

October 2023

Cyber Threat Intelligence Summary

Contents

1	Okta gets breached. Again.	03
2	Critical vulnerabilities being exploited in Cisco IOS XE software	05
3	ICC to prosecute 'Cyber' war crimes	06
4	In brief!	07
5	Deep Dive – SANDWORM	08
6	Summary	10

Welcome to this month's summary of events, brought to you by e2e-assure's CTI team. It's been another eventful period since our last publication, with the disclosure of a major breach and another, exploited vulnerability breaking only just in time to make it into this month's edition. As well as these, we'll review events surrounding the International Criminal Court, take a deep dive into the notorious threat actor 'Sandworm' and round up the best of the rest, in brief.

| Okta gets breached. Again.

In what appears to risk becoming an unfortunate theme, the identity provider Okta has disclosed yet another breach of its systems. More worryingly, the vendor was advised of the breach by three of its customers, 1Password, BeyondTrust and Cloudflare, who noticed suspicious activity on their own systems and subsequently alerted Okta. BeyondTrust notified Okta of suspicious activity by one of its Admin accounts on 2 October and immediately took remedial action, however it took Okta over two weeks to acknowledge the breach, finally doing so on 19 October.

While the currently unidentified attackers were unable to access Okta's production systems according to a statement by Okta's Chief Security Officer David Bradbury, they did access the company's support case management system which contains customer data including HAR (HTTP Archive) files generated from browser troubleshooting sessions. These HAR files contained sensitive information including cookies and session tokens, the theft of which allowed the attacker to subsequently compromise BeyondTrust and Cloudflare admin accounts on the Okta portal via existing, open sessions.



The fact that Cloudflare's excellent IR teams were able to **contain and eradicate this threat** so fluidly speaks volumes to their cyber maturity, unfortunately it raises a polarised statement regarding Okta. We have full confidence in echoing Cloudflare's remediation advice, which is to:

- Enable Hardware MFA for all user accounts. Passwords alone do not offer the necessary level of protection against attacks. We strongly recommend the usage of hardware keys, as other methods of MFA can be vulnerable to phishing attacks.



Investigate and respond to:

- All unexpected password and MFA changes for your Okta instances.
- Suspicious support-initiated events.
- Ensure all password resets are valid and force a password reset for any under suspicion.
- Any suspicious MFA-related events, ensuring only valid MFA keys are present in the user's account configuration.



Monitor for:

- New Okta users created.
- Reactivation of Okta users.
- All sessions have proper authentication associated with it.
- All Okta account and permission changes.
- MFA policy overrides, MFA changes, and MFA removal.
- Delegation of sensitive applications.
- Supply chain providers accessing your tenants.



Review session expiration policies to limit session hijack attacks:

- Utilize tools to validate devices connected to your critical systems, such as Cloudflare Access Device Posture Check.
- Practice Defence in Depth for your detection and monitoring strategies.

Additionally, if you think you may be impacted by this incident, we urge you to reach out to us - our people are standing ready to assist yours. For more information and some really useful insights, check out this recent [LinkedIn post](#) from our CEO @Rob Demain as well as [this](#) threat-specific page from the NCSC.

Critical vulnerabilities being exploited in Cisco IOS XE software

As we were producing the content for this publication, news broke of two, actively exploited vulnerabilities in Cisco's IOS-XE software used to power many of the firm's high-end and enterprise devices, including elements of the ASR, ISR, NCS & Catalyst ranges. These are being tracked as CVE-2023-20273 & [CVE-2023-20198](#), the

latter of which has gained the highest possible CVSS rating of '10' as it allows a remote, unauthenticated user to create an account with privilege level 15 access, ultimately gaining control of the entire system. The former allows a remote, authenticated attacker to inject arbitrary commands as the root user.

Currently this is no workaround however Cisco were quick to release a [patch](#) for the affected systems, detailed here and which can be located via your support portal for in-life systems. The Web UI is the specific component affected by this vulnerability, running the following command will return the enabled status of this component:

```
show running-config | include ip http server|secure|active
```

If you're not able to immediately deploy patches to remediate, the following code example demonstrates how to restrict access to a trusted network, using 192.168.0.0/24 as an example reference:

```
!  
ip http access-class 75  
ip http secure-server  
!  
access-list 75 permit 192.168.0.0 0.0.0.255  
access-list 75 deny any  
!
```

Be sure to save the running config so your changes do not revert at the next reboot! There is little other information available at this stage, including attribution however Cisco's TALOS division have released a [technical advisory](#), including IOCs which e2e-assure immediately ingested into our threat intelligence platforms.



We quickly ascertained that our own systems are unaffected and continue to work closely with our customers to assist in remediation, containment and eradication. If you think you may be affected by this, please reach out to our Account and Support teams as soon as possible.

