

Cyber Threat Intelligence Summary

April 2024



Contents

1	xz-utils	03
2	LabHost takedown	04
3	Kapeka - the latest threat from Sandworm	05
4	IN BRIEF	06
5	DEEP DIVE – APT41	07
6	Summary	08

Welcome to our Anniversary edition of the e2e-assure CTI Briefing! It's been a whole year of bringing you the freshest, breaking news from the cyber threat intelligence realm, deep-dive reports on threat activity groups and the reassuring steps the e2e-assure team are taking to keep you safe.

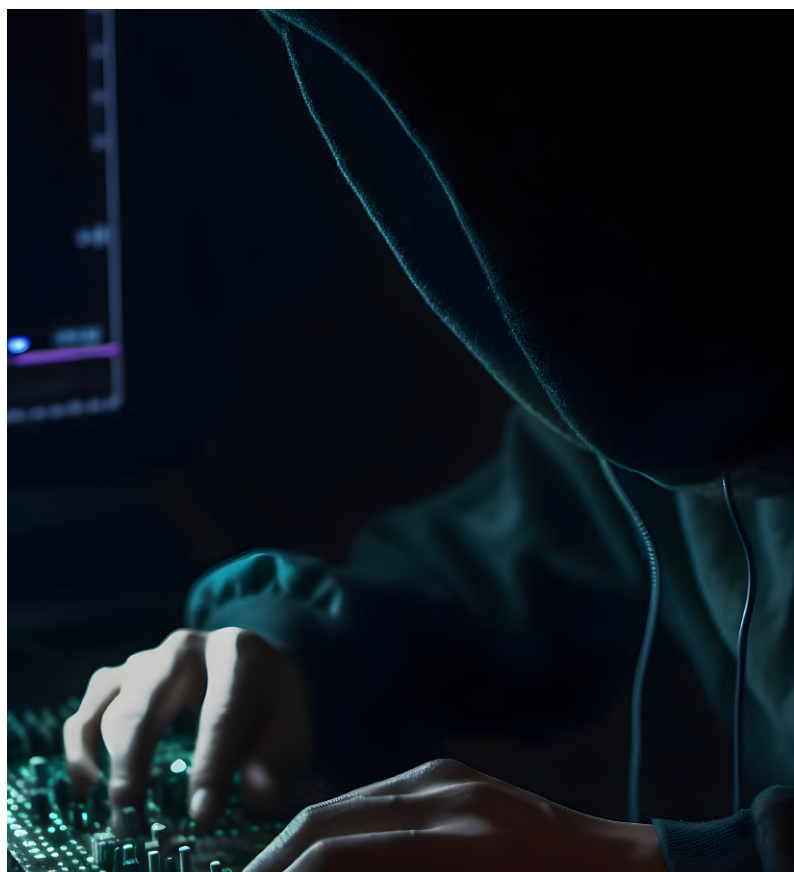
This month doesn't waver from that tempo and we've got an edition filled with software vulnerabilities, law enforcement takedowns as well as the regular round-up of news articles and a deep-dive into APT41, the notorious and highly advanced threat activity group known to be aligned with Chinese interests.

xz-utils

As March drew to a close, software developer and Microsoft employee Andres Freund identified a critical vulnerability in xz-utils, specifically in versions 5.6.0 and 5.6.1, thereafter referred to as CVE-2024-3094. This vulnerability poses a significant threat due to its potential to enable remote code execution (RCE) through an SSH authentication bypass and is purported to have been introduced by another project maintainer, Jia Tan, in February of this year.

XZ Utils, widely used for data compression across Linux and macOS systems, contains a backdoor in the mentioned versions that could allow unauthorised remote access. This vulnerability was introduced by one of the maintainers of XZ Utils, who injected malicious code during the build process of the library. The compromised versions have a mechanism designed to bypass SSH authentication, providing the attacker with remote access to affected systems.

The vulnerability involves sophisticated manipulation during the build process where specific macros and scripts embed the malicious code within the software without it being visible in the public Git repositories. This code is only active under certain conditions and is designed to interfere with the SSHD process, which can lead to elevated CPU usage during



login attempts and facilitate unauthorised access under the guise of normal user authentication.

