

UK Public Sector

Threat Landscape Report: January 2022 – Present

TLP: GREEN



Key Findings

- The ransomware and digital extortion threat to the United Kingdom (UK) Public Sector is likely on an upward trajectory, underpinned by increased attacks against the UK education sector. Threat actors are likely disproportionately targeting the education sector, which finished 2022 as the most frequently targeted industry in the UK.
- Advertisements in open forums for illicit access into UK Public Sector entities remained low. Brokers moved towards private communication methods with sellers.
- The UK Public Sector likely faced an increased threat of spear phishing, smishing, callback phishing (vishing), and phishing techniques that bypass multi-factor authentication (MFA).
- Exposure of private information on the surface and dark web very likely increased the risk to UK Public Sector VIPs of being victims of malicious exploitation.
- The growth in impersonating phishing domains very likely drove an increased threat to UK Public Sector entities in 2022 and Q1 2023. ZeroFox Intelligence observed a 40 percent increase in malicious or fraudulent domains in 2022.

Key Cyber Threats to the UK Public Sector in 2023

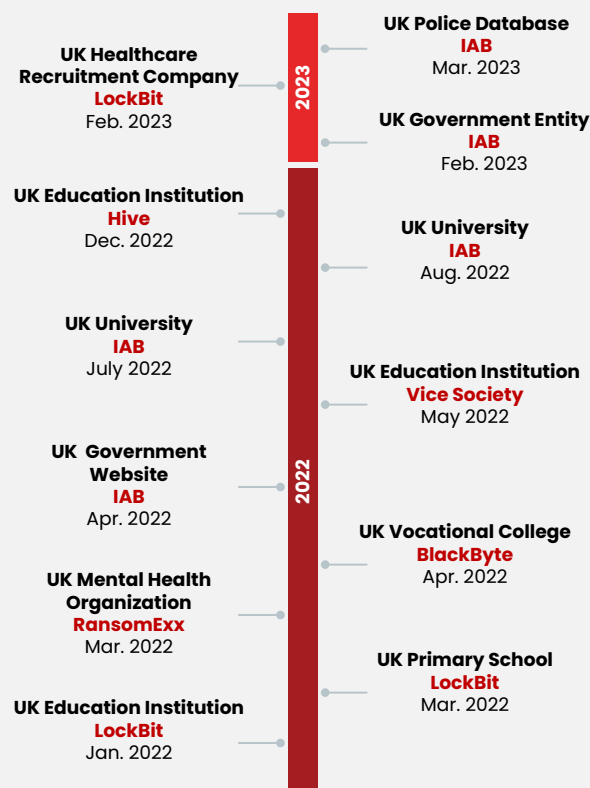
 Increased threats from spear phishing, smishing callback phishing, and techniques to bypass MFA	 Data breaches resulting from threat actors stealing credentials, sensitive corporate information, and other data
 Ransomware and digital extortion outfits conducting attacks against UK Public Sector targets and their third-party providers	 Initial Access Brokers (IABs) moving towards private communication channels with sellers, making identification and mitigation more difficult
 Spyware and infostealer modules deployed to intercept or exfiltrate sensitive data	 VIP impersonations and account takeovers used to spread disinformation or malinformation
 Malicious domains impersonating legitimate UK Public Sector entities leveraged to target members of the public	 Adversarial nation-states using proxies to target UK Public Sector entities to advance policy goals while maintaining plausible deniability

Overview

The UK Public Sector almost certainly remains an attractive target for threat actors seeking a competitive or political advantage, or a financial return, given the breadth of sensitive data held, large budgets, and strategic importance to national and international operations. Although attacks impacting the sector almost certainly remained underreported, threat actors successfully targeted both public sector targets and their third-party providers, highlighting the fragility of public sector entities' cybersecurity practices and the potential impact that successful targeting can have. For the purposes of this report only, the term "UK Public Sector" refers to:

- Central Government Departments
- Local Authorities
- Public Agencies / Bodies
- State-owned Corporations
- Education Institutions
- Public Sector Healthcare Institutions

Selected Cyber Incidents Against the UK Public Sector, 2022–2023



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 5:00 PM (DST) on March 30, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

