Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Kimsuky Disseminate TrollAgent Leveraging Stolen Certificates

Date of Publication	Admiralty Code	TA Number
February 21, 2024	A1	TA2024068

Summary

First appeared: December 2023
Attack Region: Korean countries
Malware: TrollAgent
Threat Actor: Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)
Targeted Industries: Construction
Affected Platform: Windows
Attack: The Kimsuky group, backed by North Korea, used TrollAgent malware via a fake security program to target a Korean construction association's website, stealing data and enabling remote control between December 2023 and January 2024.

Attack Regions

Kimsuky group

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

Attack Details

#1

Kimsuky group has been targeting a Korean construction-related association's website. This attack involves the distribution of malware disguised as legitimate security programs during the installation process. Users logging into the website are prompted to install these security programs, unaware that one of them contains malicious code.

#2

The malicious code includes a backdoor malware allowing remote access to compromised systems and an infostealer known as "TrollAgent," which steals various sensitive information, including browser data. These malware instances are signed with valid certificates from a domestic defense company, aiming to bypass antivirus detection. The attack was active between December 2023 and January 2024.

#3

Furthermore, the attacker has a history of targeting nuclear power-related companies with similar tactics. To mitigate this threat, users are advised to update their security software promptly to prevent malware infection when installing programs from compromised websites.

Recommendations

Regular Software Updates: Ensure that all security software, including antivirus programs and web browsers, are regularly updated to their latest versions. Updated software often includes patches for known vulnerabilities and improved malware detection capabilities.

Exercise Caution: Exercise caution when prompted to install any software, especially from unfamiliar or suspicious sources. Verify the legitimacy of the software and its source before proceeding with the installation.

Enhanced Security Measures: Implement additional security measures such as endpoint protection, intrusion detection systems, and firewalls to help detect and prevent unauthorized access and malware infections.

Network Segmentation: Implement network segmentation strategies to isolate critical systems and separate computers running outdated operating systems. This helps contain potential infections and limits the spread of malware within the network

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0007 Discovery	TA0005 Defense Evasion
T1217 Browser Bookmark Discovery	TA0011 Command and Control	TA0009 Collection	TA0006 Credential Access
T1218.011 Rundll32	T1218 System Binary Proxy Execution	T1204 User Execution	T1204.002 Malicious File
T1036 Masquerading	T1584 Compromise Infrastructure	T1608.001 Upload Malware	T1608 Stage Capabilities
T1027.002 Software Packing	T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores	T1005 Data from Local System
T1480 Execution Guardrails	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	013c4ee2b32511b11ee9540bb0fdb9d1, 035cf750c67de0ab2e6228409ac85ea3, 19c2decfa7271fa30e48d4750c1d18c1, 27ef6917fe32685fdf9b755eb8e97565, 2aaa3f1859102aab35519f0d4c1585dd, 2b678c0f59924ca90a753daa881e9fd3, 4168ff8b0a3e2f7e9c96afb653d42a01, 4222492e069ac78a55d3451f4b9b9fca, 42ea65fda0f92bbeca5f4535155125c7, 6097d030fe6f05ec0249e4d87b6be4a6, 62fba369711087ea37ef0b0ab62f3372, 7457dc037c4a5f3713d9243a0dfb1a2c, 7b6d02a459fdaa4caa1a5bf741c4bd42, 87429e9223d45e0359cd1c41c0301836, 88f183304b99c897aacfa321d58e1840,

TYPE	VALUE
MD5	c8e7b0d3b6afa22e801cacaf16b37355, d67abe980a397a94e1715df6e64eedc8, dc636da03e807258d2a10825780b4639, E4a6d47e9e60e4c858c1314d263aa317, 9e75705b4930f50502bcbd740fc3ece1, a67cf9add2905c11f5c466bc01d554b0, b532f3dcc788896c4844f36eb6cee3d1, B97abf7b17aeb4fa661594a4a1e5c77f, 8d4af59eebdcda10f3c88049bb097a3a, 9360a895837177d8a23b2e3f79508059
SHA1	120891212a78114fe114217012c2a000727e034b, 3d1731fa03f2bb8b3ca74ab49c83923428e58362, 4a705f58918c00431de453d5b5f621fa42ff7169, 4c8b7d968806f8108ccde6ac07a37b8174ac44bf, 4eea45c22881a092ac7a8b0a5379076d5803e83e, 6d531b021b20febf1dafa730582944eb82d9c6f3, e6be97ca9e79b45c671c6531908f70b353d47994
SHA256	2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e, 61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92, 6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9, 955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b, a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9, f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3, ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca
URLs	hxxp://ai[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://ai[.]bananat[.]p-e[.]kr/index[.]php, hxxp://ai[.]daysol[.]p-e[.]kr/index[.]php, hxxp://ai[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://ai[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ai[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://ai[.]negapa[.]p-e[.]kr/index[.]php, hxxp://ai[.]selecto[.]p-e[.]kr/index[.]php, hxxp://ai[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ar[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ca[.]bananat[.]p-e[.]kr/index[.]php,

