Jul 21 2023

NETMANAGEIT

Intelligence Report

Threat Group Assessment: Mallox Ransomware

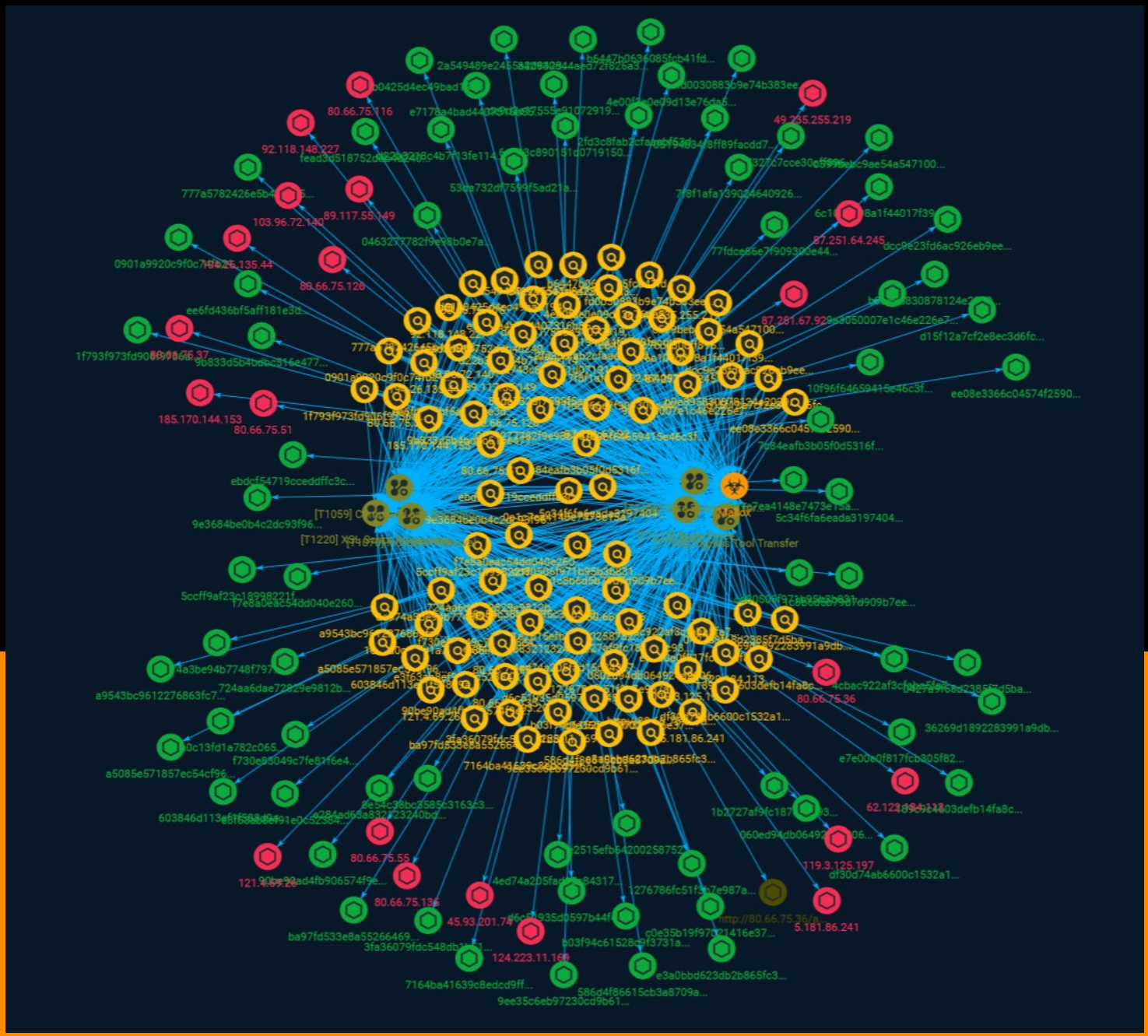

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Mallox (aka TargetCompany, FARGO and Tohnichi) is a ransomware strain that targets Microsoft (MS) Windows systems. It has been active since June 2021, and is notable for exploiting unsecured MS-SQL servers as a penetration vector to compromise victims' networks.

