Jan 03 2024

NETMANAGEIT

Intelligence Report

Trend Analysis on Kimsuky Group's Attacks Using AppleSeed

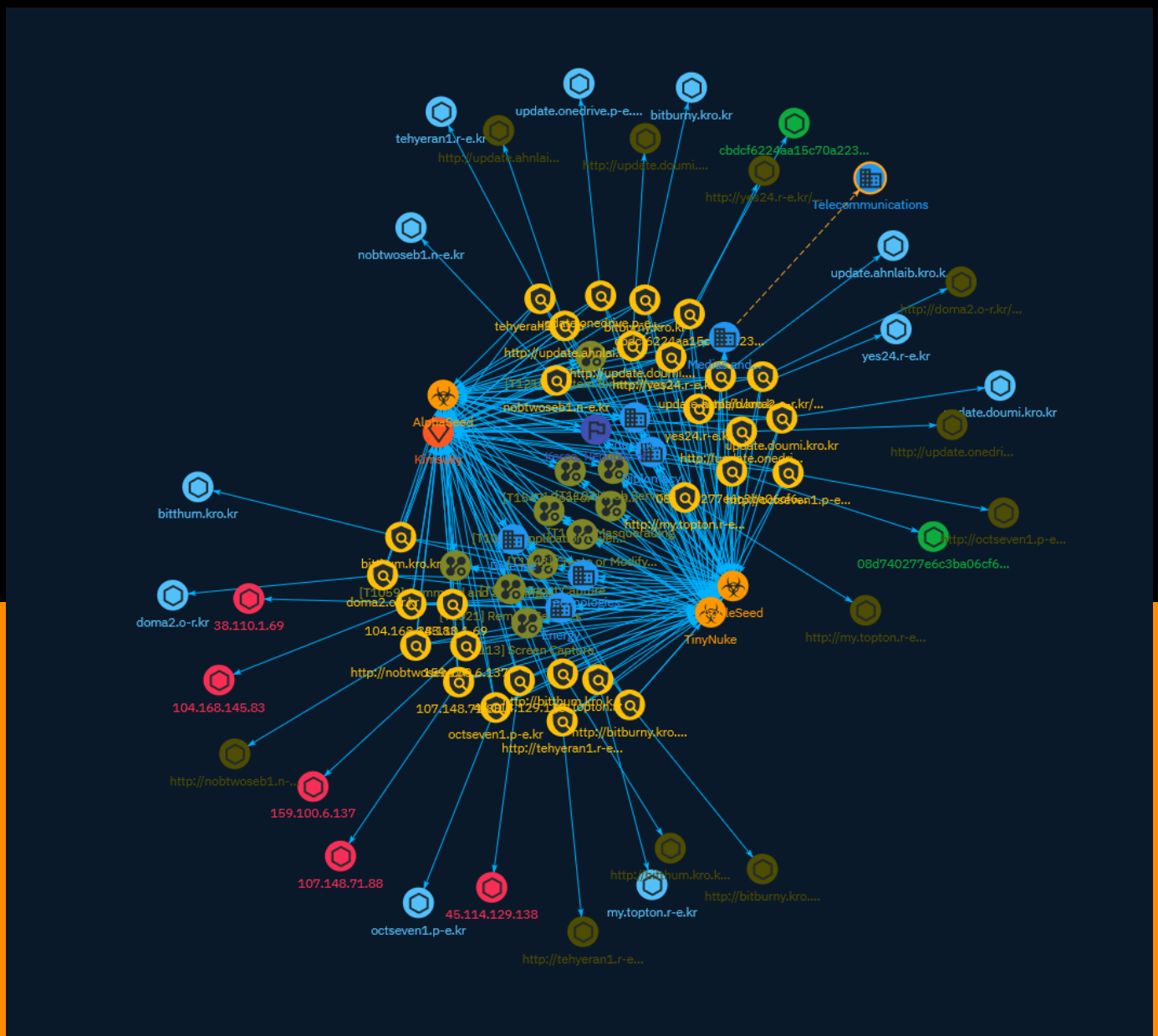

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Kimsuky Group, a North Korean-based cyber-attack group, is continuing to use the same malware that was first identified in 2022, but is still using AppleSeed in its attacks.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
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

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Create or Modify System Process

ID

T1543

Description

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/

T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

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.

