Aug 07 2023

NETMANAGEIT

Intelligence Report

North Korea Compromises Sanctioned Russian Missile Engineering Company

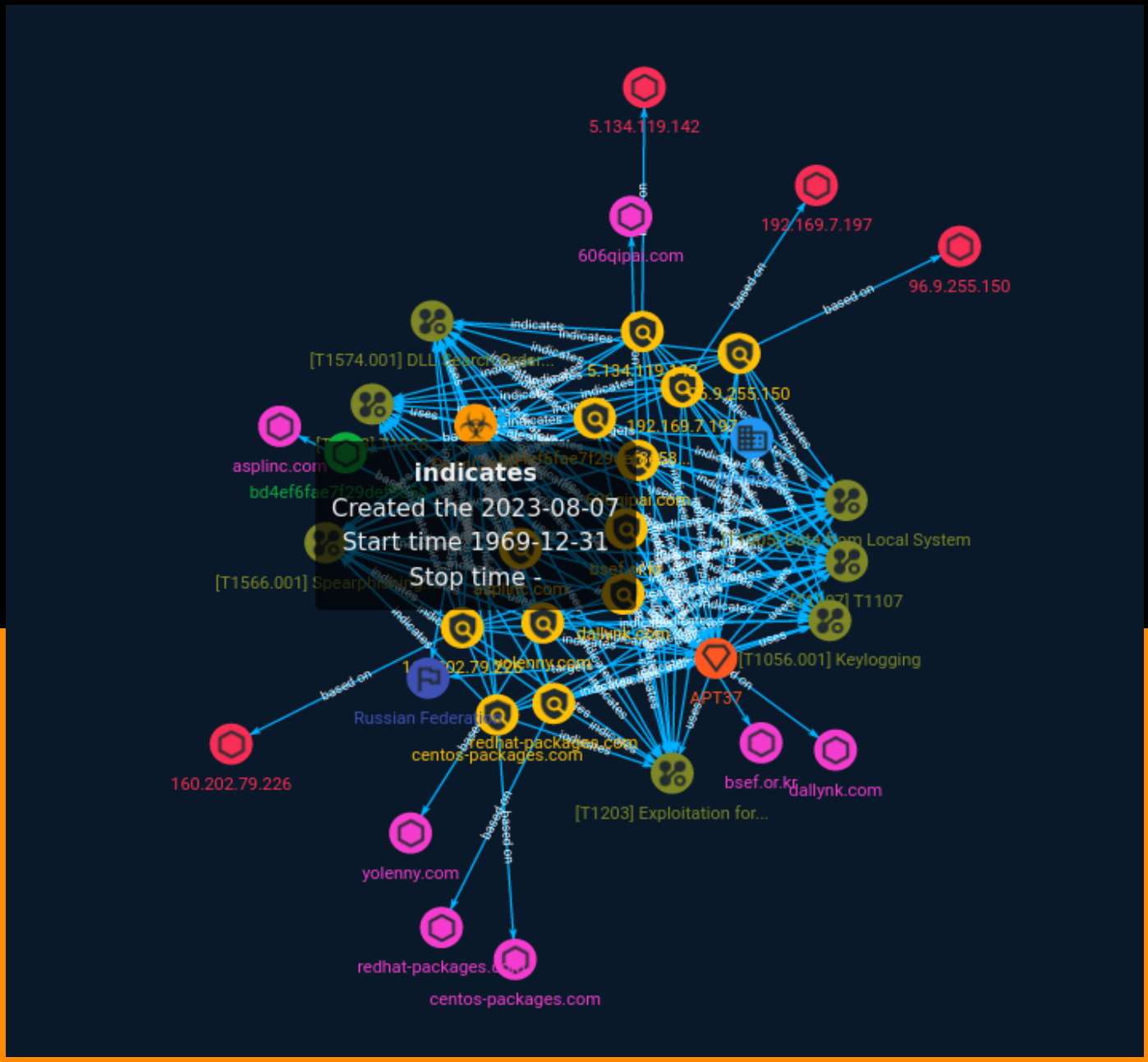

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Malware 13
- Attack-Pattern 14
- Intrusion-Set 19
- Country 20
- Sector 21

Observables

- Domain-Name 22
- StixFile 23

- IPv4-Addr 24

External References

- External References 25

Overview

Description

SentinelLabs identified an intrusion into the Russian defense industrial base, specifically a missile engineering organization NPO Mashinostroyeniya. Their findings identify two instances of North Korea related compromise of sensitive internal IT infrastructure within this same Russian DIB organization, including a specific email server, alongside use of a Windows backdoor dubbed OpenCarrot. Their analysis attributes the email server compromise to the ScarCruft threat actor. We also identify the separate use of a Lazarus Group backdoor for compromise of their internal network.