Confidence

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

15 / 100

Indicator

Name
724aa6dae72829e9812b753d188190e16fb64ac6cd39520897d917cfdccc5122
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '724aa6dae72829e9812b753d188190e16fb64ac6cd39520897d917cfdccc5122']
Name
80.66.75.135
Pattern Type
stix
Pattern
[ipv4-addr:value = '80.66.75.135']
Name

05194b34f8ff89facdd7b56d05826b08edaec9c6e444bdc32913e02cab01afd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05194b34f8ff89facdd7b56d05826b08edaec9c6e444bdc32913e02cab01afd4']

Name

f730e83049c7fe81f6e4765ab91efbb7a373751d51fdafe697a4977dc7c1ea11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f730e83049c7fe81f6e4765ab91efbb7a373751d51fdafe697a4977dc7c1ea11']

Name

cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a']

Name

7c84eafb3b05f0d5316fae610d9404c54ef39383d0fe0e3c07407a26bb9f6750

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c84eafb3b05f0d5316fae610d9404c54ef39383d0fe0e3c07407a26bb9f6750']

Name

1e2515efb64200258752d785863fd35df6039441a80cb615dfff4fbdffb484ec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e2515efb64200258752d785863fd35df6039441a80cb615dfff4fbdffb484ec']

Name

6c743c890151d0719150246382b5e0158e8abc4a29dd4b2f049ce7d313b1a330

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c743c890151d0719150246382b5e0158e8abc4a29dd4b2f049ce7d313b1a330']

Name

2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d54cb014

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d54cb014']

Name

0463277782f9e98b0e7a028cea0f689a81cf080fa0d64d4de8ef4803bb1bf03a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0463277782f9e98b0e7a028cea0f689a81cf080fa0d64d4de8ef4803bb1bf03a']

Name

87.251.64.245

Pattern Type

stix

Pattern

[ipv4-addr:value = '87.251.64.245']

Name

80.66.75.36

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.36']

Name

0e1c7ea4148e7473e15a8e55413d6972eec6e24ef365e9f629884f89645de71a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e1c7ea4148e7473e15a8e55413d6972eec6e24ef365e9f629884f89645de71a']

Name

1b2727af9fc187cd5c932c6defe50b983ad7508b4196ad6c5ff5e96686277c56

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b2727af9fc187cd5c932c6defe50b983ad7508b4196ad6c5ff5e96686277c56']

Name

45.93.201.74

Description

ISP: IT Resheniya LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Server: nginx/1.23.3 Date: Sat, 11 Feb 2023 13:14:23 GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 45.93.201.74:1025 ncalrpc: WindowsShutdown ncacn_np: \\M051111\PIPE\InitShutdown ncalrpc: WMsgKRpc06C130 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\M051111\PIPE\InitShutdown ncalrpc: WMsgKRpc06C130 ncalrpc: WMsgKRpc0C12D1 ncalrpc: WMsgKRpc05704F3 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-26eb846021b81414cc ncacn_np: \ \M051111\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-e21fbc06cba3526c71 ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-26eb846021b81414cc ncacn_np: \\M051111\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-e21fbc06cba3526c71 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-e21fbc06cba3526c71 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-d9d9347f9d41710a17 ncacn_np: \\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc:

OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0C12D1 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc ncalrpc: LRPC-08e7959b9a09235c97 ncacn_ip_tcp: 45.93.201.74:1026 ncacn_np: \\M051111\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: LRPC-08e7959b9a09235c97 ncacn_ip_tcp: 45.93.201.74:1026 ncacn_np: \\M051111\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-08e7959b9a09235c97 ncacn_ip_tcp: 45.93.201.74:1026 ncacn_np: \ \M051111\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-08e7959b9a09235c97 ncacn_ip_tcp: 45.93.201.74:1026 ncacn_np: \ \M051111\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: 45.93.201.74:1026 ncacn_np: \\M051111\pipe\eventlog ncalrpc: eventlog 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: DeviceSetupManager ncacn_np: \ \M051111\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-d9d9347f9d41710a17 ncacn_np: \\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: DeviceSetupManager ncacn_np: \\M051111\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-d9d9347f9d41710a17 ncacn_np: \\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: DeviceSetupManager ncacn_np: \ \M051111\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-d9d9347f9d41710a17 ncacn_np: \\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:

OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2
201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider:
appinfo.dll ncalrpc: DeviceSetupManager ncacn_np: \\M051111\pipe\SessEnvPublicRpc
ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-d9d9347f9d41710a17 ncacn_np: \
\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel
ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 30b044a5-a225-43f0-b3a4-
e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-d9d9347f9d41710a17
ncacn_np: \\M051111\PIPE\srvsvc ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 1a0d010f-1c33-432c-
b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 45.93.201.74:1027
ncalrpc: ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 98716d03-89ac-44c7-
bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll
ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \
\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc:
IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs
ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \
\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc:
IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy
Manager client server endpoint ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-
a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint
ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \
\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc:
IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition
Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 a398e520-d59a-4bdd-
aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL
ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \
\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc:
IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp:
45.93.201.74:1027 ncalrpc: ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc:
senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2
86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler
Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 45.93.201.74:1027 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc:
OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 378e52b0-
c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service
Remoting Protocol provider: taskcomp.dll ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc
ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2

1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\M051111\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLE047919D78A0B530F523C62821F80 ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-8993f8e08ab53cfa97 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\M051111\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: LRPC-81b154a8c8e046d9b9 ncalrpc: OLEAB92B4904E3F1395C2A8D7AE5052 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-81b154a8c8e046d9b9 ncalrpc: OLEAB92B4904E3F1395C2A8D7AE5052 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-9c7eb4c86f02ba1ea0 ncalrpc: LRPC-6767ea5b647efa37ba f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-9c7eb4c86f02ba1ea0 ncalrpc: LRPC-6767ea5b647efa37ba 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-9c7eb4c86f02ba1ea0 ncalrpc: LRPC-6767ea5b647efa37ba dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-6767ea5b647efa37ba 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\M051111\PIPE\wkssvc ncalrpc: LRPC-6181c4c21465bcf997 ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-6181c4c21465bcf997 ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-6181c4c21465bcf997 ncalrpc: DNSResolver 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 45.93.201.74:1028 ncalrpc: LRPC-528315f00cfda99f3e 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 45.93.201.74:1028 ncalrpc: LRPC-528315f00cfda99f3e ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 45.93.201.74:1028 ncalrpc: LRPC-528315f00cfda99f3e 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 45.93.201.74:1028 ncalrpc: LRPC-528315f00cfda99f3e 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 45.93.201.74:1028 ncalrpc: LRPC-528315f00cfda99f3e 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 45.93.201.74:1029 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: 45.93.201.74:1030 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 45.93.201.74:1033 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: \\M051111\pipe\lsass 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-4cf5179a60552c57b6 ncalrpc: LRPC-4cf5179a60552c57b6 ncalrpc: LRPC-4cf5179a60552c57b6 b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-e4bd34bd41d38113f3 ``` ---------- **137:** ``` NetBIOS Response: MAC Address: 3C:EC:EF:70:AC:9E ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.93.201.74']

Name

ee6fd436bf5aff181e3d4b9a944bf644076e902a1bbf622978b5e005522c1f77

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee6fd436bf5aff181e3d4b9a944bf644076e902a1bbf622978b5e005522c1f77']

