Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Redfly Targets Critical Infrastructure in Asia with ShadowPad Trojan

Date of Publication	Admiralty Code	TA Number
September 18, 2023	A1	TA2023376

Summary

First Appearance: February, 2023
Attack Region: Asia
Affected Industries: Windows
Actor Name: Redfly
Malware: ShadowPad, Packerloader
Attack: Redfly, an espionage group, targeted Asian critical infrastructure, compromising a national grid for six months using ShadowPad. This underscores a rising trend in such attacks, raising global concerns. Their operation involved stealing credentials, maintaining persistence, and compromising multiple computers.

Attack Regions

Attack Details

#1

Redfly is an espionage actor group that has been targeting critical national infrastructure (CNI) across Asia, compromising a national grid for up to six months using the ShadowPad Trojan. This attack is part of a rising trend in CNI targeting by threat actors, posing significant concerns for governments and organizations globally. Redfly's operation involved stealing credentials, maintaining persistence, and compromising multiple computers on the network.

#2

The ShadowPad Trojan, a modular remote access tool, was utilized in this attack, with a variant of it using the domain websencl[.]com for command-and-control purposes. Additionally, the attackers employed the Packerloader tool to load and execute shellcode and a keylogger to capture keystrokes.

#3

The timeline of the attack reveals the intruders' persistent presence, beginning in February 2023 and continuing until August 2023. They conducted various activities, including credential theft, registry manipulation, and DLL side-loading, suggesting a well-coordinated and sustained operation.

#4

The increase in attacks against CNI in recent years is a growing concern, as threat actors can disrupt power supplies and essential services during periods of heightened political tension. Although there is no evidence of disruptive activity by Redfly in this case, the threat remains, given past instances of CNI attacks.

#5

Governments and CNI organizations worldwide need to remain vigilant and enhance their cybersecurity measures to protect critical infrastructure from persistent threats like Redfly.

Recommendations

Network Segmentation: Implement strong network segmentation to isolate critical systems from less critical ones. This can prevent lateral movement by attackers within the network.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Employ advanced IDS and IPS solutions to monitor network traffic for suspicious activity and block known threats. These systems can help detect and stop attacks in real-time.

Endpoint Security: Use robust endpoint protection solutions that include antivirus, anti-malware, and behavior-based detection to safeguard individual devices from malware and other threats.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0011 Command and Control	TA0005 Defense Evasion	TA0003 Persistence
TA0002 Execution	TA0040 Impact	TA0002 Execution	TA0009 Collection
T1584 Compromise Infrastructure	T1036 Masquerading	T1027 Obfuscated Files or Information	T1203 Exploitation for Client Execution
T1059 Command and Scripting Interpreter	T1486 Data Encrypted for Impact	T1140 Deobfuscate/Decode Files or Information	T1012 Query Registry
T1573.001 Symmetric Cryptography	T1573 Encrypted Channel	T1055.001 Dynamic-link Library Injection	T1055 Process Injection
T1056.001 Keylogging	T1056 Input Capture	T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow
T1059.001 PowerShell			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	websencl[.]com
Filepath	%SYSTEMROOT%\Intel\record.log
SHA256	73993d3b9aebf8dee50a144cf7e56b49d222a42600171df62c13d3f96824db60, 01f4e6f32070234b4203507be22cfb9d3d73b4bbd5100f62271e2161ec8813b7, 8dbc8b756cb724e2d6dc9c7c40f22c48022a8ee48da6685c4ccf580c6b5183cf, 2e642afdd36c129e6b50ae919ca608ac0006ce337f2a5a7a6fb1eef6a4ad99e7, 32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a, 16f413862efda3aba631d8a7ae2bfff6d84acd9f454a7adaa518c7a8a6f375a5, 656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c, ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646, 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3, d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3

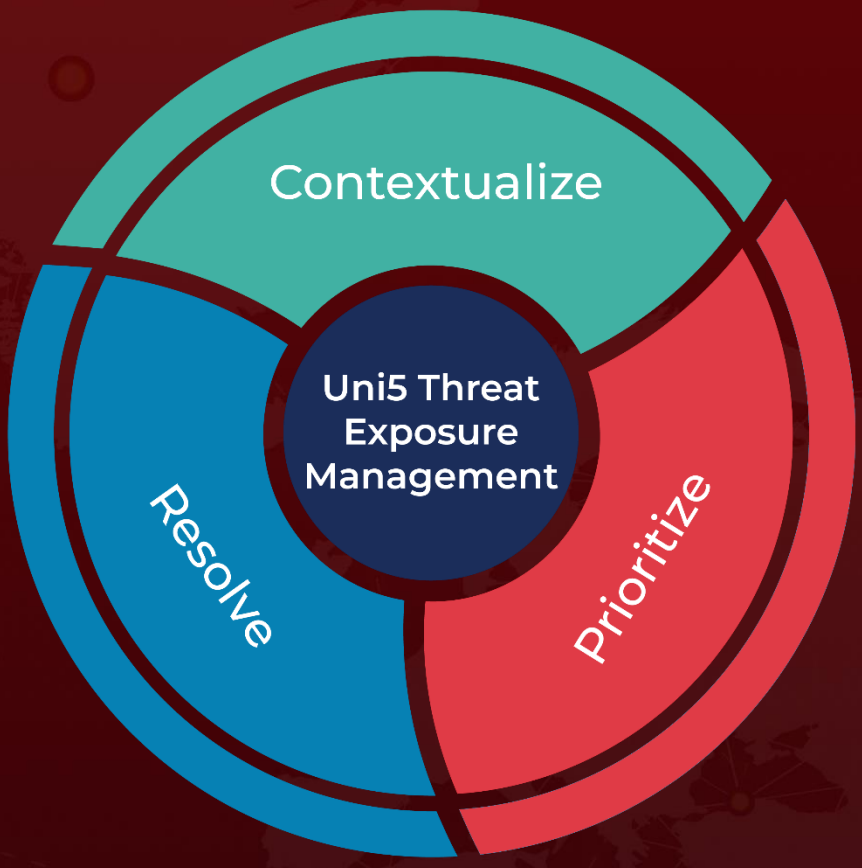
References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks

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 18, 2023 . 8:30 AM

More at www.hivepro.com