April 2023

Cyber Threat Intelligence Summary

e2e assure

*Welcome to the inaugural **Threat Intelligence briefing** from e2e's Cyber Threat Intelligence team. Each month we will be reviewing the most prevalent issues affecting our customers along with interesting articles from across the Internet.*

This month we're thinking about ransomware as well as looking at 3CX, fake ChatGPT browser extensions, darknet seizures and an overview of the threat actor dubbed APT43.

Contents

Ransomware

- **Ransomware recognised as a national security threat**
- **Private CNI Sector to be subject to Cyber Resilience regulations**
- **March 2023 record-breaking month for Ransomware attacks**

Belfast was a very busy city for numerous reasons last week, most importantly for this article it was the location for Cyber UK23. The e2e-assure team were present and had a whole range of insightful conversations with business owners, security officers as well as fellow cyber security pioneers.

The opening keynote was delivered by Deputy Prime Minister, Oliver Dowden. He wasn't holding back with his view on the severity of the current situation, a stand-out quote pertaining to ransomware is very clear on the motives of some nation states that turn a blind eye to underground organisations attacking businesses in the west:

> **"...ransomware is no longer just a crime. It is a national security threat - and our response needs to reflect the severity of that threat. These are attacks on our citizens, our businesses and our democracy. They are an attempt to undermine our society."***

Another big discussion around ransomware included the shift in objectives by attackers to just stealing data as opposed to encrypting it, unfortunately Capita would appear to be the latest victim of this trend: **Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information - SecurityWeek**

This move away from encrypting data enables attackers to operate more stealthily and puts a far greater emphasis on businesses being able to stop ransomware campaigns as early in the process as possible, strong user account security posture and Intelligence-led detection are a key countermeasure to this threat.

(Editor's note: We'll be publishing an article dedicated to the evolving Ransomware landscape in early May but in the interim, here's our latest observations).

* (Full transcript available here: CyberUK speech - GOV.UK (www.gov.uk))

An additional stand out moment during the keynote speech was the reference to the NCSC threat alert to Critical National Infrastructure (CNI), as Dowden stated:

> **We have experienced attempted attacks in the past - but these groups operate differently. Instead of seeking to profit or spy on us, their primary motive is to disrupt or destroy our infrastructure. These adversaries are ideologically motivated, rather than financially motivated. Secondly, though these perpetrators are aligned to national actors, crucially, they are often not controlled by those foreign states. That makes them more opportunistic, and less likely to show restraint. Together, those factors make the current situation particularly concerning.****

In response to this threat, the UK government is mandating that all private sector businesses involved in CNI will be subject to cyber resilience regulations. An updated version of the National Cybersecurity Strategy has been packaged into the GovAssure program and will be underpinned by the NCSC Cyber Assessment Framework (CAF).

Some key steps that all business can take:

- **Improve** the security posture of your user accounts to dramatically reduce the likelihood of the pre-ransomware objectives of Account Takeover (ATO) and Business Email Compromise (BEC). See our article on for detailed guidance **Top 10 tips for securing Microsoft 365 – blog.e2e-assure.com**, implementing Threat Detection solutions for surfacing anomalous account activity is a strong recommendation also.

- **Secure** your computing endpoints with an intelligence-led Endpoint Detection & Response solution, when implemented and managed appropriately this will detect and block ransomware payloads delivered via corporate communication channels.

- **Monitor** network traffic for signs of attacker movement and communication, Network Threat Detection & Response solutions are particularly effective as they are invisible to attackers and add a layer of security to Operational Technology / Industrial Control System infrastructure without the need to deploy agent software on legacy equipment.

** (Full transcript available here: CyberUK speech - GOV.UK (www.gov.uk))

March 2023 concluded with the dubious accolade of the highest number of reported ransomware attacks on record at 459, although the real figure is likely to be much higher when factoring in the unreported and deliberately withheld. With the rise of ransomware-as-a-service (RaaS), 'double extortion' techniques and the amalgamation with supply-chain attacks, there is no doubt that this will remain one of the most prevalent threats to digital existence for some time to come.

