

### | Key Findings Q2 Public Sector

- The threat to public sector organizations from ransomware and digital extortion (R&DE) likely remained broadly consistent in Q2 2023, bucking an upward trend seen in almost all other sectors. This is likely driven by Clop operatives’ statement that they would not extort government organizations as part of their successful exploitation of a zero-day vulnerability in MOVEit file transfer software.
- The threat of nefarious actors exploiting Common Vulnerabilities and Exposures (CVEs) remained high in Q2 2023, with threat actors continuing to target commonly-used software modules and products reportedly utilized by multiple federal, national, and central government entities.
- Search Engine Optimization (SEO) poisoning and leveraging of malicious Google adverts to disseminate malware continued on an upward trajectory.
- ZeroFox Intelligence assesses with low confidence that the threat to the public sector from malware deployment increased in Q2 2023, underpinned by indications of increased Advanced Persistent Threat (APT) activity targeting government entities globally.
- Illicit access to public sector organizations advertised in dark web forums reduced in Q2 2023, bucking an overall upward trend seen in most other sectors.

### Public Sector Threats

| Categories                 | Q3 2022 | Q4 2022 | Q1 2023 | Q2 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 Q2 2023



APTs leveraging custom malware against public sector Information Technology and Operational Technology systems



Ransomware and digital extortion outfits targeting public sector entities and third-party service providers



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



Threat actors conducting spear phishing, smishing, and callback phishing campaigns, as well as leveraging techniques to bypass Multi-Factor Authentication (MFA)



Threat actors exploiting vulnerabilities in commonly-used software modules to target public sector bodies



Initial Access Brokers (IABs) conducting illicit access sales via private means of communication, making identification and mitigation more difficult



Spyware and infostealer modules deployed to intercept or exfiltrate sensitive data



Data breaches resulting from threat actors stealing credentials, sensitive public information, and other data

**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 July 10, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



### SOCIAL ENGINEERING

ZeroFox Intelligence identified no significant change in the threat to the public sector from social engineering in Q2 2023. The threat remained high to public sector employees, as well as members of the public via government entity impersonation.[1] Threat actors leveraged topical lures—such as tax-return season—in spear-phishing, smishing, and telephone-oriented attacks.[2,3] Threat actors impersonated government entities to steal credentials and sensitive information.[4,5] Malicious apps continued to be used to disseminate malware, posing a high risk for government entities that permit employees to sync personal devices with corporate networks.[6,7] SEO poisoning likely remained on an upward trajectory, as well as campaigns leveraging malicious Google ads that promote popular software to distribute malware.[8,9] Threat actors continued to turn to less traditional file types in malicious emails, including OneNote, restricted permission messages (RPMMSG), and Windows Script.[10,11]

#### Forward Look:

- SEO poisoning and the use of malicious Google ads are likely to continue on an upward trajectory.

#### Recommendations:

- Leverage ZeroFox to conduct ongoing monitoring for impersonating domains and provide alerts and support for mitigation.

No notable change in threat from previous quarter

### VULNERABILITY EXPLOITATION

There was likely little change in threat from nefarious actors exploiting CVEs to target public sector entities in Q2 2023. The Cybersecurity and Infrastructure Security Agency's (CISA) updates to its Known Exploited Vulnerabilities (KEV) catalog included critical exploits that almost certainly impacted public sector entities, including exploits impacting iOS systems, Google Chrome, and Barracuda Email Security products.[12,13] Public sector entities were very likely impacted by critical vulnerabilities in VMware enabling remote code execution.[14] Clop's May 2023 exploitation of CVE-2023-34362, a zero-day exploit in MOVEit file transfer software, demonstrated the potential impact exploitation of these CVEs can have; while public sector entities were compromised in the attack, Clop operatives stated that they have no interest in extorting government organizations.

#### Forward Look:

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

#### Recommendations:

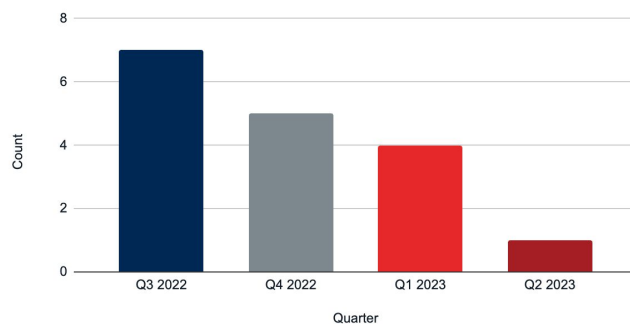
- Use the ZeroFox Platform's Intelligence Search capability to investigate vulnerabilities and associated exploits.

