Joint Publication
Structured Cooperation between CERT-EU and ENISA
TLP:CLEAR | 15/02/2023 | JP-23-01 | v1.0

JP-23-01 - Sustained activity by specific threat actors

Summary

The EU Cybersecurity Agency (ENISA) and the CERT for the EU institutions, bodies and agencies (CERT-EU) would like to draw the attention of their respective audiences on particular Advanced Persistent Threats (APTs), known as APT27, APT30, APT31, Ke3chang, GALLIUM and Mustang Panda. These threat actors have been recently conducting malicious cyber activities against business and governments in the Union.

On 19 July 2021, the EU has urged Chinese authorities to take actions against malicious cyber activities undertaken from their territory, and linked to APT31 [1]. These malicious cyber activities, which had significant effects, targeted government institutions and political organisations in the EU and Member States, as well as key European industries.

On 18 July 2022, Belgium has also urged Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors. These activities can be linked to the hacker groups known as APT 27, APT 30, APT 31, and GALLIUM [2]. Moreover, commercial firms indicated that Ke3chang and Mustang Panda are likely operating from the territory of China [3][4][5].

These threat actors present important and ongoing threats to the European Union. Recent operations pursued by these actors focused mainly on information theft, primarily via establishing persistent footholds within the network infrastructure of organisations of strategic relevance.

ENISA and CERT-EU call for all public and private sector organisations in the EU to apply the recommendations included in this document in a consistent and systematic manner. These recommendations aim to reduce the risk of being compromised by the mentioned APTs, as well as substantially improve the cybersecurity posture and enhance the overall resilience of these organisations against cyberattacks.

Recommendations

All public and private sector organisations in the EU are strongly advised to follow common cyber hygiene recommendations. Our previously published best practices [24] and the corresponding security guidance [35] provide a solid basis for mitigating cyberattacks.

Following the analysis of the available information on the aforementioned threat actors (see below) and of some of their major tactics, techniques, and procedures, ENISA and CERT-EU draw a number of complementary recommendations to foster the defensive capabilities of the intended audience. Each organisation which wants to apply these recommendations is fully responsible for the implementation, according to its business needs and priorities.

For best practices issued by the relevant CSIRTs of the EU Member States, please refer to their websites [31].

Additionally, CERT-EU and ENISA emphasise the importance of participating in information sharing communities and reviewing your national/governmental CSIRT's security guidance [25] and public resources detailing tactics, techniques and procedures associated with the threat actors [26].

Prevention

To reduce your cyber risks through good cyber hygiene:

- Follow the security best practices proposed by vendors to harden their products and manage high-privileged accounts and key assets.
- Strive to maintain current asset inventories. The inventories shall include both, physical (i.e. on-prem servers, endpoints, etc.) and virtual assets (i.e. instances in the Cloud, virtual machines, etc.) and installed software. This allows the timely identification of systems impacted by vulnerabilities. A patch prioritisation strategy defined in a policy should particularly cover critical assets like hardware and software directly exposed to the Internet.
- Block or severely limit egress Internet access for servers or other devices that are seldom rebooted. As they are coveted by threat actors for establishing backdoors, these systems are often used to create persistent beacons to Command and Control (C2) infrastructure.
- Follow best practices for identity and access management. A robust password policy shall be enforced for all accounts and multi-factor authentication must be used where applicable. Tightly manage and monitor the lifecycle of all accounts. Promote the use of password managers throughout the organisation.
- Adopt a backup strategy and use the 3-2-1 rule approach which states that organisations should keep three complete copies of their data, two of which are locally stored on different types of media, and at least one copy is stored off-site [34].
- Ensure tight and proper access controls for end users and, most crucially, external third-party contractors with access to internal networks and systems (i.e. managed service and cloud service provider access). Consider requesting proofs for the security claims made by providers of these services.
- Segment the network to isolate critical systems, functions, or resources – specifically implement isolation in regards of interconnections with Internet and third parties.
- Secure your cloud environments before moving critical assets there. Use the strong security controls that are available on cloud platforms and properly segment cloud system management from on-premise system management to ensure that threat actors cannot easily jump from one environment to the other.

