

# Cyber Threat Intelligence Summary

---

January 2024



# Contents

<b>1</b>	<b>Microsoft breach by MIDNIGHT BLIZZARD</b>	<b>03</b>
<b>2</b>	<b>Two Zero-Day vulnerabilities discovered in widespread attack on Ivanti VPNs</b>	<b>04</b>
<b>3</b>	<b>LockBit strike again: Taiwanese manufacturer Foxsemicon hit</b>	<b>06</b>
<b>4</b>	<b>IN BRIEF</b>	<b>07</b>
<b>5</b>	<b>DEEP DIVE – APT29</b>	<b>09</b>
<b>6</b>	<b>Summary</b>	<b>10</b>

It might be the start to 2024, but we've already got plenty of interesting and in some cases, eyebrow-raising events to bring you.

Notably, in the last week of authoring, tech leviathan Microsoft acknowledged a breach by notorious Russia-attributed threat actor APT29, aka Midnight Blizzard and in the same week Taiwanese semiconductor manufacturer Foxsemicon reported that they'd been hit by LockBit.

We'll take a closer look at these events, along with an overview of the notable attacks underway against customers of Ivanti's VPN products, a critical vulnerability in Gitlab's software, an extended 'In Brief' round-up and if that wasn't enough, a topical deep-dive into Microsoft's most recent nemesis, APT29.

## Microsoft breach by MIDNIGHT BLIZZARD

Coming not too many months after Microsoft inadvertently relinquished control of some of their code-signing keys to China-attributed threat actor STORM-0558 is the news that once again, the tech giant have been breached, this time by veteran threat actor APT29/Cozy Bear which MS refer to under their naming convention as Midnight Blizzard.

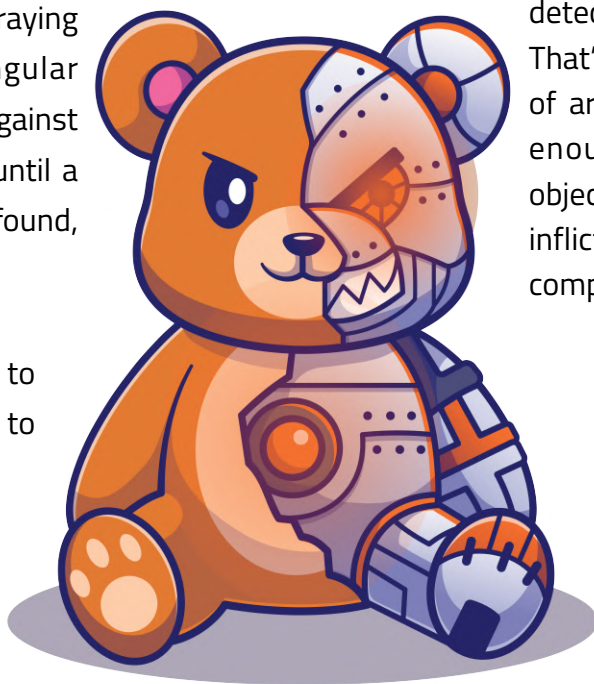
On Friday, 19th January Redmond [announced](#) that the hacking group had compromised a 'legacy non-production test tenant account' by means of a password spraying attack, whereby a singular password is 'sprayed' against multiple target accounts until a matching combination is found, which in this case it was.

As others have been quick to point out, this appears to indicate that contrary to its [own advice](#), Microsoft had failed to implement 2FA/MFA

against one of its own accounts, resulting in the threat actor gaining a foothold in to their corporate network. We're not aware of the specific next steps taken in terms of lateral movement and privilege escalation, however it seems to have been a relatively short route from there to gaining the ability to compromise multiple accounts across Microsoft's senior leadership, legal and cyber security teams. Equally concerning is the announcement that this breach occurred in November of last year

and was seemingly ongoing until detection less than a fortnight ago. That's a dwell time for the attacker of around eight weeks, more than enough time to achieve their objectives and have the potential to inflict longer lasting damage or compromise.

In contrast, Microsoft were quick to say in a statement that the breach was not due to a vulnerability in their software



or services and have agreed to release further information 'as appropriate'. We can't help but wonder what extent of any investigation will fall into that category! While small comfort may be drawn from the fact that if it can happen to Microsoft then it can happen to anybody, the stronger part of the issue is that it shouldn't be happening to any organisation, of any size.



## Learnings from this breach:

Multi-factor authentication isn't a silver bullet and threats such as fatigue attacks do exist, however in the case of a low-sophistication, brute force attack such as this one, it would have intercepted the authentication mechanism and forced a decision into friendly, human hands. Multiple solutions exist at low/no-cost including Microsoft's own, making the once arduous task of implementing across a corporate network seamless and without the need for downtimes.