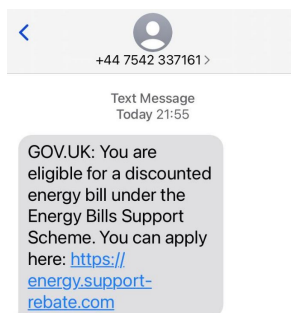


Social Engineering

Social engineering by financially and politically-motivated threat actors remains one of the greatest threats to the UK Public Sector, although campaigns are almost certainly underreported. Human error continues to be a barrier to effective security and a lucrative exploitation vector. Targeted campaigns continued on an upward trajectory throughout 2022 and into 2023, including spear phishing, smishing, and Telephone-Oriented Attack Delivery (TOAD).[1,2] While traditional “spray-and-pray” campaigns remain, ZeroFox Intelligence observed an increase in highly-personalized messages targeting employees—including of large public sector organizations—in which threat actors impersonated staff members, remote working services, and authentication providers.

Case Study: UK Government Impersonation Scam

UK Public Sector entities’ susceptibility to being both the subject and the target of social engineering campaigns remained high in 2022.[3] As early as September 2022, threat actors were observed impersonating various UK Public Sector entities—including government departments, Ofgem, and UK Help—in smishing and phishing messages to members of the public inviting them to apply for £400 as part of the Energy Bills Support Scheme.[4] Low-sophistication, spray-and-pray campaigns that leverage topical lures can prove effective, particularly in cases of emerging government policy that are not well understood by members of the public. ZeroFox Intelligence has also observed phish kits that leverage impersonations of UK government entities.

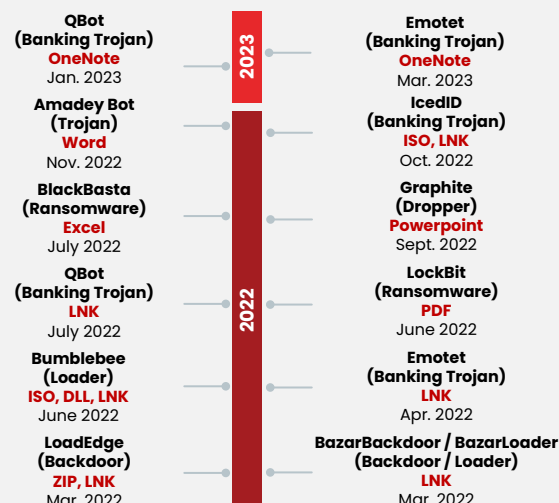


Source: <https://www.which.co.uk/news/article/beware-of-this-scam-text-offering-you-fake-government-energy-bill-support-anqap4d5uglm>

ZeroFox Intelligence assesses with medium confidence that the threat from smishing and TOAD increased in 2022, with frequent reporting of highly-effective, targeted campaigns. Attacks have been observed targeting organizations’ employees, either directly or via enterprise third-party providers.[5] Smishing and TOAD campaigns have facilitated follow-on malicious activity, including use as an intrusion vector by malware strains known to be leveraged against industry targets.[6] Threat actors have also evolved to increasingly leverage hybrid approaches, using phishing or smishing messages to initiate a follow-on phone conversation.[7] Campaigns added legitimacy to malicious emails by impersonating security teams and encouraging victims to return a phone call to authenticate fraudulent activity.

Malicious email attachments very likely remained one of the most prevalent means of threat actors distributing malware to UK Public Sector end users and is expected to remain so for the foreseeable future. While macro-enabled documents continued to be leveraged throughout 2022, ZeroFox Intelligence identified increased use of Windows image files (ISO), archives (RAR), Windows Shortcut files (LNK), and OneNote files to deploy malicious payloads.[8] This shift was very likely driven in part by Microsoft’s move towards disabling VBA macros by default, making it more likely users would be alerted to potentially unsafe files.[9] Until recently, Mark-of-the-Web controls did not apply to some ISO and LNK files, and can still be bypassed leveraging OneNote files. This results in malware execution without warning to the user.

Selected Campaigns Leveraging Malicious Attachments



The threat to the UK Public Sector from MFA bypass likely increased, including adversary-in-the-middle attacks now being incorporated into broader Phishing-as-a-Service offerings. Threat actors increasingly leveraged techniques where traditionally-strong MFA gives little or no protection. This includes “in-the-middle” techniques, MFA fatigue, and OAuth Consent phishing. Victims are unlikely to be aware of threat actors positioned between them and a legitimate destination, granting threat actors authenticated sessions within enterprise environments.

