Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Chinese Hackers Turn to RA World Ransomware for Profit

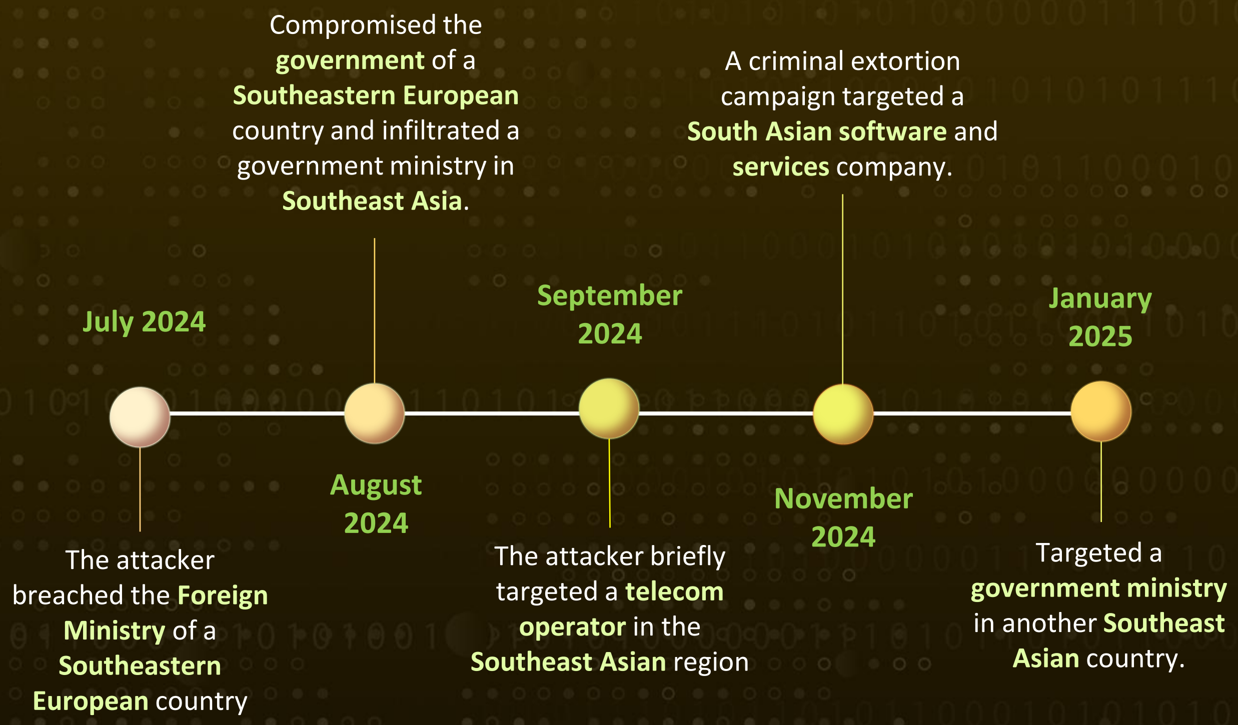
Date of Publication	Admiralty Code	TA Number
February 18, 2025	A1	TA2025047

Summary

Attack Commenced: 2024
Threat Actor: Emperor Dragonfly (aka Bronze Starlight, DEV-0401, Cinnamon Tempest, SLIME34, SLIME34)
Malware: RA World ransomware (aka RA Group ransomware), PlugX
Targeted Regions: Europe, Asia

Attack: A sophisticated ransomware attack in November 2024 revealed a troubling shift in cyber threats. Linked to the Chinese hacking group Emperor Dragonfly, the attack targeted a South Asian software firm, exploiting a known firewall vulnerability to breach its network.

Attack Timeline



July 2024

The attacker breached the **Foreign Ministry** of a **Southeastern European** country

August 2024

Compromised the **government** of a **Southeastern European** country and infiltrated a government ministry in **Southeast Asia**.

September 2024

The attacker briefly targeted a **telecom operator** in the **Southeast Asian** region