- Implement a resilient email policy that includes adequate mechanisms for filtering and scrutinising malicious content. A secure email gateway can further enhance the protection of the recipients.
- Consider preventing attacks based on the so-called Pass-the-Ticket technique on Active Directory environments [27].
- Invest in cybersecurity education. This includes encouraging your cybersecurity professionals to enrol in specialised professional training courses in their domain and performing concise awareness campaigns for end users.

Detection

Detection refers to actions that will help expose malicious cyber activities in your network:

- Implement robust log collection and regularly review alerts triggered by security components. You may refer to ENISA's guidance on proactive detection (pp. 12 - 18) which comprehensively covers sources of telemetry [36]. It is specifically advisable to collect event logs linked to unauthenticated creation, modification, use, and permission changes associated with privileged accounts, and to review network connections from IP ranges associated with non-corporate VPN Tor, and similar services.
- Monitor the activities of devices in your network with appropriate tools like Endpoint Detection and Response (EDR) and User and Entity Behaviour Analytics (UEBA), since a substantial part of network traffic is encrypted nowadays. This applies to both servers and endpoints. It is crucial to ensure that your EDR is set to alert mode if monitoring or reporting is disabled, or if communication is lost with a host agent for more than a reasonable amount of time.
- Use carefully curated cyber threat intelligence to proactively search your logs for possible signs of compromise.
- Detect traces of compromise in your network through well-conceived, regular threat hunting based, for example, on the MITRE ATT&CK® framework [26].
- Use intrusion detection signatures and NetFlow to spot suspicious traffic at network boundaries and detect conditions that may indicate software exploitation or data exfiltration.
- Prevent and detection PowerShell based attacks [28], in order to stop attackers from gaining full control of a Windows-based infrastructure or business-related operator accounts.
- Invest in detecting lateral movements which exploit NTLM and Kerberos protocols in a Windows environment [29].
- Train your users to immediately report any suspicious activity to your local cybersecurity team.

Response

Incident response is composed of several phases: Preparation, Identification, Containment, Clean-up, Recovery, and Lessons learned. To successfully respond to an incident, ENISA and CERT-EU strongly advise to:

- Create and maintain an incident response plan. Ensure you have documented the procedures to reach out and swiftly communicate with your national or governmental CSIRT [31], and to provide access to forensics evidence when asked by relevant parties. The security white paper "Data Acquisition Guidelines for Investigation Purposes" contains related technical guidelines [30]. At the minimum, you should have an up-to-date list of key contacts for your strategic suppliers and service providers. Prepare and verify these procedures are tested and known to all the local incident handlers.

- Be able to assess the incident severity, for example based on its scale and impact. Handling of more advanced attacks may require engaging external security service providers who may offer professional advice and personnel. A suitable service provider should have solid experience in APT handling, and expertise in memory, storage and network forensics, as well as log data collection and analysis. Operating system experts – and Active Directory log analysis experts in particular – can be of great help too.
- Avoid common mistakes in incident handling such as:
  - ignoring a security event without assessing what triggered it and the potential impact;
  - pre-emptively blocking or probing infrastructure used by threat actors (pinging, making DNS queries, browsing, etc.);
  - mitigating the affected systems before responders can collect and/or recover evidence;
  - ignoring telemetry sources, such as network, system and access logs;
  - fixing the symptoms, ignoring the root causes and doing partial containment and recovery;
  - forgoing keeping a detailed record of actions taken and the event timeline.
- Incident response requires communication among several internal stakeholders and it is strongly recommended to have clear, concise communication guidelines prepared and tested in advance.

If personal data is in the scope of the incident, seek the advice of your Data Protection Officer and/or your legal team.

