Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

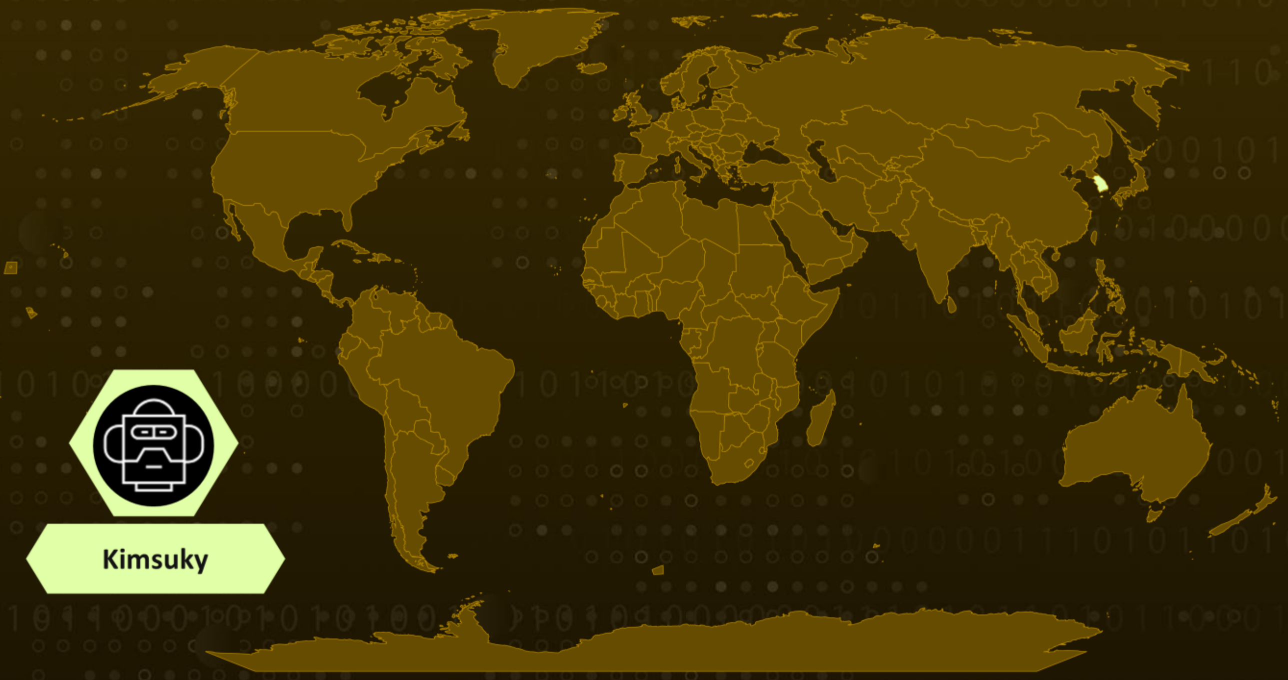
Kimsuky Expands Its Arsenal with New Backdoor

Date of Publication	Admiralty Code	TA Number
May 17, 2024	A1	TA2024192

Summary

Discovered: February 2024
Attack Region: South Korea
Affected Platform: Linux
Targeted Industries: Government
Actor: Kimsuky (aka Velvet Chollima, Springtail, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082)
Malware: Gomir, Troll Stealer, GoBear
Attack: The North Korean hacker group Kimsuky has been deploying a new Linux malware named Gomir, which is a variant of the GoBear backdoor, in their recent campaign targeting government organizations in South Korea. Gomir is nearly identical in structure to GoBear, with significant code sharing between the two malware. It is delivered via trojanized software installers, highlighting the persistent threat from Kimsuky to South Korean entities.

Attack Regions



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

Attack Details

#1 The North Korean cyber-espionage group Kimsuky has developed a new Linux backdoor called Gomir. This malware has been linked to recent attacks on South Korean government organizations. Kimsuky, known for targeting public sector organizations in South Korea, first gained attention in 2014. The group conducts spear-phishing campaigns by posing as journalists, academics, and experts in East Asian affairs with credible ties to North Korean policy circles.

#2 In February 2024, South Korean security firm S2W documented a Kimsuky campaign that introduced a new malware family named Troll Stealer via Trojanized software installation packages. Troll Stealer can steal various types of information from infected computers, including files, screenshots, browser data, and system information. Written in the Go programming language, it shares code with previous Kimsuky malware and can copy the Government Public Key Infrastructure (GPKI) folder from infected computers, suggesting a focus on government agencies.

#3 In the previous campaign, Kimsuky used Troll Stealer and GoBear, both signed with legitimate certificates. In their recent campaign, they employed GoBear's Linux variant called Gomir. Gomir is similar to the Windows-based GoBear backdoor but adapts or omits features dependent on the operating system. It installs itself with persistence and checks for superuser privileges. If it detects such privileges, it establishes persistence by creating a systemd service, starts it, deletes its original executable, and terminates the initial process. In the absence of superuser privileges, it sets up a crontab entry for persistence.

#4 Gomir facilitates the execution of 17 distinct commands including, pausing communication, executing shell commands, reporting the current working directory, probing network endpoints, terminating its process, reporting executable pathnames, collecting statistics, configuring a fallback shell, pausing communication until a specified date and time, starting a reverse proxy, creating arbitrary files, and extracting files from the system.