Forward Look:

- Malicious email attachments that circumvent Mark-of-the-Web controls will likely increasingly be used to disseminate malware.
- Threat actors are very likely to increasingly leverage MFA-bypassing social engineering techniques.

Recommendations:

- Communicate to employees about 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.

FOOTNOTES

- <https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/>
- <https://www.bleepingcomputer.com/news/security/attackers-hijack-uk-nhs-email-accounts-to-steal-microsoft-logins/>
- <https://www.ncsc.gov.uk/news/ncsc-reveals-top-government-email-impersonation-scams-taken-down-in-2022>
- <https://www.independent.co.uk/news/uk/home-news/energy-bill-support-scheme-apply-scam-b2191610.html>
- <https://cloudsek.com/threatintelligence/apollo-otp-bot-exploiting-google-voice-for-mfa-bypass>
- <https://www.infosecurity-magazine.com/news/pegasus-spyware-uk-prime-minister/>
- <https://socradar.io/a-new-rising-social-engineering-trend-callback-phishing/>
- <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trojanized-onenote-document-leads-to-remote-control-malware/>
- <https://thehackernews.com/2022/07/microsoft-resumes-blocking-office-vba.html>



Malicious Domains

The growth in impersonating phishing domains very likely drove an increased threat to UK Public Sector entities in 2022 and Q1 2023. ZeroFox Intelligence observed a 40 percent increase in malicious or fraudulent domains in 2022.[10] These malicious domains were demonstrably effective, leveraged by threat actors to steal credentials, compromise a network, conduct financial fraud, or deploy malicious payloads. Threats to the sector broadly fall into two categories: threat actors impersonating entities' legitimate domains to target members of the public; and threat actors impersonating third-party services to target public sector organizations' employees.[11] UK Public Sector entities remain attractive targets for domain impersonations given their trusted status amongst members of the public, increasing the likelihood of engagement. While threat actors are expected to continue developing their tactics to create more convincing phishing domains, the threat is not expected to change significantly in the near term. Monitoring for and attempting removal of impersonating domains can provide substantial mitigation for this threat, phishing domains will very likely continue to be a "whack-a-mole" problem.

Phishing domains observed in 2022 typically impersonated government services or third-party technology service providers, replicating their home or login pages. In sophisticated campaigns, threat actors included the brand name in the domain name or path, duping less vigilant victims into assuming it was an authentic site. The use of HTTPS—over HTTP—increased, adding an increased appearance of legitimacy to malicious domains. Phishing domains often capitalized on global events, such as the cost-of-living crisis and Russia's invasion of Ukraine. While identified malicious domains were predominantly established by financially-motivated threat actors, politically-motivated threat actors also launched effective campaigns.[12]

ZeroFox Intelligence identified an increase in the use of domain shadowing. Threat actors created multiple malicious subdomains under compromised domains to host phishing pages, steal credentials, and distribute malware. By registering multiple subdomains, pages can be discarded and rotated quickly to avoid detection. The malicious pages do not impact the operation of the legitimate site, and address bars may only display the main domain, which has a good reputation.

Forward Look:

- Malicious domains impersonating public sector entities are likely to continue on an upward trajectory, though are unlikely to change significantly in nature.

Recommendations:

- Engage a reputable threat intelligence vendor to conduct ongoing monitoring for impersonating domains and provide alerts and support for mitigation.
- Establish clear policies and procedures for removing malicious domains, including identifying and notifying the appropriate authorities and stakeholders.

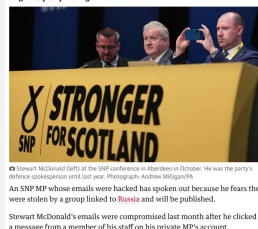
VIP Impersonations & Account Takeover

Exposure of private information on the surface and dark web very likely increased the threat to UK Public Sector VIPs of being victims of malicious exploitation through social engineering, spear phishing attacks, impersonation, account takeover, and malware deployment. Key personnel—including Members of Parliament, senior civil servants, executive board members, and high profile individuals—remained at heightened risk of being targeted by adversaries with political, monetary, retaliatory, and social motivations.[13,14] The continued growth of online personas and brands has very likely placed increased strain on organizations' security departments to manage such threats.

