Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

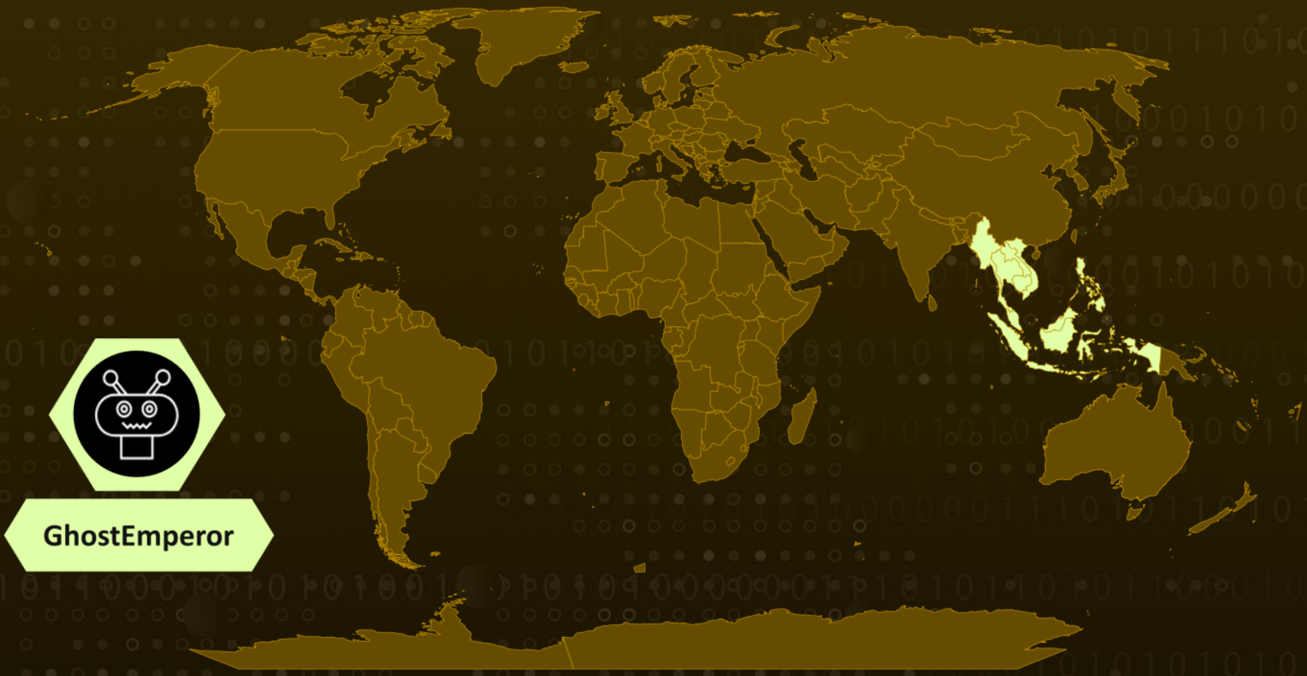
GhostEmperor the Threat Actor Who Outwits Security Measures

Date of Publication	Admiralty Code	TA Number
July 25, 2024	A1	TA2024285

Summary

First Seen: 2020
Threat Actor: GhostEmperor
Malware: Demodex Rootkit
Targeted Countries: Brunei, Cambodia, EastTimor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam
Targeted Industries: Telecommunications and Government
Attack: GhostEmperor, a highly sophisticated Chinese-speaking cyber threat actor, has been executing advanced cyber-espionage campaigns since 2020. Primarily targeting government entities and telecom companies in Southeast Asia, this group is renowned for its unique arsenal of cyber tools and techniques, which are designed to establish persistence and evade detection on compromised systems.

Attack Regions



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

Attack Details

#1 GhostEmperor is a sophisticated Chinese-speaking threat actor known for its advanced cyber-espionage campaigns since 2020, targeting government entities and telecom companies in Southeast Asia. This group employs a unique arsenal of tools and techniques, focusing on establishing persistence and evading detection on compromised systems.

#2 A distinctive feature of GhostEmperor's operations is their use of a Windows kernel-mode rootkit known as Demodex, enabling deep infiltration and stealth. Their campaigns are meticulously planned and executed, often exploiting zero-day vulnerabilities in internet-facing applications or spear-phishing campaigns to gain initial access.

#3 Upon gaining initial access, GhostEmperor deploys custom malware to establish a persistent presence. The Demodex rootkit, a critical component of their toolkit, operates at the kernel level, making it extremely difficult to detect and remove. This sophisticated rootkit uses advanced techniques to avoid detection, including EDR evasion and a reflective loader to execute the Core-Implant.

