

# Cyber Threat Intelligence Summary

---

March 2024



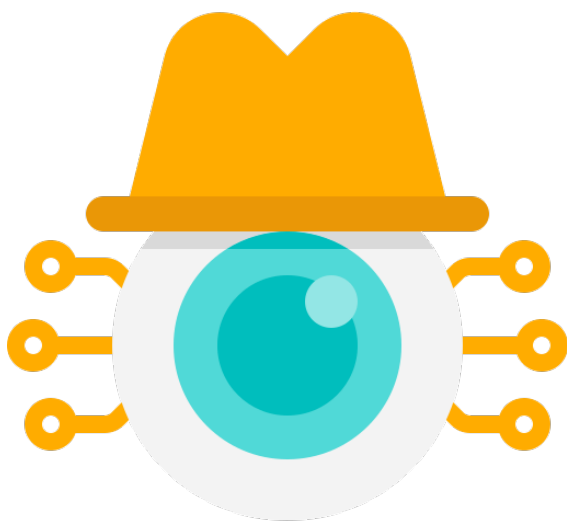
# Contents

<b>1</b>	<b>Kimsuky &amp; DEEP#GOSU</b>	<b>03</b>
<b>2</b>	<b>MISP – The open-source platform at the heart of Cyber Threat Intelligence</b>	<b>05</b>
<b>3</b>	<b>Microsoft breach (Jan '24) – Update</b>	<b>06</b>
<b>4</b>	<b>IN BRIEF</b>	<b>07</b>
<b>5</b>	<b>DEEP DIVE – APT31</b>	<b>08</b>
<b>6</b>	<b>Summary</b>	<b>11</b>

# | Kimsuky & DEEP#GOSU

Over the last few weeks, we've been observing renewed activity from the North Korea-attributed threat activity group 'Kim Suky' aka APT43 (Mandiant), Velvet Chollima (CrowdStrike) and Emerald Sleet (Microsoft) as have the threat research team over at Securonix, who have uncovered a campaign of espionage and theft targeting South Korean entities. Dubbed 'DEEP#GOSU', the campaign incorporates an attack chain that leverages cloud services including Dropbox for downloading staged malware and Google Docs for C2, advanced living-off-the-land techniques and AV evasion techniques.

Kimsuky, officially known as the Kim Suky Group, is a North Korean state-sponsored threat activity group recognised for its cyber espionage operations. This group has been active since at least 2012 and primarily targets South Korean government entities, although its operations have expanded globally, focusing on security, foreign policy, and economic interests that could be beneficial to the North Korean government.



Common Cyber Attack Techniques used by Kimsuky

- Spear-phishing campaigns
- Water-holing attacks
- Malware distribution to infiltrate the networks of its targets

The group is known for its focus on gathering intelligence related to foreign policy and national security issues, as well as stealing sensitive information from various industries such as:



**Military**



**Political organisations**



**Research institutions**

One of the distinguishing features of Kimsuky's operations is its methodical approach to reconnaissance and the use of custom-developed malware and tools. The group has been observed using tailored phishing emails that leverage social engineering techniques to trick victims into disclosing their personal information or downloading malicious attachments. Once they have gained access to a system, Kimsuky's operatives deploy further malware to maintain persistence, collect data, and exfiltrate the gathered intelligence back to their C2 servers.

In addition to direct cyber attacks, Kimsuky is also adept at conducting cyber surveillance and information warfare. The group has been implicated in attempts to manipulate public opinion and spread disinformation, particularly in contexts that could affect North Korea's geopolitical standing.

Over the years, international cyber security communities and government organisations have exposed various campaigns attributed to Kimsuky, leading to increased efforts to thwart their activities. Despite these efforts, Kimsuky remains a persistent threat due to its evolving

In one of the stages, a compressed Base64 string downloaded from Dropbox is decompressed to reveal a binary file that turns out to be an open-source Remote Access Trojan (RAT) known as TruRat/TutRat or C# R.A.T. This has capabilities like keylogging, remote desktop access and device control underscoring the campaign's intent to gain comprehensive control over infected hosts. Despite the RAT's relatively old age and the likelihood of detection by anti-virus programs, its innovative loading and execution method directly into memory helps bypass some levels of detection.



tactics and the strategic importance of the intelligence targets it pursues. The group's activities underscore the broader challenges of state-sponsored cyber espionage and the ongoing tensions on the Korean Peninsula.