The prevalence of personal information in open sources is almost certainly lowering the barriers to entry for threat actors, who require only basic research skills to launch well-tailored social engineering campaigns against public sector targets. Threat actors leverage digital channels containing private information on VIPs—such as birth dates, addresses, contact details, or hobbies—in lures, as well as sensitive information exposed in prior data breaches. Social media platforms, including those of VIPs' family members, often openly disclose sensitive details that could be used for identity theft and impersonation—including in spear phishing emails designed to target colleagues that are laden with malicious links and attachments. The prevalence of video and podcast interviews in open sources also enable threat actors to add authenticity to social engineering lures and craft malicious synthetic media. Once compromised, official accounts can be used to spread disinformation or malinformation.

Scottish MP Stewart McDonald fears emails hacked by Russia-linked group

SNP MP for Glasgow South says he is victim of sophisticated and targeted spear phishing attack



Source: [hXXps://www.theguardian\[.\]com/politics/2023/feb/08/scottish-mp-stewart-mcdonald-emails-hacked-russia-linked-group](https://www.theguardian.com/politics/2023/feb/08/scottish-mp-stewart-mcdonald-emails-hacked-russia-linked-group)



Source: [hXXps://ukdefencejournal\[.\]org\[.\]uk/british-army-twitter-account-hacked/](https://ukdefencejournal[.]org[.]uk/british-army-twitter-account-hacked/)

Forward Look:

- ZeroFox Intelligence anticipates an increase in impersonations and account takeovers of UK Public Sector entities in 2023.

Recommendations:

- Protect customers and employees by detecting and removing phishing websites and malicious URLs.
- Proactively monitor for impersonations of entities or domains related to your entity, and collaborate with ZeroFox to submit takedown requests.

FOOTNOTES

[10] ZeroFox Intelligence Internal Collections

[11] [hXXps://www.theguardian\[.\]com/business/2022/sep/26/online-fraudsters-adapt-tactics-to-exploit-uk-cost-of-living-crisis](https://www.theguardian.com/business/2022/sep/26/online-fraudsters-adapt-tactics-to-exploit-uk-cost-of-living-crisis)

[12] [hXXps://www.proofpoint\[.\]com/uk/blog/threat-insight/chasing-currents-espionage-south-china-sea](https://www.proofpoint.com/uk/blog/threat-insight/chasing-currents-espionage-south-china-sea)

[13] [hXXps://www.bbc\[.\]co\[.\]uk/news/uk-scotland-64601774](https://www.bbc.com/news/uk-scotland-64601774)

[14] [hXXps://ukdefencejournal\[.\]org\[.\]uk/british-army-twitter-account-hacked/](https://ukdefencejournal.org.uk/british-army-twitter-account-hacked/)

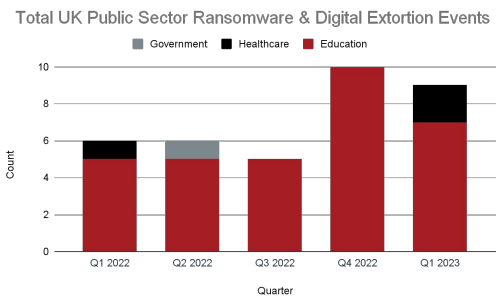


Ransomware and Digital Extortion (R&DE)

The threat of R&DE to the UK Public Sector is likely on an upward trajectory, with increased attacks in Q4 2022 and Q1 2023.[15] The rise was driven by increased attacks against the UK education sector, although ZeroFox Intelligence notes that victims include both state schools and academies (charities, third sector). The threat to central government entities and the National Health Service (NHS) directly remained low throughout the reporting period, with threat actors very likely preferring to pursue perceived softer targets—such as agencies or public bodies—that might garner less attention and retaliation from authorities. Most industries and geographies saw a reduction in R&DE threat throughout 2022, with incidents remaining below 2021 levels. This overall reduction was likely caused in part by difficulty eliciting payments from victims. Financially and politically-motivated extortionists very likely view the wider UK Public Sector as an attractive target, believing entities’ high profiles, large revenues, proprietary and sensitive information held, and strategic role in global affairs might make victims more likely to pay ransoms.

