Sep 06 2023

NETMANAGEIT

Intelligence Report

New Agent Tesla Variant Being Spread by Crafted Excel Document

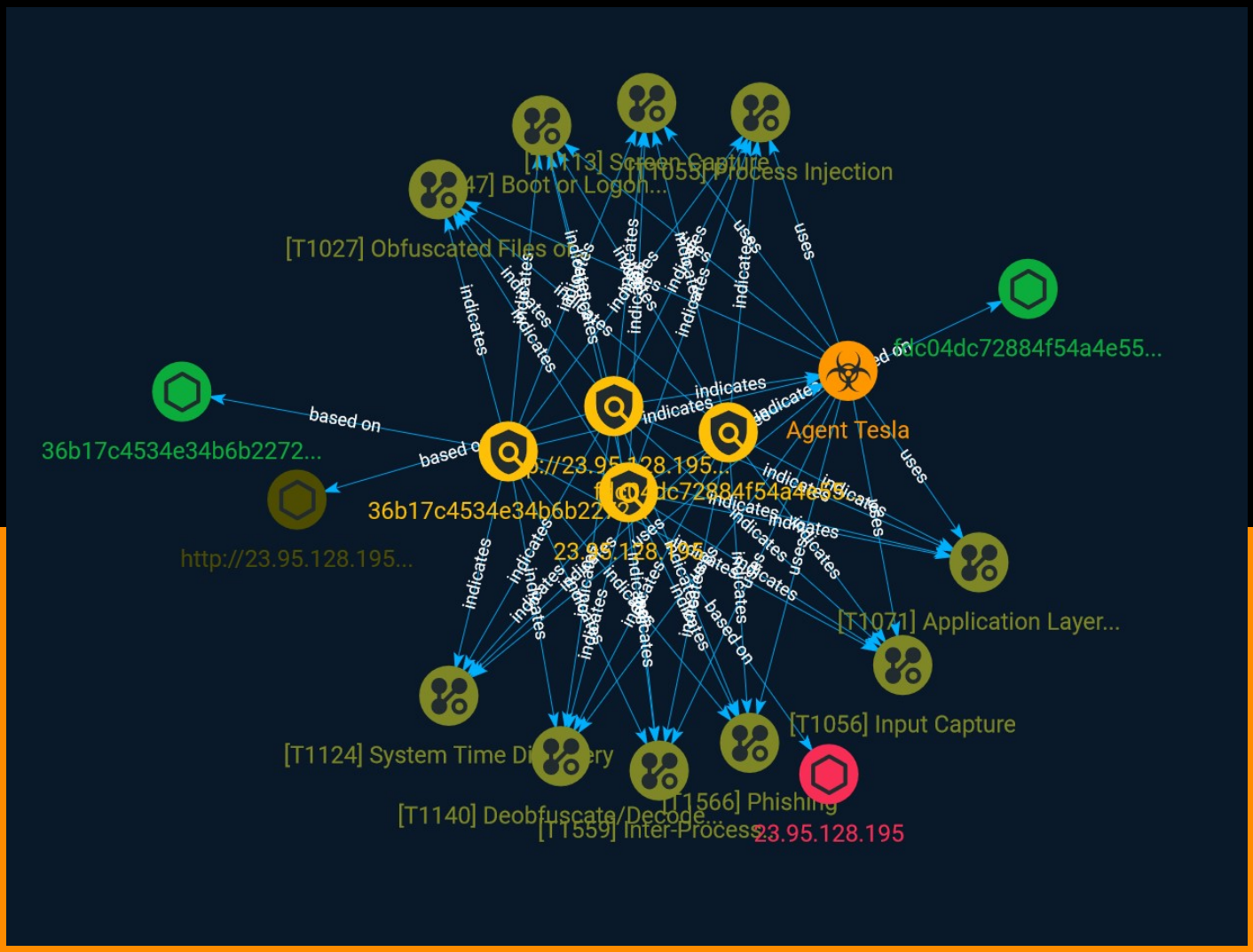

Table of contents

Overview

Entities

Observables

External References

Overview

Description

FortiGuard Labs captured a phishing campaign that spreads a new Agent Tesla variant. This well-known malware family uses a .Net-based Remote Access Trojan (RAT) and data stealer to gain initial access. It is often used for Malware-as-a-Service (MaaS).

