Sep 01 2023

NETMANAGEIT

Intelligence Report

Analysis of Andariel's New Attack Activities

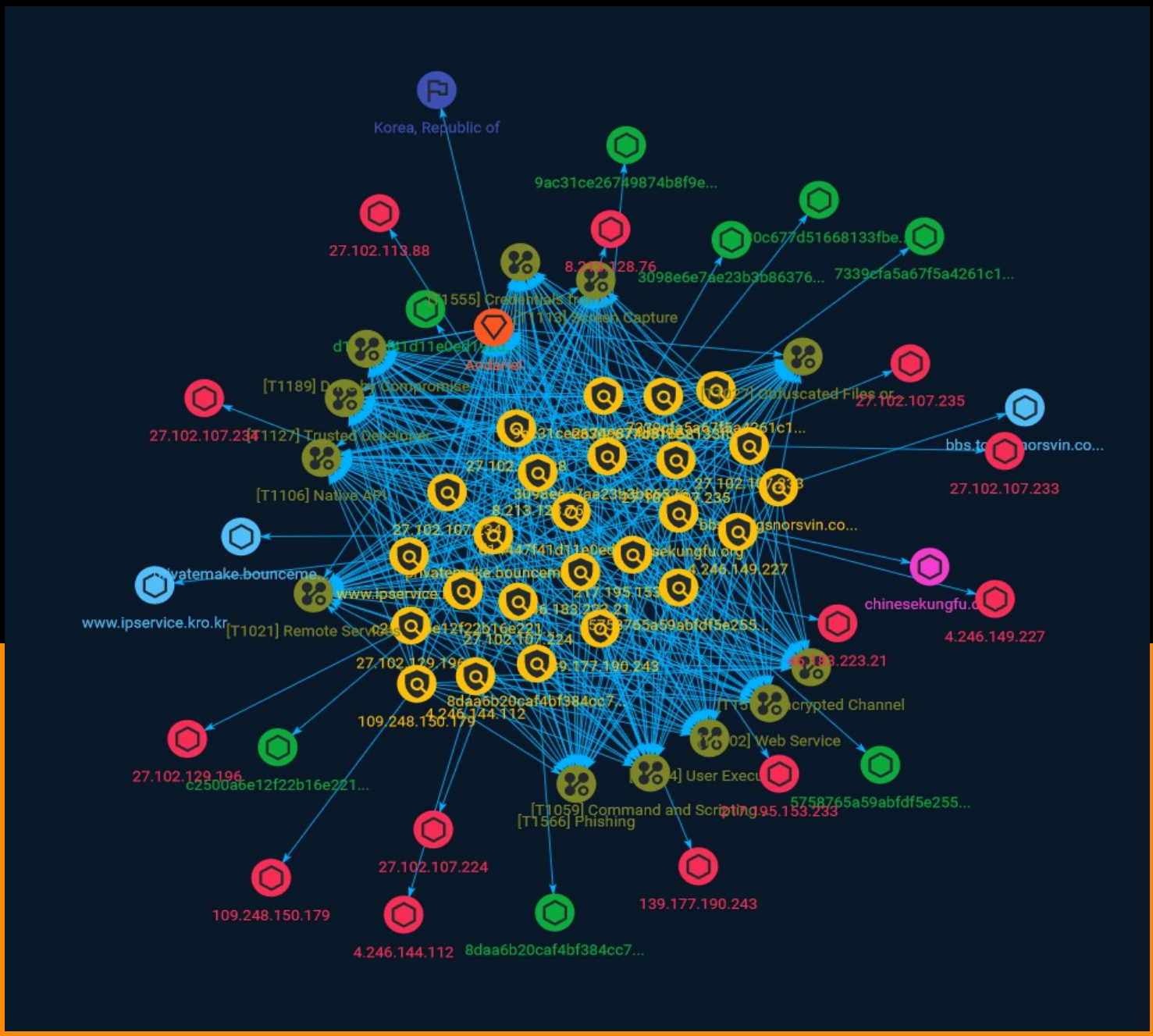

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Andariel threat group which usually targets Korean corporations and organizations is known to be affiliated with the Lazarus threat group or one of its subsidiaries. Attacks against Korean targets have been identified since 2008. Major target industries are those related to national security such as national defense, political organizations, shipbuilding, energy, and communications. Various other companies and institutes in Korea including universities, logistics, and ICT companies are also becoming attack targets. [1] (this report only supports the Korean version)