As part of our initial threat assessments and pre-onboarding, we check for this and help you to integrate into your defence architecture if you haven't done this already and give you some hardening tips where it is in place. Speak to our Consultants to learn more about this.

## Two Zero-Day vulnerabilities discovered in widespread attack on Ivanti VPNs

Cyber security firm and forensics leaders Volexity have [shared](#) details of two zero-day exploits uncovered as part of a breach investigation on a customer's network – [CVE-2023-46805](#) and [CVE-2024-21887](#) are authentication bypass and command injection vulnerabilities which when chained together trivialise the effort required to run arbitrary commands on Ivanti's Connect Secure (ICS) VPN appliances.

The initial attack has been attributed to little-known threat actor UTA0178 who are believed to be Chinese state-sponsored or endorsed, but with evidence of over 1,700 devices globally, Volexity are assessing with confidence that the exploits are now in the wild and being actively weaponised. The observed finesse of the attack, the attacker's elite skill level and ease of persistence and traversal via 'Living Off The Land' ([e2e CTI Briefing – May 2023](#)) as described in Volexity's excellent writeup certainly point to an activity group near the top of their game.



Ivanti have reacted swiftly and released detailed [mitigation steps](#), with patches for the affected products due to be released from this week and in their evolving document, point to their inbuilt integrity checking tool as a starting point to discover compromised devices. They correctly stress that no evidence of a compromise is not an assurance that one hasn't occurred and therefore recommend that their mitigation steps are undertaken in parallel with sound network investigations and forensics, good advice. So concerned were the USA's NCSC-equivalent CISA, that they took the unusual step of issuing an [Emergency Directive](#) that echoed the vendor and Volexity's mitigation steps. Additionally, Volexity and Mandiant have released incident response reports containing IOCs & TTPs that were automatically ingested into our systems, while the latter has also released some useful [Yara rules](#) for post-exploitation detection.



If you're running Ivanti (formerly Pulse Connect Secure) kit in your infrastructure and are worried you may be vulnerable or need guidance through the remediation of a confirmed compromise, our Analysts and Incident Response experts are ready to help you, get in touch with us today.



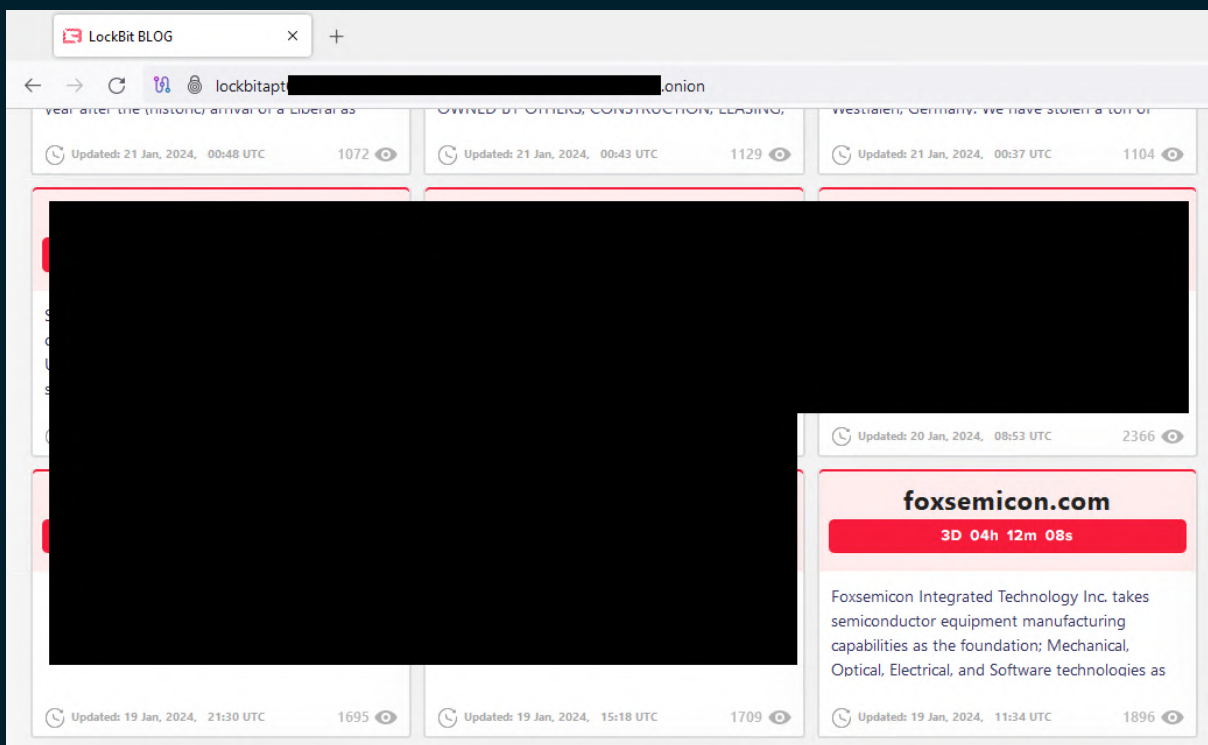
```
rule M_Hunting_Backdoor_ZIPLINE_1 {
  meta:
    author = "Mandiant"
    description = "This rule detects unique strings in ZIPLINE, a passive ELF backdoor that waits for incoming TCP connections to receive commands from the threat actor."
  strings:
    $s1 = "SSH-2.0-OpenSSH_0.3xx" ascii
    $s2 = "$(exec $installer $@)" ascii
    $t1 = "./installer/do-install" ascii
    $t2 = "./installer/bom_files/" ascii
    $t3 = "/tmp/data/root/etc/ld.so.preload"
  ascii
    $t4 = "/tmp/data/root/home/etc/manifest/exclusion_list" ascii
  condition:
    uint32(0) == 0x464c457f and
    filesize < 5MB and
    ((1 of ($s*)) or
    (3 of ($t*)))
}
```