#5 Kimsuky's latest campaign highlights the development of new Linux malware and the increasing use of software installation packages and updates as infection vectors by North Korean espionage actors. Kimsuky often targets software on third-party sites or pretends to be official applications.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Trusted Installers: Always download software from the official website of the software vendor. Avoid third-party websites as they may host tampered versions of the software.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1217 Browser Information Discovery
T1036 Masquerading	T1059 Command and Scripting Interpreter	T1057 Process Discovery	T1056 Input Capture
T1082 System Information Discovery	T1543 Create or Modify System Process	T1543.002 Systemd Service	T1053 Scheduled Task/Job

T1053.003 Cron	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1005 Data from Local System
T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1204 User Execution	T1204.002 Malicious File
T1189 Drive-by Compromise	T1070 Indicator Removal	T1070.004 File Deletion	T1529 System Shutdown/Reboot
T1546 Event Triggered Execution	T1546.016 Installer Packages		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213, 7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0, d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b, 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc, 8e45daace21f135b54c515dbd5cf6e0bd28ae2515b9d724ad2d01a4bf10f93bd, 6c2a8e2bbe4ebf1fb6967a34211281959484032af1d620cbab390e89f739c339, 47d084e54d15d5d313f09f5b5fcdea0c9273dcddd9a564e154e222343f697822, 8a80b6bd452547650b3e61b2cc301d525de139a740aac9b0da2150ffac986be4, 380ec7396cc67cf1134f8e8cda906b67c70aa5c818273b1db758f0757b955d81, ff945b3565f63cef7bb214a93c623688759ee2805a8c574f00237660b1c4d3fd, cc7a123d08a3558370a32427c8a5d15a4be98fb1b754349d1e0e48f0f4cb6bfc,

TYPE	VALUE
SHA256	8898b6b3e2b7551edcceffbef2557b99bdf4d99533411cc90390eeb278d11ac8, ecab00f86a6c3adb5f4d5b16da56e16f8e742adfb82235c505d3976c06c74e20, d05c50067bd88dae4389e96d7e88b589027f75427104fdb46f8608bbcf89edb4, a98c017d1b9a18195411d22b44dbe65d5f4a9e181c81ea2168794950dc4cbd3c, 831f27eb18caf672d43a5a80590df130b0d3d9e7d08e333b0f710b95f2cde0e0, bc4c1c869a03045e0b594a258ec3801369b0dcabac193e90f0a684900e9a582d, 5068ead78c226893df638a188fbe7222b99618b7889759e0725d85497f533e98
IPv4	216[.]189[.]159[.]34

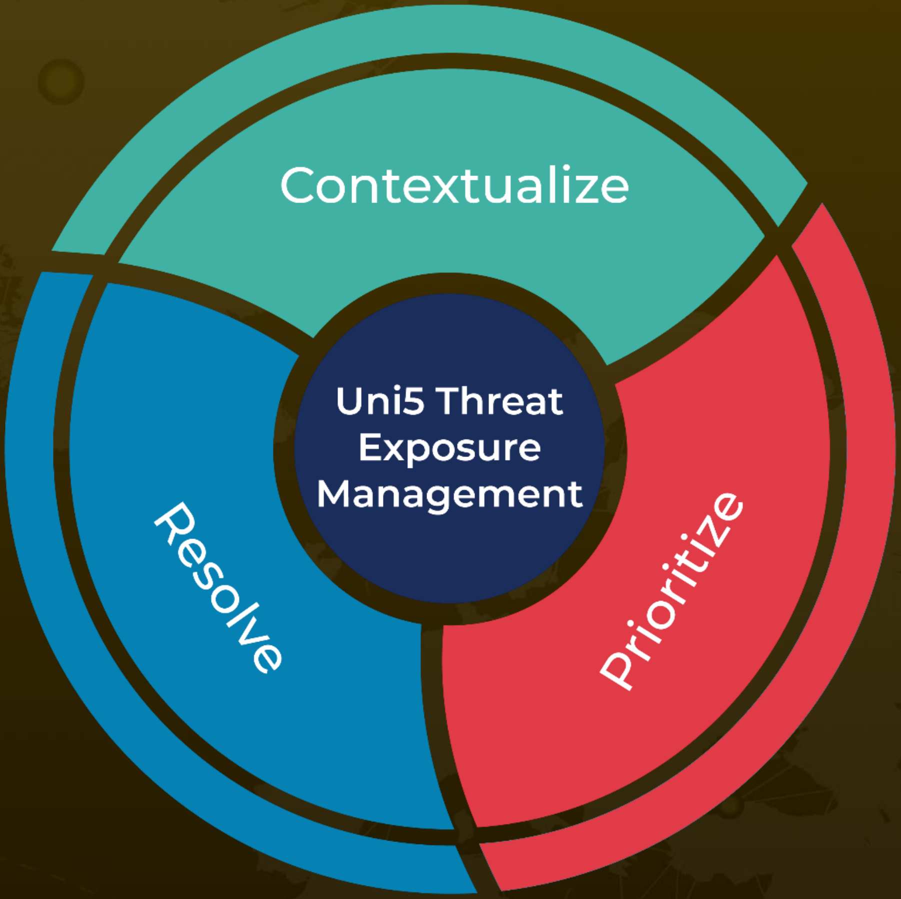
References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage

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 17, 2024 • 7:30 AM

More at www.hivepro.com