Increased professionalization of the cybercriminal marketplaces in 2022 lowered the barriers to entry for threat actors and drove diversification in the Tactics, Techniques, and Procedures (TTPs) observed across deployments of a given payload, making identification and disruption more difficult. Ransomware attacks increasingly involved interconnected parties: IABs selling access, developers providing encryption and exfiltration tooling, and ransomware affiliates deploying payloads against the victim and managing ransom negotiations.

UK Public Sector entities remained at greatest threat from attacks against third-party suppliers, including manufacturing, shipping, consulting, and software service providers. The impact of extortion attacks on the sector is almost certainly underestimated given its reliance on adjacent industries and international supply chains. Such attacks also enable adversarial nation-states to utilize criminal collectives as a proxy to advance foreign policy goals while maintaining plausible deniability. It is a realistic possibility that state-linked actors will increasingly leverage ransomware-as-a-service operations as a cover for malicious activity.[16]



Source: ZeroFox Intelligence

Case Study: LockBit Attack on Advanced, August 2022

In August 2022, LockBit ransomware was used in the targeting of Advanced, a managed software provider servicing the NHS.[17] The attack resulted in widespread disruption to the NHS, including outages to patient management systems for surgeries, care homes, and mental health services. Advanced disclosed that threat actors obtained initial access by leveraging legitimate third-party credentials before moving laterally across the network, escalating privileges, conducting reconnaissance, and deploying the ransomware payload. Sensitive data was copied and exfiltrated immediately prior to the encryption of the Advanced systems. Reporting stated it may take the NHS more than a year to recover from this attack. LockBit emerged as the primary global R&DE threat in 2022 and was leveraged in nearly a quarter of all attacks.

The R&DE threat to the UK education sector increased significantly during the reporting period, finishing 2022 as the most frequently targeted UK industry. Attacks focused particularly on local authority-run state schools, academies, and universities. While academies are registered charities and therefore not local authority-owned, threat actors are likely largely unaware or undeterred by this nuance. The education sector globally saw a much bigger resurgence in the R&DE threat towards the end of 2022 than other sectors.

Quarter	Geography		Industry		Dependency
	Percentage of Global R&DE Targeting UK	Percentage of Global Education R&DE Targeting UK Education	Percentage of Global R&DE Targeting Global Education	Percentage of UK R&DE Targeting UK Education	Discrepancy Between Actual UK Education R&DE Cases and Estimated Cases Given Independence
Q1 2022	6.2%	13.2%	5.8%	12.5%	+2.7
Q2 2022	6.1%	16.1%	5.2%	13.9%	+3.1
Q3 2022	4.7%	16.7%	5.4%	19.2%	+3.6
Q4 2022	5.8%	20.0%	8.6%	29.4%	+7.1

Threat actors are likely disproportionately targeting the UK education sector. Following a statistical analysis of R&DE incidents, ZeroFox Intelligence assesses with moderate confidence that geography and industry are dependent factors when assessing the threat to the UK education sector. This means an influencing relationship exists between these two variables, which results in threat actors targeting the UK education sector more frequently than would be anticipated. This disparity has existed since as early as January 2021 and is increasing. In 2022, the UK education sector faced an average of four attacks per quarter above what would be expected, and seven more in Q4 2022. The reasons for this discrepancy are unclear but likely varied, ranging from poor security practices to a possible perception that UK educational institutions are wealthier and more susceptible to paying larger ransom demands to an anti-UK political bias amongst extortion operators.

