Mar 19 2024

NETMANAGEIT

Intelligence Report

Exploiting Korean Asset Management Solutions (MeshAgent)

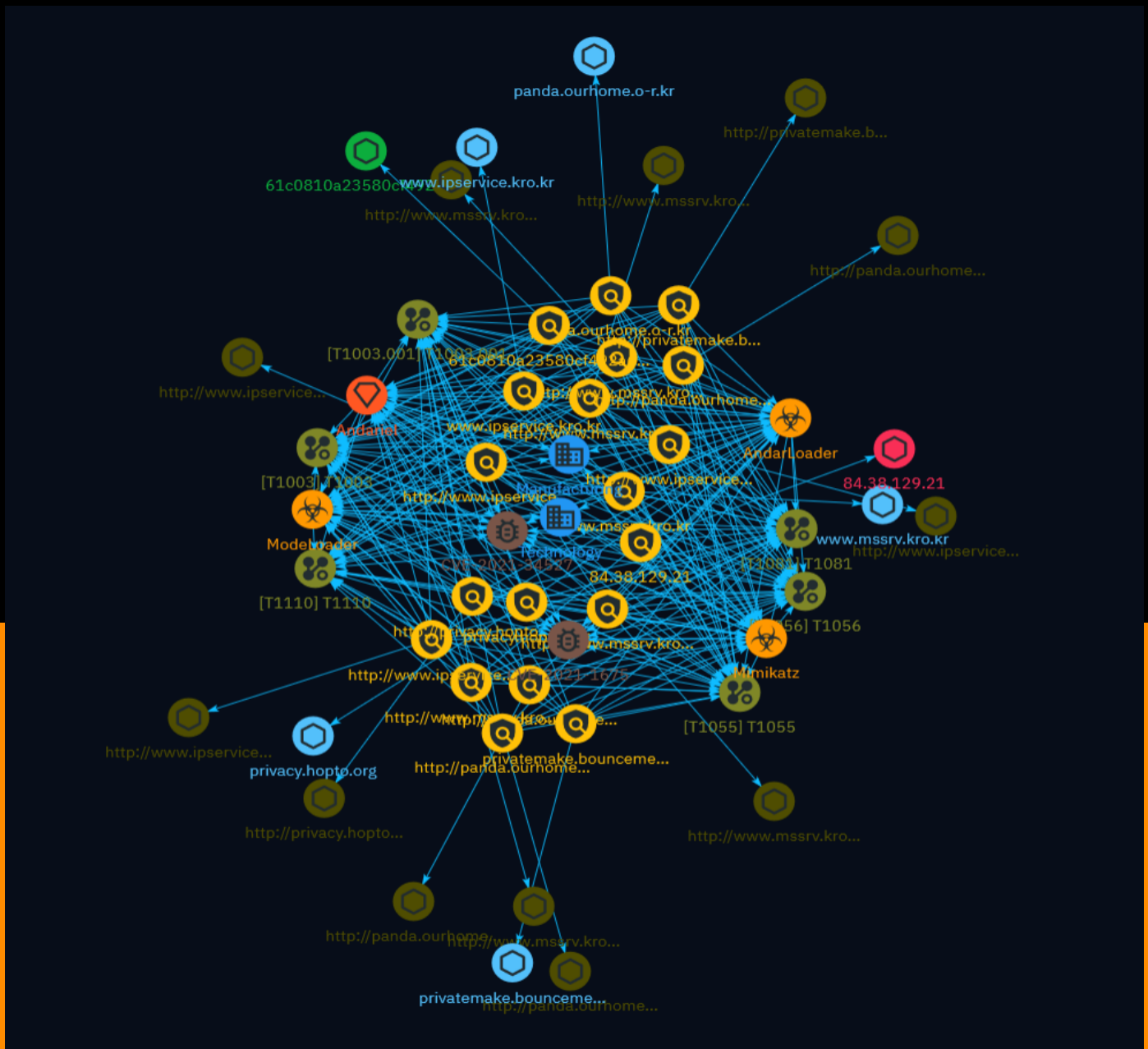

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Andariel group exploited Korean asset management solutions to install malware such as AndarLoader and ModeLoader. The group used solutions like MeshAgent for remote control. They installed backdoors, took control of systems, and stole credentials.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
www.mssrv.kro.kr
Pattern Type
stix
Pattern
[hostname:value = 'www.mssrv.kro.kr']
Name
privacy.hopto.org
Pattern Type
stix
Pattern
[hostname:value = 'privacy.hopto.org']
Name
panda.ourhome.o-r.kr

Pattern Type

stix

Pattern

[hostname:value = 'panda.ourhome.o-r.kr']

Name

http://www.mssrv.kro.kr/view.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** mssrv.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.mssrv.kro.kr/view.php']

Name

http://www.mssrv.kro.kr/modeView.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:**

True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** mssrv.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.mssrv.kro.kr/modeView.php']

Name

http://www.mssrv.kro.kr/modeWrite.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** mssrv.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.mssrv.kro.kr/modeWrite.php']

Name

http://www.mssrv.kro.kr/modeRead.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** mssrv.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.mssrv.kro.kr/modeRead.php']

Name

http://www.ipservice.kro.kr/view.php

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** ipservice.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.ipservice.kro.kr/view.php']

Name

http://www.ipservice.kro.kr/modeRead.php

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** ipservice.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.ipservice.kro.kr/modeRead.php']

