

Key Findings

- The threat to public sector employees and members of the public from smishing and callback phishing (vishing) remained high.
- The threat of nefarious actors exploiting Common Vulnerabilities and Exposure (CVEs) likely increased in Q1 2023, with threat actors continuing to target commonly-used software modules and products reportedly used by multiple federal, national, and central government entities.
- The threat from ransomware and digital extortion likely increased, underpinned by a significant increase in LockBit deployment against sector targets. Threat actors may be becoming increasingly emboldened to target high-value public sector targets, believing that any blowback will be small or inconsequential.
- 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.
- Malware-as-a-service offerings sustained low barriers to entry for threat actors seeking to target public sector entities.

Public Sector Threats

Categories	Q2 2022	Q3 2022	Q4 2022	Q1 2023
Social Engineering				
Vulnerability Exploitation				
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

Key Cyber Threats to the Public Sector in Q1 2023

- Ransomware and digital extortion outfits targeting public sector entities and third-party service providers
- Threat actors exploiting vulnerabilities in commonly-used software modules to target public sector bodies
- High threats stemming from spear phishing, smishing, callback phishing, and techniques to bypass Multi-Factor Authentication
- State-aligned threat actors conducting cyber espionage against public sector bodies and personnel
- Initial Access Brokers (IABs) selling illicit access to established buyers via private means of communication, making identification and mitigation more difficult
- State-aligned threat actors leveraging custom-made malware against public sector Information Technology and Operational Technology systems
- Infostealers and botnets stealing credentials and remotely controlling infected Internet-of-Things devices
- Saturated trojan markets sustaining low barriers to entry and high pace of new Indicators of Compromise (IOCs)

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 (EDT) on April 10, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

SOCIAL ENGINEERING

ZeroFox Intelligence observed no significant change in the threat to public sector entities from social engineering campaigns in Q1 2023. Financially and politically-motivated actors conducted successful attacks against the sector, targeting government representatives, employees, and members of the public with phishing domains, smishing, and telephone-oriented attack delivery campaigns.[1,2,3,4] Industry-agnostic campaigns conducted by actors with a history of targeting the sector also remained prevalent.[5] Threat actors leveraged topical lures—such as tax-return season—in low-sophistication impersonation campaigns, encouraging members of the public to visit malicious domains and phishing pages. Malware distribution via malicious email attachments remained highly prevalent, and there is some indication of an increase in Search Engine Optimization (SEO) / Search Engine Results Pages (SERP) poisoning by strains known to target the sector, including—but not limited to—GootKit, IcedID, BatLoader, RedLine, and Vidar.[6,7] ZeroFox Intelligence also notes an increase in malicious campaigns leveraging Google ads as a means of distributing and delivering malware.[8,9]

Forward Look:

- The threat to public sector entities from spear-phishing, smishing, and malicious domains will likely remain high.
- The threat to the sector from SEO/SERP poisoning and Google ads will continue on an upward trajectory.

Recommendations:

- Communicate to employees and the public about emerging trends in social engineering scams.
- Leverage ZeroFox Intelligence's Attack Surface Assessment to understand the threats faced.

No notable
change in
threat from
previous quarter

INITIAL ACCESS BROKERS (IABs)

ZeroFox Intelligence assesses with low confidence that there was no significant change in the threat to government entities from IABs in Q1 2023.[10] Brokers continued to leverage private channels for selling to well-established buyers, exercising high levels of caution to avoid law enforcement scrutiny. Advert content continued to typically focus on vulnerabilities in remote working infrastructure, including Virtual Private Networks and Remote Desktop Protocol.

Forward Look:

- The threat to public sector organizations will likely continue to manifest via brokers leveraging private communication channels to sell access to established buyers.

Recommendations:

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

No notable
change in
threat from
previous quarter

VULNERABILITY EXPLOITATION

Public sector organizations likely faced an increased threat of nefarious actors exploiting CVEs, with Q1 2023 seeing the highest percentage of disclosed vulnerabilities rated critical (18.4 percent) on record.[11,12] The Cybersecurity and Infrastructure Security Agency's (CISA) updates to its Known Exploited Vulnerabilities (KEV) catalog included high and critical severity vulnerabilities that almost certainly impact public sector entities, including exploits impacting iOS operating systems, Google Chrome, Microsoft Windows, and Zoho ManageEngine.[13] Public sector entities very likely remained affected by vulnerabilities in hardware and software for industrial control systems, such as Sewio and Siemens.[14,15] Other critical CVEs disclosed in Q1 2023 impacted SAP products, which are reportedly used by multiple federal, national, and central government entities. Public sector organizations were disproportionately unaffected by Clop's January 2023 successful exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software. While organizations in most industries were extorted, public sector entities accounted for less than 4 percent of victims.[16]

Forward Look:

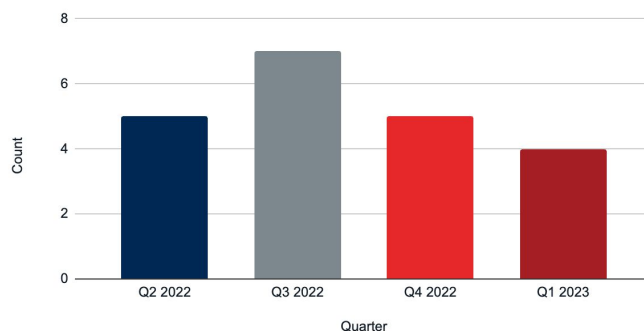
- Vulnerabilities in commonly-used software modules and remote working infrastructure will very likely continue to dominate the exploit landscape.

