Mythic Leopard APT Group - Brandefense

Published: 2022-08-12 · Archived: 2026-04-05 15:03:05 UTC

Threat Actor ID

Known Names	**Mythic Leopard (CrowdStrike)Transparent Tribe (Proofpoint)** **APT 36 (Mandiant)** **ProjectM (Palo Alto)** **TEMP.Lapis (FireEye)** **Copper Fieldstone (SecureWorks)** **Earth Karkaddan (Trend Micro)**
Suspected State Sponsor	**Pakistan**
First Seen	**2013**
Motivation	**Information theft and espionage**
Tools Used	**Amphibeon, beendoor, Bezigate, Bozok, BreachRAT, CapraRAT, Crimson RAT, DarkComet, Luminosity RAT, Mobzsar, MumbaiDown, njRAT, ObliqueRAT, Peppy RAT, QuasarRAT, SilentCMD, Stealth Mango, UPDATESEE, USBWorm, Waizsar RAT**
Target Industries	**Aviation, Government, Healthcare,Defense, Hospitality Military,** **NGOs and Nonprofits, Oil and Gas**

Introduction

Mythic Leopard is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India’s government and the Indian Army or related assets in India and Afghanistan. Mythic Leopard used several proprietary malware families for Windows and Android operating systems. The group is typically known for espionage activities.

Group’s Mission and Vision

Mythic Leopard, also known as PROJECTM and Transparent **Tribe,** is a highly prolific group whose activities can be traced as far back as 2013, in a series of espionage operations against Indian diplomats and military personnel in some embassies in Saudi Arabia and Kazakhstan.

When the IP addresses thought to belong to Mythic Leopard were tracked, it was determined that they originated from Pakistan. The attacks were part of a broader multi-vector operation, such as phishing email campaigns and watering hole websites, delivering specialized RATs called Crimson and Peppy. These RATs can leak information, take screenshots, and record webcam streams.

Mythic Leopard also creates fake domains that mimic legitimate military and defense organizations as a core component of their operations. It was found that the threat actor used several delivery methods in a campaign. These are executables masquerading as installers of legitimate applications, archive files, and malicious docs to target Indian entities and individuals. These chains of infection were seen in the placement of different types of implants not observed before.

Russia sees European security organizations such as NATO and OSCE as a threat to them. For this reason, it targets both the member states of such organizations and the individuals affiliated with these organizations.

Targeted Countries and Industries

It has been determined that Mythic Leopard carries out Information theft and espionage activities and organizes malware campaigns against many different countries, mainly India-targeted attacks.

In the attacks carried out, it was observed that the Mythic Leopard APT group targeted the critical systems of the following countries;

	• Afghanistan		• Germany		• Netherlands
	• Australia		• India		• Oman

	• Austria		• Iran		• Pakistan
	• Azerbaijan		• UK		• Romania
	• Belgium		• USA		• Saudi Arabia
	• Botswana,		• UAE		• Spain
	• Bulgaria		• Japan		• Sweden
	• Canada		• Kazakhstan		• Thailand
	• China		• Kenya		• Turkey
	• Czech		• Nepal		
	• Mongolia		• Malaysia		

Operations by Year

Operation “Transparent Tribe”

In 2012, there were two attacks within minutes of each other on officials at the Indian embassies in Saudi Arabia and Kazakhstan. Both emails contained a malware attachment and appeared to have been sent from the IP address of Contabo, a hosting provider.

SmeshApp Attack

In 2016, the Indian television channel CNN-IBN discovered that Pakistani authorities were collecting data on Indian troop movements using an Android app called SmeshApp.

Operation “C-Major”

In 2016, Researchers reported on a third phishing campaign, operation C-Major, organized by the Mythic Leopard. This campaign targeted Indian military officials through targeted phishing emails and distributed

spyware to its victims through an Adobe Reader vulnerability.

In 2017, another hacking campaign was detected in which attackers impersonated the Indian think tank IDSA (Institute for Defense Studies and Analysis) and sent spear phishing emails to target Central Bureau of Investigation (CBI) officials and possibly Indian Army officials.

In 2019, it was found that Mythic Leopard has undergone an evolution, accelerating its activities, launching major infection campaigns, developing new tools, and strengthening its focus on Afghanistan.