No notable change in threat from previous quarter

### INITIAL ACCESS BROKERS

ZeroFox Intelligence assesses with low confidence that the threat from nefarious actors advertising access into public sector organizations in deep and dark web forums reduced in Q2 2023. The number of posts fell in Q2 2023, bucking an overall upward trend seen in most other sectors.[15] ZeroFox Intelligence notes the possibility that access to public sector organizations is either so valuable or likely to draw unwanted attention from authorities that IABs are disproportionately selling it in private channels directly to trusted buyers. Advertisement content across all sectors continued to typically focus on vulnerabilities in remote working infrastructure, including Virtual Private Networks and Remote Desktop Protocol.

Advertised IAB Access into Public Sector Organizations by Quarter



Source: ZeroFox Intelligence

#### Forward Look:

- IABs will continue to increasingly leverage private communication channels to give first refusal to established buyers.

#### Recommendations:

- Proactively monitor for IAB operators advertising access to organizations directly, as well as to partners and suppliers.
- Subscribe to the ZeroFox Advanced Web Search and Dark Ops Curated Intelligence for early warnings and indicators of threat actor chatter.

Indication of decrease in threat from previous quarter

#### FOOTNOTES

[1] <https://www.cfrl.com/technology/chinese-hackers-use-g7-ruse-to-target-australian-government-officials-20230615-p5dgqg>  
[2] <https://www.bleepingcomputer.com/news/security/irs-authorized-efilecom-tax-return-software-caught-serving-js-malware/>  
[3] <https://twitter.com/HMRCgovuk/status/1662021031614111753?s=20>  
[4] <https://blogs.blackberry.com/en/2023/04/massive-spear-phishing-campaign-impersonating-spain-tax-agency>  
[5] [https://content.govdelivery.com/attachments/USSTATEBPA/2023/06/01/file\\_attachments/2514954/Joint\\_CSA\\_NK\\_Using\\_Social\\_Engineering\\_20230531.pdf](https://content.govdelivery.com/attachments/USSTATEBPA/2023/06/01/file_attachments/2514954/Joint_CSA_NK_Using_Social_Engineering_20230531.pdf)  
[6] <https://www.bleepingcomputer.com/news/security/new-android-fluorose-malware-steals-your-passwords-2fa-codes/>  
[7] <https://www.bleepingcomputer.com/news/security/take-in-browser-windows-updates-push-aurora-info-stealer-malware/>

[8] <https://www.bleepingcomputer.com/news/security/google-ads-push-bumblebee-malware-used-by-ransomware-gangs/>  
[9] <https://www.bleepingcomputer.com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/>  
[10] <https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-use-encrypted-rpmmsg-messages/>  
[11] <https://www.bleepingcomputer.com/2023/04/new-qbot-banking-trojan-campaign.html>  
[12] <https://nvd.nist.gov>  
[13] <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>  
[14] <https://www.bleepingcomputer.com/news/security/cisa-orders-govt-agencies-to-patch-bugs-exploited-by-russian-hackers/>  
[15] ZeroFox Intelligence Internal Collections



## BOTNETS

Botnets continued to pose a high threat to public sector organizations in Q2 2023 via stealing credentials and remotely-controlling infected devices. ZeroFox Intelligence ingested over 150 million credentials harvested by infostealer families commonly deployed by botnets, of which Raccoon was most active.[16] European and North American public sector entities continued to see a high threat of Distributed Denial of Service (DDoS) attacks, particularly from Russia-aligned groups.[17,18] However, the impact of attacks remained limited, typically rendering websites unusable for a short period of time.

### Forward Look:

- The threat to public sector entities from compromised credentials is likely on an ongoing upward trajectory.
- Russia-aligned threat actors' DDoS attacks against public sector institutions will likely continue to have limited impact.

### Recommendations:

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

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 increased in Q2 2023, underpinned by indications of increased APT activity targeting government entities globally. This includes disclosures of campaigns by previously undocumented actors.[19,20,21,22,23] Infostealers and trojans remained highly prevalent, facilitating cyber espionage and data breaches, with the public sector frequently impacted by data leaks of sensitive information.[24] In Q2 2023, prolific threat actors updated well-established strains such as Qbot, and launched new strains, including threat actors with a history of targeting public sector entities.[25] Dissemination of powerful loaders designed to facilitate the deployment of follow-on malicious payloads remained high.[26,27]

### Forward Look:

- Disclosures of a range of APTs targeting public sector entities will likely increase in coming quarters.
- Malware-as-a-service offerings will very likely sustain low barriers to entry for threat actors.