3CX Supply-chain attack

- **Novel, 'double supply-chain' attack**
- **Threat Actor attributed to North Korea**
- **Suggestion of CNI businesses impacted in North America and Europe**

3CX is the hugely popular VoIP platform, providing telephony services via on-premises and cloud hosted solutions to some of the world's largest organisations, including Coca-Cola, Mercedes-Benz and the UK's NHS. On 30 March, their CEO Nick Galea posted a **statement** on the 3CX forum to acknowledge that malware had been discovered in the Desktop application (software phone) of the product suite.

This appears to be an advanced supply-chain attack involving DLL-sideloading that is being attributed to North Korean threat actor LABYRINTH CHOLLIMA aka UNC4736, believed to be an offshoot group from the notorious LAZARUS group. Windows and MacOS were both affected, with an **updated** version now released containing patches for the affected vulnerability.

Mandiant's high-level summary of this indicates the threat actor deploying the TAXHAUL malware to be loaded by a legitimate process which then communicated back to a known set of C2 servers. This is being tracked under CVE-2023-29059 which has been given a 'High' risk score of 7.8; e2e's advice remains in-line with the vendor, which is to uninstall the affected versions immediately and replace with the patched version.

If you're interested in a deep-dive technical writeup, John Hammond at Huntress provides an excellent one **here**. e2e have been tracking this activity since the outset and have collated an extensive set of IOCs within our intelligence databases which are currently being updated daily and automatically shared with our customers.

This is a fluid and developing situation, highlighted by the vendor's latest **statement**, courtesy of Mandiant revealing the initial access methods used by the attacker as well as the specific strain of malware deployed, named VEILEDSIGNAL, a "backdoor written in C that is able to execute shellcode and terminate itself." It is now determined that initial access

was gained because of a 3CX employee installing a compromised version of the X_Trader software application on to their machine, from where it deployed DLL side-loading techniques to gain persistence across their network including into the build environments, which led to the trojan installation within 3CX's softphone offering.

The novel and concerning aspect of this breach is the double supply-chain compromise - breaching a smaller supplier to gain access to a larger one. Mandiant's CTO Charles Carmakal has been quoted as saying "This is the first time in history that Mandiant's ever observed a software supply chain attack of one company lead to the software supply chain attack of another company and another product."

There has been a **suggestion from Symantec** that the initial supply chain attack on X_Trader has been further reaching than initially estimated, affecting at least two Critical National Infrastructure (CNI) clients in the USA and Europe, without giving further information at this stage.

We envisage that this story will remain in the headlines for the coming weeks and plan to include a conclusive overview in next month's summary.

'FakeGPT'

- **Unauthorised API use leads to account takeover**
- **Suspected objective is funding of terrorist groups**
- **Malicious browser extension based on legitimate open source project**

After the world got to hear about ChatGPT, it was inevitable that criminals would attempt to leverage its popularity, what could be referred to as 'degenerative AI'. Multiple, malicious extensions for Google Chrome have made their way into the browser's app store and although the known variants have been removed, it's safe to assume that we haven't seen the last of this vector.

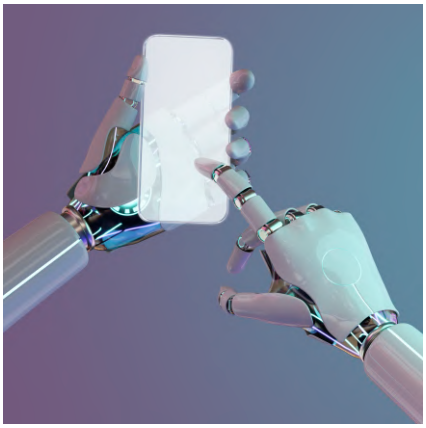
The aim of this malware appears to be financially motivated, hijacking Facebook accounts with a particular focus on Facebook business accounts, likely because of the accounts' reach and available platform marketing credits as well as access to the developer's Graph API, allowing the threat actor to access all your account details and make powerful actions using API calls. Additionally, by abusing Chrome's 'declarativeNetRequest' API call, the malware can circumvent Facebook's protection and fool the platform into believing that this is a legitimate request.

