

# Cyber Threat Intelligence Summary

---



February 2024



# Contents

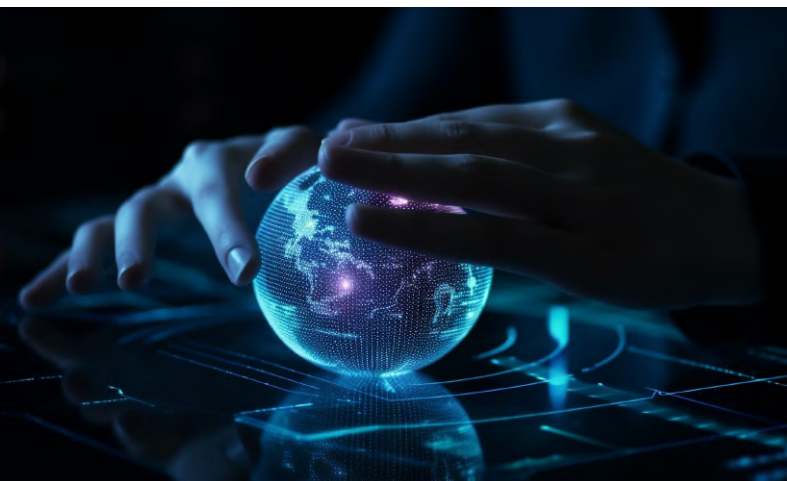
|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introducing... '#MOAB' aka The Mother Of All Breaches</b>           | <b>03</b> |
| <b>2</b> | <b>AnyDesk notifies of breach</b>                                      | <b>04</b> |
| <b>3</b> | <b>UK utility provider Southern Water confirms Ransomware incident</b> | <b>06</b> |
| <b>4</b> | <b>IN BRIEF</b>  | <b>07</b> |
| <b>5</b> | <b>DEEP DIVE – HELIX KITTEN</b>  | <b>09</b> |
| <b>6</b> | <b>Summary</b>   | <b>10</b> |

2024 really is treating us to some cyber highlights already with the #MOAB being reported on earlier this month.

In this month's summary we will also discuss the AnyDesk and Southern Water breaches before we deep dive into threat actor group HELIX KITTEN. We've got some interesting insights and, as always, our recommendations to protect against these threats. Enjoy!

## Introducing... '#MOAB' aka The Mother Of All Breaches

When a data breach warrants its own hashtag, you know it's going to be significant and the latest one uncovered by Ukrainian cyber security researcher Volodymyr 'Bob' Diachenko at [Security Discovery](#), significant is probably an understatement. At 12 Terabytes of data comprising over 26 billion (yep, that's a 'B') records, this is the largest breach dataset that we know of being collated in one place. Bob is no stranger to uncovering evidence of bad things, having used Shodan to uncover 279 million PII records stored in an unsecured AWS bucket back in 2019.



In context, the majority of these records are collated from breaches already disclosed and in some cases (MySpace) a long time ago, however one of the largest online collator of breach datasets holds around 15 billion records from over 2,500 data breaches so at a rough estimate, that's still a very significant 9 billion potentially new credential sets released into the wild.

The top two record sets relate to Chinese social media platforms Tencent QQ and Weibo with LinkedIn, Adobe, Canva and Telegram also being found among the Top 50. From our own analysis on the list of leaked domains, the sources appear to be indiscriminate and not politically or ideologically-motivated although using a breakdown of the geographically-aligned TLDs we did observe a higher concentration of .cn (Chinese) registered domains.

On 24th January, the data breach search engine [Leak Lookup](#) claimed responsibility for the exposed dataset and stated that the records were no longer available, citing "firewall misconfiguration" as the cause, something Bob confirmed when we spoke to him this week. The owner stated that access to the dataset was available from "early December 2023" so it's a certainty that the data has been downloaded in its entirety by threat actors seeking to enhance their password-guessing success using techniques such as [credential stuffing](#). For the curious, the complete list of breached domains is available [here](#).