#4 Throughout their attacks, GhostEmperor maintains a low profile, using advanced evasion techniques such as process hollowing, memory-resident malware, and legitimate Windows tools to minimize their footprint. In 2023, GhostEmperor continued to use stealth techniques and the Demodex rootkit, with some alterations in the infection chain and a slightly different C++ DLL variant.

Recommendations

Enhance Email Security Measures: Implement robust email filtering solutions to detect and block malicious attachments, such as ZIP and .lnk files. Educate users about phishing tactics and the dangers of opening attachments from unknown or suspicious sources.

Utilize Behavioral Analytics: Leverage behavioral analytics to detect unusual activities and potential signs of compromise, such as abnormal process behavior or unexpected network traffic.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration	T1190 Exploit Public-Facing Application
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1204 User Execution
T1047 Windows Management Instrumentation	T1543 Create or Modify System Process	T1055 Process Injection	T1055.012 Process Hollowing
T1027 Obfuscated Files or Information	T1070 Indicator Removal	T1014 Rootkit	T1082 System Information Discovery
T1041 Exfiltration Over C2 Channel	T1573 Encrypted Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4bb191c6d3a234743ace703d7d518f8f, 95e3312de43c1da4cc3be8fa47ab9fa4, d8ebfd26bed0155e7c4ec2ca429c871d
SHA1	43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de, a59cca28205eeb94c331010060f86ad2f3d41882, bab2ae2788dee2c41065850b2877202e57369f37
Domain	imap[.]dateupdata[.]com
IPv4	193[.]239[.]86[.]168

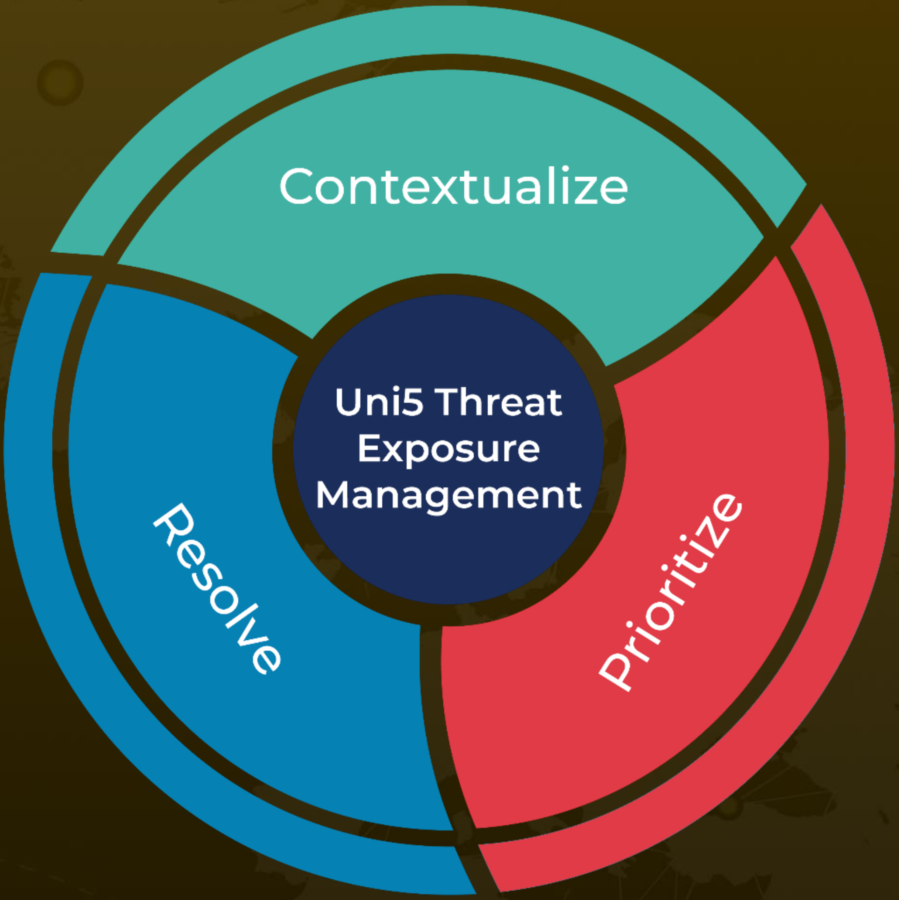
References

https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/

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

July 25, 2024 • 8:00 AM

More at www.hivepro.com