FOOTNOTES

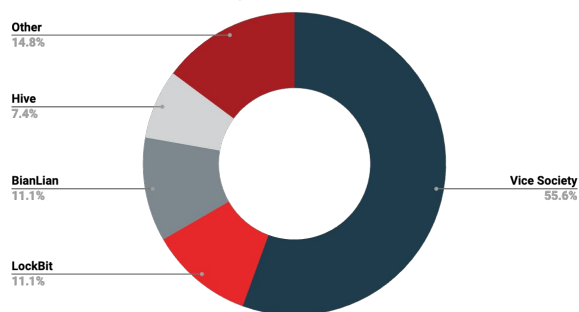
[15] ZeroFox Intelligence Internal Collections
[16] <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>
[17] <https://www.independent.co.uk/news/health/nhs-cyber-attack-hospitals-b2153382.html>



Case Study: Vice Society Ransomware

Vice Society was the most prolific R&DE threat to the UK education sector, responsible for approximately 60 percent of attacks in 2022.[18] Approximately 40 percent of Vice Society's global attacks in 2022 targeted the education sector, with a particular focus on organizations in Europe and the United States. Identified as early as June 2021, Vice Society is atypical in that its operators primarily leverage other existing ransomware-as-a-service (RaaS) payload offerings.[19] This includes Hello Kitty/Five Hands, BlackCat, QuantumLocker, and Zeppelin variants the group also deployed a new custom payload in December 2022 dubbed "PolyVice." Operators are known to gain access to victim networks through phishing, leveraging compromised credentials, and exploiting vulnerabilities in public-facing applications. Operators utilize standard double extortion techniques, exfiltrating data before holding it for ransom.

R&DE Attacks Against UK Public Sector, 2022



Source: ZeroFox Intelligence

ZeroFox Intelligence anticipates an increase in "hack-and-leak" tactics, with threat actors removing the encryption angle of their attacks and instead relying on data exfiltration and ransom demands. Payloads deployed by extortion collectives will also likely increasingly incorporate data corruption functionality.[20] Threat actors may also resort to more extreme pressure tactics to elicit payment from victims under threat of significant reputational damage and legal ramifications. It is a realistic possibility that extortion operatives will increasingly collaborate, passing leaked data between them and resulting in victims being required to pay ransom demands to multiple entities before their data is removed from various leak sites.

> Forward Look:

- Ransomware will most likely be targeted at manufacturers and software service providers to maximize the impact on downstream UK Public Sector dependents.
- Threat actors may resort to more extreme pressure tactics to elicit payment from victims, causing 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.

Data Breaches

The risk to the UK Public Sector from data breaches, including theft of sensitive data and compromised credentials, very likely increased in 2022. The potential exposure is underpinned by high-profile breaches impacting public sector entities, the prevalence of spyware and stealer modules within malware payloads, increased professionalization of dark web marketplaces, and interconnectivity of victim organizations.[21] Public sector entities almost certainly remained attractive targets for threat actors attempting to steal sensitive political and personal information, intellectual property, email accounts and password hashes, financial documents, and internal correspondence.

Compromising user accounts, irrespective of their associated privileges, provides threat actors opportunities for malicious behavior, including payload delivery, lateral movement, credential stuffing, account takeover, and social engineering. Public sector entities should be aware of the threat posed when they, or their third-party associates, become a victim of a data breach. Weak passwords and password reuse are of considerable concern, with ZeroFox Intelligence research indicating that more than half of enterprise executives reuse their passwords.

ZeroFox Intelligence analyzed its Compromised Accounts Database of over 10 billion compromised credentials, identifying hundreds of email addresses and passwords for multiple public sector domains since January 2022, which could lead to the compromise of corporate accounts as well as wider compromise where the passwords are reused.[22] This includes password log entries from well-known information stealers that have successfully stolen login credentials associated with accounts related to public sector employees.

Domain	Compromised Credentials Identified (Jan. 2022–Present)
gov[.]uk	56
edu[.]uk	15
nhs[.]uk	725
parliament[.]uk	513
police[.]uk	1
sch[.]uk	26
gov[.]scot	16
nhs[.]scot	34
gov[.]wales	8

> Forward Look:

- The threat to UK Public Sector entities from data breaches and cyber espionage will very likely continue on an upward trajectory.
- Public Sector entities are expected to be increasingly implicated in third-party breaches.

> Recommendations:

- Proactively monitor for network access sales to obtain critical early warning of an impending cyberattack and to help identify malicious actors, including insiders, meaning to harm your network.
- Ensure good password hygiene.