ICC to prosecute 'Cyber' war crimes

In a statement last month that we were surprised gained little attention, the International Criminal Court's Lead Prosecutor, Karim Khan announced his intention to prosecute illegal cyber activity affecting civilian, critical infrastructure. The threshold is to be determined under the Rome Statute, the treaty under which the ICC's authority to prosecute is determined. Khan was quoted as saying

“Cyber warfare does not play out in the abstract. Rather, it can have a profound impact on people's lives. Attempts to impact critical infrastructure such as medical facilities or control systems for power generation may result in immediate consequences for many, particularly the most vulnerable. Consequently, as part of its investigations, my Office will collect and review evidence of such conduct.”

The Russia/Ukraine conflict has not been specifically addressed in relation to this statement, however an official, 'Article 15' statement submitted to the ICC by the Human Rights Centre at UC-Berkeley's School of Law urged the ICC to consider the very same in respect of SANDWORM, a prolific and destructive threat actor associated with Russian national interests and who are widely believed to have been responsible for devastating attacks on Ukraine's national infrastructures on multiple occasions.



As well intentioned as this statement may be, it is not without its challenges. One of the primary challenges in addressing cyber warfare is the absence of a clear and universally accepted set of rules and norms governing cyber operations. Traditional international laws, such as the Geneva Conventions, were formulated in a different era and are ill-equipped to handle the complexities of cyber conflict. The ICC, designed to prosecute war crimes, crimes against humanity, and genocide, lacks specific provisions to address cybercrimes effectively.

One potential solution to this may instead be the establishment of an International Cybercrime Court. This specialised court could define cyberwar crimes, establish precedents, and set the stage for international cooperation in combating cyber threats. It would also serve as a deterrent, sending a clear message that the international community is committed to holding perpetrators accountable for their actions on

the Internet as well as the physical battlefield. Further, the ICC could play a crucial role in adjudicating cases involving state-sponsored cyber-attacks, which are increasingly common and pose a significant challenge to traditional diplomacy. These attacks often blur the line between criminal activity and statecraft, making it difficult to attribute responsibility and take appropriate action. The ICC's expertise in handling complex legal issues could provide a path towards resolving these disputes impartially and in accordance with international law.

It is interesting to note that in the same period that this statement was released, the ICC suffered an acknowledged data breach now being touted as an '[Espionage Raid](#)' as well as a Russian spy in its midst, masquerading as an Intern. Coincidence? We think not and continue to watch with interest.



In brief!

A round-up of the best of the rest, articles we used for research that didn't make the final cut but we feel are still worthy of a mention –

[China's social-media attacks are part of a larger 'cognitive warfare' campaign](#)

[German financial regulator's website hit by DDoS attack](#)

[Ukraine security services involved in hack of Russia's largest private bank](#)

[Lazarus group exploits Adobe Reader vulnerability CVE-2023-26369](#)

[CIA builds its own 'ChatGPT'](#)

Finally and although not strictly CTI-related, it would be remiss of us not to mention e2e-assure's recent return to the [International Cybersecurity Expo](#) as one of its founding partners. One thing that is absolutely relevant to mention is the amount of conversations we had where CTI featured centrally, supporting the outcomes of our recent research that indicated business leaders are keener than ever to better understand the threats posed to them (the 'what'), but also increasingly demand insight to the 'who and the 'why'.

Deep Dive – SANDWORM

One of the most destructive and feared threat activity groups in the world today, we take an overview of this Russian-attributed group who are also known as VOODOO BEAR, IRON VIKING, BlackEnergy and less commonly, Telebots.

Strongly believed to be a part of Russia's GRU, specifically 'Military Unit 74455', so much so that in October 2020, a United States grand jury indicted GRU Officers Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko and Petr Nikolayevich Pliskin in relation to offences previously attributed to the group.



