Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

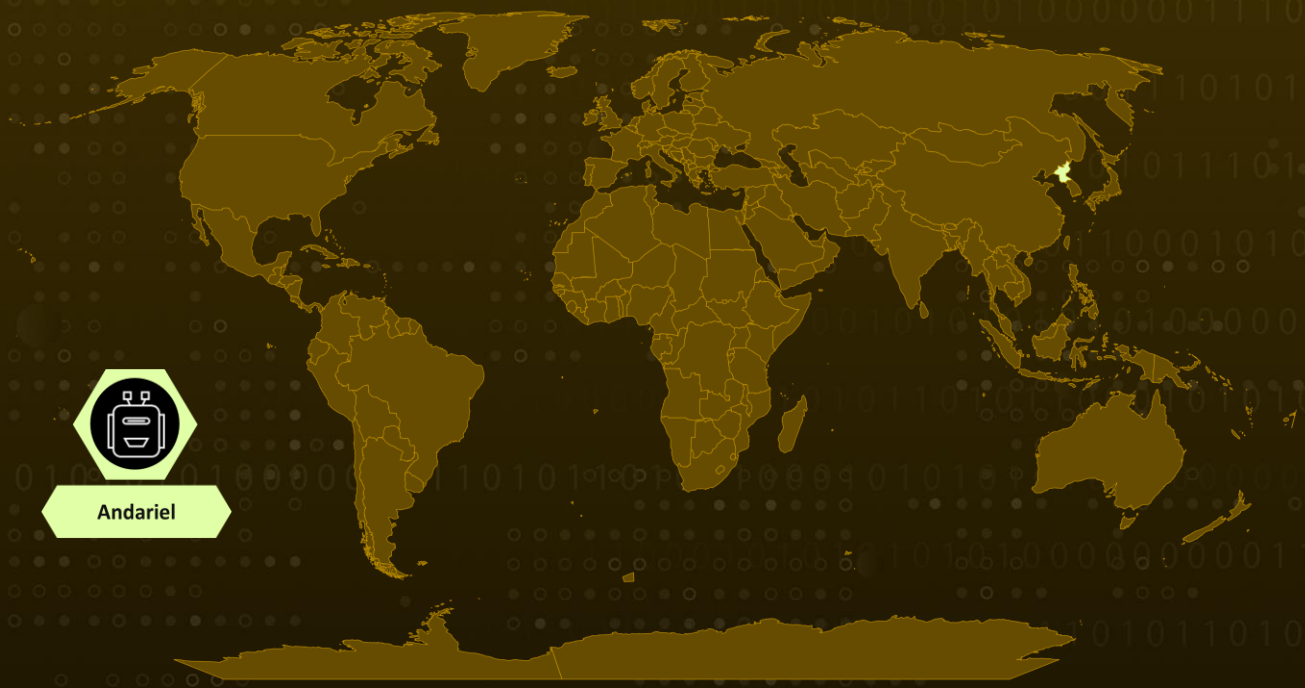
Andariel group unleashes New EarlyRat Malware

Date of Publication	Admiralty Code	TA Number
June 30, 2023	A1	TA2023284

Summary

First Appearance: 2009
Actor Name: Andariel (aka DarkSeoul, Silent Chollima, Onyx Sleet, OperationTroy, Guardian of Peace, GOP, WHOis Team)
Target Countries: Primarily South Korea
Target Sectors: Government Agencies, Military Organizations, Financial Services
Actor Details: Andariel is a sub-group of Lazarus and is remarkably stealthy in its operation. Recently they have developed new malware called EarlyRat.

Actor Map



Actor Details

#1 Andariel is a subgroup of the Lazarus group and has been active since 2009. It started with Information Theft and Cyber Espionage activities mainly in defense sector, However after 2016, It shifted focus to monetary gain purpose and was engaged in Ransomware attacks, attacks in banking sector and Technology sector.

#2 Andariel employs various attack vectors, including Spear-Phishing, Watering hole, and Supply chain tactics. They have created their own malwares like Rifdoor, and Phandoor for cyber operations and have recently developed new malware called EarlyRat.

