

November 2023

Cyber Threat Intelligence Summary

Contents

1	ONATO websites breached for the second time. By the same Threat Actor.	03
2	Citrix..Bleeds	04
3	BREAKING – Fortinet discloses critical vulnerability in FortiSIEM product	05
4	SIM vendor Lyca subject to cyber attack	06
5	Ransomware victim reported to SEC. By the Threat Actor.	07
6	In brief!	07
7	Deep Dive – LockBit	08
8	Summary	10

It's well and truly Winter out there, the established maxim of less kinetic offensive equals more cyber offensive is certainly holding true. Welcome to another edition where we've jostled over what to leave out for fear of rewriting War & Peace!

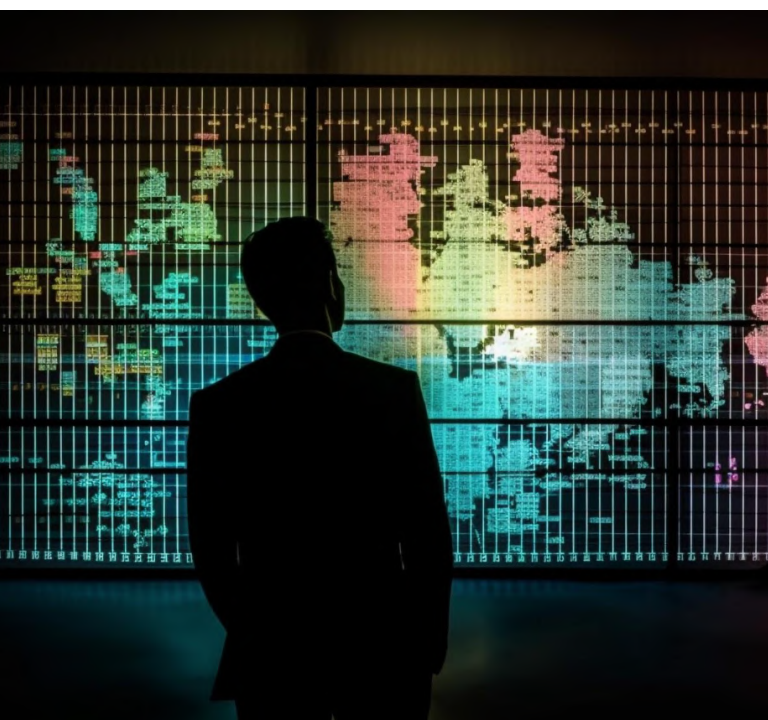
Targeted attacks and ransomware outbreaks are rampant, not a day has gone by recently without a breach disclosure or a chunk of CNI offline somewhere in the world. Speaking of disclosure and reporting, even the threat actors are at it as you'll read in this edition.

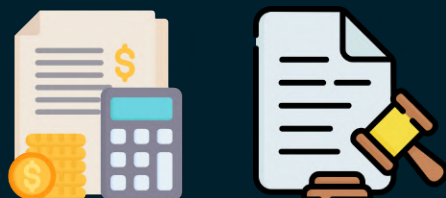
NATO websites breached for the second time. By the same Threat Actor.

Coming only months after the first, reported breach of NATO's 'Communities of Interest' portal website in July, the same website plus an additional five others belonging to the defence alliance have been compromised. This has resulted in the illegal exfiltration of 9GB of unclassified data. To make matters worse, responsibility for the attacks was claimed by the same group. SiegedSec, aka the 'gay, furry hackers' [posted on X](#) (formerly Twitter) the strapline "Siegedsec:2 Nato:0" along with screenshots alleged to be dumped from the breach.



Since their recognition as a collective in February 2022, the group appear to have adopted a broadly Hacktivist ideology while not discounting the opportunity for financial gain. This is something that they realise through the compromise of mainly smaller companies worldwide, with defacements and the subsequent extortion of stolen data. While they appear to be closely aligned with the pro-Ukrainian group GhostSec (the group have also claimed other, unproven associations), a number of security researchers have drawn parallels with the infamous 'Lulzsec' group, prominent over a decade ago and more recently, LAPSUS\$.