The DEEP#GOSU attack unfolds in several stages, beginning with the execution of a malicious PowerShell script contained within a shortcut file. This script is designed to silently execute a specifically crafted malicious .lnk file, authenticate, decrypt, and execute further malicious code downloaded from Dropbox, and clean up traces of its execution. One of the noteworthy aspects of this campaign is its fileless execution technique, which involves running malware directly in memory to evade traditional anti-virus detection methods.

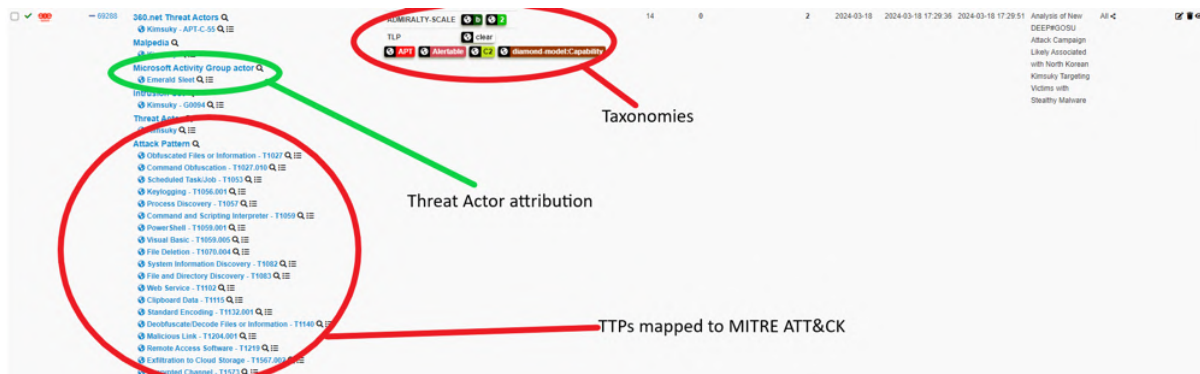
The campaign also utilizes VBScript to execute additional malicious activities, including more downloads from Dropbox. This stage involves dynamically writing and executing PowerShell files on the disk, showcasing the campaign's complex and layered approach to maintain persistence and control over compromised systems.

We've tracked APT43 since day one and have amassed a wealth of data around their operations, TTPs and capability sets, enriched with datasets such as DEEP#GOSU. Get in touch with us to find out how you can gain access to this intelligence.

# MISP – The open-source platform at the heart of Cyber Threat Intelligence

Stepping away from the news, we take up some column inches to celebrate a project that sits at the heart of the CTI programme at e2e-assure and many other organisations around the world.

So, what is MISP and why has it become so pivotal in the field of CTI? In its simplest form, MISP is a web-frontend for a SQL database that stores cyber-security 'Events', comprising Attributes which are the individual datapoints used to identify adversary capabilities and



The [MISP Project](#) is an open-source Threat Intelligence Platform (TIP) solution that started life in 2011 as a personal project of then-Belgian MOD employee Christophe Vandeplass who was frustrated at the disparate and sometimes chaotic methodologies available for the processing and sharing of Indicators of Compromise (IOCs) available at the time. And so CyDefSIG as it was referred to at the time was born, receiving a positive response from Christophe's employers and subsequently NATO, who became involved with the project a year later. Within the next year, NATO had hired the amazingly talented Andras Iklody and MISP had its first, full-time developer; the project continued to grow exponentially and Andras now heads up a team of volunteers who maintain what has become one of the Internet's most popular, community-led projects. (You can read more information about the history on the project's ['Who'](#) page).

infrastructure. Throw into that mix advanced correlations, mapping, geolocation and visualisations, automations and the ability to map activity against multiple frameworks including [Mitre ATT&CK](#), make it open-source and fully extensible and you have a (Malware) Information Sharing Platform that is capable of tracking adversarial campaigns and the structured collation of all threat intelligence.

MISP's open-source nature encourages a community-driven approach to security. It allows us to customise and extend its capabilities to fit our specific use-cases, fostering innovation and continuous improvement in threat detection methodologies. The platform's robust API facilitates integration with existing security tools and systems, enabling a seamless flow of information and automating the dissemination of threat intelligence across our internal and customer platforms.

MISP excels in its ability to classify and qualify data, ensuring that we can prioritise threats based on their relevance and severity. This targeted approach enables more efficient allocation of resources and enhances the overall effectiveness of the e2e-assure SOC. Having grown from a singular instance deployed as an enrichment tool to our SIEM, Cumulo,

e2e-assure now manage multiple instances across on-premise and cloud environments with integrations to Azure Sentinel and also offer a fully-managed 'MISP-As-A-Service' to customers wishing to integrate with their own intelligence programmes.

