Feb 19 2024

NETMANAGEIT

Intelligence Report

Kimsuky abuses a valid certificate to distribute TrollAgent

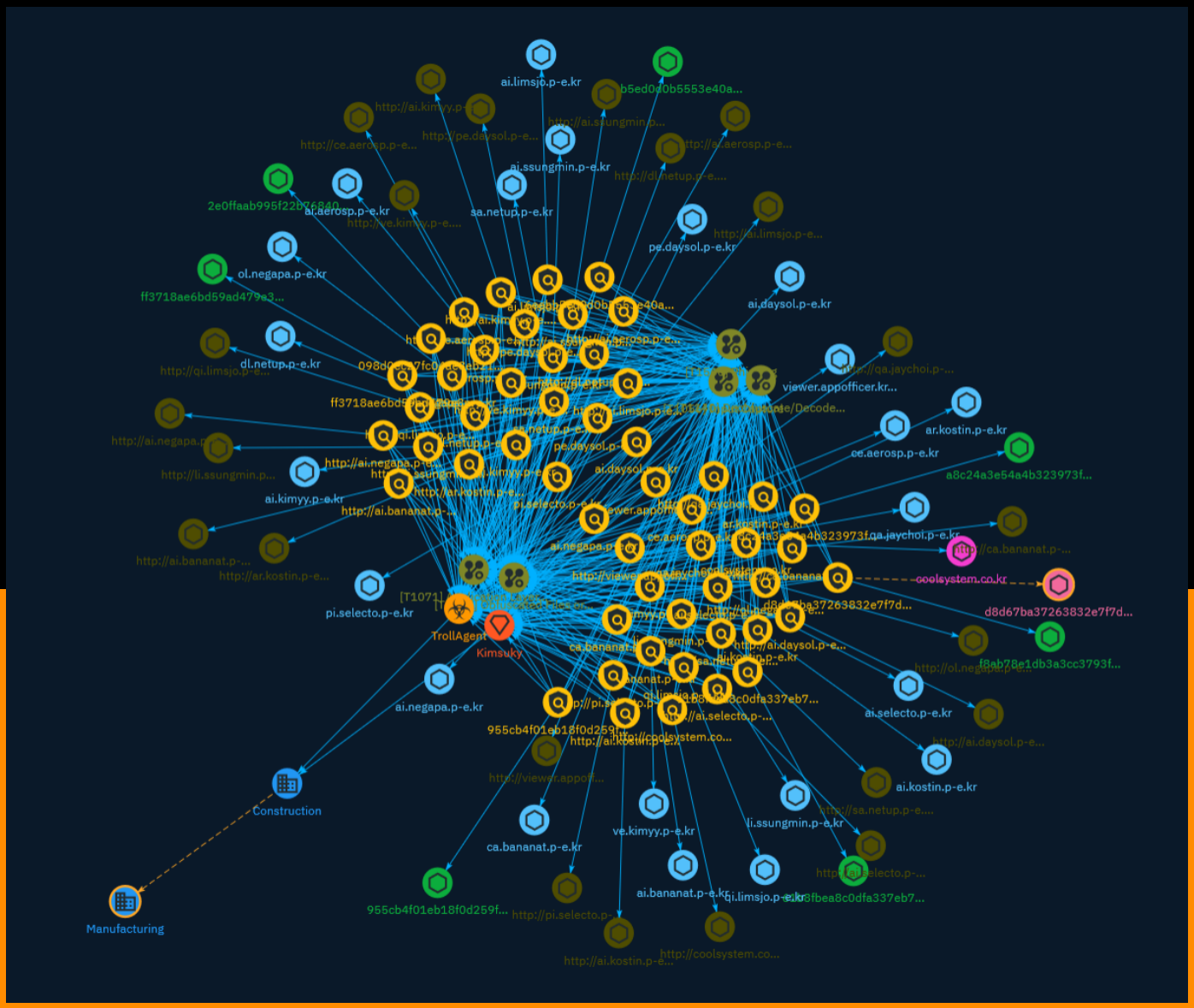

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 30
- Intrusion-Set 31
- Attack-Pattern 32
- Sector 36

