May 10 2024

NETMANAGEIT

Intelligence Report

Profiling Traffickers: Cerberus

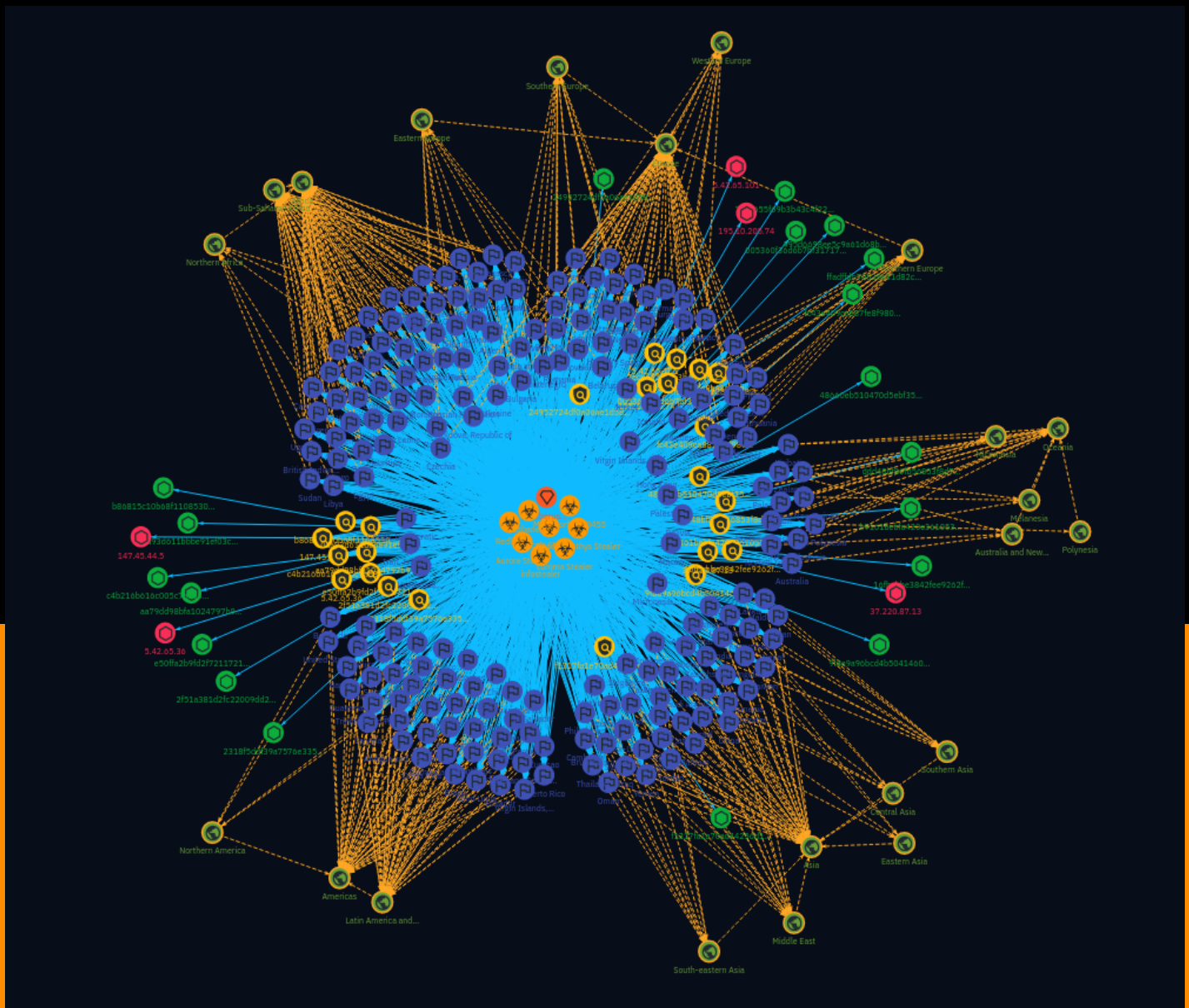

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This analysis delves into the activities of a group of malware operators known as Cerberus (formerly Amnesia) Team, who specialize in spreading infostealers, particularly in the Commonwealth of Independent States (CIS) region. It provides insights into their operations, tactics, and the evolution of their malware campaigns over time, shedding light on the ever-evolving landscape of cybercriminal activities.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

