities will likely increasingly be sold via private or direct communication methods.

Recommendations:

- Employ ZeroFox 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

Advertised IAB Access into Public Sector Organizations by Quarter



Source: ZeroFox Intelligence

BOTNETS

Most public sector bodies around the world saw a negligible change in the threat from botnets in Q3 2022, which continued to pose a threat via stealing credentials and remotely-controlling infected devices. Some public sector entities, particularly in Eastern Europe, likely saw an increase in threat.[19,20,21] Public sector organizations should be wary of being targeted directly or having their systems leveraged in politically-motivated DDoS attacks.[22,23] In Q3 2022, ZeroFox Intelligence ingested almost 45 million credentials harvested by infostealer families commonly deployed by botnets, of which RedLine was most active.[24] Emotet's resurgence continued, reportedly infecting almost 1.3 million devices since the start of 2022 and now pushing Quantum and BlackCat ransomware.[25]

Forward Look:

- The threat of public sector organizations' systems being targeted in botnet attacks by Russia-aligned entities is likely to increase.
- Emotet is expected to pose an increasing threat to public sector 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

No notable
change in
threat from
previous quarter

MALWARE

ZeroFox Intelligence assesses with low confidence that the threat to the public sector from malware deployment in Q3 2022 remained broadly consistent with previous quarters, with the landscape continuing to be shaped largely by Russia's ongoing war in Ukraine. The greatest threat to public sector entities came from cyber espionage; campaigns by multiple threat actors—including state linked entities—were identified in Q3 2022.[13,14,15,16] Public sector entities are disproportionately impacted by data leaks of sensitive information.[17] Spyware modules remain of concern, including from malicious modules within fraudulent apps.[18] Low barriers to entry and the pace of trojan updates continued to sustain a high threat to the sector.

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 public sector institutions with malware containing espionage and destructive components.

Recommendations:

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

FOOTNOTES

[12] ZeroFox Intelligence Internal Collections
[13] <https://www.bleepingcomputer.com/news/security/belgium-says-chinese-hackers-attacked-its-ministry-of-defense/>
[14] <https://www.mandiant.com/resources/blog/qpt29-continues-targeting-microsoft>
[15] <https://www.itnews.com.au/news/chinese-state-hackers-targeted-australian-federal-and-local-govt-584649>
[16] <https://thehackernews.com/2022/09/chinese-hackers-target-government.html>
[17] <https://www.cybercoop.com/central-american-hacking-group-releases-emails/>
[18] <https://www.forbes.com/sites/thomasbrewster/2022/09/04/whatsapp-and-signal-fakes-are-spyware-from-india-and-pakistan-facebook-warns/?sh=dce8f0207c9b>

[19] <https://stisc.gov/jmd/ro/comunicat-informativ-privind-tentativele-de-atac-cibernetice-din-ultimele-72-de-ore>
[20] <https://www.infosecurity-magazine.com/news/features/estonias-battle-against-a-deluge/>
[21] <https://www.bankinfosecurity.com/lithuanian-energy-firm-experiences-ddos-a-19555>
[22] <https://nsm.no/aktuelt/malwarede-tjenestekataloger-mot-norske-nettsteder>
[23] <https://www.reuters.com/world/asia-pacific/taiwan-defence-ministry-website-hit-by-cyber-attacks-amid-china-tensions-2022-08-04/>
[24] ZeroFox Intelligence Internal Collections
[25] <https://www.advintell.com/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022>

RANSOMWARE

The public sector likely saw a slight reduction in the overall threat from ransomware and digital extortion in Q3 2022, with a fall in the frequency of attacks—including against local governments.

However, threat actors continued to demonstrate a high degree of capability, with indications of an increase in attacks against critical infrastructure and government functions.[26,27,28,29,30] Extortion attempts remain below 2021 levels, likely caused in part by difficulty eliciting payments from victims.[31] ZeroFox Intelligence continued to see impactful attacks against government systems, typically targeting smaller or less technologically-advanced nations. Incidents this quarter also highlighted the high threat of attacks against third-party providers that could impact multiple downstream customers.[32] The supply chain threat is compounded by developments in extortion tactics, with ALPHV/BlackCat providing leaked victim data in a searchable format.[33] 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.[34] The updating of exfiltration tool Exmacter 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.