Name

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a

feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Sector

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Name

Telecommunications

Description

Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Name

Medias and audiovisual

Description

Communication outlets used to deliver information by print, broadcast or Internet and people working in these outlets.

Name

Technologies

Description

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
tehyeran1.r-e.kr
Pattern Type
stix
Pattern
[hostname:value = 'tehyeran1.r-e.kr']
Name
http://update.doumi.kro.kr/aha/
Pattern Type
stix
Pattern
[url:value = 'http://update.doumi.kro.kr/aha/']
Name
octseven1.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'octseven1.p-e.kr']

Name

cbdcf6224aa15c70a22346594d1956c0589a9411beb75a003eaccb15db4370a5

Description

SHA256 of 1f7d2cbfc75d6eb2c4f2b8b7a3eec1bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cbdcf6224aa15c70a22346594d1956c0589a9411beb75a003eaccb15db4370a5']

Name

my.topton.r-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'my.topton.r-e.kr']

Name

104.168.145.83

Description

ISP: Hostwinds LLC. **OS:** None ---------- Hostnames: - hwsrv-1113209.hostwindsdns.com - client-104-168-145-83.hostwindsdns.com ---------- Domains: - hostwindsdns.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_5.3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAx/FTzz4tCGrl2sXnuPoA7EeuYckM/Sgnn/1cKcf+FpllTCJB dSieTL/dbKrwpPTVq1bMD3KhQSXgvUCV5BXUOCfHZ+G7dQCOM762gcl57zFZIr/25PsfbFBLg3qY AQmFt8+RJtjhSZ/3BtWevN72SfwahGu4+KlDIfz3bjbFaIXkOWGM1UD9ZwO20XOie4wUHA2UOEVw tmkGJJltTsz1+86q1S4EE9IMqSBCVLg8lMj/pj6cP7f9a+NipJsH2BJloPk95FeCTlO3sQpanGP8 qu8kuxMQsgjrKKO5OOHAh+dWuWO3sZknVvODGXy7/ab3rSy1L0rVXOu2hM8DXIXJ9Q== Fingerprint: 4f:22:43:54:41:05:14:af:ca:15:21:d7:89:9a:a0:5a Kex Algorithms: diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 29 Nov 2023 05:55:19 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Content-Length: 1201 Content-Type: text/html;charset=UTF-8 ``` HEARTBLEED: 2023/11/29 05:55:50 104.168.145.83:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.168.145.83']

Name

nobtwoseb1.n-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'nobtwoseb1.n-e.kr']

Name

38.110.1.69

Description

ISP: GTHost **OS:** Windows (build 10.0.17763) ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-5436HJJGFTP NetBIOS Domain Name: WIN-5436HJJGFTP NetBIOS Computer Name: WIN-5436HJJGFTP DNS Domain Name: WIN-5436HJJGFTP FQDN: WIN-5436HJJGFTP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.110.1.69']

Name

yes24.r-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'yes24.r-e.kr']

Name

http://update.onedrive.p-e.kr/aha/

Pattern Type

stix

Pattern

[url:value = 'http://update.onedrive.p-e.kr/aha/']

Name

bitthum.kro.kr

Pattern Type

stix

Pattern

[hostname:value = 'bitthum.kro.kr']

Name

http://doma2.o-r.kr//

Pattern Type
stix
Pattern
[url:value = 'http://doma2.o-r.kr//']
Name
http://tehyeran1.r-e.kr//
Pattern Type
stix
Pattern
[url:value = 'http://tehyeran1.r-e.kr//']
Name
http://update.ahnlaib.kro.kr/aha/
Pattern Type
stix
Pattern
[url:value = 'http://update.ahnlaib.kro.kr/aha/']
Name
http://yes24.r-e.kr/aha/

Pattern Type

stix

Pattern

[url:value = 'http://yes24.r-e.kr/aha/']