195.10.205.74

Description

- **Zip Code:** N/A - **ISP:** Partner Hosting - **ASN:** 215826 - **Organization:** Partner Hosting - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** hosted-by.csrdp.host - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** North Holland - **City:** Amsterdam - **Latitude:** 52.35 - **Longitude:** 4.92

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.10.205.74']

Name

e50ffa2b9fd2f72117215aae4bd556181a1c43f0e485ee2ede668ae67ff8b37d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e50ffa2b9fd2f72117215aae4bd556181a1c43f0e485ee2ede668ae67ff8b37d']

Name

ffadffdb70628e31d82c7f79dbb60ee917f09d47c085a19e1ac6e6e1e35f65d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffadffdb70628e31d82c7f79dbb60ee917f09d47c085a19e1ac6e6e1e35f65d2']

Name

ddd48bf86fb56853f8d7ec54bdd9922044f4f6a97aa16c4b1b6da4d162c63f50

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ddd48bf86fb56853f8d7ec54bdd9922044f4f6a97aa16c4b1b6da4d162c63f50']

Name

b86815c10b68f1108530338128c8f0a79d358ee91bc43082a2314985fa4db1ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b86815c10b68f1108530338128c8f0a79d358ee91bc43082a2314985fa4db1ba']

Name

b9161bebfa420e361053fe2d28cbacb9f59e12bb2e9ae6dc241326ec5b32429a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9161bebfa420e361053fe2d28cbacb9f59e12bb2e9ae6dc241326ec5b32429a']

Name

aa79dd98bfa1024797b92c3016e931180faf9baa462e751a8eb9061fbfd7a06c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa79dd98bfa1024797b92c3016e931180faf9baa462e751a8eb9061fbfd7a06c']

Name

7eca655f69b3b43c4f228dbd149b73247166872ba92691f7fb00f7f35bb89e41

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7eca655f69b3b43c4f228dbd149b73247166872ba92691f7fb00f7f35bb89e41']

Name

9f8a9a96bcd4b50414604cbd67f282226a2af227972833725e133c60da35ad43

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f8a9a96bcd4b50414604cbd67f282226a2af227972833725e133c60da35ad43']

Name

147.45.44.5

Description

ISP: Karina Rashkovska **OS:** Windows Server 2022 (build 10.0.20348) ---------- Services: **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 147.45.44.5:49664 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: \\WIN-BS656MOF35Q\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 147.45.44.5:49664 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: \\WIN-BS656MOF35Q\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 147.45.44.5:49664 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: \\WIN-BS656MOF35Q\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: 147.45.44.5:49664 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: \\WIN-BS656MOF35Q\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 147.45.44.5:49665 ncalrpc: WindowsShutdown ncacn_np: \\WIN-BS656MOF35Q\PIPE\InitShutdown ncalrpc: WMsgKRpc05DCD0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-BS656MOF35Q\PIPE\InitShutdown ncalrpc: WMsgKRpc05DCD0 ncalrpc: WMsgKRpc06F7B1 ncalrpc: WMsgKRpc0399922 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-715f8f55352cb2c85a ncalrpc: LRPC-4217f5691fb2b9aab2 ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-715f8f55352cb2c85a ncalrpc: LRPC-4217f5691fb2b9aab2 ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-4217f5691fb2b9aab2 ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-9e9a948c26a69b307f ncalrpc: LRPC-ef3487886dddd87da7