FOOTNOTES

[18] ZeroFox Intelligence Internal Collections

[19] [hXXps://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0](https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0)

[20] [hXXps://www.csoonline.com/article/3674848/ransomware-operators-might-be-dropping-file-encryption-in-favor-of-corrupting-files.html](https://www.csoonline.com/article/3674848/ransomware-operators-might-be-dropping-file-encryption-in-favor-of-corrupting-files.html)

[21] [hXXps://www.bleepingcomputer.com/news/security/british-council-exposed-more-than-100-000-files-with-student-records/](https://www.bleepingcomputer.com/news/security/british-council-exposed-more-than-100-000-files-with-student-records/)

[22] ZeroFox Intelligence Internal Collections

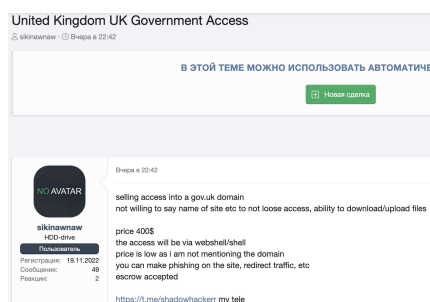


Initial Access Brokers (IABs)

ZeroFox Intelligence assesses with low confidence that the threat to the UK Public Sector from IABs posting illicit access sales on open forums remained low in 2022 and into 2023.[23] Sales in open forums specifying access to UK Public Sector entities were infrequent and are likely to remain so for the foreseeable future, given brokers' desire to avoid scrutiny and retaliation. The IAB landscape remains highly volatile—more so than other cyber threats.

The use of open forums to advertise illicit access has been on a downward trajectory when compared with the 2021 peak. The fall in activity is likely in part explained by Russia's invasion of Ukraine, with some IABs implicated in the conflict; continued disruption to underground marketplaces; and a shift towards IABs preferring private channels to sell directly to well-established buyers—often ransomware operatives—rather than advertising in forums in order to avoid law enforcement scrutiny. The reduction in advertised access does not necessarily indicate a reduction in threat or lack of demand from buyers, and threat actors very likely remain motivated to gain network access to UK Public Sector entities. Identifying and mitigating 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.

The greatest threat to UK Public Sector entities from IABs stems from illicit access sold into third-party providers' enterprise environments. Of those openly advertising access into public sector entities, reputable threat actors mainly advertise access to third-party software services used by public sector entities on well-established Russian and English language marketplaces. Access to Western entities posted in open channels became increasingly rare throughout the year, as did access to managed service and software providers.



In February 2023, a moderately credible threat actor advertised web shell access to the internal network of an unnamed UK government entity on the predominantly Russian-language deep web forum "XSS." The actor charged USD 400 for the access. They did not provide any further details about the access, opting for interested buyers to contact them via Telegram.

Source: ZeroFox Intelligence

> Forward Look:

- The IAB threat will very likely rebound in 2023, with the threat to UK Public Sector entities remaining heavily influenced by developments in Russia's war in Ukraine.

> Recommendations:

- Subscribe to the ZeroFox Advanced Web Search and Dark Ops Curated Intelligence for early warnings and indicators of threat actor chatter regarding your organization.
- Security teams should monitor for IAB operators advertising direct access to their organization, as well as to those of their partners and suppliers.

Botnets

Botnets pose a significant threat to UK Public Sector entities on at least two key fronts: stealing credentials and remotely controlling infected devices. Credentials harvested by botnets are often sold or traded on dark web marketplaces, and infections that leak employee credentials are often part of the initial stages before a corporation falls victim to an R&DE event. While the UK Public Sector faced increased threat from Distributed Denial of Service (DDoS) attacks in 2022 and into 2023, particularly from Russian-aligned actors, the UK threat has not increased as much as seen elsewhere in Europe.[24] The impact of attacks continued to be limited, typically resulting in websites being taken offline for a short period of time rather than complete system shutdown.

ZeroFox identified compromised systems infected with Vidar, Redline, and Racoon malware families, from which login credentials associated with UK Public Sector entities were exfiltrated.[25] These compromised systems yield stolen user data in the form of botnet logs and contain login credentials and additional system information, such as browser cookies—increasing the likelihood of phishing, spam, and onward fraud operations targeting public sector users. Threat actors that purchase this data from underground marketplaces potentially gain access to the entirety of a victim's login credentials and cookies, which allows them to emulate the victim's browser session and user agent to achieve unauthorized access in account takeover attacks.