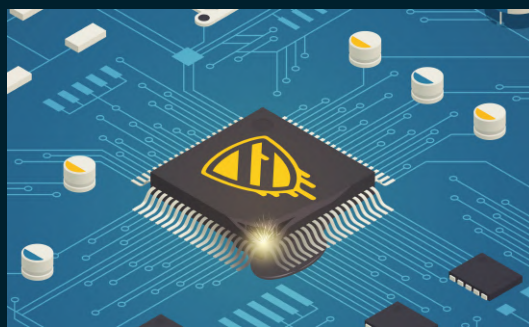
Affected Industries include healthcare, finance and legal.

Targeted industries have included legal, financial, healthcare and finance across the world, with a noticeable concentration around developing nations in the southern hemisphere. The Asian sub-continent and South America are the specific region with the most activity. One of their more prominent and recent actions while wearing their Hactivist hats, is the 'doxing' (public release of personal, identifiable data) of several US Supreme Court Justices. Apparently, this is in response to the overturning of the controversial Roe v Wade ruling, relating to US abortion laws. Home addresses and credit card data for at least four of the Justices was uploaded widely to darknet forums, after SiegedSec claimed a successful breach of the Kentucky and Arkansas state governments.

Although NATO have acknowledged that they are investigating circulated reports of a breach, they remain conservative about further statement beyond the standard "... additional security measures... ..no impact on NATO missions..." – we're following SiegedSec closely so expect more on this group in future editions!

Citrix..Bleeds

And the winner of this month's most impactful vulnerabilities goes to...virtualisation and SaaS leader Citrix for two unauthenticated buffer overflow vulnerabilities in their NetScaler ADC and Gateway products. With a 9.4 out of 10 CVSS rating this low complexity vulnerability with the [CVE 2023-4966](#) is being actively exploited in the wild and has already been held responsible for the successful breach of China's largest bank, the ICBC - allegedly by LockBit. A recent attack on car manufacturer Toyota may also feature on the victims list as Kevin Beaumont [notes](#) on X/Twitter, that large portions of their Internet-facing infrastructure appears to be susceptible to the vulnerability.



Affecting all versions of the NetScaler software between versions 12.1 & 14.1 inclusive, this vulnerability works by crafting an HTTP GET request with an HTTP Host header greater than a certain length, resulting in the contents of system memory being returned. This in turn allows existing, authenticated sessions to be hijacked and their tokens stolen, thereby effectively bypassing MFA and other authentication requirements. While Citrix disclosed this and released patches in early October, threat-hunting firm Mandiant (now part of Google) have stated that they observed active exploitation by an unknown threat actor as far back as August of this year. Mandiant also published a detailed, technical analysis with remediation strategies that you can find [here](#).

Following on from the massive pre-auth RCE ([CVE-2023-3519](#)) that hit the company in July and resulted in over 1,300 backdoored devices, Citrix will be likely feeling the heat for urgent reviews in the secure code review process.

If you think you're impacted, what can you do about it? Following these steps can aid in remediation if you're unsure you should take advice from your trusted security partner. At e2e-assure we have already been in touch with all our affected clients to ensure they've followed this advice, get in touch if you need our help:

- Isolate the affected device from the network. If this is not possible, implement strict ingress IP filter to minimise the attack surface.
- Apply patches available from the vendor, following [this document](#).
- Kill existing sessions using these commands (or reboot the device):

```
kill icaconnection -all
```

```
kill rdp connection -all
```

```
kill pcoipConnection -all
```

```
kill aaa session -all
```

```
clear lb persistentSessions
```

It's worth noting that devices which are not configured as a gateway (and that includes VPN & RDP proxies) or configured as an AAA server, are not impacted by this vulnerability. That said, ensuring your devices are running the latest software from the manufacturer is the best starting point to ensure device compliance and protection.