Name

http://www.ipservice.kro.kr/index.php

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620017657, 'iso': '2021-05-03T00:54:17-04:00'} - **IPQS: Domain:** ipservice.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://www.ipservice.kro.kr/index.php']

Name

http://privatemake.bounceme.net:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 27720 - **DNS Valid:** True - **Parking:** False - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Internet Connection - **Domain Age:** {'human': '23 years ago', 'timestamp': 997410254, 'iso': '2001-08-09T22:24:14-04:00'} - **IPQS: Domain:** privatemake.bounceme.net - **IPQS: IP Address:** 158.247.7.206

Pattern Type

stix

Pattern

[url:value = 'http://privatemake.bounceme.net:443']

Name

http://panda.ourhome.o-r.kr/view.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1619448313, 'iso': '2021-04-26T10:45:13-04:00'} - **IPQS: Domain:** panda.ourhome.o-r.kr - **IPQS: IP Address:** 84.38.133.184

Pattern Type

stix

Pattern

[url:value = 'http://panda.ourhome.o-r.kr/view.php']

Name

http://privacy.hopto.org:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 9831 - **DNS Valid:** True - **Parking:** False - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '24 years ago', 'timestamp': 950817410, 'iso': '2000-02-17T14:56:50-05:00'} - **IPQS: Domain:** privacy.hopto.org - **IPQS: IP Address:** 158.247.7.206

Pattern Type

stix

Pattern

[url:value = 'http://privacy.hopto.org:443']

Name

http://panda.ourhome.o-r.kr/modeView.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1619448313, 'iso': '2021-04-26T10:45:13-04:00'} - **IPQS: Domain:** panda.ourhome.o-r.kr - **IPQS: IP Address:** 84.38.133.184

Pattern Type

stix

Pattern

[url:value = 'http://panda.ourhome.o-r.kr/modeView.php']

Name

http://panda.ourhome.o-r.kr/modeRead.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1619448313, 'iso': '2021-04-26T10:45:13-04:00'} - **IPQS: Domain:** panda.ourhome.o-r.kr - **IPQS: IP Address:** 84.38.133.184

Pattern Type

stix

Pattern

[url:value = 'http://panda.ourhome.o-r.kr/modeRead.php']

Name

61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1']

Name

84.38.129.21

Description

- **Zip Code:** N/A - **ISP:** DataClub - **ASN:** 203557 - **Organization:** DataClub - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** ip-129-21.dataclub.info - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Drenthe - **City:** Meppel - **Latitude:** 52.7 - **Longitude:** 6.18

Pattern Type

stix

Pattern

[ipv4-addr:value = '84.38.129.21']

Name

privatemake.bounceme.net

Pattern Type

stix

Pattern

[hostname:value = 'privatemake.bounceme.net']

Name

www.ipservice.kro.kr

Pattern Type

stix

Pattern

[hostname:value = 'www.ipservice.kro.kr']

Malware

Name
Mimikatz

Name
ModeLoader

Name
AndarLoader

Attack-Pattern

Name
T1081
ID
T1081
Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name

T1110

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

T1003.001

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate

Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as comsvcs.dll can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate

functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Vulnerability

Name
CVE-2021-1675
Description
Microsoft Windows Print Spooler contains an unspecified vulnerability that allows for remote code execution.
Name
CVE-2021-34527
Description
Microsoft Windows Print Spooler contains an unspecified vulnerability due to the Windows Print Spooler service improperly performing privileged file operations. Successful exploitation allows an attacker to perform remote code execution with SYSTEM privileges. The vulnerability is also known under the moniker of PrintNightmare.

Intrusion-Set

Name

Andariel

Description

[Andariel](https://attack.mitre.org/groups/G0138) is a North Korean state-sponsored threat group that has been active since at least 2009. [Andariel](https://attack.mitre.org/groups/G0138) has primarily focused its operations--which have included destructive attacks--against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. [Andariel](https://attack.mitre.org/groups/G0138)'s notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle. (Citation: FSI Andariel Campaign Rifle July 2017)(Citation: IssueMakersLab Andariel GoldenAxe May 2017)(Citation: AhnLab Andariel Subgroup of Lazarus June 2018)(Citation: TrendMicro New Andariel Tactics July 2018)(Citation: CrowdStrike Silent Chollima Adversary September 2021) [Andariel](https://attack.mitre.org/groups/G0138) is considered a sub-set of [Lazarus Group](https://attack.mitre.org/groups/G0032), and has been attributed to North Korea's Reconnaissance General Bureau.(Citation: Treasury North Korean Cyber Groups September 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Hostname

Value
www.mssrv.kro.kr
privacy.hopto.org
panda.ourhome.o-r.kr
www.ipservice.kro.kr
privatemake.bounceme.net

Url

Value
http://www.mssrv.kro.kr/view.php
http://www.mssrv.kro.kr/modeWrite.php
http://www.mssrv.kro.kr/modeView.php
http://www.mssrv.kro.kr/modeRead.php
http://www.ipservice.kro.kr/view.php
http://www.ipservice.kro.kr/modeRead.php
http://www.ipservice.kro.kr/index.php
http://privatemake.bounceme.net:443
http://privacy.hopto.org:443
http://panda.ourhome.o-r.kr/view.php
http://panda.ourhome.o-r.kr/modeView.php
http://panda.ourhome.o-r.kr/modeRead.php

IPv4-Addr

Value
84.38.129.21

StixFile

Value
61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1

External References

- https://asec.ahnlab.com/en/63192/
- https://otx.alienvault.com/pulse/65f98cc24ac62ec6d1ea3fff