> Forward Look:

- The UK Public Sector will likely face an increased threat from Russia-aligned DDoS attacks, though these will be likely have limited impact.
- Expansion of the botnet market will continue, with new botnets emerging to target web servers, modems, routers, Internet-of-Things (IoT) products, and mobile devices.

> Recommendations:

- Subscribe to the ZeroFox botnet and compromised account alerts to identify any exposure of employee or customer credentials in the wild.

FOOTNOTES

[23] ZeroFox Intelligence Internal Collections

[24] <https://cert.euroopa.eu/>

[25] ZeroFox Intelligence Internal Collections



Malware

ZeroFox Intelligence assesses with low confidence that the threat to the UK Public Sector from malware remained high, with no significant changes observed in malware capabilities.[26] Attacks against UK Public Sector targets very likely remained underreported due to a lack of public disclosure, lack of victim awareness, and sophisticated techniques deployed that enable threat actors to evade detection. The sector almost certainly remained an attractive target for financially and politically-motivated threat actors, including nation-state entities.[27] The threat is unlikely to reduce in the near term given the ease of malware acquisition, impact on victims, and potential to obtain highly-sensitive information. This information is highly valuable and can provide sophisticated threat actors the ability to conduct follow-on malicious activity, including targeting third parties with tailored forms of social engineering.

The greatest malware threat to UK Public Sector entities remained from infostealer modules, often used in conjunction with other malware or incorporated into broader trojans. Such modules facilitate data breaches, cyber espionage, and deployment of additional malicious payloads. Market saturation remained high in 2022, with increased Malware-as-a-service (MaaS) offerings granting ease of acquisition and maintaining low barriers to entry. Services are sold for as little as USD 5 for a two-month subscription.[28] The threat is unlikely to reduce in the near term, with public sector entities in Western nations likely facing an increased threat from wipers leveraged by Russia-aligned entities in the coming year.

Although spyware received significant media attention in 2022 and into 2023, including as it pertained to the targeting of politicians, lawyers and journalists, there was likely no significant change in the threat posed to UK Public Sector entities. Nefarious actors, including nation-states, almost certainly continued to leverage commodity spyware to target UK Public Sector organizations and VIPs.[29] Modules of concern enabled keylogging, credential and session cookie theft, and the deployment of follow-on malicious payloads that granted attackers the ability to take full control of a device or system. In Q4 2022 and Q1 2023, details continued to emerge on the extent of nation-state surveillance using spyware.[30,31] The European Parliamentary Committee investigated the use of Pegasus and other spyware (PEGA) and published its draft findings in November 2022, highlighting the illegitimate use of spyware in various European countries. Legislation on its own is unlikely to change the threat significantly in the short term.[32] Sanctions against suppliers may drive buyers towards alternative, or underground, spyware vendors. Nation-states and cybercriminals that have already demonstrated a disregard for such rules are unlikely to be deterred by new restrictions.

> Forward Look:

- ZeroFox Intelligence anticipates continued disclosures in 2023 of historic abuses of spyware use against UK Public Sector entities and VIPs.
- MaaS 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 and Ransomware.

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.

FOOTNOTES

[26] ZeroFox Intelligence Internal Collections

[27] [hXXps://www.bbc.com/news/uk-64405220](https://www.bbc.com/news/uk-64405220)

[28] [hXXps://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html](https://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html)

[29] [hXXps://www.theguardian.com/politics/2022/apr/18/no-10-suspected-of-being-target-of-being-target-of-nso-spyware-attack-boris-johnson](https://www.theguardian.com/politics/2022/apr/18/no-10-suspected-of-being-target-of-being-target-of-nso-spyware-attack-boris-johnson)

[30] [hXXps://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/](https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus/)

[31] [hXXps://www.washingtonpost.com/politics/2022/12/01/here-first-journalists-us-citizen-are-suing-nso-group/](https://www.washingtonpost.com/politics/2022/12/01/here-first-journalists-us-citizen-are-suing-nso-group/)

[32] [hXXps://www.eurpol.europa.eu/en/committees/en/pega-findings/product-details](https://www.eurpol.europa.eu/en/committees/en/pega-findings/product-details)