Threat actor overview

APT27

Name	Likely motive	Examples of associated tools
APT27 (aka Lucky Mouse, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union)	Information theft; ransomware operation	Ghost, ASPXSpy, ZxShell RAT, HyperBro, PlugX RAT, Windows Credential Editor, FoundCore, China Chopper, gsecdump, HTTPBrowser, Impacket, ipconfig, Mimikatz, NBTscan, Net, OwaAuth, pwdump, ZxShell.
Threat actor description		

APT27 has been observed targeting a broad range of organisations across a wide geographic area, including Europe, North and South America, Africa, the Middle East, and the Asia Pacific (APAC) region. The group has been primarily observed conducting watering hole and spear-phishing attacks as its key means of gaining initial footholds within target networks [7]. Since 2020, APT27 operators have also been observed engaging in ransomware-based cybercriminal activities, suggesting members of the group may be conducting financially motivated activity, in addition to standard exfiltration-driven activities [8]. APT27 is also known for its high degree of operational sophistication and frequently alters its attack strategies. In order to obfuscate its their activities, evade detection and maintain long-term network persistence, APT27 deploys fileless malware and pivots within the target networks. Incidents linked to APT27 have also been recorded alongside clusters of activity from other threat groups, assessed to be operating from the same nation state such as APT30, APT31, and GALLIUM.

Recent operations

In January 2022, Germany's domestic intelligence services – the Bundesamt für Verfassungsschutz (BfV) – published information regarding an ongoing data gathering campaign affecting German companies which the agency attributed to APT27 [9].

While the BfV declined to indicate the names or sectors of the commercial entities targeted, their report notes the attacks are representative of an increase in the use of HyperBro malware by Chinese threat groups against German targets [10].

In July 2022, Belgium's Minister of Foreign Affairs released a statement regarding the Belgian government's detection of an espionage campaign against the country's Interior and Defence Ministries. The Foreign Ministry linked the campaign to APT27 alongside three other groups with assessed ties to China: APT30, APT31, and GALLIUM [2].

In October 2022, the France-based private incident response provider Intrinsec published a report detailing a security incident faced by an unnamed customer in spring 2022, which the company attributed to APT27. Intrinsec indicated APT27's operation was conducted over the course of at least a year and involved the exploitation of the target's MS Exchange server via the ProxyLogon vulnerabilities chain. After gaining initial access, the group proceeded to compromise five domains over nine months, before ultimately deploying HyperBro malware to exfiltrate many gigabytes of data over a 17-day period [11].

APT31

Name	Likely motive	Examples of Examples of associated tools
APT31 (aka Judgment Panda, Zirconium, Bronze Vinewood)	Information theft	Cobalt Strike, DopboxAES Rat, SalsaTrade, PakDoor
Threat actor description		
APT31 operations date back to at least 2010. The group became more difficult to track in recent years. APT31 has been working on new methods to avoid detection, including the creation of its own anonymising proxy, which is hosted on a global network of hacked routers. Since the French national cybersecurity agency (ANSSI) report of July 2021 [12] detailing the use of this anonymisation proxy network, a general decline in these operations has been noted.		
Recent operations		
In 2020, the Norwegian police security service (PST) concluded a two years and a half investigation of a 2018 cyberattack against the Norwegian state administration and the cloud service provider Visma AG. According to public news, the threat actor behind the attacks was APT31 [13]. The Parliament of Finland had fallen victim to a breach in December 2020. In March 2021, the Finnish national authorities disclosed that their investigations pointed to APT31 [14]. In July 2021, the French national cybersecurity agency (ANSSI) warned of an ongoing campaign by the APT31 threat actor against a large number of French organisations [15].		

GALLIUM

Name	Likely motive	Examples of Examples of associated tools
GALLIUM (Softcell)	Information theft	PlugX, ChinaChopper, Poison Ivy, HTRAN, Mimikatz, NBTscan, Netcat, PsExec, BlackMould, WinRAR, Windows Credential Editor (WCE), PingPull
Threat actor description		
GALLIUM has been active since at least 2012, primarily targeting telecommunications companies, financial institutions, and government entities in several regions of the world. GALLIUM has developed the capability to target not only Windows, but also Linux (32/64-bit) systems through Remote Access Tools (RATs).		
Recent operations		
In July 2022, Belgium's Minister of Foreign Affairs released a statement regarding the Belgian government's detection of an espionage campaign against the country's Interior and Defence Ministries. The Foreign Ministry linked APT27 alongside three other groups with assessed ties to China: APT30, APT31, and GALLIUM [2]. GALLIUM has been identified on 13 June 2022 by the security company Palo Alto Networks' Unit42. The group has been expanding its operations, beyond its original telecommunications sector, to government and finance. Its targeting, according to the analysis, includes, at least, entities from one European country [16].		