Name

107.148.71.88

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: - 1804879704.ob.doanyhere.cn ---------- Domains: - doanyhere.cn ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.10 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDlEQcCEaZYX/j2BJsOP10mZRCG6mBEcFQLVzHm2TUM/+hU HSyCz8tRuglaNiywCud2rvhdngT1NecYaGD8kH7DH57GfXvMBx0ELOW/IvallFn9CsUfVuD+8pmW 5feulD0v+9P+WojStpsPFAgC/5wFXvlV9YyoEUBr/roMdrhImhzklNVnvYNWc19lFHlunOH3poAh F/geN4kOh4FkH1BqgH1DjC+vtwWb5GgiV60/rcRWAxR/NKcIgNbM66f0+vVYercvYFUDK6mvFfGJ 2gD6VtHme7O+p6wd/ tdTM+0hqQC+4TDgUeD3+DfGFquN8FWIqaYn26WJegIubdjuXH2kVIHBs6pt rwz8IgUKbsgEFt+VHyJK35Pyx6LgxOooA4OOCYJEIHL4djGtaP5SE6WfOAyYAPYTc3hsTtW2pIIt Ojo5zgslMzq2qabXkrhyV4I8TCRUGPCWmo5FU6d6Ye+Pou/uJqhw+YAmrAzF8//VUhto5mBjtWfg NpYx1JzJdIc= Fingerprint: bd:97:50:bb:95:6d:42:54:24:58:3e:3e:4a:02:26:1f Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Wed, 20 Dec 2023 20:45:19 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 X-Powered-By: PHP/8.2.12 Content-Length: 0 Content-Type: text/html; charset=UTF-8 ``` ---------- **443:** ``` HTTP/1.1 200 OK

Date: Fri, 22 Dec 2023 12:26:23 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Content-Length: 1203 Content-Type: text/html;charset=UTF-8 ``` HEARTBLEED: 2023/12/22 12:26:48 107.148.71.88:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.71.88']

Name

08d740277e6c3ba06cf6e4806132d8956795b64bb32a1433a5f09bdf941a1b72

Description

SHA256 of f3a55d49562e41c7d339fb52457513ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '08d740277e6c3ba06cf6e4806132d8956795b64bb32a1433a5f09bdf941a1b72']

Name

http://bitburny.kro.kr/aha/

Pattern Type

stix

Pattern

[url:value = 'http://bitburny.kro.kr/aha/']

Name

doma2.o-r.kr

Pattern Type

stix

Pattern

[hostname:value = 'doma2.o-r.kr']

Name

http://my.topton.r-e.kr/address/

Pattern Type

stix

Pattern

[url:value = 'http://my.topton.r-e.kr/address/']

Name

http://bitthum.kro.kr/hu/

Pattern Type

stix

Pattern

[url:value = 'http://bitthum.kro.kr/hu/']

Name

update.onedrive.p-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'update.onedrive.p-e.kr']

Name

update.ahnlaib.kro.kr

Pattern Type

stix

Pattern

[hostname:value = 'update.ahnlaib.kro.kr']

Name

http://nobtwoseb1.n-e.kr//

Pattern Type

stix

Pattern

[url:value = 'http://nobtwoseb1.n-e.kr//']

Name

bitburny.kro.kr

Pattern Type

stix

Pattern

[hostname:value = 'bitburny.kro.kr']

Name

http://octseven1.p-e.kr//

Pattern Type

stix

Pattern

[url:value = 'http://octseven1.p-e.kr//']

Name

159.100.6.137

Description

ISP: firstcolo GmbH **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: - my.shoping.kro.kr ------------------------- Domains: - kro.kr ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Date: Tue, 26 Dec 2023 22:04:38 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 X-Powered-By: PHP/8.2.12 Content-Length: 0 Content-Type: text/html; charset=UTF-8 ``` ------------------ **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 159.100.6.137:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \SRV81441181\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 159.100.6.137:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \SRV81441181\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 159.100.6.137:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \SRV81441181\pipe\lsass 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 159.100.6.137:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\SRV81441181\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 159.100.6.137:49665 ncalrpc: WindowsShutdown ncacn_np: \\SRV81441181\PIPE\InitShutdown ncalrpc: WMsgKRpc071F10 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\SRV81441181\PIPE\InitShutdown ncalrpc: WMsgKRpc071F10 ncalrpc: WMsgKRpc03DA1F2 ncalrpc: WMsgKRpc0E6FC23 ncalrpc: WMsgKRpc01026BD5A4 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-35bcb63b3c2bf6038a ncalrpc: LRPC-b192b98ce52f7ff1f9 ncalrpc: LRPC-cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-35bcb63b3c2bf6038a ncalrpc: LRPC-b192b98ce52f7ff1f9 ncalrpc: LRPC-cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-b192b98ce52f7ff1f9 ncalrpc: LRPC-cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-

cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-153bae5b4ce949a31e ncalrpc: LRPC-311d5b71a66ba77179 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-35bcb63b3c2bf6038a ncalrpc: LRPC-b192b98ce52f7ff1f9 ncalrpc: LRPC-cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-b192b98ce52f7ff1f9 ncalrpc: LRPC-cdbe06e28e6017962f ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 0d47017b-b33b-46ad-9e18-fe96456c5078 version: v1.0 ncalrpc: umpo 95406f0b-b239-4318-91bb-cea3a46ff0dc version: v1.0 ncalrpc: umpo 4ed8abcc-f1e2-438b-981f-bb0e8abc010c version: v1.0 ncalrpc: umpo 0ff1f646-13bb-400a-ab50-9a78f2b7a85a version: v1.0 ncalrpc: umpo 6982a06e-5fe2-46b1-b39c-a2c545bfa069 version: v1.0 ncalrpc: umpo 082a3471-31b6-422a-b931-a54401960c62 version: v1.0 ncalrpc: umpo fae436b0-b864-4a87-9eda-298547cd82f2 version: v1.0 ncalrpc: umpo e53d94ca-7464-4839-b044-09a2fb8b3ae5 version: v1.0 ncalrpc: umpo 178d84be-9291-4994-82c6-3f909aca5a03 version: v1.0 ncalrpc: umpo 4dace966-a243-4450-ae3f-9b7bcb5315b8 version: v2.0 ncalrpc: umpo 1832bcf6-cab8-41d4-85d2-c9410764f75a version: v1.0 ncalrpc: umpo c521facf-09a9-42c5-b155-72388595cbf0 version: v0.0 ncalrpc: umpo 2c7fd9ce-e706-4b40-b412-953107ef9bb0 version: v0.0 ncalrpc: umpo 88abcbc3-34ea-76ae-8215-767520655a23 version: v0.0 ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-f64a1087457d233179 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLE10C61FCD97231E3A07087D8E7B80 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-89fbb67459fa163b4c ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 0361ae94-0316-4c6c-8ad8-c594375800e2 version: v1.0 ncalrpc: umpo 5824833b-3c1a-4ad2-

bdfd-c31d19e23ed2 version: v1.0 ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-7c2e6e74fff7bbb6aa ncalrpc: LRPC-67ef14fc018d14d63b ncalrpc: IUserProfile2 ncalrpc: LRPC-9466f67f02236552aa ncalrpc: senssvc ncalrpc: LRPC-de31bc3528165a29e7 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-6fb139c477bc68ba6a 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-b36d7566c32368dc7e ncalrpc: OLE3D95AA7DFEE41B704F2814BC6C34 ncalrpc: LRPC-153bae5b4ce949a31e 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-bc0df905ba99c1a3aa a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-bb98b49fb23a4120a4 ncalrpc: LRPC-311d5b71a66ba77179 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 159.100.6.137:49666 ncacn_np: \ \SRV81441181\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-e9e2a899b6244fb193 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-881387b9ce9510a1b4 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 159.100.6.137:49667 ncalrpc: LRPC-e0c3973d35540952ab ncalrpc: ubpmtaskhostchannel ncacn_np: \ \SRV81441181\PIPE\atsvc ncalrpc: LRPC-2a503ea4ad3bc82054 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 159.100.6.137:49667 ncalrpc: LRPC-e0c3973d35540952ab ncalrpc: ubpmtaskhostchannel ncacn_np: \\SRV81441181\PIPE\atsvc ncalrpc: LRPC-2a503ea4ad3bc82054 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-e0c3973d35540952ab ncalrpc: ubpmtaskhostchannel ncacn_np: \ \SRV81441181\PIPE\atsvc ncalrpc: LRPC-2a503ea4ad3bc82054 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\SRV81441181\PIPE\atsvc ncalrpc: LRPC-2a503ea4ad3bc82054 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \ \SRV81441181\PIPE\atsvc ncalrpc: LRPC-2a503ea4ad3bc82054 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-2a503ea4ad3bc82054 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-76e1c24dcc17f69c6b 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-8a98a301ffa7089b25 ncalrpc: DNSResolver 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: 16605fd4-4b3e-4f67-bb71-9f6264f20d9a ncalrpc: LRPC-4b7df408bfef1f528f