The exploit targets several major Linux distributions that incorporate XZ Utils, such as Fedora, Debian & Ubuntu, Arch Linux, and openSUSE among others. Although it primarily affects systems with public SSH access, the scope of the vulnerability is extensive due to the widespread use of the affected software versions.



To mitigate this threat, affected organisations and users are advised to revert to versions of XZ Utils that precede the compromised 5.6.0 and 5.6.1 releases. Additional recommendations include conducting vulnerability scans to identify exploitable systems, applying the principle of least privilege to system operations, and ensuring that all software updates and patches are applied promptly. The following Kusto query can be used as a template to customise in your own environment, to detect vulnerable versions of the software:

```
let VulnerableVersions = dynamic(['5.6.0',  
'5.6.1']);  
Heartbeat  
| where AppName == 'XZ-UTILS'  
| where Version in (VulnerableVersions)  
| project ComputerName, Version,  
TimeGenerated
```

This backdoor serves as a critical reminder of the risks associated with supply chain attacks, where even trusted software updates can be a vector for cyber security threats. The response to this issue involves not only technical remediation but also an analysis of security processes and the establishment of more stringent controls over software build and distribution environments.

LabHost takedown

The takedown of LabHost, a significant Phishing-as-a-Service (PhaaS) provider, was a coordinated effort led by the UK's Metropolitan Police Service, involving international law enforcement and private sector partners. This major operation occurred on April 18, 2024, and was pivotal in disrupting the phishing activities orchestrated by LabHost.



LabHost, launched in late 2021, became notorious for facilitating phishing attacks on a large scale. The service allowed cybercriminals to access over 40,000 phishing domains, targeting financial institutions and other services primarily in North America but also globally. For a monthly subscription fee, users of LabHost could easily deploy sophisticated phishing schemes using tools provided by the service. One of the key tools offered was "LabRat," an advanced feature for capturing two-factor authentication (2FA) codes, enabling attackers to bypass security measures of targeted systems. The Met have so far identified almost 70,000 UK victims with over 2,000 criminals identified in the course of their activity. So far, 37 arrests have been made.

The operation to dismantle LabHost began approximately a year before the takedown and involved meticulous planning and coordination

across 19 countries. This international collaboration included law enforcement agencies and private sector entities such as Microsoft, Trend Micro, Chainalysis, Intel 471, and The Shadowserver Foundation. The crackdown led to the arrest of 37 individuals, including the original developer of LabHost, and the seizure of numerous servers and domains related to the service.

Following the takedown, authorities communicated with around eight hundred LabHost users, informing them that their activities had been monitored and documented, which included the amounts paid to LabHost, the sites accessed, and data received. This post-operation phase also involved ongoing investigations targeting individuals connected with the service, emphasizing the broad and continuing impact of the operation on global cyber-crime networks.

This successful takedown marks a significant achievement in the fight against cyber-crime, highlighting the effectiveness of collaborative efforts between law enforcement and the cyber security industry in tackling complex cyber threats.

Kapeka - the latest threat from Sandworm

We've written extensively in the past about the notorious Sandworm hacking group and only last month highlighted their latest moniker of APT44 care of the CrowdStrike teams. The latest output from the group appears to be a strain of malware currently known as 'Kapeka'.

Kapeka is a sophisticated malware identified as a flexible backdoor primarily targeting Eastern Europe, particularly noticed in attacks since mid-2022. It is believed to be developed and deployed by the Russian hacker group known as Sandworm, which is a part of Russia's GRU. Sandworm has been implicated in numerous cyber-espionage activities and disruptive attacks across Ukraine and other regions, making it a prominent figure in state-sponsored cyber operations.



Kapeka is designed as a Windows DLL, capable of collecting extensive information from infected systems. It operates by deploying a dropper that sets up a backdoor on the victim's machine. This backdoor is adept at evading detection by self-deleting after executing its payload and establishing persistence mechanisms like scheduled tasks or registry modifications, depending on the system's privileges. The backdoor component is notably complex, utilizing AES-256 encryption to secure its communications and employing techniques to blend in with legitimate system processes for stealth.



The malware's primary functionalities include the ability to execute commands remotely via its command-and-control (C2) server, collect sensitive data, and potentially deliver further malicious payloads. Kapeka's deployment coincides with Russia's ongoing conflict with Ukraine and is viewed as part of the broader toolkit used by Sandworm to advance Russian cyber warfare objectives.