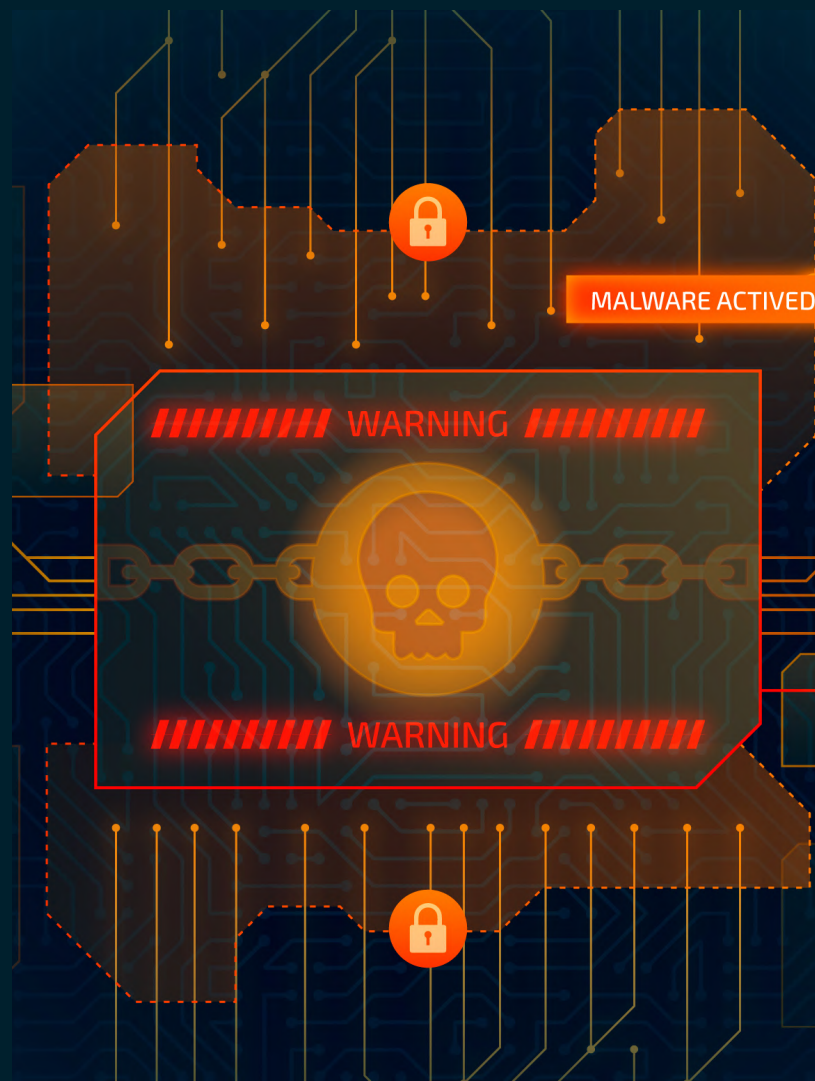
Source: Security Affairs

Active since at least 2013, Sandworm first gained widespread attention in 2014 when they were linked to a series of high-profile cyberattacks against various targets, primarily in Eastern Europe. The group's initial activities were primarily focused on espionage and data theft, targeting government organizations, military institutions, and most notably critical infrastructure in Ukraine and her neighbours. These early attacks exhibited a high level of technical sophistication, using zero-day vulnerabilities and advanced malware.

Sandworm was widely believed to be responsible for the NotPetya ransomware outbreak in 2017. This ransomware, initially disguised as a typical ransomware attack, quickly became apparent as a destructive wiper malware designed to cause maximum damage. NotPetya affected numerous organisations globally, causing billions of dollars in damage. Beyond these 'headline-grabbing' incidents, Sandworm has maintained a long-running campaign of espionage against government and military targets, especially in Ukraine and Eastern Europe. They have targeted critical infrastructure, diplomatic missions, and military units collecting sensitive information and conducting advanced cyber-espionage operations.



As we've discussed in these briefings previously, attribution is always the hardest element of any investigation and when dealing with a nation-state actor such as Sandworm, the stakes are raised even higher. That said and although dealing with this calibre of actor, they are not immune to error as evidenced by their failure in 2022 to recreate a previously successful attack on Ukraine's power infrastructure with Industroyer2/CaddyWiper, as they had with its primary namesake back in 2016. Over time, network & host artefacts along with tooling and TTPs, the holy grail of the pyramid, have been observed and collected by cyber defenders worldwide but especially those at CERT-UA, for whom Sandworm is a very personal nemesis. Sandworm's assault on the Ukrainians appears to be relentless, with the sovereign nation reporting a renewed wave of attacks against their Telcos and Internet Service Providers, ongoing since at least May 2023.



The group retain a scorecard with more successes than failures and of course, this is based only on the attacks that we're aware of. This is not a threat actor who is given to touting their spoils of war on the dark web for example, so it remains highly likely that there have been a much greater number of successful operations by them than is ever likely to be reported. Such is their notoriety, that an entire book has been written about the group, *'Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers'* by the brilliant [Andy Greenberg](#) contains almost every piece of publicly available information about Sandworm and is presented in such a gripping way that this author lost a weekend to it. (His 'Tracers in the Dark' publication is pretty good too).





Let's connect!

That rounds up October, research for November's edition is already underway although the world may be yet to dictate what makes it and what doesn't!

We hope you've enjoyed the content and we welcome any feedback you have at cti@e2e-assure.com