Confidence

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

15 / 100

Indicator

Name
27.102.107.235
Description
CC=KR ASN=AS45996 DAOU TECHNOLOGY
Pattern Type
stix
Pattern
[ipv4-addr:value = '27.102.107.235']
Name
3098e6e7ae23b3b8637677da7bfc0ba720e557e6df71fa54a8ef1579b6746061
Description
Win64:TrojanX-gen\ [Trj] SHA256 of 1ffccc23fef2964e9b1747098c19d956
Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = '3098e6e7ae23b3b8637677da7bfc0ba720e557e6df71fa54a8ef1579b6746061']

Name

privatemake.bounceme.net

Pattern Type

stix

Pattern

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

Name

d14447f41d11e0ed192d9161a60cee139fe8b01d921bbdff56abc01a5a653161

Description

HackTool:Win32/Mimikatz.D SHA256 of 5291aed100cc48415636c4875592f70c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd14447f41d11e0ed192d9161a60cee139fe8b01d921bbdff56abc01a5a653161']

Name

27.102.107.224

Description

ISP: DAOU TECHNOLOGY **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDycrdV/PaZK2/ssRECrDOs+WfNPtOuvizb+i+aUPBUqMVv RWgA/ZsTYo1z2LN4Naewt1gTjP5XGQ1L2eG9RFD2AxYLnExmkuudN2RWNyENQW4bnUpMmB1kgGZl vv2CjOIbo3ccRDgn/ZvM4fMWMn1+zhPNAGp/s5Oq6r61CkvyocjXkFum07DlZr39cQbEQaYnwQnJ 1BBLFzXV3XVoMhNtotd2H/+3uPlEzAugZyyu5/NVna9FdgsVw9gFNg8UkZrKE7+4Sb3fcXWsjrZF 9zgHuXhbpz6+JcH/rPh6RFbQ6NOYDmkVCSIfrDZZ+x+hCe/kRZS9IJcS50XM51ScoTE7 Fingerprint: a7:5e:ea:26:ce:89:11:d3:06:78:6b:f0:b3:89:57:96 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '27.102.107.224']

Name

chinesekungfu.org

Pattern Type

stix

Pattern

[domain-name:value = 'chinesekungfu.org']

Name

4.246.144.112

Description

CC=US ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '4.246.144.112']

Name

27.102.113.88

Description

ISP: DAOU TECHNOLOGY **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCajMi1Kjkhgt8YuYmLt0VAn/ZteVv5efe6Qy3JhLoAUCqMdGw92Y5z0a+bcmpP813zhboaD3FxSm9d5BzhXPXA0jxjiYA6iMFz/64PjPmRSwYKWVv+hC2IiJEij67ZPzs48Bq8A7SDizz1uWrGAA1xF3+Te2Zl5CafTwzM0M5sY2aT2XNqRrLXhhpJuHRgt7X0lqom

BXqXxgzoyxMWV0LoI6MoAp9fPgAqj1krOMLML68iuQWhUm8LnEqLY7wsgPAxXIdUsMpyg1bjG8oc WubaA7A27V8/Nr9fla18oM+CdrLCXpr1locZRsYtvbfYBMPwGepNU2is/NrnlM8NS70+oNY+DyTT Jnrrd72ar8itdPkFI8JmLaqa0R3MXq+y2OTgn4MkGJyc/mDdE39zO++Fe4UflchfLAX1nsLWh4+n hSFyBX1ElQS9ZC+9RX1Pc7a+AW+E+OQqBFbHPVCQyw73MKmP8PwRrToevg6Ivo7h2WpzvNg/IGeh bU3U4uxhE00= Fingerprint: d7:4c:28:fa:12:1b:26:6e:7e:84:57:d9:c8:1b:fe:ea 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 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '27.102.113.88']

Name

217.195.153.233

Description

CC=NL ASN=AS395092 SHOCK-1

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.195.153.233']

Name

www.ipservice.kro.kr

Pattern Type

stix

Pattern

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

Name

7339cfa5a67f5a4261c18839ef971d7f96eaf60a46190cab590b439c71c4742b

Description

SHA256 of 9112efb49cae021abebd3e9a564e6ca4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7339cfa5a67f5a4261c18839ef971d7f96eaf60a46190cab590b439c71c4742b']