More disturbingly than the financial impact, is the fact that overtaken accounts are seemingly being renamed and used as part of a wide-ranging bot campaign to push ISIS/ Daesh-related content.

The potential to bring about serious, reputational damage to the legitimate account owner cannot be understated.

A series of deep dives into this by Guardio Lab's Nati Tal can be found **here** and **here**. The original (legitimate) open-source project on which the later variant was based is available on **GitHub** for those wishing to make use of it, or more preferably you can make use of OpenAI's **API** calls to build own applications

We would strongly recommend against the installation of unverified browser extensions and are happy to assist with verification, advice and the implementation of bespoke solutions.



Genesis darknet market

- **Worldwide law enforcement collaborate to takedown dark web marketplace**
- **Strong synergy between state and private sector organisations**
- **Dutch Police release compromise checking web tool**

The beginning of April witnessed the end of the notorious darknet marketplace dubbed Genesis, at least that was the aim of a collaborative effort led by the FBI's Operation Cookie Monster. The organisation claims to have seized control of the operation's domains and infrastructure, however the site operators (who appear to have thus far evaded capture) have indicated that the Tor. onion url is still active and that new domains will appear soon, whilst warning of the potential for fake urls cropping up. Genesis has been active since 2017 and is one of the most prolific brokers of stolen and leaked credentials, at one point having over 1.5 million available for sale from as little as $0.70 offering access to all the household-name platforms on the web.

The Dutch Police, who are heavily involved in supporting the FBI, have released an interesting **write-up** after working closely with cybersecurity firms Trellix and Computest to produce a comprehensive set of anti-malware signatures that are now being propagated among AV vendors. They state that merely changing your password is insufficient as malware dropped to infected users will ensure that the criminals are notified of the change and your new password.

They have also released a useful **web-based tool**, that checks to see if your credentials were found on Genesis, emailing you if this is the case. The recommendation is to clean infected machines and then action a credential change. We supplement this advice with that of enabling 2FA on all available accounts; while not a silver bullet, it is an effective measure in preventing unauthorised access to your accounts. e2e are closely monitoring developments around Genesis and will bring you further updates as they emerge.

APT-43

- **North Korean sub-group targeting South Korea and North America**
- **Effective approach to credential harvesting and phishing campaigns**

APT-43, also dubbed 'Thallium' or 'Archipelago' are a prolific threat actor, assessed with high confidence as being closely aligned with the DPRK in North Korea. Targeting government, research establishments and manufacturing services, it is believed that their aims are focused around advancing the nation's nuclear weapons programme, funded through their secondary motivation of financial-based cybercrime operations.

Using advanced social engineering tactics and domain masquerading to support credential harvesting, their geopolitical targets appear to focus predominantly on South Korea and the USA, although their reach has been observed worldwide. Best known for their use of the gh0st RAT malware and LATEOP, a Visual Basic-derived backdoor malware variant which appears to be unique to this threat actor.

APT-43 are a highly-fluid operation, constantly evolving their TTPs to suit a particular engagement. What can you do to guard against their activities?

Educate

Train your users to spot a phishing attempt and encourage them to use functionality such as that built in to O365, to report threats to your security teams.

Patch

Keeping systems up to date removes the opportunity for APT-43 and others to leverage a vulnerability in outdated software.

Detect

Deploy a solution such as e2e's Threat Detection service to spot attacks at the outset and stop them, dead.

At e2e, we track these operations and their dynamics to allow us to spot emerging threats and act upon them before they gain a foothold in our clients' networks. Utilising the open-source MISP **platform** allows us to correlate TTPs, network activity, malware samples and other forms of intelligence from multiple sources to build an in-depth picture of threat actor activity and to share this with our partners and the wider infosec community.

Let’s connect!

Thanks for taking the time to read our briefing, we’re happy to provide further information on any of the topics we’ve covered here.

We love having conversations about and helping people with Cyber Threat Intelligence, drop us an email - **cti@e2e-assure.com**