LockBit remained the sector's primary digital extortion threat and was responsible for almost half of all attacks. Black Basta, flagged in Q2 2022 as an emerging actor, continued its upward trajectory. Security teams should be wary of updated versions of strains that frequently target the sector and their associated IOCs, including Hive, as well as the unusually high number of new ransomware strains identified this quarter.[35] In coming months, public sector entities in Europe may see an increased extortion threat from Russia-aligned threat actors—a trend that has already started.[36,37]

Forward Look:

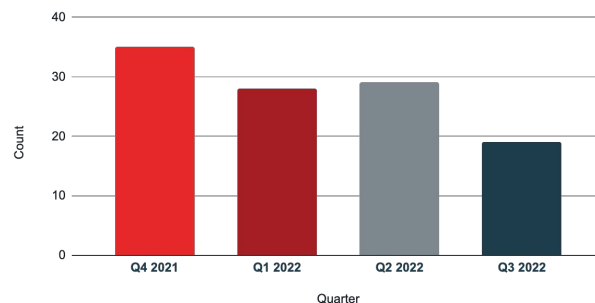
- ZeroFox Intelligence anticipates ransomware and digital extortion attempts against public sector organizations will likely increasingly leverage destructive modules.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims that cause greater operational downtime, reputational 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.

Indication of decrease in threat from previous quarter

Total Public 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.[38] 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.[39]

FOOTNOTES

[26] <https://www.hindustantimes.com/india-news/ransomware-attack-hits-goa-s-flood-monitoring-system-demand-crypto-as-payment-101857188573572.html>
 [27] <https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/>
 [28] <https://www.bleepingcomputer.com/news/security/argentinian-judiciary-of-c-rdoba-hit-by-play-ransomware-attack/>
 [29] <https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-disrupts-govt-agency-in-dominican-republic/>
 [30] <https://www.govinfosecurity.com/chilean-court-system-hit-ransomware-attack-a-20159>
 [31] ZeroFox Intelligence Internal Collections
 [32] <https://www.cpmagazine.com/cyber-security/identity-management-firm-entrust-suffers-a-security-breach-ransomware-gang-obtains-files/>

[33] <https://blog.cyble.com/2022/07/06/clphv-ransomware-expands-its-arsenal-of-extortion-techniques/>
 [34] <https://www.itworldcanada.com/article/lockbit-ransomware-gang-adding-ddos-attacks-to-its-threats/500301>
 [35] New ransomware strains identified this quarter include Lilith, Cheers, Yanluowang, Omega, RedAlert, BianLian, Royal, Monster, Agenda, and PlayCrypt.
 [36] <https://www.securityweek.com/montenegro-reports-massive-russian-cyberattack-against-govt>
 [37] <https://www.timesofindia.com/uk/ransomware/ransomware-attack-disrupts-bosnia-and-herzegovina-parliament-servers-stalls-opera-tions-for-two-weeks-10983>
 [38] <https://fidoalliance.org/specifications/>
 [39] 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 public sector will likely continue to be heavily influenced by Russia's war in Ukraine. ZeroFox Intelligence anticipates pro-Russia threat actors and state-linked entities will likely increasingly target countries and organizations with malware in retaliation for perceived stances taken during the war. While unlikely, 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, and ZeroFox expects threat actors to increasingly seek to bypass MFA to compromise public sector environments. Malicious domains impersonating government entities will almost certainly remain highly prevalent, with ZeroFox Intelligence anticipating a Q4 2022 increase in financial relief scams leveraging the cost of living and economic downturn. ZeroFox Intelligence also anticipates increased targeting of authentication providers.

Pro-Russia threat actors and state-linked entities have already begun targeting countries and public sector bodies with malware and DDoS attacks. ZeroFox Intelligence expects this trend to continue, likely impacting sector organizations perceived as being unsupportive of—or opposed to—Russia. Public sector entities should expect to be increasingly targeted via third-party providers, particularly those afforded trusted access within a network.

ZeroFox Intelligence anticipates a continued increase in IABs leveraging both private means of communication to sell access and 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.



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