Name

139.177.190.243

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - 139-177-190-243.ip.linodeusercontent.com ---------- Domains: - linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOTGAkWn0LkfgZDUaoJfNfw + vHDXqkJe+1SZvc+2rX256U/MoHJaGi2VhwDW/zWCC8nfZsZBEr7J8Fss1/U8b/g= Fingerprint: 6c:ff:f6:95:dd:63:bf:30:e3:94:b3:ec:21:1b:db:69 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 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 Server: nginx/1.18.0 (Ubuntu) Date: Fri, 25 Aug 2023 06:31:37 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Fri, 07 Jul 2023 23:47:31 GMT Connection: keep-alive ETag: "64a8a413-264" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.177.190.243']

Name

c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c

Description

GoLandBuildPE SHA256 of 9d7bd0caed10cc002670faff7ca130f5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c']

Name

bbs.topigsnorsvin.com.ec

Pattern Type

stix

Pattern

[hostname:value = 'bbs.topigsnorsvin.com.ec']

Name

109.248.150.179

Description

CC=NL ASN=AS203557 DataClub S.A.

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.248.150.179']

Name

e830c677d51668133fbea5d900b7a8e0d8cdfed0a396f50be314c0591bf71f74

Description

Win32:TrojanX-gen\ [Trj] SHA256 of ac0ada011f1544aa3a1cf27a26f2e288

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e830c677d51668133fbea5d900b7a8e0d8cdfed0a396f50be314c0591bf71f74']

Name

5758765a59abfdf5e255df4d0447f92132891d1b325faaa2fb155ebb41cba818

Description

Win32:TrojanX-gen\ [Trj] SHA256 of 0211a3160cc5871cbcd4e5514449162b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5758765a59abfdf5e255df4d0447f92132891d1b325faaa2fb155ebb41cba818']

Name
27.102.107.234
Description
CC=KR ASN=AS45996 DAOU TECHNOLOGY
Pattern Type
stix
Pattern
[ipv4-addr:value = '27.102.107.234']
Name
27.102.107.233
Description
CC=KR ASN=AS45996 DAOU TECHNOLOGY
Pattern Type
stix
Pattern
[ipv4-addr:value = '27.102.107.233']
Name
46.183.223.21

Description

ISP: DataClub S.A. **OS:** Windows (build 10.0.17763) ---------- Hostnames: - nat1.gratezer.com ---------- Domains: - gratezer.com ---------- 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: IP-223-21 NetBIOS Domain Name: IP-223-21 NetBIOS Computer Name: IP-223-21 DNS Domain Name: IP-223-21.dataclub.eu FQDN: IP-223-21.dataclub.eu ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.183.223.21']

Name

8.213.128.76

Description

ISP: Alibaba (US) Technology Co., Ltd. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **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: 10.0.0.146:49152 ncalrpc: WindowsShutdown ncacn_np: \\JOKER\PIPE\InitShutdown ncalrpc: WMsgKRpc040A50 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\JOKER\PIPE\InitShutdown ncalrpc: WMsgKRpc040A50 ncalrpc: WMsgKRpc042C21 ncalrpc: WMsgKRpc0504272 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-

a073-73560f8d9e3e version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo 5c9a4cd7-ba75-45d2-9898-1773b3d1e5f1 version: v1.0 annotation: Device Install Service RPC Interface ncalrpc: LRPC-da1317e1c3e6d6c65e 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-b84b24aa7f77d5bdf8 ncacn_np: \\JOKER\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-9c1f2796b5026415c2 ncalrpc: actkernel ncalrpc: umpo ncalrpc: DeviceSetupManager ncacn_np: \\JOKER\PIPE\srvsvc ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-023ccfc84f5cc474d1 ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc ncacn_ip_tcp: 10.0.0.146:49153 ncacn_np: \\JOKER\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-023ccfc84f5cc474d1 ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc ncacn_ip_tcp: 10.0.0.146:49153 ncacn_np: \\JOKER\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc ncacn_ip_tcp: 10.0.0.146:49153 ncacn_np: \\JOKER\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-

bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncacn_ip_tcp: 10.0.0.146:49153 ncacn_np: \ \JOKER\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: 10.0.0.146:49153 ncacn_np: \\JOKER\pipe\eventlog ncalrpc: eventlog 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: OLE359A88A9F1907F262005ABB0E21E ncalrpc: LRPC-f249becfd2d8058273 ncacn_np: \\JOKER\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-f249becfd2d8058273 ncacn_np: \ \JOKER\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-2ef471948533db4222 ncalrpc: DeviceSetupManager ncacn_np: \\JOKER\PIPE\srvsvc ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 10.0.0.146:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc:

OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\JOKER\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLE4B171D4F04BBFE7ABAE202420B3E ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-277f4fb4bf069a65c9 b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 10.0.0.146:49155 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: \\JOKER\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: 10.0.0.146:49155 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: \\JOKER\pipe\lsass 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-13737f67ef5749100e ncalrpc: LRPC-442be9fb5d26ebe7c5 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-13737f67ef5749100e ncalrpc: LRPC-442be9fb5d26ebe7c5 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-13737f67ef5749100e ncalrpc: LRPC-442be9fb5d26ebe7c5 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-442be9fb5d26ebe7c5 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\JOKER\PIPE\wkssvc ncalrpc: DNSResolver ncalrpc: nlaapi ncalrpc: nlaplg ncalrpc: keysvc eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: DNSResolver ncalrpc: nlaapi ncalrpc: nlaplg ncalrpc: keysvc f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: DNSResolver ncalrpc: nlaapi ncalrpc: nlaplg ncalrpc: keysvc 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 10.0.0.146:49156 ncalrpc: LRPC-77408915c9cf5c0a28 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 10.0.0.146:49156 ncalrpc: LRPC-77408915c9cf5c0a28 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 10.0.0.146:49156 ncalrpc: LRPC-77408915c9cf5c0a28 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 10.0.0.146:49156 ncalrpc: LRPC-77408915c9cf5c0a28 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 10.0.0.146:49156 ncalrpc: LRPC-77408915c9cf5c0a28

367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 10.0.0.146:49162 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: 10.0.0.146:49164 b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-e4f1260001821d28cf 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0504272 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-ac354ae019a08ab141 ncalrpc: LRPC-ac354ae019a08ab141 ncalrpc: LRPC-ac354ae019a08ab141 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '8.213.128.76']

Name

4.246.149.227

Description

CC=US ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '4.246.149.227']

Name

27.102.129.196

Description

CC=KR ASN=AS45996 DAOU TECHNOLOGY

Pattern Type

stix

Pattern

[ipv4-addr:value = '27.102.129.196']

Name

9ac31ce26749874b8f9e080cbe10e6d9c4d0fa9c8edb17685291e031d7f82949

Description

Win32:TrojanX-gen\ [Trj] SHA256 of c892c60817e6399f939987bd2bf5dee0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ac31ce26749874b8f9e080cbe10e6d9c4d0fa9c8edb17685291e031d7f82949']

Name

8daa6b20caf4bf384cc7912a73f243ce6e2f07a5cb3b3e95303db931c3fe339f

Description
Win64:TrojanX-gen\ [Trj] SHA256 of 0a09b7f2317b3d5f057180be6b6d0755
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8daa6b20caf4bf384cc7912a73f243ce6e2f07a5cb3b3e95303db931c3fe339f']

Intrusion-Set

Name

Andariel

Description

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

Country

Name
Korea, Republic of

Attack-Pattern

Name
Trusted Developer Utilities Proxy Execution
ID
T1127
Description
Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.
Name
Encrypted Channel
ID
T1573
Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

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

Credentials from Password Stores

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing]

(https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

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

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

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e.,

[Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising] (https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

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

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)

Domain-Name

Value
chinesekungfu.org

StixFile

Value
9ac31ce26749874b8f9e080cbe10e6d9c4d0fa9c8edb17685291e031d7f82949
7339cfa5a67f5a4261c18839ef971d7f96eaf60a46190cab590b439c71c4742b
c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c
d14447f41d11e0ed192d9161a60cee139fe8b01d921bbdff56abc01a5a653161
e830c677d51668133fbea5d900b7a8e0d8cdfed0a396f50be314c0591bf71f74
8daa6b20caf4bf384cc7912a73f243ce6e2f07a5cb3b3e95303db931c3fe339f
3098e6e7ae23b3b8637677da7bfc0ba720e557e6df71fa54a8ef1579b6746061
5758765a59abfdf5e255df4d0447f92132891d1b325faaa2fb155ebb41cba818

Hostname

Value
www.ipservice.kro.kr
bbs.topigsnorsvin.com.ec
privatemake.bounceme.net

IPv4-Addr

Value
4.246.149.227
8.213.128.76
4.246.144.112
27.102.107.234
217.195.153.233
27.102.113.88
139.177.190.243
27.102.129.196
46.183.223.21
27.102.107.233
109.248.150.179
27.102.107.235
27.102.107.224

External References

- https://otx.alienvault.com/pulse/64f0a87de1d155ccb31c3561
- https://asec.ahnlab.com/en/56405/