Confidence

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

15 / 100

Indicator

Name
bsef.or.kr
Pattern Type
stix
Pattern
[domain-name:value = 'bsef.or.kr']
Name
asplinc.com
Pattern Type
stix
Pattern
[domain-name:value = 'asplinc.com']
Name
192.169.7.197

Pattern Type
stix
Pattern
[ipv4-addr:value = '192.169.7.197']
Name
yolenny.com
Pattern Type
stix
Pattern
[domain-name:value = 'yolenny.com']
Name
606qipai.com
Pattern Type
stix
Pattern
[domain-name:value = '606qipai.com']
Name
96.9.255.150

Pattern Type
stix
Pattern
[ipv4-addr:value = '96.9.255.150']
Name
centos-packages.com
Pattern Type
stix
Pattern
[domain-name:value = 'centos-packages.com']
Name
bd4ef6fae7f29def8e5894bf05057653248f009422de85c1e425d04a0b2df258
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bd4ef6fae7f29def8e5894bf05057653248f009422de85c1e425d04a0b2df258']
Name

dallynk.com

Pattern Type

stix

Pattern

[domain-name:value = 'dallynk.com']

Name

160.202.79.226

Description

ISP: QuickPacket, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Fri, 04 Aug 2023 00:17:17 GMT Content-Type: text/html Content-Length: 566 Connection: keep-alive ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 160.202.79.226:49152 ncalrpc: WindowsShutdown ncacn_np: \\WIN-ED5QE0THDTU\PIPE\InitShutdown ncalrpc: WMsgKRpc0C8CB0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-ED5QE0THDTU\PIPE\InitShutdown ncalrpc: WMsgKRpc0C8CB0 ncalrpc: WMsgKRpc0CAA31 ncalrpc: WMsgKRpc0157A452 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-73b0c585fad3b42dcd ncacn_np: \\WIN-ED5QE0THDTU\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-a7d9a2e2e150bd0a2b ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-73b0c585fad3b42dcd ncacn_np: \\WIN-ED5QE0THDTU\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-a7d9a2e2e150bd0a2b ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-a7d9a2e2e150bd0a2b ncalrpc: actkernel ncalrpc: umpo ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc:

actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-afb6600d8555ce93f8 ncacn_ip_tcp: 160.202.79.226:49153 ncacn_np: \\WIN-ED5QE0THDTU\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-afb6600d8555ce93f8 ncacn_ip_tcp: 160.202.79.226:49153 ncacn_np: \\WIN-ED5QE0THDTU\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: LRPC-afb6600d8555ce93f8 ncacn_ip_tcp: 160.202.79.226:49153 ncacn_np: \\WIN-ED5QE0THDTU\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-afb6600d8555ce93f8 ncacn_ip_tcp: 160.202.79.226:49153 ncacn_np: \\WIN-ED5QE0THDTU\pipe\eventlog ncalrpc: eventlog f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 160.202.79.226:49153 ncacn_np: \\WIN-ED5QE0THDTU\pipe\eventlog ncalrpc: eventlog 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-1153845f485a7d5a3e ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-

ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 160.202.79.226:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-ED5QE0THDTU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLED1D3877EFF990EEBD9A01310EF6A ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-5e6542ff3587415650 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\WIN-ED5QE0THDTU\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: LRPC-b5eab1c15d9483a2dc ncalrpc: OLEADC3FB6C663B8F350DA591E15F68 da5a86c5-12c2-4943-ab30-7f74a813d853 version: v1.0 annotation: RemoteRegistry Perflib Interface protocol: [MS-PCQ]: Performance Counter Query Protocol provider: regsvc.dll ncacn_np: \\WIN-ED5QE0THDTU\PIPE\winreg 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-b5eab1c15d9483a2dc ncalrpc: OLEADC3FB6C663B8F350DA591E15F68 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-5ec54a8b30899a108f ncalrpc: LRPC-3fa5278694fe66f046 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-5ec54a8b30899a108f ncalrpc: LRPC-3fa5278694fe66f046 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-5ec54a8b30899a108f ncalrpc: LRPC-3fa5278694fe66f046 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-3fa5278694fe66f046 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-ED5QE0THDTU\PIPE\wkssvc ncalrpc: LRPC-8a1eb3e559a78aa9c2 ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-8a1eb3e559a78aa9c2 ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-8a1eb3e559a78aa9c2 ncalrpc: DNSResolver b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-66d7c68e67909fc3c7 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 160.202.79.226:49155 ncalrpc: LRPC-5290a379253765794c 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 160.202.79.226:49155 ncalrpc: LRPC-5290a379253765794c ae33069b-

a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 160.202.79.226:49155 ncalrpc: LRPC-5290a379253765794c 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 160.202.79.226:49155 ncalrpc: LRPC-5290a379253765794c 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 160.202.79.226:49155 ncalrpc: LRPC-5290a379253765794c 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 160.202.79.226:49157 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-ED5QE0THDTU\pipe\lsass 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 160.202.79.226:49158 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: 160.202.79.226:49159 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-66a4a70aefcdcad16f ncalrpc: LRPC-66a4a70aefcdcad16f ncalrpc: LRPC-66a4a70aefcdcad16f 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0157A452 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 09 Jul 2023 17:56:35 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-ED5QE0THDTU NetBIOS Domain Name: WIN-ED5QE0THDTU NetBIOS Computer Name: WIN-ED5QE0THDTU DNS Domain Name: WIN-ED5QE0THDTU FQDN: WIN-ED5QE0THDTU ``` ---------- **8081:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Fri, 28 Jul 2023 11:48:20 GMT Content-Type: text/html Content-Length: 566 Connection: close

nginx

``` ----------
```

Pattern Type
stix
Pattern
[ipv4-addr:value = '160.202.79.226']
Name
5.134.119.142
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.134.119.142']
Name
redhat-packages.com
Pattern Type
stix
Pattern
[domain-name:value = 'redhat-packages.com']

Malware

Name
OpenCarrot

Attack-Pattern

Name
T1058
ID
T1058
Name
T1107
ID
T1107
Name
DLL Search Order Hijacking
ID
T1574.001
Description
Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load

into a program. (Citation: Microsoft Dynamic Link Library Search Order)(Citation: FireEye Hijacking July 2010) Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution. There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program.(Citation: FireEye fxsst June 2011) Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft Security Advisory 2269637) Adversaries may also directly modify the search order via DLL redirection, which after being enabled (in the Registry and creation of a redirection file) may cause a program to load a different DLL.(Citation: Microsoft Dynamic-Link Library Redirection)(Citation: Microsoft Manifests) (Citation: FireEye DLL Search Order Hijacking) If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program. Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

Name

Keylogging

ID

T1056.001

Description

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include: * Hooking API

callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data. * Reading raw keystroke data from the hardware buffer. * Windows Registry modifications. * Custom drivers. * [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

Name

Spearphishing Attachment

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems

may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Intrusion-Set

Name
APT37

Description
[APT37](https://attack.mitre.org/groups/G0067) is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. [APT37](https://attack.mitre.org/groups/G0067) has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.(Citation: FireEye APT37 Feb 2018)(Citation: Securelist ScarCruft Jun 2016)(Citation: Talos Group123) 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
Russian Federation

Sector

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

Domain-Name

Value
centos-packages.com
yolenny.com
asplinc.com
dallynk.com
redhat-packages.com
606qipai.com
bsef.or.kr

StixFile

Value
bd4ef6fae7f29def8e5894bf05057653248f009422de85c1e425d04a0b2df258

IPv4-Addr

Value
5.134.119.142
96.9.255.150
160.202.79.226
192.169.7.197

External References

- https://otx.alienvault.com/pulse/64d0e945d730800037cf33ea
- https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/