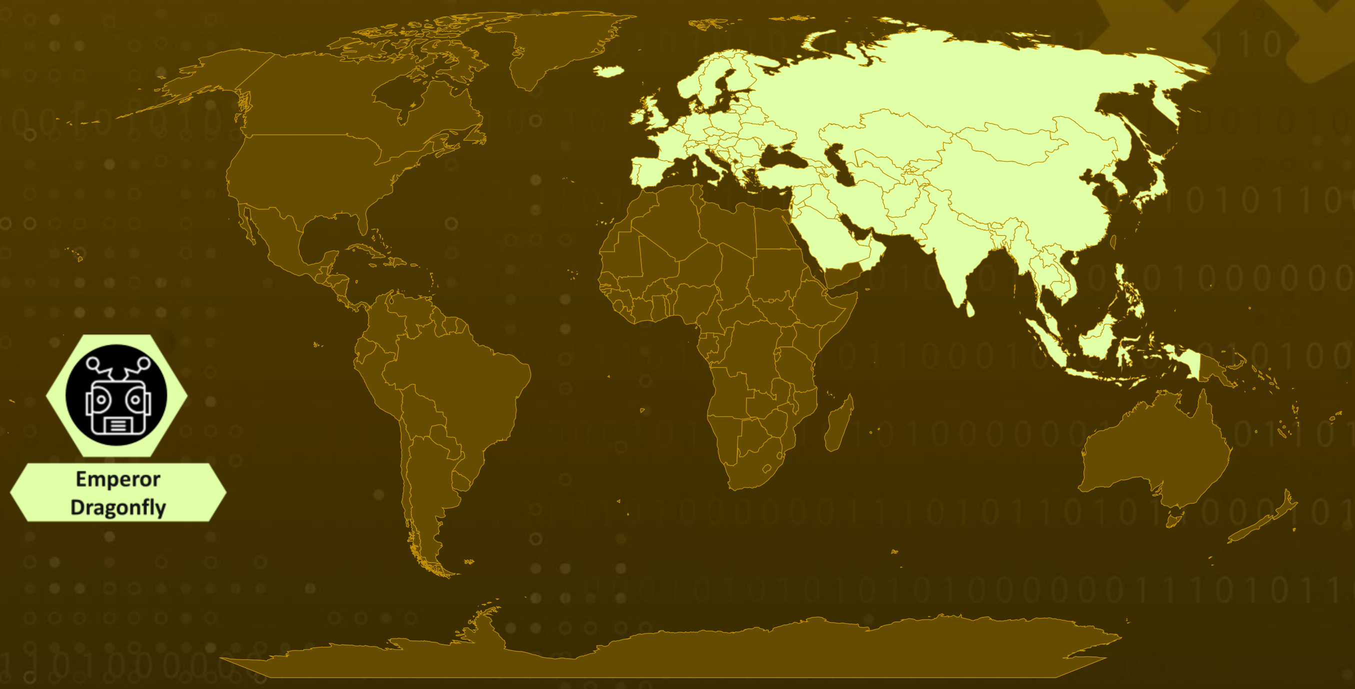
November 2024

A criminal extortion campaign targeted a **South Asian software** and **services** company.

January 2025

Targeted a **government ministry** in another **Southeast Asian** country.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-0012	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS software	✓	✓	✓

Attack Details

#1

In November 2024, a ransomware attack on a South Asian software and services company highlighted the growing overlap between cyber espionage and financially motivated cybercrime. The attack was linked to Emperor Dragonfly (also known as **Bronze Starlight**), a China-based hacking group typically associated with espionage operations.

#2

However, instead of solely gathering intelligence, the group deployed RA World ransomware a rebranded version of the **RA Group**. The breach reportedly began when the hackers exploited a known vulnerability in Palo Alto's PAN-OS firewall software (CVE-2024-0012) to gain access to the company's network.

#3 Once inside, they allegedly stole administrative credentials from the intranet before extracting Amazon S3 cloud credentials from a Veeam server. These stolen credentials allowed them to access and exfiltrate sensitive data before launching the ransomware encryption process.

#4 A crucial aspect of the attack was using PlugX (also known as Korplug), a backdoor commonly linked to Chinese state-sponsored hacking groups like Mustang Panda. The attackers used a method called DLL sideloading, in which a legitimate Toshiba executable was leveraged to load a malicious dynamic link library (DLL), ultimately deploying the PlugX backdoor.

#5 The attack also shares characteristics with past operations by Emperor Dragonfly, which is known for deploying short-lived ransomware families and maintaining long-term access through tools like NPS Proxy. Additionally, it aligns with a broader espionage campaign observed between July 2024 and January 2025, during which government ministries and telecom operators in Southeastern Europe and Asia were targeted for intelligence gathering.

#6 This incident raises concerns about a possible shift in tactics, where cyber tools originally designed for espionage are being repurposed for profit-driven attacks. If this pattern continues, it could signal a new wave of cyber threats, with state-backed hackers increasingly blurring the lines between intelligence gathering and financial extortion.

Recommendations

Patch Critical Vulnerabilities: Immediately apply security updates for Palo Alto PAN-OS (CVE-2024-0012) and other known vulnerabilities that could be exploited for initial access. Regularly monitor vendor security advisories and implement patches promptly to prevent zero-day exploits.

Enhance Cloud and Data Security: Secure cloud credentials using strong encryption and role-based access control (RBAC) to prevent misuse if compromised. Ensure that sensitive data stored on platforms like Amazon S3 is tightly controlled. Use immutable backups for cloud data to protect it from being encrypted or stolen during ransomware attacks.