### Recommendations:

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

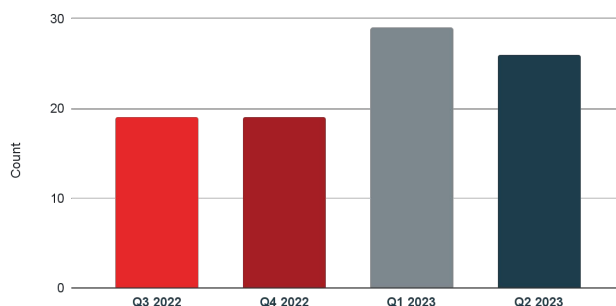
Indication of increase in threat from previous quarter

## RANSOMWARE & DIGITAL EXTORTION

The threat to public organizations from R&DE likely remained broadly consistent in Q2 2023, bucking an upward trend seen in almost all other sectors.[28] Across the landscape, the number of R&DE incidents increased more than 50 percent, whereas attacks against the public sector fell slightly from Q1 2023. This discrepancy is very likely underpinned by Clop operatives' statement that they would not extort government organizations as part of its successful exploitation of a zero-day vulnerability in MOVEit file transfer software.

LockBit remained the primary digital extortion threat to the sector. However, both the total number and proportion of attacks that leveraged the strain fell. Instead, ZeroFox Intelligence identified increased prevalence of well-established strains, such as BlackByte, Play, and Royal, as well as emerging strains like Akira and Rhysida. Local government and third-party service providers remained most likely to be targeted. This likely reflects a continuation of threat actors' perception that attacks against such targets will garner little blowback. Despite a fall in the proportion of attacks targeting the Asia-Pacific region, North America-based entities remained the most frequently targeted, with entities in Europe also seeing an elevated level of threat.

Total Public Sector Ransomware and Digital Extortion Events by Quarter



Source: ZeroFox Intelligence

### Forward Look:

- The R&DE threat to the public sector is unlikely to change significantly in the short term.
- With little blowback, threat actors will likely become increasingly emboldened in targeting public sector entities.

### 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

[16] ZeroFox Intelligence Internal Collections  
[17] [https://www.techrepublic.com/article/ddos-attacks-finland-israel/?web\\_view=true](https://www.techrepublic.com/article/ddos-attacks-finland-israel/?web_view=true)  
[18] <https://thecyberexpress.com/ukrainian-organizations-attacked-by-nomane/>  
[19] <https://www.gov.uk/web/boas-wednesday/espionage-campaign-linked-to-russian-intelligence-services>  
[20] <https://thehackersnews.com/2023/05/new-apt-group-red-stinger-targets.html>  
[21] <https://thehackersnews.com/2023/05/sophisticated-downex-malware-campaign.html>  
[22] <https://www.bleepingcomputer.com/news/security/goldenjackal-state-hackers-silently-attacking-govts-since-2019/>  
[23] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>

[24] <https://www.theguardian.com/australia-news/2023/jun/26/hwt-ebsworth-hack-sensitive-information-from-dozens-of-government-agencies-may-be-compromised>  
[25] <https://thehackersnews.com/2023/04/new-qbot-banking-trojan-campaign.html>  
[26] [https://cyberwarzone.com/batloader-malware-dropper-continues-to-pose-a-threat-to-organizations-in-2023/?web\\_view=true](https://cyberwarzone.com/batloader-malware-dropper-continues-to-pose-a-threat-to-organizations-in-2023/?web_view=true)  
[27] <https://www.bleepingcomputer.com/news/security/new-pindos-javascript-dropper-deploys-bumblebee-icedid-malware/>  
[28] ZeroFox Intelligence Internal Collections



## OUTLOOK

ZeroFox Intelligence anticipates the R&DE threat to the public sector will likely remain broadly consistent in Q3 2023, with continued diversification in the strains used in attacks.

Illicit access to public sector entities advertised in dark web forums will likely remain lower than other sectors, with threat actors leveraging private communication channels to give first refusal to established buyers.

ZeroFox Intelligence anticipates little change to the social engineering threat to public sector organizations in Q3 2023. SEO poisoning and the leveraging of malicious Google advertisements to disseminate malware will likely continue on an upward trajectory.

ZeroFox Intelligence anticipates disclosures of APTs and nation-state actors targeting public sector entities will likely increase in Q3 2023, with malicious modules enabling espionage, data exfiltration, and broader system corruption.



## 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](https://zerofox.com/request-a-demo)

### > Learn More:

Visit [zerofox.com](https://zerofox.com)

Contact us at [sales@zerofox.com](mailto:sales@zerofox.com) / 855.736.1400