Observables

- Hostname 37
- Domain-Name 39

- Url 40
- StixFile 42
- Artifact 43

External References

- External References 44

Overview

Description

A malicious TrollAgent malware was found to be downloaded when attempting to install security software from a South Korean construction association website. The malware can steal information and receive commands from attackers. Users should keep antivirus software updated to prevent infection.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
viewer.appofficer.kro.kr
Pattern Type
stix
Pattern
[hostname:value = 'viewer.appofficer.kro.kr']
Name
ve.kimyy.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 've.kimyy.p-e.kr']
Name
sa.netup.p-e.kr

Pattern Type
stix
Pattern
[hostname:value = 'sa.netup.p-e.kr']
Name
qa.jaychoi.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'qa.jaychoi.p-e.kr']
Name
pi.selecto.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'pi.selecto.p-e.kr']
Name
pe.daysol.p-e.kr

Pattern Type
stix
Pattern
[hostname:value = 'pe.daysol.p-e.kr']
Name
li.ssungmin.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'li.ssungmin.p-e.kr']
Name
dl.netup.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'dl.netup.p-e.kr']
Name
ce.aerosp.p-e.kr

Pattern Type
stix
Pattern
[hostname:value = 'ce.aerosp.p-e.kr']
Name
ca.bananat.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'ca.bananat.p-e.kr']
Name
ai.ssungmin.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'ai.ssungmin.p-e.kr']
Name
ai.selecto.p-e.kr

Pattern Type
stix
Pattern
[hostname:value = 'ai.selecto.p-e.kr']
Name
ai.kimyy.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'ai.kimyy.p-e.kr']
Name
ai.daysol.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'ai.daysol.p-e.kr']
Name
ai.bananat.p-e.kr

Pattern Type
stix
Pattern
[hostname:value = 'ai.bananat.p-e.kr']
Name
ai.aerosp.p-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'ai.aerosp.p-e.kr']
Name
coolsystem.co.kr
Pattern Type
stix
Pattern
[domain-name:value = 'coolsystem.co.kr']
Name
http://ve.kimyy.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ve.kimyy.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ve.kimyy.p-e.kr/index.php']

Name

http://viewer.appofficer.kro.kr/index.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:** viewer.appofficer.kro.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://viewer.appofficer.kro.kr/index.php']

Name

http://sa.netup.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** sa.netup.p-e.kr - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://sa.netup.p-e.kr/index.php']

Name

http://qi.limsjo.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** qi.limsjo.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://qi.limsjo.p-e.kr/index.php']

Name

http://qa.jaychoi.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** qa.jaychoi.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://qa.jaychoi.p-e.kr/index.php']

Name

http://pi.selecto.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** pi.selecto.p-e.kr - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://pi.selecto.p-e.kr/index.php']

Name

http://pe.daysol.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** pe.daysol.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://pe.daysol.p-e.kr/index.php']

Name

http://ol.negapa.p-e.kr/index.php

Description

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

True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ol.negapa.p-e.kr - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://ol.negapa.p-e.kr/index.php']

Name

http://li.ssungmin.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** li.ssungmin.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://li.ssungmin.p-e.kr/index.php']

Name

http://dl.netup.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** dl.netup.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://dl.netup.p-e.kr/index.php']

Name

http://coolsystem.co.kr/admin/mail/index.php

Pattern Type

stix

Pattern

[url:value = 'http://coolsystem.co.kr/admin/mail/index.php']

Name

http://ce.aerosp.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ce.aerosp.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ce.aerosp.p-e.kr/index.php']

Name

http://ca.bananat.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ca.bananat.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ca.bananat.p-e.kr/index.php']

Name

http://ar.kostin.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ar.kostin.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ar.kostin.p-e.kr/index.php']

Name

http://ai.ssungmin.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.ssungmin.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.ssungmin.p-e.kr/index.php']

Name

http://ai.selecto.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.selecto.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.selecto.p-e.kr/index.php']

Name

http://ai.negapa.p-e.kr/index.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': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.negapa.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.negapa.p-e.kr/index.php']

Name

http://ai.limsjo.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.limsjo.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.limsjo.p-e.kr/index.php']

Name

http://ai.kostin.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.kostin.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.kostin.p-e.kr/index.php']

Name

http://ai.kimyy.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.kimyy.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.kimyy.p-e.kr/index.php']