## Microsoft breach (Jan '24) – Update

Since we reported on the Microsoft breach in January's edition of this briefing, information from the vendor has been scant while opinion in the industry weighs heavily on the potential fallout in the weeks, months and possibly years to come. It has been widely acknowledged and confirmed in [this statement](#) from Microsoft, that the threat activity group they refer to as 'Midnight Blizzard' (APT29/Nobelium/Cozy Bear) were behind the attack. The group are an active service unit of the Russian SVR, the foreign intelligence service that succeeded the Soviet-era KGB and one of the most capable and dangerous threat activity groups in the world today, responsible for the devastating SolarWinds attack in 2020, the famed DNC hacks and repeated attacks on multiple, Western governments.

The fact that initial access was ultimately due to an insecure 'legacy test' account, internet-facing with no 2FA in place has meant that sympathy has been somewhat limited and how the adversary managed to traverse the Microsoft ecosystem from what should have been an isolated dev environment into the corporate email system, remains unclear. The fact that as of the most recent reports, Microsoft have been unable to confirm that they've eradicated the actor's presence from their networks is somewhat embarrassing,



although an amount of leeway may be given when considering the adversary. But the fact that the threat actor has apparently gained access to production source code for yet to be identified Microsoft products is a game changer and one that puts every Microsoft customer at risk.

Tom Kellermann of Contrast Security was quoted in The Independent as saying "This has tremendous national security implications, the Russians can now leverage supply chain attacks against Microsoft's customers." This has the potential to be a whole level worse than the development of a single or even multiple zero-day exploits, with access to the source code an attacker can craft 'native' exploits that integrate seamlessly with the legitimate operating system

and are virtually undetectable. Having the source code for Microsoft's PKI tooling could have similarly devastating affects.

There's been no official statement from Microsoft since the beginning of the month, this is definitely one that we'll see play out over the course of 2024 and we have no doubt that we'll be re-visiting it again!



## IN BRIEF

[NIST releases v2.0 of its Cybersecurity Framework](#)

[French Government under intense & sustained DDoS Attacks](#)

[Apple heads off in-the-wild Zero-Day exploits with emergency patches](#)

[Ivanti releases patch for ANOTHER Critical RCE vulnerability](#)

[Scottish NHS Trust dealing with attack and exfiltration of PII](#)

[Chinese PC manufacturer ships units infected with Redline malware](#)

[International Monetary Fund investigates 'Cyber-Security Incident'](#)

[Tor Project introduces new tooling to combat censorship](#)



## DEEP DIVE – APT31

APT31 have featured heavily in the IT and mainstream presses recently, culminating in an [announcement](#) on 25 March by the UK Foreign Office that sanctions were being enforced against two Chinese nationals and one organisation for their involvement in malicious cyber activity aimed at interfering with UK democratic process. Foreign Secretary Lord Cameron is quoted in the announcement, saying:

**“It is completely unacceptable that China state-affiliated organisations and individuals have targeted our democratic institutions and political processes. While these attempts to interfere with UK democracy have not been successful, we will remain vigilant and resilient to the threats we face.**