TYPE	VALUE
URLs	hxxp://pi[.]selecto[.]p-e[.]kr/index[.]php, hxxp://qa[.]jaychoi[.]p-e[.]kr/index[.]php, hxxp://qi[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://sa[.]netup[.]p-e[.]kr/index[.]php, hxxp://ve[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://viewer[.]appofficer[.]kro[.]kr/index[.]php, hxxp://ce[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://coolsystem[.]co[.]kr/admin/mail/index[.]php, hxxp://dl[.]netup[.]p-e[.]kr/index[.]php, hxxp://li[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ol[.]negapa[.]p-e[.]kr/index[.]php, hxxp://pe[.]daysol[.]p-e[.]kr/index[.]php

References

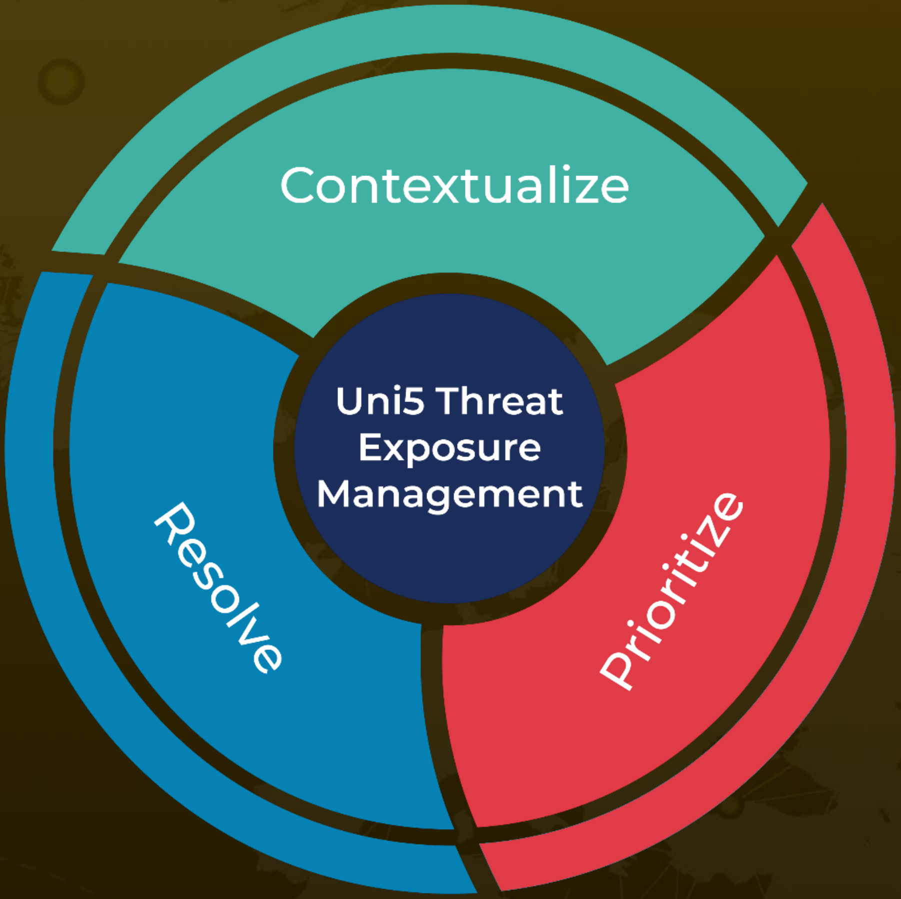
https://asec.ahnlab.com/ko/61666/

https://www.hivepro.com/threat-advisory/kimsuky-groups-intriguing-exploits-with-appleseed-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

February 21, 2024 • 4:30 AM

More at www.hivepro.com