Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

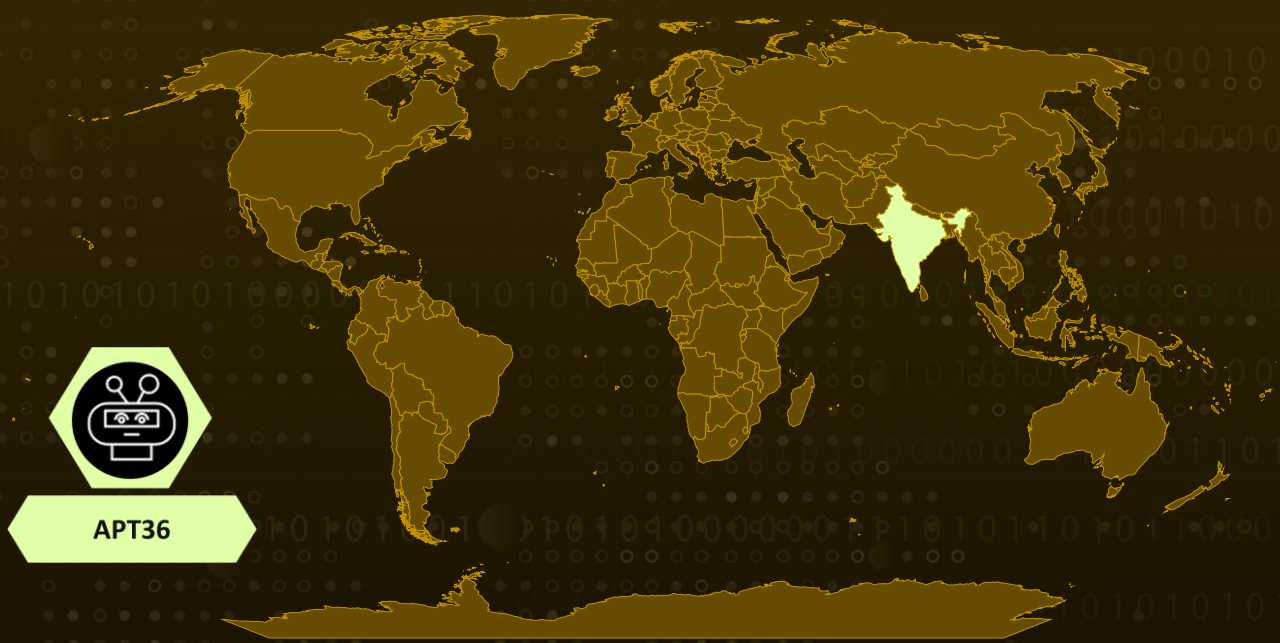
APT36's Covert Linux Attack on India's Defense Sector

Date of Publication	Admiralty Code	TA Number
July 10, 2025	A1	TA2025212

Summary

Attack Commenced: June 7, 2025
Targeted Country: India
Targeted Industries: Defense, Government
Targeted OS: BOSS (Bharat Operating System Solutions) Linux
Actor: APT36 (aka Mythic Leopard, Transparent Tribe, ProjectM, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, C-Major)
Attack: APT36, a Pakistan-based threat group, is back with a stealthy cyber-espionage campaign targeting India's defense sector, this time focusing on Linux systems, especially those running BOSS Linux. Disguised as a cybersecurity advisory, the attack begins with a phishing email carrying a ZIP file that contains a .desktop shortcut. Once opened, it silently downloads a malicious ELF binary in the background while showing a fake PowerPoint to distract the user. This clever mix of social engineering and technical trickery lets the attackers quietly gain access, steal sensitive data, and maintain control, putting critical defense infrastructure at serious risk.

Attack Regions



Attack Details

#1 A recent cyber-espionage campaign attributed to Pakistan-based threat group **APT36** has taken a sharp turn toward targeting Linux systems, with a particular focus on BOSS Linux, an operating system widely adopted by Indian government agencies. This campaign zeroes in on personnel in India's defense sector, leveraging carefully crafted phishing emails that carry malicious ZIP file attachments.

#2 The phishing lure typically arrives as an archive named "Cyber-Security-Advisory.zip", which contains a .desktop file disguised as a legitimate shortcut. When opened, the file's embedded command sequence runs silently through a Bash shell, initiating a chain reaction. It uses curl to fetch a seemingly harmless PowerPoint file from an attacker-controlled server, a disguised HTML document loaded via iframe to mimic a genuine cybersecurity blog. While the victim views this decoy, the background script proceeds to download the actual malware: a binary named BOSS.elf, which is granted executable permissions and run discreetly on the system.

#3 This malware isn't just opportunistic, it's purpose-built for espionage. Once active, it collects system-level data such as hostname, CPU, and memory details to profile the target machine. It uses a logging function to monitor connections, commands issued and received, and any errors, providing real-time visibility to the attacker. File discovery functions like Main.getDrives and os.readDir enable it to search local drives for sensitive documents, while main.loadConfig fetches C2 configuration data to guide its actions.

#4 A critical part of the malware's functionality is its persistent communication with a remote command-and-control (C2) server. It initiates a TCP connection to the IP Address and employs SetKeepAlive and setKeepAlivePeriod to maintain regular contact, retrying every 30 seconds. Additionally, it uses the Go-based library to covertly capture screenshots of the victim's desktop, adding a layer of surveillance that could expose confidential visual data such as documents or communications.