## Recommendations

---

e2e-assure's SOC is operating with increased vigilance around identity-based and social engineering attacks based on this information and we recommend the following steps to safeguard against the risk of breach resulting from the exposure of this information:

- Deploy Multi-Factor Authentication (MFA) in supported environments, giving precedence to accounts on internet-facing systems and services. This helps reduce the risk of unauthorised access by addressing threats associated with password reuse or password guessing techniques utilising on the information present in the dataset.
- Encourage employees to exercise heightened awareness regarding password security and the identification of social engineering attempts and reinforce user awareness training on topics related to identity protection and social engineering.
- Review your email security controls to ensure you are effectively preventing the delivery of suspected phishing emails targeting employees.
- Consider making a corporately managed password management system available to employees to encourage the use of strong passwords for work use.
- Consider integrating corporate identity controls with <https://haveibeenpwned.com/> using natively-supported configuration or via the API to prevent users from choosing account passwords already found in breaches, carry out password audits and return breach data held for specific domains among other uses: <https://haveibeenpwned.com/API/v3>
- Encourage employees to sign-up to legitimate and free breach notification services such as <https://haveibeenpwned.com/> to monitor their personal user credentials and notify them when their accounts may be at risk. This will also have a secondary effect of discouraging password reuse between personal and corporate user accounts.
- Consider utilising a corporate identity monitoring service to get advance notification of sensitive employee credentials being discussed, exposed or offered for sale on underground marketplaces and forums.
- Critically, speak to us! We are experts in the design and implementation of security controls and monitoring, as the UK's premier SOC & XDR provider we work alongside organisations of all sizes, increasing their security posture with tailored and affordable protection solutions.

## AnyDesk notifies of breach

On 2 February, popular Remote Access software company AnyDesk notified customers and the world at large via [their website](#) that they had been the victim of an unauthorised intrusion by an unknown threat actor. The statement went on to say that they had enacted their IR plan, including calling in the services of CrowdStrike. Seeking to reassure clients that this was not a Ransomware-related incident, [further statement](#) on 5 February indicated that the company had found no evidence of the exfiltration of customer data. Although not explicitly stated, from reading between the lines it appears that their [code-signing certificate](#) (used to validate the authenticity of their software) has been stolen, which would give a threat actor the ability to impersonate valid software with a malicious variant. The vendor's recommendation is to update to the latest version of the software, downloadable from [their portal](#).

In response to the inevitable questions of account security, their statement included the carefully-worded statement

**“We do not believe that this is the case. However, unfortunately we cannot rule out the theoretical possibility for a short period of time. Consequently, as a precautionary measure, we have forced a password reset for all customers” which is legalese for “we don’t know and are covering all our bases with this statement.”**

Responding to claims that stolen AnyDesk credentials were available for sale on the notorious dark web forum exploit.in, the company sought to downplay these and instead speculated that these had been historically harvested using infostealer software on compromised machines, rather than relating to this most recent breach. Cyber security firm Resecurity have written an in-depth [blog post](#) regarding the breach, which partly casts doubt over this claims, highlighting the timestamp of 3rd Feb 2024 on a screenshot supplied by the threat actor whom they had engaged in dialogue. Resecurity pointed out that the majority of accounts they viewed did not have 2FA enabled, a strong indicator of its role in frustrating threat actors.



There is some good news; the stolen certificate has a unique digital fingerprint, making it easy to hunt for and detect on the network. Our experts at e2e-assure are pleased to be provide you with the following Kusto (KQL) queries that will detect the presence of the certificate and latterly, the presence of AnyDesk traffic on your network:

```
DeviceFileCertificateInfo | where CertificateSerialNumber == '0dbf152deaf0b981a8a938d53f769db8' | summarize Count = count() by DeviceName
```

```
DeviceNetworkEvents | where InitiatingProcessVersionInfoCompanyName == 'philandro Software GmbH' and InitiatingProcessVersionInfoProductName == 'AnyDesk' | where ActionType == 'ConnectionSuccess' | summarize Count = count() by RemoteUrl
```

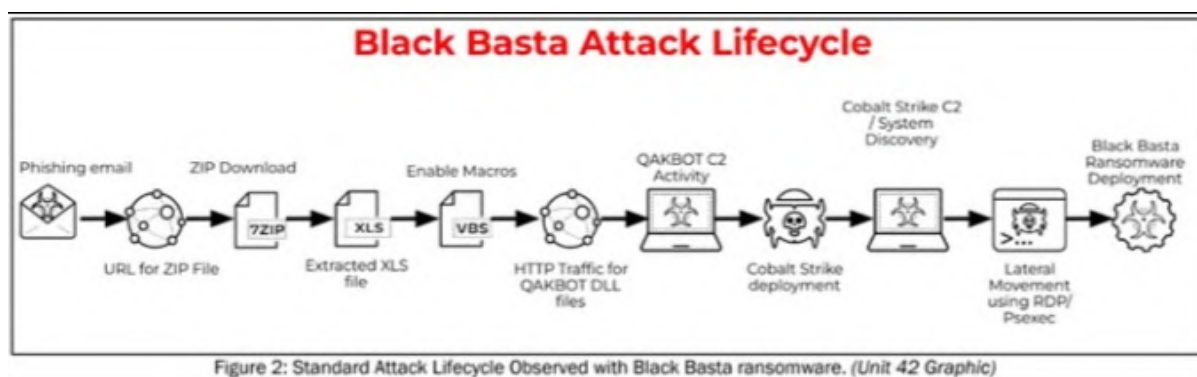


These queries were provided instantly to existing customers via our SOC and Consultancy teams who have conducted extensive hunting across those estates, providing advice and remediation as appropriate. We have pleasure in sharing with you and stand ready to assist your teams should you have concerns relating to this.