Ke3chang (APT15)

Name	Likely motive	Examples of associated tools
Ke3chang (aka Vixen Panda, Nickel, APT15)	Information theft	Okrum, Ketrikan, Neoichor, RoyalDNS, RoyalCli, Mimikatz, RemoteExec (similar to PsExec)
Threat actor description		
Ke3chang conducts cyber operations with the purpose of stealing data. The group has been active since at least 2010. Ke3chang has targeted several sectors, including energy, government, and the military. Until 2021, Ke3chang's favoured method for initial access was spear-phishing, using compromised or spoofed email addresses. More recently, Ke3chang has been observed exploiting vulnerabilities in public-facing software.		
Recent operations		
In December 2021, Microsoft reported on Ke3chang conducting a series of attacks against several organisations in Europe, Latin America, and other regions [6]. According to the Microsoft's report, at least 11 European entities were targeted. In 2021 and 2022, CERT-EU detected exploitation attempts of vulnerabilities in some EU institutions, bodies or agencies (EUIBAs), likely linked to Ke3chang.		

Mustang Panda

Name	Likely motive	Examples of Examples of associated tools
Mustang Panda (aka RedDelta, TA416, Bronze President, Temp.Hex, HoneyMyte)	Information theft	Cobalt Strike, PlugX, RedDelta, WildPressure, VBScript, PoisonIvy
Threat actor description		
Mustang Panda was first observed in 2017, but has possibly been conducting operations since at least 2014. Mustang Panda has targeted government entities, nonprofit, religious, and other non-governmental organisations in the EU, the US, Germany, Mongolia, Myanmar, Pakistan, and Vietnam, among others. Since end 2021 - early 2022, CERT-EU has observed an uptick in campaigns targeting entities in the EU. Mustang Panda uses both proprietary and publicly available hacking tools. Mustang Panda uses several different initial access methods, including (primarily) spear-phishing with malicious attachments or links, watering hole attacks, and infected USB drives.		
Recent operations		

In 2022, Mustang Panda was observed using public documents belonging to EU Institutions, bodies or agencies (EUIBAs) as lures in spear-phishing campaigns. The targets were mainly ministries of foreign affairs and the diplomatic sector. Detected spear-phishing campaigns impersonated officials in order to be more credible.

In a March 2022 report, Proofpoint identified malicious activity by Mustang Panda, in which the group targeted European diplomatic entities, including one involved in refugee and migrant services [4].

In April 2022, threat researchers from Secureworks, a cybersecurity vendor, published a report that revealed Mustang Panda's targeting of Russian officials [5].

Between October and December 2022, several security firms, including Trend Micro and BlackBerry, reported on spear-phishing activity by Mustang Panda using EU lures [32][33].

Tactics, Techniques and Procedures (TTPs)

The analysis of these threat actors' TTPs focuses on some of the major patterns noticed in the last few months and is not intended to be exhaustive.

Reconnaissance and scanning

- According to an ANSSI report, APT31 has been using offensive IT infrastructure which is likely built as a botnet of compromised SOHO (Small Offices/Home Offices) devices. The infrastructure builds anonymous proxy chains that support TCP, UDP, and raw communications with the victim [15].
- According to reports from both Sekoia and Trend Micro, in August 2022, APT27 had compromised the servers of MiMi, an instant messaging application primarily used in China in a supply-chain attack that intended to spread malware [17].
- A Reuters news report linked Mustang Panda to the breach of the IT systems of the African Union and the monitoring of security camera video feeds (2020) [18].

