Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

The Unseen Thread Linking Sandman APT and KEYPLUG Backdoor

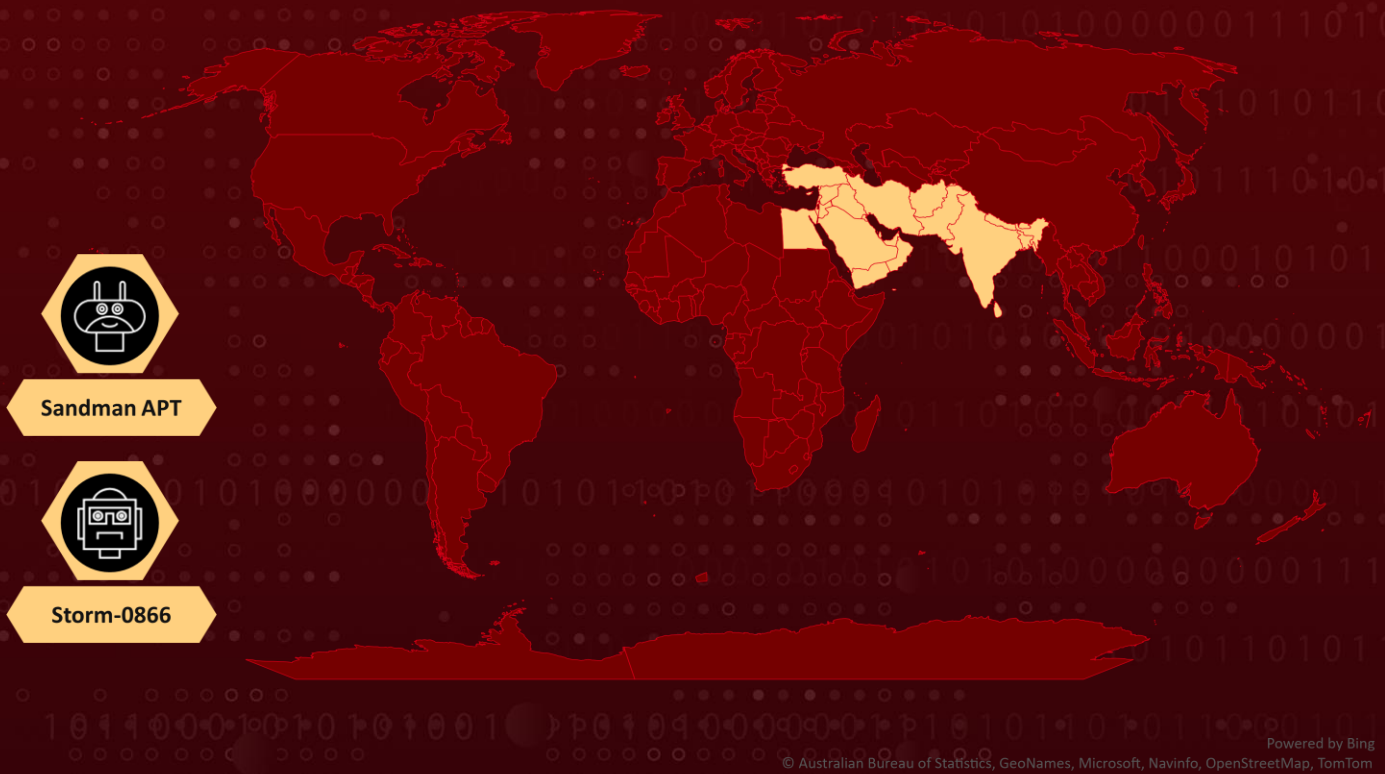
Date of Publication	Admiralty Code	TA Number
December 12, 2023	A1	TA2023499

Summary

Attack Began: 2023
Threat Actor: Sandman, and Storm-0866 (aka Red Dev 40)
Malware: LuaDream, KEYPLUG (aka ELFSHELF)
Attack Region: The Middle East, and South Asia
Targeted Industries: Telecommunication providers, and Government entities.

Attack: The Sandman Advanced Persistent Threat (APT) is closely linked to suspected threat clusters originating from China, specifically identified as Storm-0866, also known as Red Dev 40. Within the same victim environments, the Sandman's Lua-based malware, LuaDream, and the KEYPLUG backdoor have been observed coexisting.

Attack Regions



Attack Details

#1 The Sandman Advanced Persistent Threat (APT) is linked to suspected threat clusters originating from China, specifically identified as Storm-0866, also known as Red Dev 40. This group is recognized for deploying the KEYPLUG backdoor. There is a noticeable correlation between Sandman and Storm-0866 in terms of infrastructure control and management practices, involving choices of hosting providers and domain naming conventions.