7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \
\SRV81441181\PIPE\wkssvc ncalrpc: LRPC-871011474ab77e4abd eb081a0d-10ee-478a-
a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc:
LRPC-871011474ab77e4abd f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation:
Witness Client Upcall Server ncalrpc: LRPC-871011474ab77e4abd
3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc:
LRPC-1c4b00017b650b57e5 ncalrpc: OLEDF0FC47C23E005B257B797742356
13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-80de0ec07e0b834efc
c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-80de0ec07e0b834efc
f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-80de0ec07e0b834efc
b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-80de0ec07e0b834efc
abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-80de0ec07e0b834efc
29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 159.100.6.137:49668
ncacn_np: \\SRV81441181\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc:
LRPC-de31bc3528165a29e7 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation:
UserMgrCli ncalrpc: LRPC-546c65513e273770bd ncalrpc:
OLEB6E0704F1FADAAC5BAD9963DBDE1 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0
annotation: UserMgrCli ncalrpc: LRPC-546c65513e273770bd ncalrpc:
OLEB6E0704F1FADAAC5BAD9963DBDE1 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0
annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-4f54ace3d2f12c5c88 ncalrpc:
LRPC-5146e8a58ca2b31d54 ncalrpc: LRPC-d4de9b31a570c8a035 ncalrpc: LRPC-
f20a1b5044177f791d f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs
ncalrpc: LRPC-5146e8a58ca2b31d54 ncalrpc: LRPC-d4de9b31a570c8a035 ncalrpc: LRPC-
f20a1b5044177f791d 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs
provider: MPSSVC.dll ncalrpc: LRPC-d4de9b31a570c8a035 ncalrpc: LRPC-f20a1b5044177f791d
dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API
provider: BFE.DLL ncalrpc: LRPC-f20a1b5044177f791d 76f03f96-cdfd-44fc-a22c-64950a001209
version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider:
spoolsv.exe ncacn_ip_tcp: 159.100.6.137:49669 ncalrpc: LRPC-cd451f97506849d62f
4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp:
159.100.6.137:49669 ncalrpc: LRPC-cd451f97506849d62f ae33069b-a2a8-46ee-a235-
ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification
Protocol provider: spoolsv.exe ncacn_ip_tcp: 159.100.6.137:49669 ncalrpc: LRPC-
cd451f97506849d62f 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-
PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp:
159.100.6.137:49669 ncalrpc: LRPC-cd451f97506849d62f 12345678-1234-abcd-
ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol
provider: spoolsv.exe ncacn_ip_tcp: 159.100.6.137:49669 ncalrpc: LRPC-cd451f97506849d62f
c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc:
OLE49FBD7E126E4CD9C63F5061EFAF4 ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics
ncalrpc: LRPC-8c09cf871efd61ee18 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0
annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc:
TeredoDiagnostics ncalrpc: LRPC-8c09cf871efd61ee18 2e6035b2-e8f1-41a7-
a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint

ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-8c09cf871efd61ee18 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-8c09cf871efd61ee18 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-0e244509f94d6068f4 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-0e244509f94d6068f4 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-fce31c84598f6b682d 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 159.100.6.137:49670 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-cf602887fed6ea4640 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-91e8c3ee789e981cc3 ncalrpc: OLE127344B76C56B8FD4C3660733729 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-ff4cd5394f10572c09 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-b6f42d034f019d20b9 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-7271e08551b5c26c00 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\SRV81441181\PIPE\ROUTER 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 159.100.6.137:49671 ncalrpc: ipsec 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc03DA1F2 ncalrpc: WMsgKRpc0E6FC23 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-f28df097605096dbdc ncalrpc: OLE9E8E7A58F81DC8F5A5BD59EB403D ncalrpc: LRPC-7445788cb827949c36 ncalrpc: OLE95E175FFD87F3565363E330262BE 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-f28df097605096dbdc ncalrpc: OLE9E8E7A58F81DC8F5A5BD59EB403D ncalrpc: LRPC-7445788cb827949c36 ncalrpc: OLE95E175FFD87F3565363E330262BE 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-f28df097605096dbdc ncalrpc: OLE9E8E7A58F81DC8F5A5BD59EB403D ncalrpc: LRPC-7445788cb827949c36 ncalrpc: OLE95E175FFD87F3565363E330262BE 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-98edebe9baec6dfec9 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-98edebe9baec6dfec9 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-98edebe9baec6dfec9 201ef99a-7fa0-444c-9399-19ba84f12a1a

