Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Breaking Down Andariel APT's Strike on South Korean Entities

Date of Publication	Admiralty Code	TA Number
May 21, 2024	A1	TA2024198

Summary

Threat Actor: Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)
Malware: Dora RAT, Nestdoor
Attack Region: South Korea
Targeted Industries: Construction, Manufacturing, Education
Attack: The Andariel APT group orchestrated a cyberattack targeting South Korean manufacturing, construction, and educational companies. They employed the Dora RAT, a backdoor like Nestdoor, and proxy tools to penetrate systems, extract data, and potentially control compromised machines.

Attack Regions

Attack Details

#1 The **Andariel** APT group conducted a sophisticated cyberattack using the Dora RAT, a backdoor like Nestdoor, and proxy tools to infiltrate systems, exfiltrate data, and potentially control compromised machines. This campaign specifically targeted South Korean companies, affecting the manufacturing, construction, and educational sectors.

#2 A significant aspect of the attack involved distributing malicious code by compromising a web server running Apache Tomcat, originally established in 2013 to spread such code. Among the deployed malware was Nestdoor, a backdoor first identified in May 2022.

#3 Nestdoor enables attackers to control an infected system through received commands and is a frequent arsenal in the Andariel group's operations. Nestdoor maintains persistence by registering itself with the task scheduler and communicating with a C&C server.

#4 Additionally, the attackers introduced a new malware, Dora RAT, developed in the Go language. Dora RAT is relatively simple, supporting reverse shell and file download/upload functions. It exists in two variants: one as a standalone executable and another injected into the explorer.exe process.

#5 Interestingly, a proxy tool previously linked to Lazarus group activities was also employed. Although not the same file, it shares an identical code size, routine, and authentication strings, suggesting possible collaboration or shared resources between these threat actors.

Recommendations

Exercise caution when interacting with online content: Avoid opening untrusted links and email attachments unless their authenticity has been verified through reliable sources.

Monitor Network Traffic: Implement robust network monitoring solutions to detect suspicious activities, such as unusual data exfiltration or communication with known malicious domains, indicative of a cyberattack.

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.

Secure Configuration Management: Enforce secure configuration management practices to harden systems and devices against common attack vectors, reducing the likelihood of successful exploitation by APT actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**TA0040** Impact	**T1113** Screen Capture	**T1056.001** Keylogging
T1584 Compromise Infrastructure	**T1584.004** Server	**T1566** Phishing	**T1204** User Execution
T1055 Process Injection	**T1027** Obfuscated Files or Information	**T1049** System Network Connections Discovery	**T1082** System Information Discovery
T1057 Process Discovery	**T1560** Archive Collected Data	**T1005** Data from Local System	**T1056** Input Capture
T1115 Clipboard Data	**T1657** Financial Theft	**T1053.005** Scheduled Task	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	7416ea48102e2715c87edd49ddbd1526, a2aefb7ab6c644aa8eeb482e27b2dbc4, e7fd7f48fbf5635a04e302af50dfb651, 33b2b5b7c830c34c688cf6ced287e5be, 4bc571925a80d4ae4aab1e8900bf753c, 951e9fcd048b919516693b25c13a9ef2, fee610058c417b6c4b3054935b7e2730, afc5a07d6e438880cea63920277ed270, d92a317ef4d60dc491082a2fe6eb7a70, 5df3c3e1f423f1cce5bf75f067d1d05c, 094f9a757c6dbd6030bc6dae3f8feab3, 468c369893d6fc6614d24ea89e149e80, 5e00df548f2dcf7a808f1337f443f3d9
Domain	kmobile[.]bestunif[.]com
IPv4:Port	45[.]58[.]159[.]237[:]443, 4[.]246[.]149[.]227[:]1443, 209[.]127[.]19[.]223[:]443, 206[.]72[.]205[.]117[:]443

References

https://asec-ahnlab-com.translate.goog/ko/65495/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

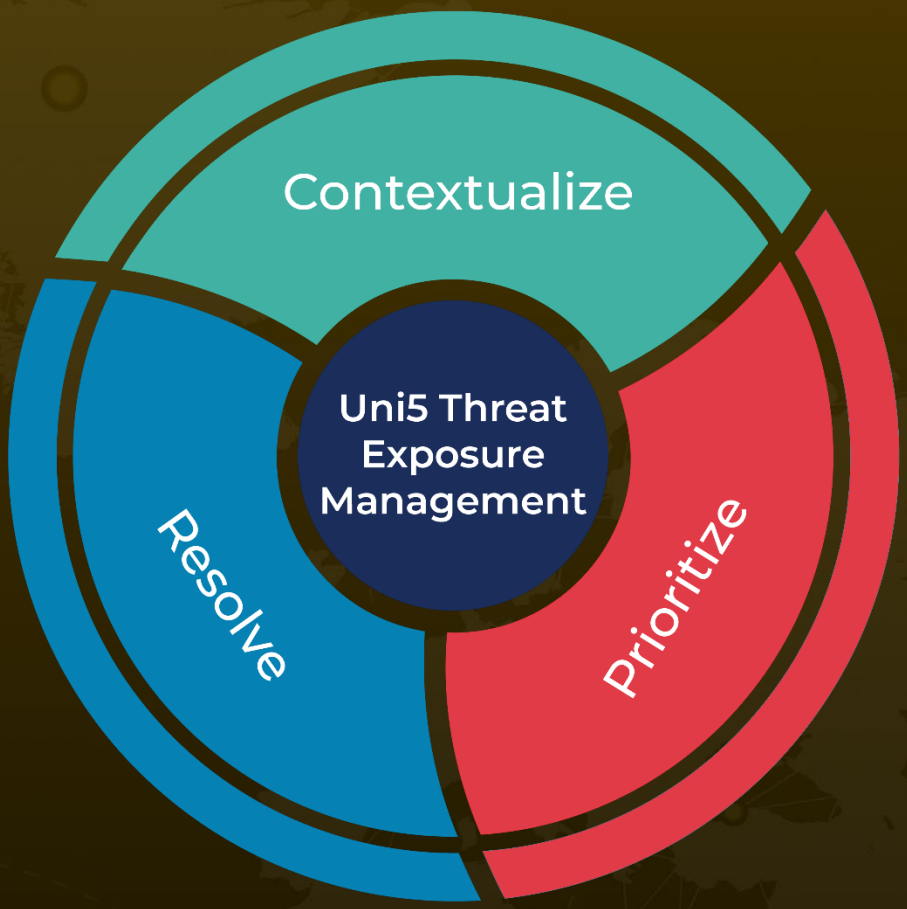
https://asec.ahnlab.com/ko/65495/

https://www.hivepro.com/threat-advisory/andariel-group-unleashes-new-earlyrat-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 21, 2024 • 9:00 PM

More at www.hivepro.com