697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-715f8f55352cb2c85a ncalrpc: LRPC-4217f5691fb2b9aab2 ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-4217f5691fb2b9aab2 ncalrpc: LRPC-7033878af9ec8c6b90 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 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-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-9ee5f46e4c553ffed6 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-6719c3a06f0667c82a ncalrpc: OLE649457880944450A0C1BFCABC358 ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: OLE649457880944450A0C1BFCABC358 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-6ca2e6adbc43807a57 ncalrpc: LRPC-e0bb5687fb1d8c6850 ncalrpc: LRPC-a47be175cd13e842bf ncalrpc: senssvc ncalrpc: IUserProfile2 ncalrpc: LRPC-f6dec243a5f8ba53ca f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-0603a05f70c47e315f a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-94e54c3083e110e9e0 ncalrpc: LRPC-9e9a948c26a69b307f e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-458bbf50147a3b9ba3 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-70c605451b7edc2492 ncalrpc: OLEE1EE28009FF30DAD29742BBBDF7A ncalrpc: LRPC-ef3487886dddd87da7 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-5cc8ecd0e4faadea1e f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 147.45.44.5:49666 ncacn_np: \\WIN-BS656MOF35Q\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-05ae416e900fb343a0 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-3c04170f3087c0b34a 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-15df04d400dd627c61 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 147.45.44.5:49667 ncalrpc: LRPC-0a362d6ad519062132 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-BS656MOF35Q\PIPE\atsvc ncalrpc: LRPC-bb20b562464eb7834f 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 147.45.44.5:49667 ncalrpc: LRPC-0a362d6ad519062132 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-BS656MOF35Q\PIPE\atsvc ncalrpc: LRPC-bb20b562464eb7834f 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-0a362d6ad519062132 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-BS656MOF35Q\PIPE\atsvc ncalrpc: LRPC-bb20b562464eb7834f 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-BS656MOF35Q\PIPE\atsvc ncalrpc: LRPC-bb20b562464eb7834f 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-BS656MOF35Q\PIPE\atsvc ncalrpc: LRPC-bb20b562464eb7834f 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-bb20b562464eb7834f 3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-ec877ff65e2b1912b2 ncalrpc: OLE8F0B0DB31DB81154637463117B78 7f1343fe-50a9-4927-

a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-BS656MOF35Q\PIPE\wkssvc ncalrpc: LRPC-e5401f33092957e5ff eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-e5401f33092957e5ff f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-e5401f33092957e5ff 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-9c6c8a747ad8e1b427 ncalrpc: DNSResolver 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: f9b0dff7-3467-4667-bc41-d05411dd75ef ncalrpc: LRPC-dcc8daa5d645a1b561 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-58d9bac5300902c7e5 ncalrpc: OLEFB9178E29C705551CD9C67C8A57A 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 147.45.44.5:49668 ncacn_np: \\WIN-BS656MOF35Q\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-f6dec243a5f8ba53ca 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-9eb76c7b7ef93df763 ncalrpc: OLEBC17E4753A00749333E9011F9FB4 c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-9eb76c7b7ef93df763 ncalrpc: OLEBC17E4753A00749333E9011F9FB4 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-9eb76c7b7ef93df763 ncalrpc: OLEBC17E4753A00749333E9011F9FB4 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-9eb76c7b7ef93df763 ncalrpc: OLEBC17E4753A00749333E9011F9FB4 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-9eb76c7b7ef93df763 ncalrpc: OLEBC17E4753A00749333E9011F9FB4 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-87149a97b827d50457 ncalrpc: LRPC-e860216c809984221a ncalrpc: LRPC-5df38f5491b281520d ncalrpc: LRPC-37ef29761ab00524fb f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-e860216c809984221a ncalrpc: LRPC-5df38f5491b281520d ncalrpc: LRPC-37ef29761ab00524fb 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-5df38f5491b281520d ncalrpc: LRPC-37ef29761ab00524fb dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-37ef29761ab00524fb 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-241c5cad7562672da2 ncalrpc: OLE4FB15F23493EE843EFF5211D7022 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-241c5cad7562672da2 ncalrpc: OLE4FB15F23493EE843EFF5211D7022 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 147.45.44.5:49669 ncalrpc: LRPC-56ad5b4e0d47ee13ef 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 147.45.44.5:49669 ncalrpc: LRPC-56ad5b4e0d47ee13ef ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 147.45.44.5:49669 ncalrpc: LRPC-56ad5b4e0d47ee13ef 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 147.45.44.5:49669 ncalrpc: LRPC-56ad5b4e0d47ee13ef 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol

