Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

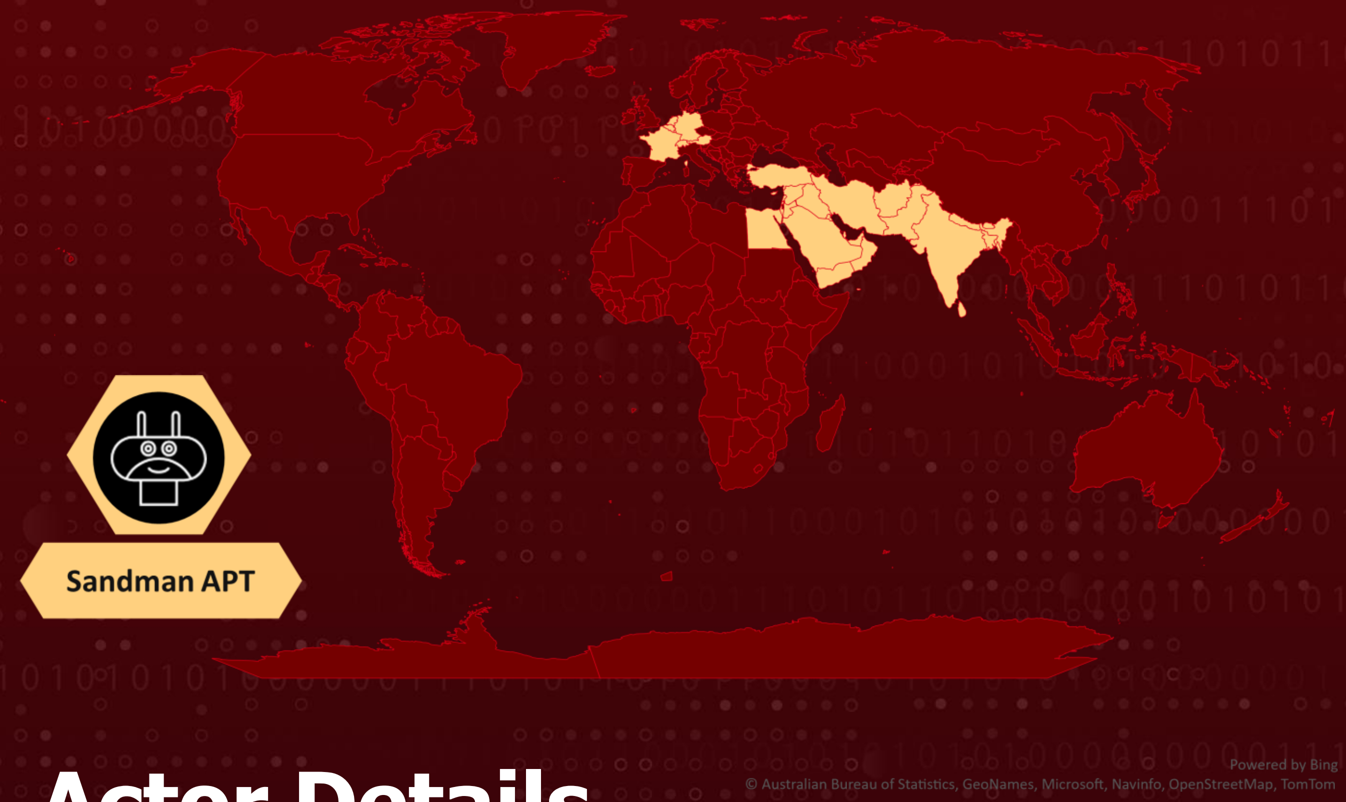
Sandman APT Strikes the Telecom Sector with the LuaDream Backdoor

Date of Publication	Admiralty code	TA Number
September 24, 2023	A1	TA2023384

Summary

Attack began: August 2023
Actor Name: Sandman APT
Target Industries: Telecommunication
Target Region: Middle East, Western Europe, and the South Asian subcontinent.
Malware: LuaDream , luajit

Actor Map


Sandman APT
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Actor Details

#1

A new threat has surfaced in the world of cybersecurity: the Sandman APT. This enigmatic group appeared mysteriously in August, and since then, they have been carrying out a highly sophisticated campaign. This group has been orchestrating a sophisticated campaign, deploying an innovative backdoor known as LuaDream and wielding the potent LuaJIT toolkit. Sandman APT has been unequivocally linked to a series of cyber assaults directed at telecommunications providers spanning the Middle East, Western Europe, and the South Asian subcontinent.

#2 The Sandman APT employs clever tactics to stealthily steal administrative credentials. They initiate a systematic reconnaissance operation within the compromised network, with a clear goal in mind: to infiltrate carefully selected workstations by using the pass-the-hash technique in tandem with the NTLM authentication protocol.

#3 The group then takes advantage of the DLL hijacking technique to execute LuaDream, a versatile and multi-protocol backdoor known for its ability to handle attacker-supplied plugins and discreetly siphon off both system and user data. The staging process used by LuaDream is a carefully designed operation, created with the specific goal of avoiding detection and hindering investigative analysis.