Confidence

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

15 / 100

Indicator

Name

http://23.95.128.195/3355/chromium.exe

Description

Threat: malware_download - Reporter: abuse_ch - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://23.95.128.195/3355/chromium.exe']

Name

23.95.128.195

Description

ISP: ColoCrossing **OS:** None ------------------------- Hostnames: - 23-95-128-195-host.colocrossing.com ------------------------- Domains: - colocrossing.com ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Date: Tue, 22 Aug 2023 10:35:12 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28 Last-Modified: Thu, 06 Apr 2023 09:24:30 GMT ETag: "1443-5f8a779c90f80" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` ----------------- **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service

ncacn_ip_tcp: 23.95.128.195:49664 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-JDPEQD10OQR\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 23.95.128.195:49664 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-JDPEQD10OQR\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 23.95.128.195:49664 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-JDPEQD10OQR\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: 23.95.128.195:49664 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-JDPEQD10OQR\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 23.95.128.195:49665 ncalrpc: WindowsShutdown ncacn_np: \\WIN-JDPEQD10OQR\PIPE\InitShutdown ncalrpc: WMsgKRpc054DF0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-JDPEQD10OQR\PIPE\InitShutdown ncalrpc: WMsgKRpc054DF0 ncalrpc: WMsgKRpc0577B1 ncalrpc: WMsgKRpc051B9582 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-64654149e2feef83f6 ncalrpc: LRPC-7d1dc3ba350ae3bec7 ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-64654149e2feef83f6 ncalrpc: LRPC-7d1dc3ba350ae3bec7 ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-7d1dc3ba350ae3bec7 ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-cbea7b8967bbc8b221 ncalrpc: LRPC-90460c7ae61d19d2c1 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-64654149e2feef83f6 ncalrpc: LRPC-7d1dc3ba350ae3bec7 ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel

ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-7d1dc3ba350ae3bec7 ncalrpc: LRPC-0c16d89e26d3151cd1 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 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-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-aa56a0ae2bab3b2fc8 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLE5CA2EE56A31520B589EC13BE5A3B ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-a0609c0dc20b710ae4 ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 0361ae94-0316-4c6c-8ad8-c594375800e2 version: v1.0 ncalrpc: umpo 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 version: v1.0 ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-1e0b505f6335d8e2bc ncalrpc: IUserProfile2 ncalrpc: LRPC-8b24e5ae4c551654a0

ncalrpc: LRPC-dd8674a7ca11ebab88 ncalrpc: senssvc ncalrpc: LRPC-6dc0c02c4a72e5c228 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-ac88d68b23bce2efc0 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-f49a961e3310436670 ncalrpc: OLE732381AAB825B62773955D86501E ncalrpc: LRPC-cbea7b8967bbc8b221 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-9e02c6e3db5e0fcfd8 a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-7eda094d485175af83 ncalrpc: LRPC-90460c7ae61d19d2c1 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 23.95.128.195:49666 ncacn_np: \\WIN-JDPEQD10OQR\pipe\eventlog ncalrpc: eventlog 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-4ecac551281c0f396d 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-303d1b28fe793dc36d 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 23.95.128.195:49667 ncalrpc: LRPC-e2d2fb1e12e2d07f4c ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-d7277f2a6887f8d0ff 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 23.95.128.195:49667 ncalrpc: LRPC-e2d2fb1e12e2d07f4c ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-d7277f2a6887f8d0ff 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-e2d2fb1e12e2d07f4c ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-d7277f2a6887f8d0ff 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-d7277f2a6887f8d0ff 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-d7277f2a6887f8d0ff 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-d7277f2a6887f8d0ff 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-b8ec1583418d2751f7 ncalrpc: OLE18BB8998E2E89277B17E4A86817A 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-33032d119ac247f3fb 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-3edd018fe9dc1f340a ncalrpc: DNSResolver 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-JDPEQD10OQR\PIPE\wkssvc ncalrpc: LRPC-3d74ecbc9ba56b1168 eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-3d74ecbc9ba56b1168 f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-3d74ecbc9ba56b1168 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-df3818dfe57269017d c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-df3818dfe57269017d f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-df3818dfe57269017d