In 2020, Mythic Leopard returned with a new campaign after a few years of (apparently) inactivity. It was found that this campaign is entirely new, C2 server was active on January 29, 2020.

Mythic Leopard started using a new module named USBWorm at the beginning of 2020 and improved its custom .NET tool named CrimsonRAT.

In 2020, Mythic Leopard was found to be conducting cyberattack campaigns by spreading fake coronavirus health advice.

Operation "Honey Trap"

In 2020, Mythic Leopard was found to carry out targeted attacks on Defense organizations in India.

In 2021, ObliqueRAT appeared to be back with a new campaign using compromised websites.

In 2021, Mythic Leopard was using a new malware to target Indian government officials.

Cyber Attack Lifecycles and TTPs (MITRE ATT&CK)

MITRE ATT&CK is an open knowledge base of threat actors' techniques, tactics, and procedures. By observing the attacks that occur in the real world, the behavior of threat actors is systematically categorized.

MITRE ATT&CK aims to determine the risks against the actions that the threat actors can take in line with their targets and make the necessary improvements and plans.

The following MITRE ATT&CK Threat Matrix has been created to provide information on the techniques, tactics, and procedures used by Mythic Leopard APT.

Tactic ID	Tactic	Technic ID	Technic
TA0042	Resource Development	T1189T1566.001 T1566.002 T1608.004	Drive-by CompromiseSpearphishing Attachment Spearphishing Link Drive-by Target

TA0001	Initial Access	T1059.005T1203 T1204.002 T1204.001	Command and Scripting Interpreter: Visual BasicExploitation for Client Execution User Execution: Malicious File User Execution: Malicious Link
TA0005	Defense Evasion	T1564.001T1036.005 T1027	Hide Artifacts: Hidden Files and DirectoriesMasquerading: Match Legitimate Name or Location Obfuscated Files or Information
TA0011	Command and Control	T1568	Dynamic Resolution

Dowload IoCs and Yara Rules

Group's Toolset and Related Malwares

Software	Descriptions
Crimson	Crimson is a remote access Trojan that has been used by Mythic Leopard since at least 2016
DarkComet	DarkComet is a Windows remote administration tool and backdoor that has been used by Mythic Leopard.
njRAT	njRAT is a remote access tool (RAT) that was first observed in 2012. It has been used by Mythic Leopard threat actors.
ObliqueRAT	ObliqueRAT is a remote access trojan, similar to Crimson, that has been in use by Mythic Leopard since at least 2020.
Peppy	Peppy is a Python-based remote access Trojan, active since at least 2012, with similarities to Crimson.

Recommendations/Mitigations

When the encountered cases were examined, it was seen that the group mostly used phishing attacks to gain initial access and took advantage of the vulnerabilities in the existing systems. In this context, precautions should be taken by considering the attack vectors used to be protected from attacks that Mythic Leopard may carry out. Important recommendations to be implemented to protect assets in the digital world and minimize the risk of exploitation arising from security vulnerabilities and device configuration are shared below.

- An integrated cyber defense platform should be used that shares threat data from email, web, cloud applications, and infrastructure.
- Make sure that multi-factor authentication is enabled for all accounts using your network.
- Internet dependency should be minimized for all critical systems, and control system devices should not be connected directly to the Internet.
- All unused legacy applications should be removed from all machines on the network to avoid abuse.
- Critical networks, such as control system networks behind firewalls, must be isolated from the external network.
- If remote access is required, secure methods such as VPN should be used.
- Unused system accounts should be removed, disabled, or renamed.
- To not be affected by known security vulnerabilities, updates that patch the vulnerabilities should be applied as soon as possible.
- Policies that require the use of strong passwords should be implemented.
- Organizations should keep backups of important data, systems, and configurations.
- The restoring capacity should be tested. Ensure that the restore capabilities support the needs of the business.
- Institution/Organization personnel should be trained to understand cybersecurity principles and not engage in behavior that could compromise network security.

Conclusion

Analysis of Mythic Leopard group and explained findings that can be used by people who work in the information technology departments, who are part of the cyber security team, and who have gained competence in areas such as security researchers, and system administrators.

Implementing cyberattack surface management for critical infrastructures targeted by the Mythic Leopard APT group will benefit the organization’s access to security maturity.