provider: spoolsv.exe ncacn_ip_tcp: 147.45.44.5:49669 ncalrpc: LRPC-56ad5b4e0d47ee13ef a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-66bc2fd455e183a86f c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-63452b26cf19b7eab6 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-63452b26cf19b7eab6 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-63452b26cf19b7eab6 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-63452b26cf19b7eab6 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-fb51650e29dc7b3489 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 147.45.44.5:49670 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-d491084991ff529edc 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-d491084991ff529edc 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-ee05b819126f971f05 ncalrpc: OLEC1F960306E95724B108213C92035 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-2151e5af16b3ed191a 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-f312cd8c88047c25c5 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\WIN-BS656MOF35Q\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: 147.45.44.5:49671 d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-962840ab831b7da8b5 d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-962840ab831b7da8b5 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0399922 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-31b86c30fec963dab0 ncalrpc: OLE6B621DF19038BEA3CBF45C957821 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-31b86c30fec963dab0 ncalrpc: OLE6B621DF19038BEA3CBF45C957821 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-31b86c30fec963dab0 ncalrpc: OLE6B621DF19038BEA3CBF45C957821 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-73c9e35c30bc7d8baa fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll

ncalrpc: LRPC-73c9e35c30bc7d8baa 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-73c9e35c30bc7d8baa 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-73c9e35c30bc7d8baa 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-73c9e35c30bc7d8baa 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-7a44853059b8992261 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-7190ed4ed05b4a9a64 ncalrpc: LRPC-7190ed4ed05b4a9a64 ncalrpc: LRPC-7190ed4ed05b4a9a64 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-31e9c955957f7eff93 ncalrpc: OLE2931C5A08B0D3B586205C3BC2027 9435cc56-1d9c-4924-ac7d-b60a2c3520e1 version: v1.0 annotation: SPPSVC Default RPC Interface provider: sppsvc.exe ncalrpc: SPPCTransportEndpoint-00001 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57 version: v1.0 annotation: Group Policy RPC Interface provider: appmgmts.dll ncalrpc: LRPC-1b8a6a6a1d400d6e33 ``` ---------- **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: WIN-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 07 May 2024 23:59:32 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '147.45.44.5']

Name

48660eb510470d5ebf35a0dfdb4c592117eaec4f07cbf01d428099f052a2fdca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48660eb510470d5ebf35a0dfdb4c592117eaec4f07cbf01d428099f052a2fdca']

Name

2f51a381d2fc22009dd2e7e27d555b7e10de4fbc954d27e506c5c3ba83481577

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f51a381d2fc22009dd2e7e27d555b7e10de4fbc954d27e506c5c3ba83481577']

Name

24952724df0a06ae1d58350bacc43c37981e46267c9f7575192e222028eb7626

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24952724df0a06ae1d58350bacc43c37981e46267c9f7575192e222028eb7626']

Name

16fbabbe3842fee9262fd42da0151f81e4375652d59b01f75a1f0dff46cda69f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '16fbabbe3842fee9262fd42da0151f81e4375652d59b01f75a1f0dff46cda69f']

Name

0aa93d611bbbe91ef03cce5ad22160fa4cea54a8e5b322f85be9b2a139e069e2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0aa93d611bbbe91ef03cce5ad22160fa4cea54a8e5b322f85be9b2a139e069e2']

Name

fc43e409ca887fe8f98079100e54a442b7ab01a2743d7e195ba2c8358a1152df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc43e409ca887fe8f98079100e54a442b7ab01a2743d7e195ba2c8358a1152df']

Name

f1317fa1e70ad44256d1282121c8ad5e12faf9a32fc6b743212726d666408967

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1317fa1e70ad44256d1282121c8ad5e12faf9a32fc6b743212726d666408967']

Name

c4b216b616c005c7ae84dfbdc5f2a99172825e1ee362555ddad8ed29f23313d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c4b216b616c005c7ae84dfbdc5f2a99172825e1ee362555ddad8ed29f23313d6']

Name

495d6698ee5c9a61d68bfd5328fa2e0979ff0ae04d1a2655e5d580e73fe6b998

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '495d6698ee5c9a61d68bfd5328fa2e0979ff0ae04d1a2655e5d580e73fe6b998']

Name

2318f5ddf39a7576e33513557c3af1498e841cef7b36acc53e80ddd700ac0d62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2318f5ddf39a7576e33513557c3af1498e841cef7b36acc53e80ddd700ac0d62']

Name

005360f36d6b7bf31717fb5ba88f844bdf5455dfbd9f84894a8c1e53f7f5ef51

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '005360f36d6b7bf31717fb5ba88f844bdf5455dfbd9f84894a8c1e53f7f5ef51']

Name

5.42.65.36

Description

RedLine Stealer botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.65.36']