#2 Notably, the Sandman's malware, LuaDream, and the KEYPLUG backdoor have been observed coexisting within the same victim environments. The modular backdoor, KEYPLUG, is a crucial component in the arsenal of STORM-0866. An interesting convergence is evident in a pair of LuaDream Command and Control (C2) domains, namely "dan.det-ploshadka[.]com" and "ssl.e-novauto[.]com."

#3 These domains have not only been utilized by LuaDream but have also served as a KEYPLUG C2 server, establishing a connection to Storm-0866. LuaDream, characterized by its Lua-based design, is a versatile and multi-protocol backdoor renowned for its ability to discreetly manage attacker-supplied plugins, extracting both system and user data.

#4 On the other hand, KEYPLUG, a modular backdoor written in C++, supports various network protocols for Command and Control (C2) traffic, including HTTP, TCP, KCP over UDP, and WSS. The collaborating threat actors are expected to persist in their cooperative efforts, consistently exploring novel approaches to enhance the functionality, flexibility, and stealth of their malware.

Recommendations

Enhance Network Security Measures: Strengthen network security protocols to guard against potential infiltrations by the Sandman APT and related threat clusters. Employ robust firewalls, and intrusion detection systems, and regularly update security software to mitigate vulnerabilities.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Zero-Trust Architecture: Consider adopting a zero-trust architecture, where no device or user is inherently trusted, and verification is required from everyone trying to access resources. This approach can limit the lateral movement within a compromised network.

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

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	dan.det-ploshadka[.]com, mode.encagil[.]com, ssl.articella[.]com, ssl.e-novauto[.]com, ssl.explorecell[.]com, yum.luxyries[.]com
IPv4	146.70.157[.]20, 172.67.216[.]63, 185.38.142[.]129, 185.51.134[.]27, 185.82.218[.]230, 37.120.140[.]205, 45.129.199[.]122, 45.80.148[.]151, 45.90.59[.]17, 5.2.67[.]176,

TYPE	VALUE
IPv4	5.2.72[.]130, 5.255.88[.]188, 79.110.52[.]160
SHA1	a7932112b7880c95d77bc36c6fcced977f4a5889, b6d759c9ea5d2136bacb1b2289a31c33500c8de8, fc8fdf58cd945619cbfede40ba06aada10de9459

References

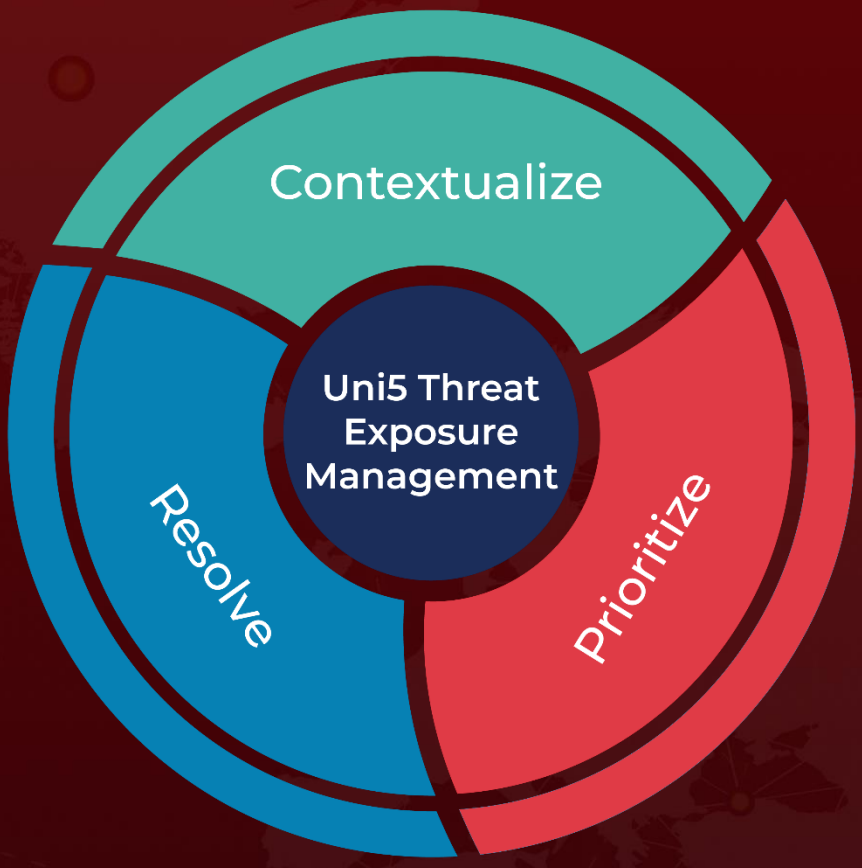
https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/

https://www.hivepro.com/threat-advisory/sandman-apt-strikes-the-telecom-sector-with-the-luadream-backdoor/

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

December 12, 2023 . 4:30 AM

More at www.hivepro.com