b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-df3818dfe57269017d abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-df3818dfe57269017d 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 23.95.128.195:49668 ncacn_np: \\WIN-JDPEQD10OQR\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-6dc0c02c4a72e5c228 3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-6e18a5c0552a3561d3 ncalrpc: OLECEFFE5334753ECDA8A9EB428E94B 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-e3bf39238b1dd9b99d ncalrpc: LRPC-2a168c9f3f5c19ba0e ncalrpc: LRPC-05ec00a3a0ba4631fc ncalrpc: LRPC-3d4f72952a490123e1 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-2a168c9f3f5c19ba0e ncalrpc: LRPC-05ec00a3a0ba4631fc ncalrpc: LRPC-3d4f72952a490123e1 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-05ec00a3a0ba4631fc ncalrpc: LRPC-3d4f72952a490123e1 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-3d4f72952a490123e1 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-b954bfa5d5f3f8183c ncalrpc: OLE9BF3AC2947E506A1434122D473B0 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-b954bfa5d5f3f8183c ncalrpc: OLE9BF3AC2947E506A1434122D473B0 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.95.128.195:49669 ncalrpc: LRPC-e6e64840ddd32e5483 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 23.95.128.195:49669 ncalrpc: LRPC-e6e64840ddd32e5483 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.95.128.195:49669 ncalrpc: LRPC-e6e64840ddd32e5483 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.95.128.195:49669 ncalrpc: LRPC-e6e64840ddd32e5483 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.95.128.195:49669 ncalrpc: LRPC-e6e64840ddd32e5483 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: OLE170C5414A9949A95C474FE792223 ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f88844c921a96b8e8d c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f88844c921a96b8e8d 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f88844c921a96b8e8d 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-f88844c921a96b8e8d 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-fefea609097a9cd442 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-fefea609097a9cd442 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 23.95.128.195:49670

b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-1da1293525cc4b250a 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-8aa1e5ed9be42ff2df ncalrpc: OLEE5C50091E47B0B5AF73146826CB2 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-13b7497ef831bee946 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-578b62f280f1876b47 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\WIN-JDPEQD10OQR\PIPE\ROUTER f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-ba22d925cb76d0375a ncalrpc: LRPC-d5fc1aea3d382a50c4 d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-d17ad7553810141cd4 d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-d17ad7553810141cd4 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-4004f2c48cd82c1526 ncalrpc: LRPC-4004f2c48cd82c1526 ncalrpc: LRPC-4004f2c48cd82c1526 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-edfc3cb13ce9be93a1 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc051B9582 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-261b706440ede3a871 ncalrpc: OLE383C0F28EE02A8CB806988142312 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-261b706440ede3a871 ncalrpc: OLE383C0F28EE02A8CB806988142312 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-261b706440ede3a871 ncalrpc: OLE383C0F28EE02A8CB806988142312 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d4e93a7c4f9cc959ce fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d4e93a7c4f9cc959ce 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d4e93a7c4f9cc959ce 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d4e93a7c4f9cc959ce 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-d4e93a7c4f9cc959ce a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-7eb974136c853f7e23 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: 23.95.128.195:60617 bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-bc3570190b4c3be6bc ncalrpc:

OLEA38614D03F16947DCA07B594A33E ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sun, 03 Sep 2023 14:05:12 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28 Last-Modified: Thu, 06 Apr 2023 09:24:30 GMT ETag: "1443-5f8a779c90f80" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` HEARTBLEED: 2023/09/03 14:05:20 23.95.128.195:443 - SAFE ---------- **3306:** ``` MariaDB: Error Message: Host '224.211.74.215' is not allowed to connect to this MariaDB server Error Code: 1130 ``` ---------- **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-JDPEQD10OQR NetBIOS Domain Name: WIN-JDPEQD10OQR NetBIOS Computer Name: WIN-JDPEQD10OQR DNS Domain Name: WIN-JDPEQD10OQR FQDN: WIN-JDPEQD10OQR ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 01 Sep 2023 17:10:30 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.95.128.195']

Name

36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda7702820efcfc3a

Description

ALF:Trojan:MSIL/AgentTesla.KM

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda7702820efcfc3a']

Name

fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904c22638

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904c22638']

Malware

Name
Agent Tesla

Description
[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

Attack-Pattern

Name

Inter-Process Communication

ID

T1559

Description

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern. Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

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

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

System Time Discovery

ID

T1124

Description

An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. (Citation: MSDN System Time)(Citation: Technet Windows Time Service) System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing `net time \\hostname` to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using `w32tm /tz`.(Citation: Technet Windows Time Service) On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show clock detail` can be used to see the current time configuration.(Citation: show_clock_detail_cisco_cmd) This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)(Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary

code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

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

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

Application Layer Protocol

ID

T1071

Description

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

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

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

Name

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)

StixFile

Value
36b17c4534e34b6b22728db194292b504cf492ef8ae91f9dda7702820efcfc3a
fdc04dc72884f54a4e553b662f1f186697daf14ef8a2dc367bc584d904c22638

IPv4-Addr

Value
23.95.128.195

Url

Value
http://23.95.128.195/3355/chromium.exe

External References

- https://otx.alienvault.com/pulse/64f8a5c3e1dd7d913cdf3bcc
- https://www.fortinet.com/blog/threat-research/agent-tesla-variant-spread-by-crafted-excel-document