Name

5.42.65.101

Description

RedLine Stealer botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.65.101']

Name
37.220.87.13
Description
Aurora Stealer botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '37.220.87.13']

Malware

Name
Rhadamanthys Stealer
Name
Dracula Stealer (Samurai)
Name
Metamorfo - S0455
Name
Aurora Stealer
Name
infostealer
Name
Lumma Stealer
Name
Redline

Name
Casbaneiro

Description
[Metamorfo](https://attack.mitre.org/software/S0455) is a Latin-American banking trojan operated by a Brazilian cybercrime group that has been active since at least April 2018. The group focuses on targeting banks and cryptocurrency services in Brazil and Mexico. (Citation: Medium Metamorfo Apr 2020)(Citation: ESET Casbaneiro Oct 2019)

Intrusion-Set

Name
Cerberus (ex-Amnesia)

Country

Name
Micronesia, Federated States of
Name
Congo, Democratic Republic of the
Name
Palestine
Name
Virgin Islands, U.S.
Name
Macao
Name
Venezuela, Bolivarian Republic of
Name
Bolivia, Plurinational State of

Name
Iran, Islamic Republic of
Name
Hong Kong
Name
French Polynesia
Name
Palau
Name
Northern Mariana Islands
Name
Kiribati
Name
Guam
Name
Papua New Guinea
Name
New Caledonia

Name
Fiji
Name
Norfolk Island
Name
New Zealand
Name
Australia
Name
Switzerland
Name
Netherlands
Name
Monaco
Name
Luxembourg
Name
Germany

Name
Liechtenstein
Name
France
Name
Belgium
Name
Austria
Name
Spain
Name
Slovenia
Name
Serbia
Name
San Marino
Name
Portugal

Name
North Macedonia
Name
Italy
Name
Malta
Name
Montenegro
Name
Greece
Name
Croatia
Name
Bosnia and Herzegovina
Name
Andorra
Name
Albania

Name
United Kingdom
Name
Sweden
Name
Norway
Name
Lithuania
Name
Latvia
Name
Isle of Man
Name
Ireland
Name
Iceland
Name
Finland

Name
Faroe Islands
Name
Estonia
Name
Denmark
Name
Jersey
Name
Guernsey
Name
Ukraine
Name
Slovakia
Name
Russian Federation
Name
Romania

Name
Moldova, Republic of
Name
Poland
Name
Hungary
Name
Czechia
Name
Bulgaria
Name
Belarus
Name
Cyprus
Name
Yemen
Name
United Arab Emirates

Name
Syrian Arab Republic
Name
Saudi Arabia
Name
Qatar
Name
Oman
Name
Lebanon
Name
Jordan
Name
Kuwait
Name
Israel
Name
Iraq

Name
Georgia
Name
Bahrain
Name
Azerbaijan
Name
Armenia
Name
Sri Lanka
Name
Nepal
Name
Pakistan
Name
Maldives
Name
India

Name
Afghanistan
Name
Bhutan
Name
Bangladesh
Name
Timor-Leste
Name
Philippines
Name
Singapore
Name
Thailand
Name
Myanmar
Name
Malaysia

Name
Cambodia
Name
Indonesia
Name
Brunei Darussalam
Name
Taiwan
Name
Japan
Name
Mongolia
Name
China
Name
Uzbekistan
Name
Turkmenistan

Name
Tajikistan
Name
Kyrgyzstan
Name
Kazakhstan
Name
United States
Name
Greenland
Name
Canada
Name
Bermuda
Name
Uruguay
Name
Suriname

Name
South Georgia and the South Sandwich Islands
Name
Peru
Name
Paraguay
Name
Guyana
Name
French Guiana
Name
Ecuador
Name
Colombia
Name
Chile
Name
Brazil

Name
Argentina
Name
Nicaragua
Name
Panama
Name
Mexico
Name
Honduras
Name
Guatemala
Name
El Salvador
Name
Costa Rica
Name
Belize

Name
Turks and Caicos Islands
Name
Trinidad and Tobago
Name
Saint Martin (French part)
Name
Saint Lucia
Name
Saint Kitts and Nevis
Name
Puerto Rico
Name
Martinique
Name
Jamaica
Name
Haiti