# LockBit strike again: Taiwanese manufacturer Foxsemicon hit

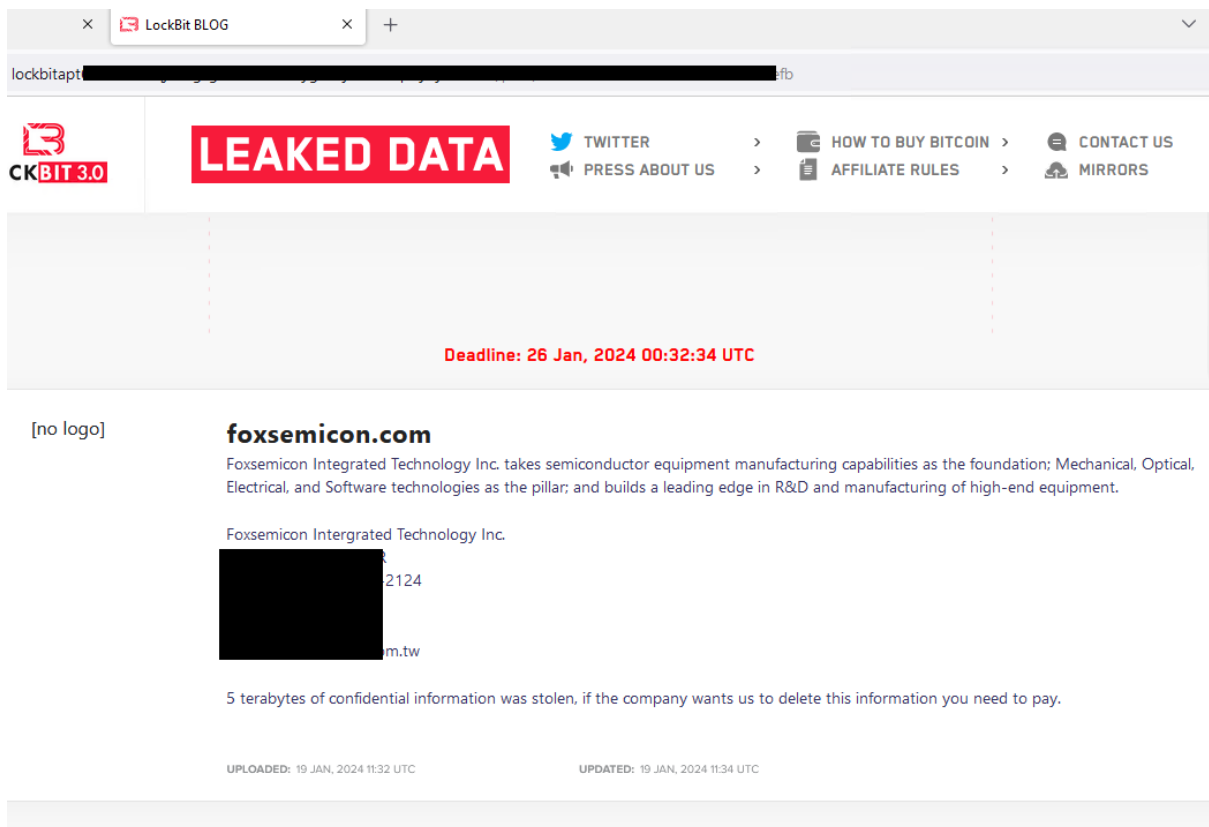
Reports have circulated in the last few days of a successful LockBit strike on one of Taiwan's largest semiconductor manufacturers, Foxconn subsidiary Foxsemicon. News sites including Recorded Future's 'The Record' [indicate](#) that around 5TB of data has been exfiltrated from the organisation, citing a defacement post on the now-restored corporate website. The threat actor's alleged haul includes substantial

amounts of customer and employee data and while an amount or any negotiation has not been made public, the touted figure of \$1 Million ransom payment although still astronomical, pales into insignificance when compared to the \$71 Million demanded by LockBit from rival Taiwanese firm Taiwan Semiconductor Manufacturing Company in June of last year.