BREAKING – Fortinet discloses critical vulnerability in FortiSIEM product

As this briefing was being prepared, the security vendor Fortinet disclosed a critical vulnerability in their popular FortiSIEM report server. Initially graded with a CVSS score of 9.8 (now downgraded to 9.3), [CVE-2023-36553](#) allows an unauthenticated attacker to [execute commands](#) issued via crafted API requests. This is achieved by simple command injection techniques that

rely on a developer's failure to properly implement data sanitisation, allowing input to be parsed directly as commands in the affected device.

FORTINET Source: New Statesman



Versions affected are between 4.7 and 5.4 of FortiSIEM Report Server, Fortinet recommends an urgent upgrade to 6.x and 7.x versions of the software. The flaw was discovered by the vendor's own security team, who state that this is an additional variant of [CVE-2023-34993](#) (also a 9.8), fixed earlier in the year.

SIM vendor Lyca subject to cyber attack

Major network operator and global leader in SIM card operations, Lyca, [reported](#) on their website last month that they had been subject to an unauthorised intrusion resulting in impact to operational systems including number porting operations and the [loss of customer data](#).



To date, Lyca have released no technical information about the attack. The only public statements released confirm they have engaged professional services and are liaising with Ofcom and the ICO. Telecoms firms have long been a favourite target of a number of prominent threat activity groups, especially those from China and Iran, as well as presenting a lucrative target to a raft of



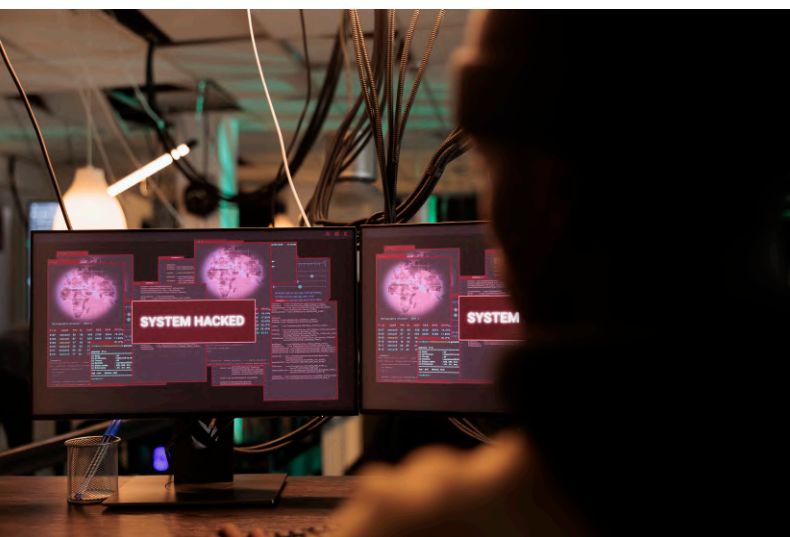
ransomware groups. We've seen a wave of such attacks spanning the globe in recent years, we will wait to see if any future TTPs & IOCs that are made available crossover with existing intrusions captured in our threat intelligence platforms.



If you are a customer, it's strongly recommended to change the password for your account and check any linked financial accounts for unrecognised transactions. Lyca has a customer services team that are reachable [here](#).

Ransomware victim reported to SEC. By the Threat Actor.

Cyber security is always full of surprises, good and bad. After being subject to a ransomware attack by the notorious group AlphV/'Black Cat' of MGM fame, software vendor MeridianLink found themselves reported to the USA's Securities and Exchange Commission. By the threat actor. A photo of an SEC submission form **posted** on Twitter/X claims to show this, although the referred regulations have not yet come into effect.



This is likely to be as much of a publicity stunt as it is an extortion tactic, although clearly designed to heap pressure on to an already stretched victim. Iliia Kolochenko, CEO at ImmuniWeb was quoted by RecordedFuture as saying "Ransomware actors will likely start filing complaints with other US and EU regulatory agencies when the victims fail to disclose a breach within the timeframe provided by law."

Gimmick or tactic, we predict that if this is that first time this has been tried, it won't be the last; from the attackers' perspective it's a minimum-effort action likely to raise the stakes for the victim more than themselves.

In brief!

