Hive Pro

Threat Level

Red

CISA: AA23-129A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

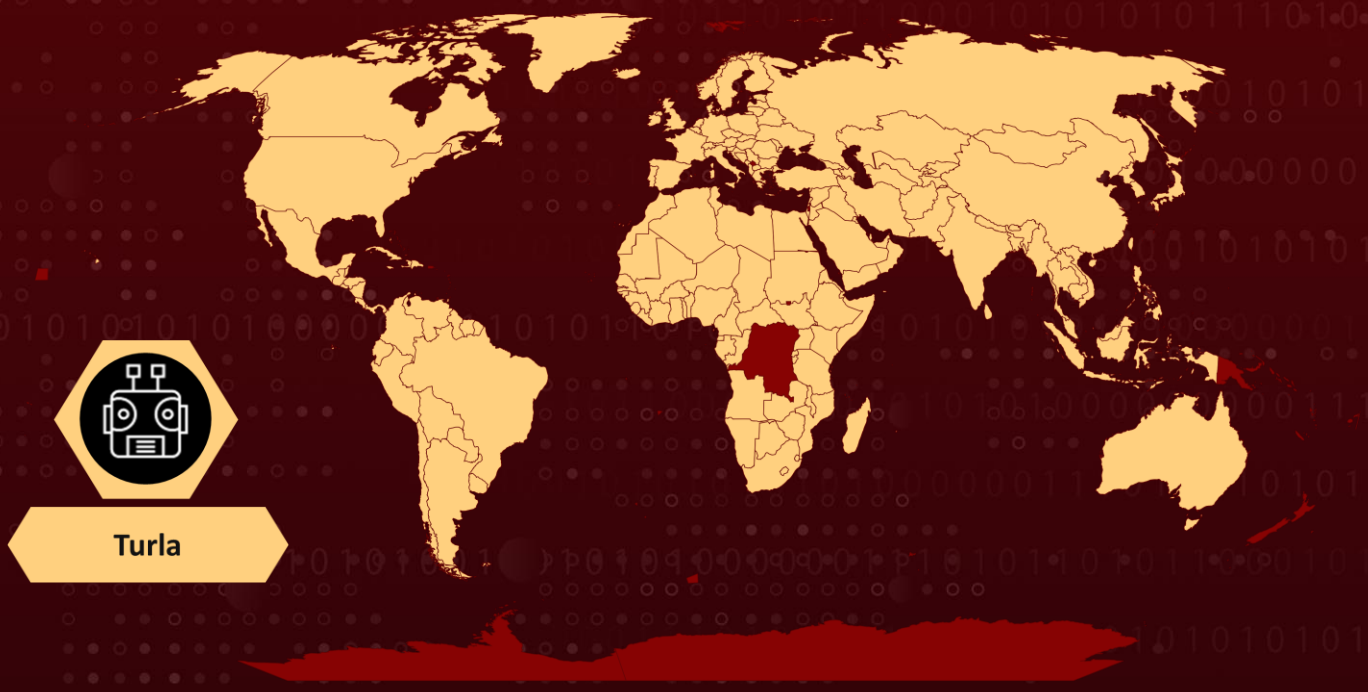
Snake a Stealthy Cyber-Espionage Malware

Date of Publication	Admiralty Code	TA Number
May 10, 2023	A3	TA2023221

Summary

First seen: 2003
Threat Actor: Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)
Cyber Espionage Tool: Snake (aka Uroburos, Urouros)
Affected OS: Windows, MacOS, and Linux
Targeted Regions: North America, South America, Europe, Africa, Asia, and Australia.
Targeted Industries: Research facilities, Education, Small Businesses, Media organizations, Government facilities, Financial Services, Manufacturing, and Communications.
Attack: Snake is a powerful cyber-espionage malware developed by FSB & linked to Turla hackers. Boasts high stealth, rigorous engineering & global reach.

Attack Regions



Attack Details

#1 Snake is a sophisticated piece of cyber-espionage malware that was developed by Russia's Federal Security Service (FSB). The malware, previously known as "Uroburos," was developed in late 2003 and finalized by early 2004. It is believed to be associated with the Turla hacking group, which is a part of the FSB's Centre 16. One of Snake's primary capabilities is its ability to achieve an unusual amount of stealth in both its host components and network communications.

#2 Additionally, its internal technological architecture is designed to enable the simple integration of new or replacement components, allowing it to operate on a range of host operating systems. Finally, Snake's implementation and software engineering design is rigorous, with the implant exhibiting a remarkably low number of errors given its complexity.

#3 Snake employs two major methods for communication and command execution: passive and active. Typically, Snake operators use active operations to connect with hop points within the malware's infrastructure. However, hop points may occasionally utilize Snake's passive approach. On the other hand, Snake's endpoints almost exclusively use the passive approach.