Given the political tension between Taiwan and China and its recent escalations, it would be easy to make a link between the two, however in the case of LockBit, Foxsemicon are dealing with a financially and not politically motivated threat actor attributed to Russia and not a Chinese state actor. No technical details have been released on the attack itself but given LockBit's history of phishing lures and their

abilities in compromising interactive sessions, it seems likely that these were the initial access methods.



Earlier articles commented on the absence of evidence from LockBit's dark web site however e2e-assure's CTI team have located posts on the threat actor's site on the Tor network, indicating that they are indeed the perpetrators. As the second image shows, the deadline is set to expire in the first hour of Friday, so we'll be keeping a close eye on developments.

## 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 –

### Critical bug in Gitlab software leads to account takeover

Gitlab, the company behind the eponymous software suite, released a raft of patches for its Community and Enterprise versions this month, patching all production releases for a nasty bug dubbed [CVE-2023-7028](#), derived from flawed code in the email verification process that could allow for unauthorised password reset emails to be sent, resulting in the takeover of that account and in the case of an administrator account, the entire system.



## Next Steps:

In addition to patching immediately, [the advisory](#) from Gitlab recommends enabling 2FA on all accounts and limiting exposure of servers to the Internet. Exploitation has not been observed in the wild but intelligence firm Cyble [claim](#) evidence of underground chatter alluding to a weaponisation of the flaw along with a large list of vulnerable servers, so mass exploitation is likely to be imminent.



- [Google releases analysis of COLDRIVER targeting Western governments](#)
- [Ukrainian arrested over million-Euro cryptojacking mining scheme](#)
- [RUSI publishes paper on harms of Ransomware on societies](#)
- [Civica denies blame for cyber attack affecting three UK councils](#)
- [ChatGPT parent OpenAI quietly removes ban on Military Use](#)
- [Former NCSC Chief Ciaran Martin to head up new Cyber Monitoring Centre](#)
- [Free this weekend? Build your own Drone tracking Radar! A different kind of intelligence collection!](#)



## DEEP DIVE – APT29

With the recent intrusion at Microsoft being attributed to this threat activity group, we thought it would be topical to take a closer look at their history and operations. APT29 (Mandiant), also referred to by multiple, alternative monikers including 'Midnight Blizzard'/'Nobelium' (Microsoft), 'Cozy Bear' (CrowdStrike), 'The Dukes' and 'Grizzle Steppe' (when operating in conjunction with APT28/Fancy Bear) are a top-tier capability group strongly asserted to be affiliated with or even an integral part of the Russian Foreign Intelligence Service (SVR), a successor to the Soviet-era KGB.

While some of these names may be unfamiliar, their recent and historical activities will likely not be; compromises such as the Pentagon hack of 2015, the 2016 attacks on the US DNC (Democratic National Committee) and related think-tanks, attacks on several NATO-allied governments across 2017 and of course the now notorious SolarWinds attack of 2020 which in turn led to the further compromise of several US Government departments have all been attributed with confidence to APT29.

It's not Microsoft's first encounter with them either, in 2022 their security team published [this blog](#) that covered a novel, post-compromise capability dubbed 'MagicWeb' that involved token manipulation on Microsoft-produced Active Directory Federation Services (ADFS) servers.

Known for having the capability to produce their own malware, the group also make extensive use of Cobalt Strike and PowerShell operations as well as being adept at 'Living off the Land' techniques, increasing stealth in their operations and making detection harder. That is not to say that lower-tech alternatives are not considered as part of operations, the group have been observed to deploy phishing campaigns and targeted supply-chain attacks in order to achieve their objectives.

As you may expect from a state-influenced actor, the group favour operations against Western Governments and NATO members, particularly elements of which are directly responsible for shaping foreign policy and those that may hold geopolitical data that would be advantageous to Russian policy makers. Related commercial entities are also very much in scope, including but not limited to the energy, telecoms and military/defence/space sectors. At e2e-assure, we have been tracking APT29 since their 'Hammertoss' attacks against the Pentagon in 2015 and have compiled a large dataset of TTPs along with campaign-specific IoCs & IoAs (Indicators of Compromise & Attack) that we use for protective monitoring and proactive threat hunting of this group. We're happy to share elements of this, get in touch to learn more.





## Let's connect!

That's it for this month's briefing, thanks for reading and we will see you next edition!

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