Name
Guadeloupe
Name
Grenada
Name
Dominican Republic
Name
Dominica
Name
Curaçao
Name
Cuba
Name
Cayman Islands
Name
Virgin Islands, British
Name
Barbados

Name
Bahamas
Name
Antigua and Barbuda
Name
Anguilla
Name
Togo
Name
Sierra Leone
Name
Senegal
Name
Nigeria
Name
Niger
Name
Mauritania

Name
Mali
Name
Liberia
Name
Guinea-Bissau
Name
Guinea
Name
Ghana
Name
Gambia
Name
Cabo Verde
Name
Burkina Faso
Name
Benin

Name
South Africa
Name
Namibia
Name
Lesotho
Name
Eswatini
Name
Botswana
Name
Gabon
Name
Equatorial Guinea
Name
Congo
Name
Chad

Name
Central African Republic
Name
Cameroon
Name
Angola
Name
Zimbabwe
Name
Zambia
Name
Tanzania, United Republic of
Name
Uganda
Name
South Sudan
Name
Somalia

Name
Rwanda
Name
Mozambique
Name
Mauritius
Name
Malawi
Name
Madagascar
Name
Kenya
Name
Ethiopia
Name
Djibouti
Name
Comoros

Name
Burundi
Name
British Indian Ocean Territory
Name
Tunisia
Name
Sudan
Name
Morocco
Name
Libya
Name
Egypt
Name
Algeria

Region

Name
Polynesia
Name
Micronesia
Name
Melanesia
Name
Australia and New Zealand
Name
Oceania
Name
Western Europe
Name
Southern Europe

Name
Northern Europe
Name
Eastern Europe
Name
Europe
Name
Middle East
Name
Southern Asia
Name
South-eastern Asia
Name
Eastern Asia
Name
Central Asia
Name
Asia

Name
Northern America
Name
Latin America and the Caribbean
Name
Americas
Name
Sub-Saharan Africa
Name
Northern Africa
Name
Africa

IPv4-Addr

Value
195.10.205.74
147.45.44.5
5.42.65.36
5.42.65.101
37.220.87.13

StixFile

Value
ffadffdb70628e31d82c7f79dbb60ee917f09d47c085a19e1ac6e6e1e35f65d2
e50ffa2b9fd2f72117215aae4bd556181a1c43f0e485ee2ede668ae67ff8b37d
ddd48bf86fb56853f8d7ec54bdd9922044f4f6a97aa16c4b1b6da4d162c63f50
b9161bebfa420e361053fe2d28cbacb9f59e12bb2e9ae6dc241326ec5b32429a
b86815c10b68f1108530338128c8f0a79d358ee91bc43082a2314985fa4db1ba
aa79dd98bfa1024797b92c3016e931180faf9baa462e751a8eb9061fbfd7a06c
9f8a9a96bcd4b50414604cbd67f282226a2af227972833725e133c60da35ad43
7eca655f69b3b43c4f228dbd149b73247166872ba92691f7fb00f7f35bb89e41
48660eb510470d5ebf35a0dfdb4c592117eaec4f07cbf01d428099f052a2fdca
2f51a381d2fc22009dd2e7e27d555b7e10de4fbc954d27e506c5c3ba83481577
24952724df0a06ae1d58350bacc43c37981e46267c9f7575192e222028eb7626
16fbabbe3842fee9262fd42da0151f81e4375652d59b01f75a1f0dff46cda69f
0aa93d611bbbe91ef03cce5ad22160fa4cea54a8e5b322f85be9b2a139e069e2

fc43e409ca887fe8f98079100e54a442b7ab01a2743d7e195ba2c8358a1152df

f1317fa1e70ad44256d1282121c8ad5e12faf9a32fc6b743212726d666408967

2318f5ddf39a7576e33513557c3af1498e841cef7b36acc53e80ddd700ac0d62

c4b216b616c005c7ae84dfbdc5f2a99172825e1ee362555ddad8ed29f23313d6

495d6698ee5c9a61d68bfd5328fa2e0979ff0ae04d1a2655e5d580e73fe6b998

005360f36d6b7bf31717fb5ba88f844bdf5455dfbd9f84894a8c1e53f7f5ef51

External References

- https://g0njxa.medium.com/profiling-traffic-cerberus-ex-amnesia-3758faba4385
- https://otx.alienvault.com/pulse/663de2a924a61f8a74567f55