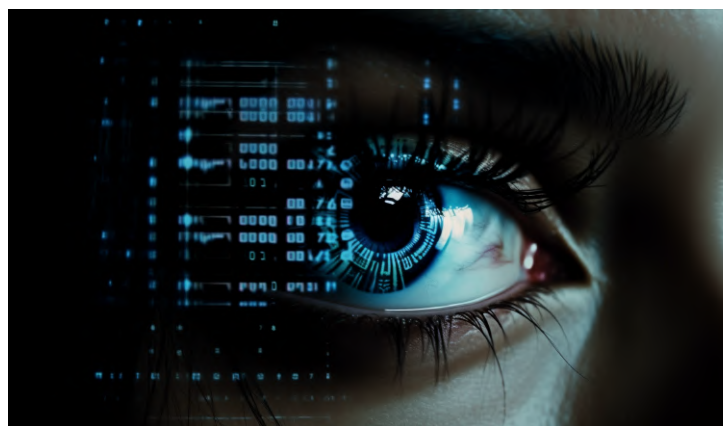
# UK utility provider Southern Water confirms Ransomware incident

Southern Water, the utility company providing water services to counties across the south of England have confirmed that they have been the victim of a ransomware incident, recently attributed to notorious Russian-based group BlackBasta.

Black Basta listed Southern Water on their dark web leak site, claiming to have stolen over 750GB of operational and customer data. At the time of writing this listing has been removed which is an indicator that the victim may have chosen to pay the ransom rather than face an ongoing situation.



A statement on the company's website on 23 January of this year addressed claims that cyber criminals had gained access to their systems and stolen data which it went on to confirm had been published. This statement highlighted that there was at that time, no evidence that customer or financial data had been accessed, although a further statement on 12 Feb acknowledged that customer data had been exfiltrated and that their estimate was that this constituted 5-10% of customer data. Given that Southern Water service approximately 7.2 million customers, at a conservative estimate this equates to the data of around 360,000 individuals and organisation now in the hands of the threat actor. According to a [report](#) by BBC news, this data included customers' dates of birth, national insurance numbers, bank account details and reference numbers.



The provider declined to comment on this aspect when questioned by IT press outlet The Register, instead sticking to their previous statement which confirmed that they had complied with all regulatory requirements, were in the process of contacting affected parties and had engaged the services of cyber security professionals. No technical details were provided about the attack but it's likely that the attack started with a phishing lure or the compromise of a vulnerable Remote Desktop server.

## IN BRIEF

The best of the rest! Before we dive into the list of equally interesting but perhaps less prominent stories from around the world, we bring you an update on VOLT TYPHOON aka Vanguard Panda and Bronze Silhouette among other monikers. After our Deep Dive on the group ([e2e-assure CTI briefing, July 2023](#)) it appears that the rest of the world have caught up! On 7 Feb, US agency CISA released [an advisory](#) in conjunction with their Five Eyes partners, warning of the danger posed by the China-attributed APT along with protective steps to be taken. Additionally SC Magazine [reports](#) how the group's attempt to rebuild their C2 infrastructure after an FBI takedown was foiled by a group of cyber security researchers. Remember, you read it here first!



- [Smartphone vendors toy with AI, includes access to your messages](#)
- [South Korea decrypts Rhysida Ransomware](#)
- [Apple announces fix for its first 0-Day of 2024](#)
- [Research by e2e-assure highlights cyber failure in nearly half of financial orgs](#)
- [Deepfake abuse on the rise – Taylor Swift imagery removed from Twitter](#)
- [2023 Ransomware payments exceed \\$1 Billion](#)
- [Canterbury, Dover and Thanet councils submit breach reports to ICO](#)
- [US DoD notifies 20,000 breach victims after data leak](#)
- [Chinese 'spy' pigeon released from Indian custody](#)



## DEEP DIVE – HELIX KITTEN

Even though the last month has been dominated by the exploits of MIDNIGHT BLIZZARD and VOLT TYPHOON our intrepid reporters once again being ahead of the curve have already brought you insights into these groups ([July 2023 & January 2024](#)) – this month we investigate another prominent activity group whose activities have increased significantly and sadly inevitably since October last year. APT34 aka HELIX KITTEN, Oilrig, COBALT GYPSY and Crambus are Iran-attributed group, believed to be state-sponsored or endorsed but certainly acting in the interests of that country's regime.