#4 At the heart of this process is the skillful use of the LuaJIT platform, a just-in-time compiler designed for the Lua scripting language. This choice is primarily motivated by the aim of making malicious Lua script code extremely difficult to detect.

#5 A significant observation is the presence of distinctive characteristics within the LuaDream malware that share similarities with another malicious strain known as "DreamLand." This connection between the two entities was discovered in March 2023, during APT activities aimed at a government entity in Pakistan. These intriguing connections hint at the potential existence of a broader and more prolonged campaign, raising the possibility that Sandman's activities might have started as early as 2022.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Sandman APT	Unknown	Middle East, Western Europe, and the South Asian subcontinent	Telecommunication
	MOTIVE		
	Information Theft and Espionage		

Recommendations

Enhance Network Monitoring: Invest in robust network monitoring and intrusion detection systems to quickly detect and respond to suspicious activities. Early detection can mitigate the damage caused by potential breaches.

Credential Security: Recognizing that Sandman APT initially steals administrative credentials, organizations should prioritize strengthening their credential security. Implementing strong password policies and multifactor authentication (MFA) can be effective in thwarting such attacks.

Software Validation: Scrutinize the use of LuaJIT and other third-party scripting platforms. Ensure that their deployment is validated, and their security implications are thoroughly assessed.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
T1190 Exploit Public-Facing Application	T1595.002 Vulnerability Scanning	T1584.004 Server	T1543 Create or Modify System Process
T1055 Process Injection	T1570 Lateral Tool Transfer	T1112 Modify Registry	T1588.001 Malware
T1007 System Service Discovery	T1560 Archive Collected Data	T1497 Virtualization/Sandbox Evasion	T1129 Shared Modules

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4, 27894955aaf082a606337ebe29d263263be52154, 5302c39764922f17e4bc14f589fa45408f8a5089, 77e00e3067f23df10196412f231e80cec41c5253, b9ea189e2420a29978e4dc73d8d2fd801f6a0db2, fb1c6a23e8e0693194a365619b388b09155c2183, ff2802cdbc40d2ef3585357b7e6947d42b875884

TYPE	VALUE
File Name	fax.dat, fax.Application, ualapi.dll, fax.cache, UpdateCheck.dll, updater.ver, fax.module
File Path	%ProgramData%\FaxConfig, %ProgramData%\FaxLib
Domains	mode.encagil[.]com, ssl.explorecell[.]com

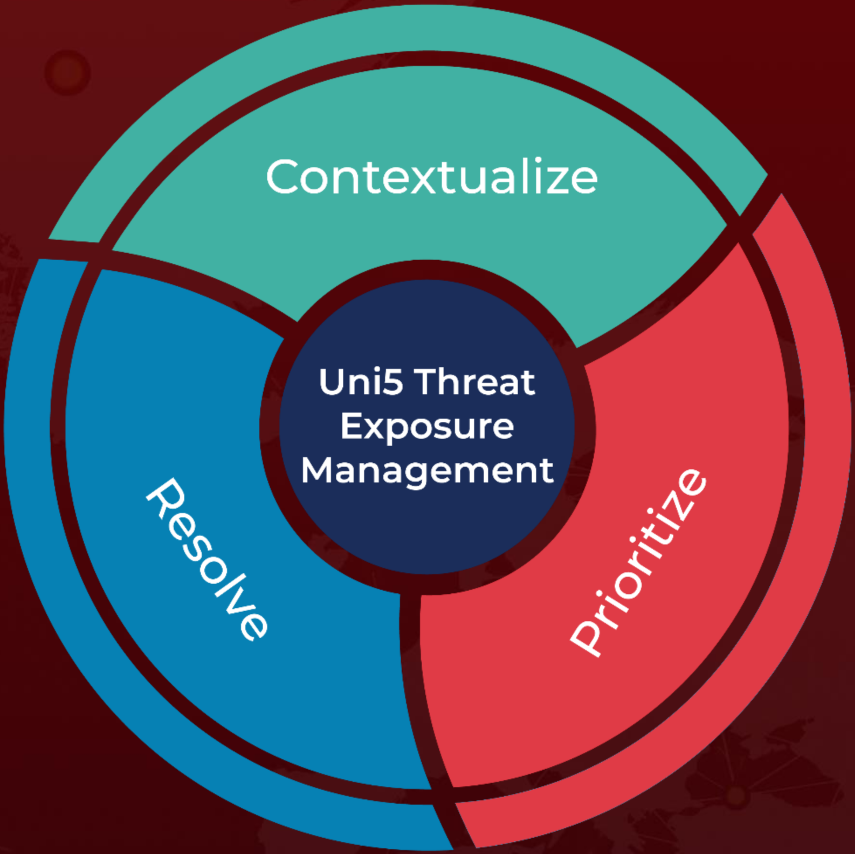
References

https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/

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

September 24, 2023 • 10:15 PM

More at www.hivepro.com