Name

http://ai.daysol.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.daysol.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.daysol.p-e.kr/index.php']

Name

http://ai.bananat.p-e.kr/index.php

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.bananat.p-e.kr - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://ai.bananat.p-e.kr/index.php']

Name

http://ai.aerosp.p-e.kr/index.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:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1622799504, 'iso': '2021-06-04T05:38:24-04:00'} - **IPQS: Domain:** ai.aerosp.p-e.kr - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://ai.aerosp.p-e.kr/index.php']

Name

qi.limsjo.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'qi.limsjo.p-e.kr']

Name

ol.negapa.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ol.negapa.p-e.kr']

Name

ar.kostin.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ar.kostin.p-e.kr']

Name

ai.negapa.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ai.negapa.p-e.kr']

Name

ai.limsjo.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ai.limsjo.p-e.kr']

Name

ai.kostin.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ai.kostin.p-e.kr']

Name

ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca']

Name

a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9']

Name

955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b']

Name

6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9']

Name

61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92']

Name

d8d67ba37263832e7f7d0a945a04afe3d9cea24e78a2d82b00463a2ab575ddb0b53f020c9967391c8469a831c3205f68d010d752a17419d7c2bb34ae8dc55384

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3']

Name

098d0ec27fc04ae8eb212efa85bdce3ad36f09c5ed934ac14a2cf120237ed1ca19ece03ca327bb4ce900672ebf0b4f3782e31df704d4b9b1141b059ee64182b9

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e']

Malware

Name
TrollAgent

Intrusion-Set

Name

Kimsuky

Description

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 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.

Attack-Pattern

Name
Input Capture
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
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a

trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Sector

Name
Construction
Description
Private entities engaged in preparation of land and construction, alteration and repair of building, structures and other real estate properties.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Hostname

Value
viewer.appofficer.kro.kr
ve.kimyy.p-e.kr
sa.netup.p-e.kr
qa.jaychoi.p-e.kr
pi.selecto.p-e.kr
pe.daysol.p-e.kr
li.ssungmin.p-e.kr
dl.netup.p-e.kr
ce.aerosp.p-e.kr
ca.bananat.p-e.kr
ai.ssungmin.p-e.kr
ai.selecto.p-e.kr
ai.kimyy.p-e.kr

ai.daysol.p-e.kr

ai.bananat.p-e.kr

ai.aerosp.p-e.kr

qi.limsjo.p-e.kr

ol.negapa.p-e.kr

ar.kostin.p-e.kr

ai.negapa.p-e.kr

ai.limsjo.p-e.kr

ai.kostin.p-e.kr

Domain-Name

Value
coolsystem.co.kr

Url

Value
http://viewer.appofficer.kro.kr/index.php
http://ve.kimyy.p-e.kr/index.php
http://sa.netup.p-e.kr/index.php
http://qi.limsjo.p-e.kr/index.php
http://qa.jaychoi.p-e.kr/index.php
http://pi.selecto.p-e.kr/index.php
http://pe.daysol.p-e.kr/index.php
http://ol.negapa.p-e.kr/index.php
http://li.ssungmin.p-e.kr/index.php
http://dl.netup.p-e.kr/index.php
http://coolsystem.co.kr/admin/mail/index.php
http://ce.aerosp.p-e.kr/index.php
http://ca.bananat.p-e.kr/index.php

http://ar.kostin.p-e.kr/index.php

http://ai.ssungmin.p-e.kr/index.php

http://ai.selecto.p-e.kr/index.php

http://ai.negapa.p-e.kr/index.php

http://ai.limsjo.p-e.kr/index.php

http://ai.kostin.p-e.kr/index.php

http://ai.kimyy.p-e.kr/index.php

http://ai.daysol.p-e.kr/index.php

http://ai.bananat.p-e.kr/index.php

http://ai.aerosp.p-e.kr/index.php

StixFile

Value
ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca
f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3
a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9
955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b
6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9
61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92
2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e

Artifact

Value
d8d67ba37263832e7f7d0a945a04afe3d9cea24e78a2d82b00463a2ab575ddb0b53f020c9967391c8469a831c3205f68d010d752a17419d7c2bb34ae8dc55384

External References

- https://otx.alienvault.com/pulse/65d34db750f6497da451c4b9