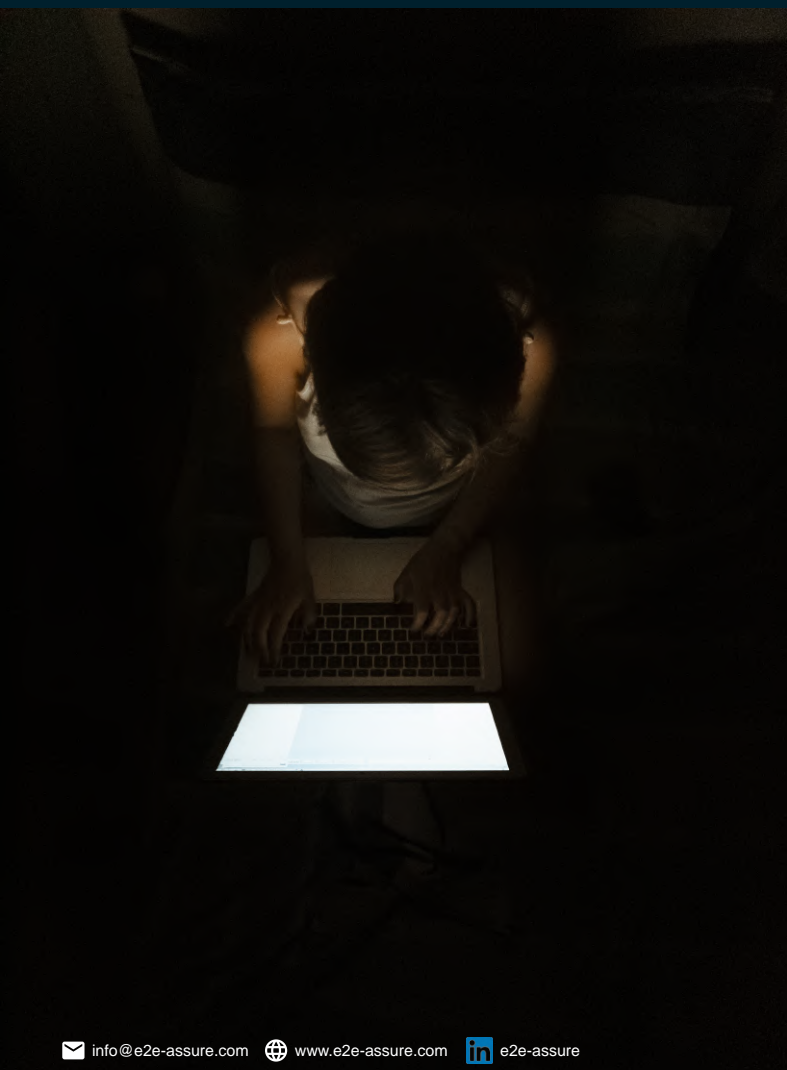
**We will always defend ourselves from those who seek to threaten the freedoms that underpin our values and democracy. One of the reasons that it is important to make this statement is that other countries should see the detail of threats that our systems and democracies face.”**

held responsible for a breach of the UK Electoral Commission between 2021 and 2022 and a secondary campaign targeting individual UK Parliamentarians that began in 2021. Simultaneously, the threat actors were working alongside their MSS counterparts dubbed Silk Typhoon but better known as ‘Hafnium’ of Exchange Server 0-Day fame; clearly a capable and active adversary that specialises in the hardest of targets and focusing primarily on state espionage, but not averse to attacking any target from which the bounty will further China’s objectives.

APT31 demonstrates a high skill level in cyber operations, employing a range of custom and complex malware tools, as well as living-off-the-land techniques to maintain stealth and persistence within compromised networks. They are known for their ability to exploit zero-day vulnerabilities, indicating a high level of technical sophistication and resource investment. One of their notable malware tools is "JUDGE," a backdoor Trojan that allows for remote control of the infected system, data exfiltration, and the deployment of additional payloads. They also use "Scanbox," a reconnaissance framework capable of profiling and collecting information from targeted systems. These tools, among others in APT31's arsenal, are meticulously designed to avoid detection and analysis, often employing encryption, obfuscation, and mimicry of legitimate network traffic and have previously been seen to exploit vulnerabilities in Java and historically, Adobe Flash.



That operational capability is further highlighted by their strategic use of spear-phishing and social engineering tactics to gain initial access to target networks. They meticulously craft phishing emails and social media messages that appear legitimate, often masquerading as trusted entities to deceive victims into compromising their own systems. This initial foothold is then exploited to establish persistent access, escalate privileges, and move laterally within networks to achieve their objectives. Their ability to adapt and tailor their approaches based on the target's profile and defences showcases their adaptability and tactical acumen.



The group's motivation primarily revolves around espionage and the collection of intelligence that could provide a strategic advantage to China. This includes the theft of intellectual property, monitoring of political dissidents, and gaining insights into policies and decisions of other governments. However, APT31 has also been implicated in operations that suggest an interest in influencing the electoral processes of other countries. These allegations involve cyber-attacks aimed at political organisations, think tanks (and individuals involved in the electoral process) aiming to gather intelligence, potentially manipulate public opinion, or sow discord. Such operations indicate APT31's role in China's broader strategy of using cyber capabilities to achieve geopolitical objectives.



In summary, APT31 is a testament to the evolving landscape of state-sponsored cyber espionage, showcasing high levels of sophistication, strategic focus, and adaptability. Their campaigns reflect the merging of cyber operations with state objectives, underscoring the importance of robust cybersecurity measures and international cooperation in countering such threats. The ongoing evolution of APT31's tactics and the breadth of their targeting underscore the persistent and adaptive nature of state-sponsored cyber threats, requiring continuous vigilance and advanced defensive strategies from the global community.





## Let's connect!

That wraps up the March 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](mailto:cti@e2e-assure.com)