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.

Indication of
increase in threat
from previous
quarter

Advertised IAB Access into Public Sector Organizations by Quarter



Source: ZeroFox Intelligence

FOOTNOTES

[1] <https://www.theguardian.com/politics/2023/feb/08/scottish-mp-stewart-mcdonald-emails-hacked-russia-linked-group>
[2] <https://www.bleepingcomputer.com/news/security/emotet-malware-distributed-as-fake-w-9-tax-forms-from-the-irs/>
[3] <https://www.armorblox.com/blog/armorblox-stops-attack-impersonating-social-security-administration/>
[4] <https://www.ft.com/content/5c32261c-b1a6-488e-9002-0ca9e0c8f1fb>
[5] <https://www.bleepingcomputer.com/2023/02/01/qakbats-evolution-continues-with-new-strategies>
[6] <https://www.bleepingcomputer.com/news/security/yorotrooper-cyberespies-target-cis-energy-orgs-eu-embassies/>
[7] <https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evade-defenses/>
[8] <https://www.bleepingcomputer.com/news/security/ransomware-access-brokers-use-google-ads-to-breach-your-network/>

[9] <https://www.pcmag.com/news/bitwarden-warns-of-scams-ads-on-google-posing-as-the-password-manager>
[10] ZeroFox Intelligence Internal Collections
[11] <https://nvd.nist.gov>
[12] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-074a>
[13] <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
[14] <https://certportal.siemens.com/productcert/pdf/ssa-482757.pdf>
[15] <https://blog.cyble.com/2023/01/27/insecure-military-ics-infrastructure-poses-a-risk-to-national-security/>
[16] ZeroFox Intelligence Internal Collections



BOTNETS

There was no significant change in the threat to most public sector organizations from botnets in Q1 2023, which continued to pose a threat via stealing credentials and remotely-controlling infected devices. In Q1 2023, ZeroFox Intelligence ingested almost 90 million credentials harvested by infostealer families commonly deployed by botnets, including Vidar, Racoon, Andromeda, and RedLine.[17] Public sector entities across Europe continued to see a high threat of Distributed Denial of Service (DDoS) attacks—with attacks in Q1 2023 claimed by pro-Russian entities affecting Serbia, Estonia, Slovakia, Austria, France and other NATO entities—although the impact of such attacks remained limited.[18,19,20,21]

Forward Look:

- The threat from botnets is unlikely to change considerably in the near term. However, public sector-linked entities in countries pledging support for Ukraine are likely to face continued high threats from Russia-aligned entities.

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

MALWARE

ZeroFox Intelligence observed no significant capability changes in the malware deployed against public sector targets in Q1 2023. Low cost malware-as-a-service offerings and the high pace of trojan and infostealer updates continued to sustain low barriers to entry for threat actors, facilitating data theft and the interception of two-factor authentication codes.[22] The public sector remained frequently impacted by data leaks of sensitive information.[23,24] The threat from cyber espionage remained high, with campaigns by state-linked entities and Advanced Persistent Threat groups identified leveraging custom malware to target public sector entities.[25,26,27] The sector likely faced a high threat from actors upgrading prolific malware strains with powerful loader capabilities, and spyware modules remained of considerable concern—including from malicious modules within fraudulent apps.[28,29,30,31,32]

Forward Look:

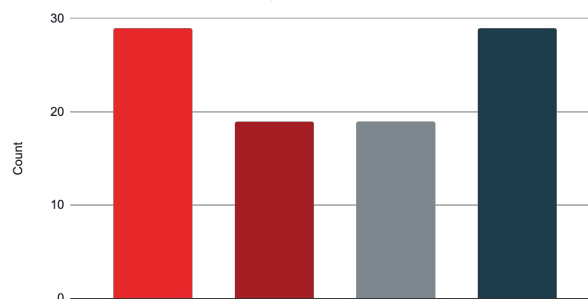
- The threat to public sector entities in countries perceived as unfriendly towards Russia will likely increase, with pro-Russian actors deploying malware with espionage and destructive components against sector targets.

Recommendations:

- Utilize the ZeroFox Platform's Intelligence Search Interface to investigate IOCs and metadata related to Malware.

