



ThreatCure

Cyber Threat Advisory

APT-k-47

Threat Actor APT

Description

APT-K-47

CATEGORY

APT Group

SEVERITY

High

Platforms

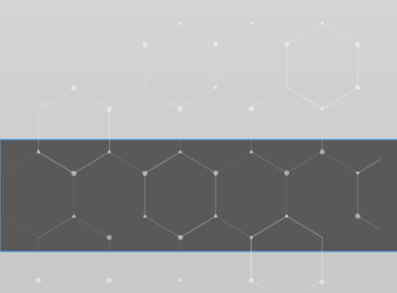
Windows

IMPACT

- Disruption to Critical Infrastructure
- Data Breaches and Credential Theft
- Economic and Reputational Damage

APT-K-47, also referred to as Mysterious Elephant, is an APT organization first identified by the Knownsec 404 Advanced Threat Intelligence Team. This group is currently **active** in **Pakistan** and has shown patterns reminiscent of other South Asian APT groups, such as Sidewinder, Confucius, and Bitter. Their operational methods largely revolve around social engineering, employing phishing tactics that exploit current events to lure victims. Notable attack vectors include vulnerabilities in Compiled HTML (CHM) files, certain document weaknesses (notably CVE-2017-11882), and flaws within WinRAR software. Their targets span various regions, including Russia, Pakistan, Bangladesh, and the United States.

In August 2023, Knownsec 404 disclosed the ORPCBackdoor tool used by APT-K-47, which has since seen a resurgence in activities. The recent wave of attacks involved the use of a new, undisclosed Trojan tool to penetrate systems successfully. Following infiltration, APT-K-47 utilized ORPCBackdoor and additional malicious payloads, conducted disk directory traversals, and exfiltrated files to their command-and-control (C2) servers. Furthermore, they compromised password information from browsers on targeted machines and transmitted this data back to their C2 infrastructure. The following sections will detail our findings from ongoing monitoring of APT-K-47's operations.



Indicator of Compromise

SHA-256

b087a214fb40e9f8e7b21a8f36cabd53fee32f79a01d05d31476e249b6f472ca
74ba5883d989566a94e7c6c217b17102f054ffbe98bc9c878a7f700f9809e910
c4817f3c3777b063f0adbc1c8e4671da533f716bab7ad2c4b9bc87295df67334
85a6ac13510983b3a29ccb2527679d91c86c1f91fdfee68913bc5d3d01eeda2b

Remediation

- **Patch Management:** Regularly update software to fix vulnerabilities, especially those in Office and WinRAR.
- **Endpoint Security:** Use EDR tools to detect and block malware like ORPCBackdoor and WalkerShell; segment networks to limit lateral movement.
- **PowerShell Restrictions:** Limit and monitor PowerShell access to prevent malicious scripting.
- **Phishing Defense:** Enhance email filtering and train users to recognize phishing tactics.
- **Credential Security:** Enforce multi-factor authentication and minimize browser-stored passwords.
- **Continuous Monitoring:** Use SIEM systems to detect abnormal network and endpoint behavior.
- **Access Control & Data Encryption:** Encrypt sensitive data and restrict access to critical resources.
- **Incident Response:** Maintain a tested incident response plan to swiftly handle breaches.



ThreatCure

Cyber Threat Advisory

Secure your byte world



Iranian Threat Actor

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