Initial access

Exploitation of Internet-facing applications

The tactic uses previously unidentified or recently discovered vulnerabilities that have not been fixed or patched. In particular:

- Microsoft observed Ke3chang in the first quarter of 2021 compromising networks using attacks on Internet-facing web applications running unpatched Microsoft Exchange and SharePoint instances. They also observed Ke3chang attack remote access infrastructure, such as unpatched VPN appliances including the Pulse Secure VPN platform [6];
- Palo Alto Networks' Unit 42 observed APT27 in April 2019 installing web shells on SharePoint servers to compromise government organisations of two different countries in the Middle East [19];
- According to Check Point Software researchers, a piece of malware used by APT31 was, almost certainly, a clone of a US-origin cyber intrusion tool. Of particular note, the clone was created before the existence of the original malware became widely known [20];

- Palo Alto Networks' Unit 42 reported that they had observed some correlation of APT27 activities with the exploitation of vulnerabilities in ManageEngine ADSelfService Plus – a self-service password management and single sign-on solution (August - September 2021) [21];
- Several entities have observed related threat actors' exploitation of the Log4shell vulnerability.

Spear-phishing

Activities by the groups examined involve:

- substantial preparation through reconnaissance;
- social engineering (e.g. distribution of credible decoy documents, impersonation of partner organisations);
- highly targeted spear-phishing activity rather than general-approach phishing campaigns.

Some characteristic phishing campaigns have been:

- Phishing via legitimate cloud storage platforms. According to Positive Technologies, the APT31 group used in 2021 and 2022 the Yandex.Disk service and Dropbox [22];
- Research from Proofpoint pointed to Ke3chang conducting spear-phishing operations, targeting European entities using lures related to Russia's war on Ukraine or to activity targeting EU Institutions, bodies and agencies [23].

References

[1] https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/
[2] https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities
[3] https://blog.talosintelligence.com/mustang-panda-targets-europe/
[4] https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
[5] https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
[6] https://www.microsoft.com/en-us/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
[7] https://cyware.com/research-and-analysis/apt27-an-in-depth-analysis-of-a-decade-old-active-chinese-threat-group-e4cc
[8] https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf
[9] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-01-26-cyberbrief.html
[10] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2022-01-bfv-cyber-brief.pdf?__blob=publicationFile&v=10
[11] https://www.intrinsec.com/apt27-analysis/?cn-reloaded=1&cn-reloaded=1
[12] https://www.cert.ssi.gouv.fr/pdf/CERTFR-2021-IOC-003.pdf
[13] https://pst.no/alle-artikler/pressemeldinger/etterforskningen-av-datanettverksoperasjonen-mot-fylkesmannsembetene-er-avsluttet/
[14] https://supo.fi/en/-/supo-identified-the-cyber-espionage-operation-against-the-parliament-as-apt31
[15] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-013b.pdf
[16] https://unit42.paloaltonetworks.com/pingpull-gallium/
[17] https://cyware.com/news/apt27-group-backdoors-mimi-chat-app-for-supply-chain-attack-eecc8010/
[18] https://www.reuters.com/article/idUSKBN28Q1DB
[19]https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
[20] https://research.checkpoint.com/2021/the-story-of-jian/
[21] https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus/
[22] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
[23] https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
[24] https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience
[25] https://github.com/enisaeu/CNW#security-best-practices
[26] https://attack.mitre.org/groups/
[27] https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
[28] https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP2019-001.pdf
[29] https://cert.europa.eu/static/WhitePapers/CERT-EU_SWP_17-002_Lateral_Movements.pdf
[30] https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP2012-004.pdf
[31] https://csirtsnetwork.eu/
[32] https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
[33] https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets
[34] https://www.enisa.europa.eu/securesme/cyber-tips/strengthen-technical-measures/secure-backups
[35] https://www.cert.europa.eu/static/WhitePapers/TLP-WHITE-CERT-EU_Security_Guidance-22-001_v1_0.pdf
[36] https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources

History

15/02/2023 1.0 Initial Release