Your monthly round-up of the best of the rest, information we gathered that didn't make the final cut, but we feel are still worthy of a mention –

- [A topical nod to SANDWORM \(covered in last month's edition!\)](#)
- [Huge cyber-attack shuts down Australian ports](#)
- [NCSC's 2023 Annual Review released](#)
- [Largest attack ever to hit Denmark takes out CNI](#)
- [Inaugural NATO Cyber conference pledges creation of 'Cyber Centre'](#)

Deep Dive – LockBit

As ransomware has featured heavily in this edition and in a reflection of the global stage, we thought it would be relevant to give you an overview of one of the sectors most ruthless and relentless operators, LockBit.

Sources vary on the creation of LockBit, but a consensus agrees on 2020 as the first year that they came to global awareness. In the ever-evolving landscape of ransomware, they have established and maintained a position of prominence, gaining a reputation as one of the most aggressive and efficient operators in that marketplace. Although far less prominent than Maze and Revil when starting out, they soon surpassed their rivals and successfully operated a ransomware-as-a-service (RaaS) model that continues to this day. This approach allows for widespread distribution and a more considerable number

of attacks. Technically, LockBit stands out for its automated encryption process, which quickly locks files across a network. This rapid encryption capability is often coupled with double extortion tactics, where they threaten to release stolen data if the ransom is not paid. Most recent is the technique of 'triple extortion' – adding sustained DDoS attacks amid demands for payment.

One of the critical technical aspects of LockBit is its ability to bypass security measures. It uses advanced techniques like living off the land (LotL) attacks, where it uses legitimate tools already present in the victim's network for malicious purposes. Additionally, LockBit employs evasion tactics to avoid detection by antivirus software and network monitoring tools.

LockBit's method follows a typical ransomware attack pattern, but with notable sophistication. Initially, they gain access to a target network, often through phishing emails, exploiting vulnerabilities or using stolen credentials. Once inside, they escalate privileges to gain more control over the system. Before deploying their ransomware, they often exfiltrate sensitive data, setting the stage for the double extortion scheme.

The ransomware encrypts files across the network, displaying a ransom note with instructions on how to pay, usually in cryptocurrency and most recently favouring Monero. LockBit typically sets a deadline for payment, after which they threaten to either increase the ransom amount or release the stolen data.



The group's targets are diverse, ranging from small businesses to large multinational corporations. They are indiscriminate in their choice of victims, affecting sectors like healthcare, legal, industrial, and government agencies. Recent victims are noted to include [Boeing](#), International law firm [Allen & Overy](#), and the Chinese state-owned bank [ICBC](#), in which the victim is alleged to have paid the ransom.

Detailed analysis of LockBit's operations and methodologies are extensively documented by cybersecurity firms such as Symantec and FireEye. These organisations regularly publish reports and threat intelligence briefings that offer insights into LockBit's evolving tactics. Around this time last year, threat researchers vx-underground [published](#) the transcript of an insightful interview with LBO, purportedly the leader of the LockBit group. Additionally, law enforcement agencies like the FBI and Europol have issued advisories and warnings about LockBit, supplying crucial information to the public and potential victims. In June 2023, the United States DoJ brought criminal charges against Russian national Ruslan Magomedovich Astamirov, for his alleged participation in the LockBit ransomware campaign. As there is no extradition treaty between the USA and Russia, we think it unlikely that this will have any affect!



LockBit is a sophisticated and adaptable cyber threat actor in the ransomware arena. Its continuous evolution of both structure and technology and effective tactics poses significant challenges for cybersecurity defenders. Understanding its operations, methodologies, and impact is crucial for organisations to develop more robust security strategies and mitigate the risks posed by such actors. At e2e-assure we constantly monitor the activities of LockBit, Conti and their peers; we have huge archives of threat data, ready to interrogate and cross-reference against emerging threats and activities. This enables us to spot trends and attacks as they develop, which in turns allows us to build proactive defences instead of hovering on a reactive 'back foot'.



Source: Wikipedia



Let's connect!

That's it for November! Join us for December's briefing when we'll be raiding our Cyber Advent calendars, finding out what's in Santa's SOC this year and wondering if the CTI team can exfil the mince pies before the CISO does!

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