version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-98edebe9baec6dfec9 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-98edebe9baec6dfec9 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-fcf807b2bf5167feb5 ncalrpc: LRPC-fcf807b2bf5167feb5 ncalrpc: LRPC-fcf807b2bf5167feb5 d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-702a01076919db3b51 d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-702a01076919db3b51 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57 version: v1.0 annotation: Group Policy RPC Interface provider: appmgmts.dll ncalrpc: LRPC-2b7bcd7b5471168eb8 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-c1a27445c8f7509d70 ncalrpc: OLE8C7FBDF88E46EFBA9BEA0AC600B5 0dd94748-2ff1-11ee-be56-0242ac120002 version: v2.0 ncalrpc: LRPC-2e92a607136c887985 ncalrpc: OLE59DF47BE8C42CB6538E6C22DB1DA f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-95efde2ab937cff7cf ncalrpc: LRPC-018dbcb803137035f1 ncalrpc: LRPC-bc8b45424c5c4931a7 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-88783f16ace42714d6 ncalrpc: OLE86015A143A923A95ECEF5C226119 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sun, 17 Dec 2023 09:02:43 GMT Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 X-Powered-By: PHP/8.2.12 Content-Length: 0 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/12/17 09:02:52 159.100.6.137:443 - SAFE ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: SRV81441181 NetBIOS Domain Name: SRV81441181 NetBIOS Computer Name: SRV81441181 DNS Domain Name: srv81441181 FQDN: srv81441181 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.100.6.137']

Name

update.doumi.kro.kr

Pattern Type

stix

Pattern

[hostname:value = 'update.doumi.kro.kr']

Name

45.114.129.138

Description

CC=KR ASN=AS45382 EHOSTICT

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.114.129.138']

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.

Country

Name
Korea, Republic of

Malware

Name
TinyNuke
Name
AlphaSeed
Name
AppleSeed
Description
[AppleSeed](https://attack.mitre.org/software/S0622) is a backdoor that has been used by [Kimsuky](https://attack.mitre.org/groups/G0094) to target South Korean government, academic, and commercial targets since at least 2021.(Citation: Malwarebytes Kimsuky June 2021)

StixFile

Value
cbdcf6224aa15c70a22346594d1956c0589a9411beb75a003eaccb15db4370a5
08d740277e6c3ba06cf6e4806132d8956795b64bb32a1433a5f09bdf941a1b72

Hostname

Value
update.ahnlaib.kro.kr
yes24.r-e.kr
nobtwoseb1.n-e.kr
tehyeran1.r-e.kr
octseven1.p-e.kr
doma2.o-r.kr
update.onedrive.p-e.kr
update.doumi.kro.kr
bitthum.kro.kr
bitburny.kro.kr
my.topton.r-e.kr

IPv4-Addr

Value
45.114.129.138
104.168.145.83
38.110.1.69
159.100.6.137
107.148.71.88

Url

Value
http://tehyeran1.r-e.kr//
http://octseven1.p-e.kr//
http://doma2.o-r.kr//
http://yes24.r-e.kr/aha/
http://update.ahnlaib.kro.kr/aha/
http://bitburny.kro.kr/aha/
http://update.doumi.kro.kr/aha/
http://update.onedrive.p-e.kr/aha/
http://nobtwoseb1.n-e.kr//
http://bitthum.kro.kr/hu/
http://my.topton.r-e.kr/address/

External References

- https://otx.alienvault.com/pulse/65957ae70bbfc54115206f34
- https://asec.ahnlab.com/en/60054/