#5 This campaign underscores a dangerous evolution in APT36's capabilities. Their pivot to Linux particularly a government-favored distribution like BOSS Linux suggests a calculated attempt to bypass traditional defenses and infiltrate critical national infrastructure. By combining technical sophistication with social engineering, this operation highlights the urgent need for organizations in the public and defense sectors to enhance threat detection on Linux environments, raise user awareness around phishing threats, and closely monitor infrastructure for signs of covert activity.

Recommendations

Remain Vigilant: Be cautious of unsolicited emails that claim to be cybersecurity advisories or government notices. If an email comes with an attachment like a .zip file or a shortcut (.desktop) file, think twice before opening it. Verify the sender through a trusted channel.

Regularly patch and update your systems: Keep your Linux systems, especially BOSS Linux, fully updated with the latest security patches. Attackers often rely on unpatched systems to get in easily.

Allow only trusted apps to run: Use application whitelisting to make sure only approved programs can run on your systems. This blocks unknown or suspicious files, like rogue ELF binaries used in this attack from executing without permission.

Block risky areas from running programs: Stop malware from running in common temporary folders like /tmp by changing settings so that no files in those areas can be executed. These folders are often targeted because they're writable by many users.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process	T1543.003 Windows Service	T1036 Masquerading

T1564 Hide Artifacts	**T1564.001** Hidden Files and Directories	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1071 Application Layer Protocol	**T1095** Non-Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1571** Non-Standard Port
T1204 User Execution	**T1592** Gather Victim Host Information	**T1082** System Information Discovery	**T1041** Exfiltration Over C2 Channel
T1113 Screen Capture			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	608fff2cd4b727799be762b95d497059a202991eb3401a55438071421b9b5e7a, ace379265be7f848d512b27d6ca95e43cef46a81dc15d1ad92ec6f494eed42ab, e528799a29e9048c1e71b78223311cad2699d035a731d1a6664fc8ddd0642064, 167b387005d6d2a55ad282273c58d1786a2ee0fa3e7e0cb361d4d61d8618ee5f
URLs	hxxps[:]//govin[.]sorlastore[.]com/uploads/BOSS[.]elf, hxxps[:]//govin[.]sorlastore[.]com/uploads/Cyber-Security-Advisory[.]pptx, hxxp[:]//169[.]254[.]169[.]254/latest/meta-data/ami-id
Domains	sorlastore[.]com, modgovin.onthewifi[.]com
IPv4:Port	169[.]254[.]169[.]254, 101[.]99[.]92[.]182[:]12520
MD5	6eb04445cad300c2878e8fbd3cb60b52, 18cf1e3be0e95be666c11d1dbde4588e
Filename	Cyber-Security-Advisory.zip

References

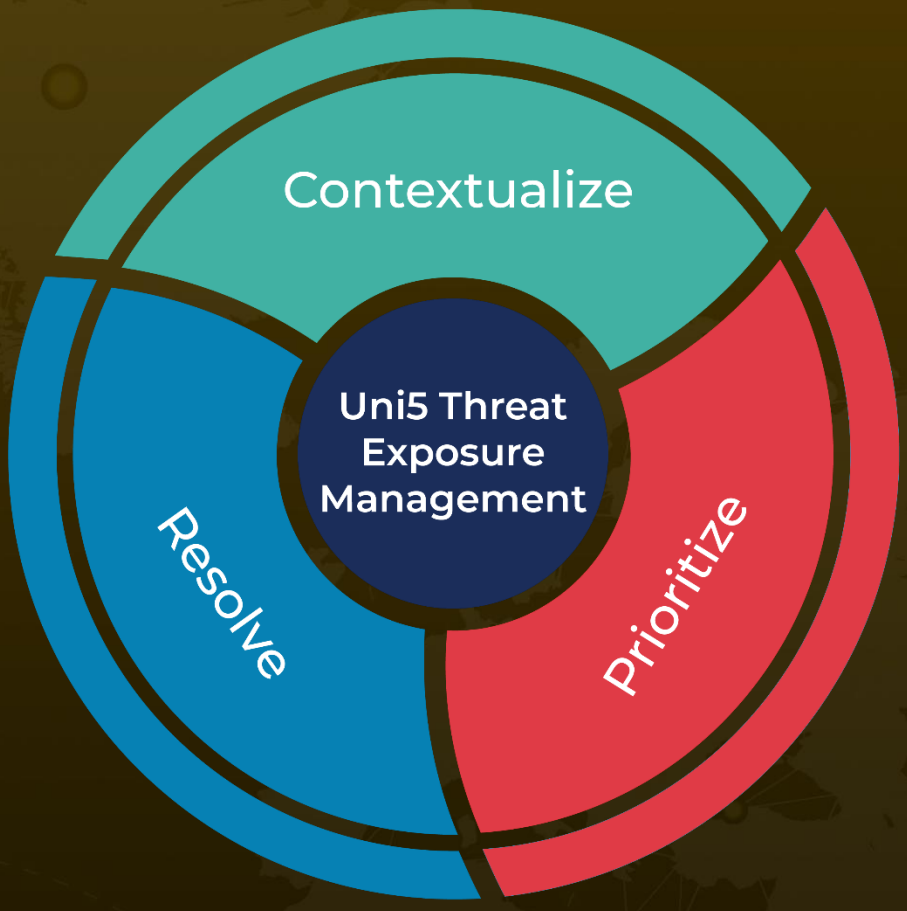
https://www.cyfirma.com/research/phishing-attack-deploying-malware-on-indian-defense-boss-linux/

https://hivepro.com/threat-advisory/apt36s-dark-playbook-crimson-codes-and-crisis-lures-strike-india/

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

July 10, 2025 • 5:30 AM

More at www.hivepro.com