The group has been active since at least 2014 and is known for conducting cyber espionage and cyber intrusion operations primarily targeting entities in the Middle East that align with the strategic interests of the Iranian government. The group's activities are aimed at sectors that are significant to regional geopolitics, including financial, government, energy, chemical, and telecommunications sectors, with a strong focus on gathering intelligence that could benefit Iran's geopolitical and strategic interests.

APT34's organisation is characterized by its use of sophisticated tools and techniques, including social engineering, spear-phishing emails, and the deployment of custom malware and backdoor exploits. The group is structured in a manner that suggests a high level of sophistication, with specialised operatives likely responsible for different phases of their cyber operations, from initial reconnaissance and exploitation to data exfiltration.

## Their wide range of TTPS include (but are not limited to):

- **Spear-Phishing Emails:** Tailored emails that target specific individuals or organizations with the intent of tricking the recipient into executing malicious attachments or clicking on malicious links.
- **Custom Malware and Backdoors:** Development and deployment of custom malware tools and backdoors to maintain access to compromised networks and exfiltrate data.
- **Web Shells:** Placing web shells on public-facing servers to establish persistence and facilitate lateral movement within a network.
- **Credential Harvesting:** Using tools and techniques to steal credentials, which are then used to move laterally across networks and access sensitive information.
- **Social Engineering:** Creating fake profiles and using compromised accounts on social media to approach and trick targets into divulging sensitive information or installing malicious software.



They have been known to use web shells for persistent access and command execution on compromised web servers. One example of a web shell commonly associated with APT34 is the "TwoFace" web shell, which demonstrates their sophistication in maintaining stealth and persistence. The TwoFace web shell allows the attackers to execute arbitrary commands, manage files, and move laterally within the network. Other, custom malware include 'Helminth' and 'BondUpdater', PowerShell-based trojans used for Initial Access and Privilege Escalation. 'Quadagent', yet another PowerShell-derived malware has been observed specifically targeting Middle Eastern entities.

One notable aspect of APT34's operations is their use of social media and email to deliver malicious attachments and links to their targets. They have been known to create fake personas and use compromised accounts to gain the trust of their targets. Once trust is established, they deploy malicious payloads that exploit vulnerabilities in software commonly used by their targets.



## Who are they targeting?

APT34's operations have been wide-ranging, targeting sectors such as finance, government, energy, telecommunications, and critical infrastructure, primarily in the Middle East. While specific victim organizations are often not publicly disclosed due to the sensitivity and potential repercussions of such information, some patterns and examples include:

- **Financial Institutions:** Banks and financial services companies in the Middle East have been targeted for their role in regional and international finance, seeking to gather economic intelligence and potentially disrupt financial operations.
- **Government Agencies:** Various ministries and governmental departments, especially those involved in foreign affairs, defence, and energy have been compromised to collect intelligence on policy-making and strategic plans.
- **Energy Sector:** Companies involved in oil and gas exploration and production have been targeted, reflecting the sector's critical importance to many Middle Eastern economies and the global energy market.

These operations often result in the theft of sensitive information that could be used to further Iranian national interests or to gain a strategic advantage over regional rivals and adversaries.



The group leverages a sophisticated array of custom tools and techniques to conduct espionage and intelligence gathering. Their focus on developing and using a variety of malware and web shells, along with their strategic choice of targets, underscores the group's role in furthering the cyber espionage objectives of their sponsors. As cyber defence mechanisms evolve, so too do the tactics and tools of groups like APT34, making it imperative for potential targets to maintain robust, adaptive cybersecurity postures.

At e2e-assure we've been tracking APT34 almost since their inception and have amassed archives of data pertaining to their activities that we utilise effectively in proactive threat hunting and protective monitoring engagements. Utilising our bespoke SIEM 'Cumulo' alongside open-source tooling such as the MISP platform allows us to correlate and analyse this data, enabling us to provide a greater degree of protection to our customers through intelligent manipulation and analytical techniques.





## Let's connect!

That wraps up the February edition of our Threat Intelligence briefing, we look forward to bringing you another exciting edition in March – thanks for reading!

We welcome any feedback you have at [cti@e2e-assure.com](mailto:cti@e2e-assure.com)