No notable change in threat from previous quarter

Total Public Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

RANSOMWARE

The threat to the public sector from ransomware and digital extortion likely increased in Q1 2023. Local government systems and public sector entities' third-party service providers remained most at risk from ransomware and digital extortion, although ZeroFox Intelligence continued to see a resurgence in threat actors targeting central government functions and critical infrastructure.[33,34,35,36] This likely represents an increasingly emboldened threat actor landscape with operators confident that such attacks will result in small and inconsequential blowback, if any.

The increase in ransomware and digital extortion threats to the public sector was driven most significantly by the increased deployment of LockBit, which more than tripled the number of sector targets hit in Q1 2023 from the previous quarter and was responsible for more than half of attacks.[37,38,39] The increase in LockBit deployment was seen across multiple other sectors. Q1 2023 also saw increased deployment of Royal ransomware and persistent targeting of sector entities by Vice Society. ZeroFox Intelligence also identified a significant increase in the proportion of attacks targeting the North American and Asia-Pacific regions—likely a continued reflection of threat actors' emboldened perception that such attacks will avoid blowback.

Indication of increase in threat from previous quarter

Forward Look:

- ZeroFox Intelligence anticipates digital extortion attempts against public sector organizations will likely increasingly abandon encryption and focus on exfiltration and extortion.

Recommendations:

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

FOOTNOTES

- [17] ZeroFox Intelligence Internal Collections
 [18] <https://www.privacyaffairs.com/russian-ddos-ukraine-estonia/>
 [19] <https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-03.pdf>
 [20] <https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CB-23-04.pdf>
 [21] <https://www.intelnews.com/serbia-reports-massive-cyberattack-on-interior-ministry-266192/>
 [22] <https://thehacknews.com/2023/03/03/infostealer-new-threat-using-facebook.html>
 [23] <https://thehacknews.com/2023/03/03/infostealer-new-threat-using-facebook.html>
 [24] <https://thehacknews.com/2023/03/03/infostealer-new-threat-using-facebook.html>
 [25] <https://www.bleepingcomputer.com/news/security/us-no-fly-list-shared-on-a-hacking-forum-government-investigating/>
 [26] <https://www.bleepingcomputer.com/news/security/new-dark-pink-apt-group-targets-govt-and-military-with-custom-malware/>
 [27] <https://www.bleepingcomputer.com/news/security/winter-vivern-hackers-exploit-zimbra-flaw-to-steal-nato-emails/>

- [28] <https://www.bleepingcomputer.com/news/security/purecrypter-malware-hits-govt-orgs-with-ransomware-info-stealers/>
 [29] <https://www.reuters.com/world/europe/polish-mayor-targeted-by-pegasus-spyware-media-2023-03-03/>
 [30] <https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/>
 [31] <https://thehacknews.com/2023/02/gootkit-malware-adapts-new-tactics-ta.html>
 [32] <https://www.bleepingcomputer.com/news/security/new-icadid-variants-shift-from-bank-fraud-to-malware-delivery/>
 [33] <https://www.bleepingcomputer.com/news/security/city-of-oakland-declares-state-of-emergency-after-ransomware-attack/>
 [34] <https://www.teissl.co.uk/news/tonga-communications-hit-with-a-ransomware-attack-11714>
 [35] <https://www.cronup.com/el-fondo-nacional-de-salud-tonasa-habia-sido-comprometida-por-un-ransomware/>
 [36] <https://www.bleepingcomputer.com/news/security/us-marshals-service-investigating-ransomware-attack-data-theft/>
 [37] ZeroFox Intelligence Internal Collections
 [38] <https://www.bleepingcomputer.com/news/security/la-housing-authority-discloses-data-breach-after-ransomware-attack/>
 [39] <https://www.cbsnews.com/detroit/news/allen-park-ransomware-threat/>



OUTLOOK

ZeroFox Intelligence assesses the threats facing the public sector will continue to evolve over the next six months, with developments continuing to be heavily influenced by Russia's war in Ukraine. Pro-Russian threat actors and state-linked entities are expected to increasingly target public sector entities in Western countries they deem as unfriendly toward Russia.

ZeroFox Intelligence anticipates that the threat from ransomware and digital extortion operations may increase in Q2 2023 as threat actors are emboldened and galvanized by recent successes. Public sector entities should expect to be increasingly targeted via third-party providers—particularly those afforded trusted access within a network. ZeroFox Intelligence anticipates continued social engineering scams impersonating public sector entities to capitalize on rising costs of living, as well as a sustained high threat from smishing and vishing campaigns targeting sector employees. In coming quarters, threat actors are expected to increasingly leverage Artificial Intelligence tools to aid the credibility of their social engineering campaigns. Identifying network access sales is expected to become increasingly difficult, with brokers continuing to leverage private means of communication to sell access, and amplifying the importance of partnerships with third-party security vendors that have access to private channels.

ZEROFOX INTELLIGENCE
May 26, 2023

APPENDIX A: ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B: 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