Kapeka's primary victims have been organisations in Ukraine and other parts of Eastern Europe. The malware has been used in attacks that could potentially lead to sabotage or destructive operations, as evidenced by its link to the Prestige ransomware attacks. Victims include sectors that are crucial to national infrastructure, such as energy, telecommunications, and transportation, which underscores the serious threat posed by this malware to critical systems.

The implications of Kapeka's deployment are significant, given the strategic interests of its operators. Its presence in the wild highlights a pattern of sophisticated, state-sponsored cyber operations aimed at achieving long-term intelligence gathering and potentially disruptive objectives. This stresses the need for robust cybersecurity measures, particularly for organisations within the geopolitical sphere of interest to Russian state actors.

Detection and defence against Kapeka involve a combination of signature-based detection (using YARA rules), behavioural analysis, and anomaly detection to identify its stealth tactics and C2 traffic patterns.

Overall, Kapeka represents a significant threat due to its sophistication, the stealthiness of its operations, and its backing by a state-sponsored entity known for aggressive cyber operations against foreign targets.

IN BRIEF

['Sandworm' gets a Mandiant makeover as APT44](#)

[OSSF says xz-utils incident may be tip of the iceberg](#)

[China-owned Nexperia Semiconductors hit by ransomware attack](#)

[Cisco warns of data exfil after Duo breach](#)

[Novel 'UNAPIMON' malware linked to APT41-affiliated intrusions](#)

['GhostR' claims to have breached London Stock Exchange](#)

[Microsoft observes APT28 leveraging 2022 Print Spooler vulnerability](#)

['TunnelVision' – a novel VPN 'de-cloaking' technique](#)



DEEP DIVE – APT41

APT41 (Mandiant), also known as Double Dragon (FireEye/Trellix), Brass Typhoon (Microsoft) and several other names, is a prolific cyber threat group that has been associated with the Chinese government. Known for a wide range of cyber activities that include espionage, intellectual property theft, and financial gain operations, the group have been in operation since at least 2012. They are believed to consist of Chinese nationals and are purportedly sponsored or tolerated by the Chinese state, evidenced in part by the group's patterns of activity that align with Chinese working hours and non-working days, and its operational goals that consistently align with China's national interests.

Motivated by both state-sponsored espionage objectives and financial gains, the group has been involved in espionage activities that align with the strategic objectives of the Chinese government, particularly in areas like healthcare, high-technology including the semiconductor industry and telecommunications. These activities typically support China's long-term goal of advancing its domestic and technological capabilities. For financial gain, APT41 has targeted the video game industry where they have manipulated virtual (crypto) currencies and conducted ransomware attacks, including those deploying the novel tactic of leveraging Windows group policy objects (GPOs) to schedule the installation of malware.



APT41 is known for its sophisticated techniques, which include the use of malware that is difficult to detect, professional-looking spear-phishing emails to infiltrate target networks and supply chain compromises. They utilise backdoors and 'bootkits' which by nature are hard to identify and have been able to inject malicious code into legitimate files to spread their malware. They have also been known to re-deploy legitimate, but stolen digital certificates in order to falsify a smokescreen of legitimacy along with malware families such as the "DeadEye" launcher and 'LOWKEY'.



APT41 has targeted a wide range of organisations globally, including organisations in over a dozen countries like France, India, Japan, and the United States. They have compromised companies in diverse industries such as telecommunications, healthcare, and high technology. In one noted instance, they were able to compromise the infrastructure of TeamViewer, the popular RMM tool, which indicates their advanced level of operational capability.

The activities of APT41 have drawn significant international attention. In 2019 and again in 2020, the U.S. Department of Justice charged five members of APT41 for attacks that affected over 100 entities worldwide, including

governments and multinational corporations. This was part of broader tensions between the U.S. and China over cyber security and espionage.

The actions of APT41, as a state-linked entity, are indicative of the broader strategy of Chinese state-sponsored cyber operations. These activities are part of a complex web of geopolitical interactions in the domain of cyber warfare and espionage.



Let's connect!

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

We welcome any feedback you have at cti@e2e-assure.com