Recommendations

- Utilize memory analysis tools, such as Volatility, to detect and analyze potential Snake compromises. To detect any potential compromise, it is recommended to utilize **the mitigation rules** provided by CISA.
- Routinely change all credentials and avoid using similar passwords and usernames to previous ones.
- Apply updates to operating systems to increase kernel space security, making it more difficult for adversaries to operate within the system.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	T1095 Non-Application Layer Protocol	T1104 Multi-Stage Channels	T1106 Native API
T1001 Data Obfuscation	T1001.003 Protocol Impersonation	T1003 OS Credential Dumping	T1014 Rootkit
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1036 Masquerading	T1040 Network Sniffing
T1046 Network Service Discovery	T1055 Process Injection	T1055.001 Dynamic-link Library Injection	T1056 Input Capture
T1056.001 Keylogging	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1071.003 Mail Protocols	T1071.004 DNS	T1074 Data Staged
T1078 Valid Accounts	T1083 File and Directory Discovery	T1090 Proxy	T1090.003 Multi-hop Proxy
T1112 Modify Registry	T1119 Automated Collection	T1132 Data Encoding	T1132.002 Non-Standard Encoding
T1135 Network Share Discovery	T1140 Deobfuscate/Decode Files or Information	T1190 Exploit Public-Facing Application	T1482 Domain Trust Discovery
T1546 Event Triggered Execution	T1546.016 Installer Packages	T1547.006 Kernel Modules and Extensions	T1559 Inter-Process Communication
T1560.003 Archive via Custom Method	T1564 Hide Artifacts	T1569.002 Service Execution	T1570 Lateral Tool Transfer
T1572 Protocol Tunneling	T1573 Encrypted Channel	T1588 Obtain Capabilities	T1610 Deploy Container

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6a4836cd5847c3d42b846d1616cc94429ec27446555b66f9abf061e7747bdca0 3c3511a9b6d98f49943cbec9355ebb8a006706f42304f608b6d9eb6f2da79718 735808b3dfad2472c5785399b6e34bf5cccef1153ad15bd1167420ff05b1a9d8 ff51c7ab066f425f73ba2005dbf3d2be4bc5344b152f18818c0ea5da81368ef0 1c05f794c40193734a68e145ca1aaf7268b37f6fe3ea2bea5f12aa2ceb24ee60 a693fe103b7177f431889a2116a5b48cd3f59a1663667bdc6bd62920be14357e 7b9c6745870b51dbf676ddc45b91ab5b241768a614c74689e96af73a4836f136 b4a93ba9ec9dad5f5a8eb01d58ddcbb3ebc60182ed040272ae295a1ce0a53b50 088ec7b0c8c7b697a2236dbb3966bd9f03c47f63a608e2455862f30bf712635f 41eeced2b87d5e4a4b46326c14e0890a24fc17e99d82f16fd5b5976c3ab66598 10b854d66240d9ee1ce4296d2f7857d2b1c6f062ca836d13d777930d678b3ca6 55047d88678f22d87a5fcec2a27d043d028102f49362c2ca6598b2fc056d8c80

References

https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_1.pdf

https://attack.mitre.org/software/S0022/

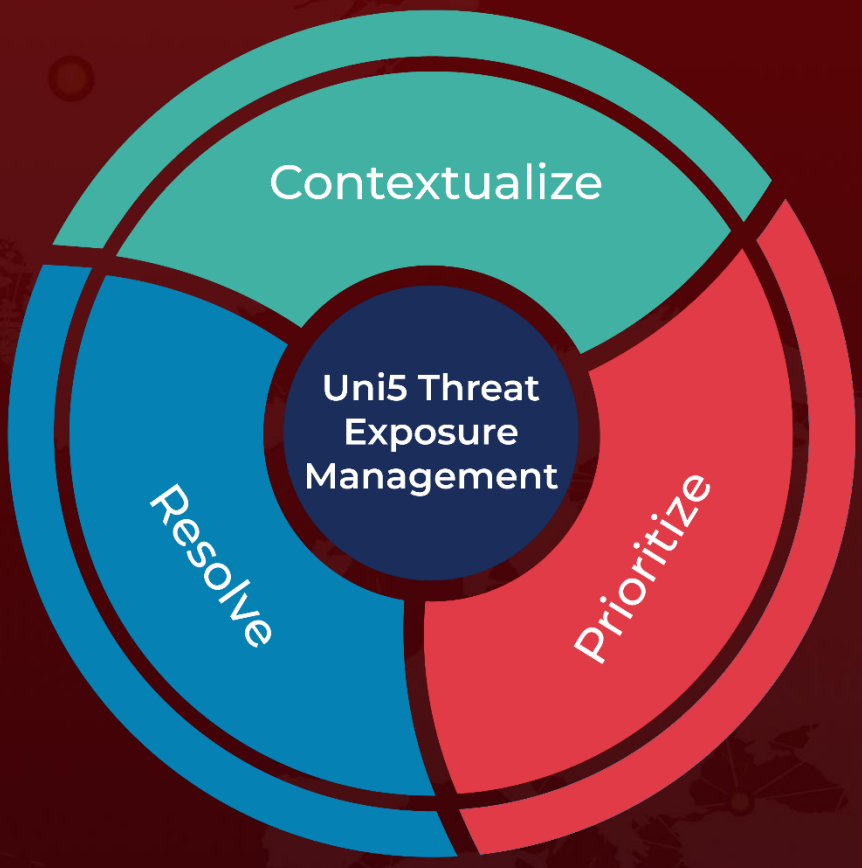
https://attack.mitre.org/groups/G0010/

https://valhalla.nextron-systems.com/info/rule/Turla_Snake_Malware

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

May 10, 2023 • 8:21 AM

More at www.hivepro.com