Conduct Ransomware Simulation Drills: Test the organization's resilience against ransomware attacks by conducting simulated scenarios to identify gaps in preparedness.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
TA0006 Credential Access	TA0009 Collection	T1083 File and Directory Discovery	T1490 Inhibit System Recovery
T1552 Unsecured Credentials	T1560 Archive Collected Data	T1573 Encrypted Channel	T1496 Resource Hijacking
T1203 Exploitation for Client Execution	T1055.001 Dynamic-link Library Injection	T1055 Process Injection	T1105 Ingress Tool Transfer
T1555 Credentials from Password Stores	T1027 Obfuscated Files or Information	T1036 Masquerading	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7bae7f21bd4adf84eb3cc281fcc3d5fc3d1e47edd0dadd86587ce8ec63df1b8f, c1e6955acdefa9769a7ae0c1abf54a26e2158154dd6ec07cc71eb06c575193d5, 18127cfd08cc49be08714d29e09ec130dcc0b19b7fcddc22c71d28fd245eb1b1, e177eb358f93ccc1ac4694feb0139e82c62d767388872d359d7c2ed0a05c2726, 6ac81aa8d3f9d86ad5a18ea42fa1829b055dd25f123f9ee90002d64d4ef7a394, 2707612939677e8ea4709ecb4f45953d4a136a9934b6d0c256917383cdaef813, 38a26fffbab5297e4229897654d2f67c6ee52b316c7ac4d4a1493d187b49ec25, bb5740d2129663ae1c46b1ea1bdd0b8c423b6eb8f6e6f2b0b158a9e833496a01
Domain	plugins[.]jetbrians[.]net, police[.]tracksyscloud[.]com, caco[.]blueskyanalytics[.]net
IPv4	158[.]247[.]213[.]167, 154[.]223[.]18[.]123

Patch Details

CVE-2024-0012: Resolved in PAN-OS versions 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1, and all subsequent releases.

Links:
https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-release-notes/pan-os-11-2-4-known-and-addressed-issues/pan-os-11-2-4-addressed-issues

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-release-notes/pan-os-11-1-5-known-and-addressed-issues/pan-os-11-1-5-addressed-issues

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-release-notes/pan-os-10-2-12-known-and-addressed-issues/pan-os-10-2-12-h1-addressed-issues

References

https://www.security.com/threat-intelligence/chinese-espionage-ransomware

https://unit42.paloaltonetworks.com/ra-world-ransomware-group-updates-tool-set/

https://hivepro.com/threat-advisory/ra-groups-custom-ransomware-hits-us-south-korea/

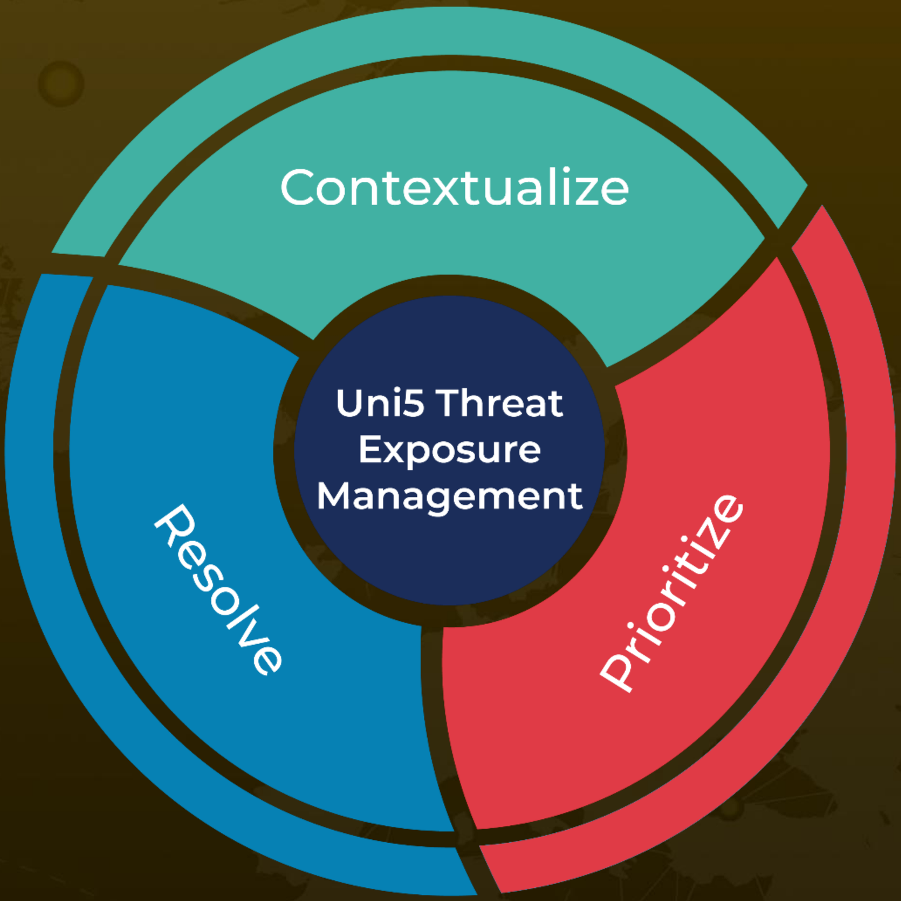
https://hivepro.com/threat-advisory/decoding-bronze-starlights-strategy-in-the-gambling-sector/

https://hivepro.com/threat-advisory/critical-zero-day-pan-os-flaws-exposing-systems-to-full-control/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 18, 2025 • 7:30 PM

More at www.hivepro.com