#3 Andariel actively exploited log4j vulnerability last year and this new Malware was discovered on one of the log-4j exploit affected system. However, Attack vector for EarlyRat is found to be Spear Phishing.

#4 EarlyRat is very simple in design and can execute given commands. It is found to be similar to MagicRat. It was dropped by a spear phishing campaign from HolyGhost / Maui ransomware campaign servers, involving macro enabled document. Once executed, It post system information to C2 server.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Andariel	North Korea **MOTIVE** Espionage, Monetary Gains	North Korea	Government Agencies, Military Organizations, Financial Services

Recommendations

Educate employees on how to recognize and report suspicious activity, including phishing emails and other social engineering tactics used by Andariel. Regular security awareness training can help improve overall cybersecurity posture.

Keep all software and systems up-to-date with the latest security patches and updates to mitigate against known vulnerabilities that may be exploited by adversaries.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**T1587** Develop Capabilities	**T1587.001** Malware	**TA0001** Initial Access
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1190** Exploit Public-Facing Application	**TA0002** Execution
T1204.002 Malicious File	**TA0009** Collection	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell
TA0003 Persistence	**T1547** Boot or Logon Autostart Execution	**TA0011** Command and Control	**T1132** Data Encoding

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	226.132.219[.]125 74.124.228[.]148

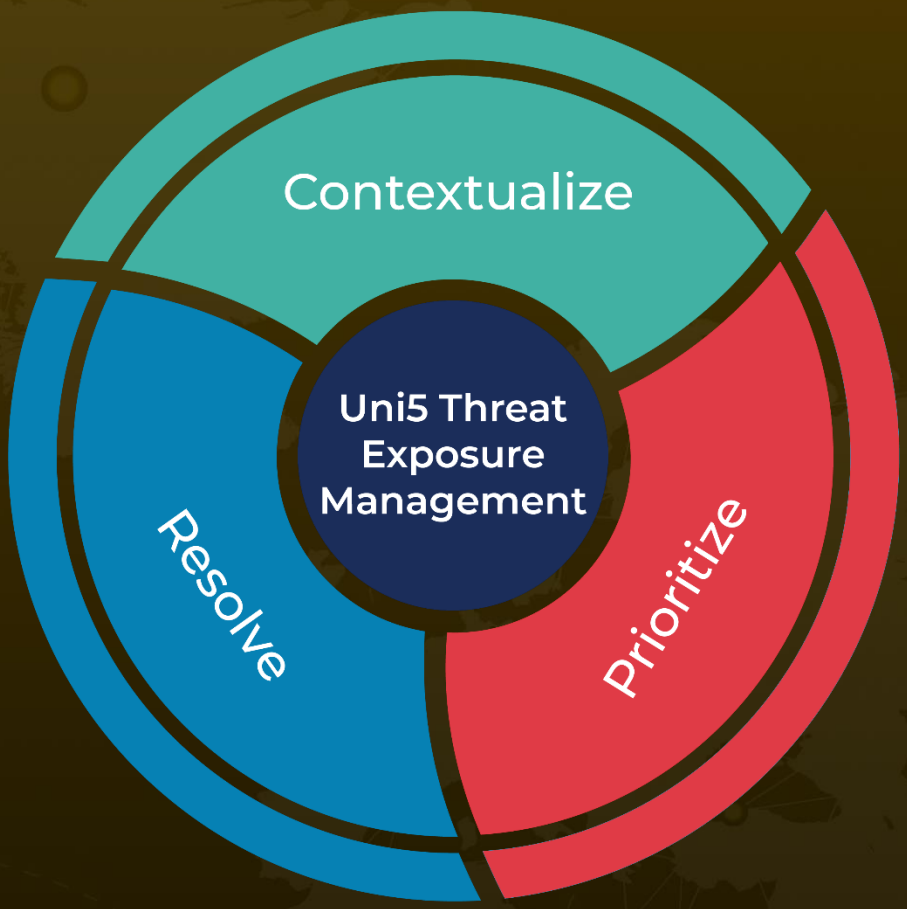
References

https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/

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

June 30, 2023 • 09:30 AM

More at www.hivepro.com