Name

ebdcf54719cceddffc3c254b0bfb1a2b2c8a136fa207293dbba8110f066d9c51

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ebdcf54719cceddffc3c254b0bfb1a2b2c8a136fa207293dbba8110f066d9c51']

Name

8e54c38bc3585c3163c3e25d037bcf55695c274aaea770f2f59f0a0910a4b572

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e54c38bc3585c3163c3e25d037bcf55695c274aaea770f2f59f0a0910a4b572']

Name

de9d3e17555e91072919dc700dc7e588cd52617debcad2f764ef9c7fbf6c9f7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de9d3e17555e91072919dc700dc7e588cd52617debcad2f764ef9c7fbf6c9f7b']

Name

http://80.66.75.36/aRX.exe

Description

Simple indicator of observable {http://80.66.75.36/aRX.exe}

Pattern Type

stix

Pattern

[url:value = 'http://80.66.75.36/aRX.exe']

Name

80.66.75.37

Description

ISP: Kakharov Orinbassar Maratuly **OS:** Windows Server 2012 R2 Datacenter 9600 ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 18 Jul 2023 01:48:17 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Tue, 13 Dec 2022 15:53:53 GMT Connection: keep-alive ETag: "6398a011-267" Accept-Ranges: bytes ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Datacenter 9600 Software: Windows Server 2012 R2 Datacenter 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 09 Jul 2023 04:03:28 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.37']

Name

d6c51935d0597b44f45f1b36d65d3b01b6401593f95cb4c2786034072ad89b63

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6c51935d0597b44f45f1b36d65d3b01b6401593f95cb4c2786034072ad89b63']

Name

10eea0c13fd1a782c065627e23e7051edc1622f2eae5fbe138725369c12f4b6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10eea0c13fd1a782c065627e23e7051edc1622f2eae5fbe138725369c12f4b6d']

Name

e7178a4bad4407316b85894307df32fdf85b597455364eb8ec4d407749e852ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7178a4bad4407316b85894307df32fdf85b597455364eb8ec4d407749e852ce']

Name

119.3.125.197

Pattern Type

stix

Pattern

[ipv4-addr:value = '119.3.125.197']

Name

194.26.135.44

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.26.135.44']

Name

cb47327c7cce30cff8962c48fa3b51e57e331e1592ea78b21589164c5396ccd9

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'cb47327c7cce30cff8962c48fa3b51e57e331e1592ea78b21589164c5396ccd9']
Name
e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf8cf4f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf8cf4f']
Name
d22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8bca
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8bca']

Name

f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bdb1a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bdb1a']

Name

80.66.75.51

Description

ISP: Kakharov Orinbassar Maratuly **OS:** Windows Server 2012 R2 (build 6.3.9600) ------------------------- 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: 80.66.75.51:49152 ncalrpc: WindowsShutdown ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\InitShutdown ncalrpc: WMsgKRpc045380 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\InitShutdown ncalrpc: WMsgKRpc045380 ncalrpc: WMsgKRpc0461D1 ncalrpc: WMsgKRpc01AE362 ncalrpc: WMsgKRpc0319BA3 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-b8960753e5ed16e733 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f9e103e64510f66110 ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-b8960753e5ed16e733 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f9e103e64510f66110 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-f9e103e64510f66110 ncalrpc: actkernel ncalrpc: umpo ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\srvsvc ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc:

OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-aaf540cc35110e1a57 ncacn_ip_tcp: 80.66.75.51:49153 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: LRPC-aaf540cc35110e1a57 ncacn_ip_tcp: 80.66.75.51:49153 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-aaf540cc35110e1a57 ncacn_ip_tcp: 80.66.75.51:49153 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-aaf540cc35110e1a57 ncacn_ip_tcp: 80.66.75.51:49153 ncacn_np: \\WIN-CLJ1B0GQ6JP\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: 80.66.75.51:49153 ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\eventlog ncalrpc: eventlog 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-230d821eb6741eaf27 ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\srvsvc ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc:

OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 80.66.75.51:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLE6DFD89500A5692BBAF07653CFA30 ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-66fccc610156060624 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: LRPC-1f615090e1afec2e62 ncalrpc: OLEB86E81B5168B6BAE87DB8B28A730 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-1f615090e1afec2e62 ncalrpc: OLEB86E81B5168B6BAE87DB8B28A730 b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-e3aa88570a4e73edb4 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-4508063d1fa25c8c67 ncalrpc: LRPC-d7e0d3c8aba50b0053 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-4508063d1fa25c8c67 ncalrpc: LRPC-d7e0d3c8aba50b0053 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-4508063d1fa25c8c67 ncalrpc: LRPC-d7e0d3c8aba50b0053 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-d7e0d3c8aba50b0053 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-CLJ1B0GQ6JP\PIPE\wkssvc ncalrpc: LRPC-485e2d68bbb1faf8a9 ncalrpc: DNSResolver

eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-485e2d68bbb1faf8a9 ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-485e2d68bbb1faf8a9 ncalrpc: DNSResolver 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 80.66.75.51:49155 ncalrpc: LRPC-e74c6be5e2e5a5524c 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 80.66.75.51:49155 ncalrpc: LRPC-e74c6be5e2e5a5524c ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 80.66.75.51:49155 ncalrpc: LRPC-e74c6be5e2e5a5524c 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 80.66.75.51:49155 ncalrpc: LRPC-e74c6be5e2e5a5524c 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 80.66.75.51:49155 ncalrpc: LRPC-e74c6be5e2e5a5524c 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 80.66.75.51:49157 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: 80.66.75.51:49158 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 80.66.75.51:49163 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-CLJ1B0GQ6JP\pipe\lsass 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc01AE362 ncalrpc: WMsgKRpc0319BA3 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-059cf8efe18082a9cf ncalrpc: LRPC-059cf8efe18082a9cf ncalrpc: LRPC-059cf8efe18082a9cf ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 19 Jul 2023 07:05:15 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.51']

Name

c599bebc9ae54a54710008042361293d71475e5fbe8f0cbaceb6ee4565a72015

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c599bebc9ae54a54710008042361293d71475e5fbe8f0cbaceb6ee4565a72015']

Name

1276786fc51f3b7e987aa95ebff0a3e1e358ee4e86e2302e472f84710271af7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1276786fc51f3b7e987aa95ebff0a3e1e358ee4e86e2302e472f84710271af7b']

Name

103.96.72.140

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.96.72.140']

Name

7f8f1afa1390246409263e606aa05e2896b8d1da7018c534e67ca530a59ebda1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f8f1afa1390246409263e606aa05e2896b8d1da7018c534e67ca530a59ebda1']

Name

a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d3f22e33ed636525

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d3f22e33ed636525']

Name

fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be65ab176

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be65ab176']

Name

1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13']

Name

5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552']

Name

80.66.75.126

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.126']

Name

e284ad63a832123240bd40b6c09565fae8525c00ddf308d5b8f5c8ce69ed6b09

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e284ad63a832123240bd40b6c09565fae8525c00ddf308d5b8f5c8ce69ed6b09']

Name

92.118.148.227

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.148.227']

Name

e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009']

Name

9e3684be0b4c2dc93f962c03275e050fed57d9be6411396f51bdf8d4bb5e21c0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e3684be0b4c2dc93f962c03275e050fed57d9be6411396f51bdf8d4bb5e21c0']

Name

d15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570']

Name

c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c']

Name

89.117.55.149

Description

ISP: Contabo GmbH **OS:** None ---------- Hostnames: - vmi1326867.contaboserver.net ---------- Domains: - contaboserver.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAACAQCfo/vp1ekcGc2EDiNm9+DYF4Kg/PWSUrEQhkSJmgqjJl+r vjcu3mBixZMbqu1hzMzmsLKM12W+iUuTStE+J03uTug6obuJc2JTEWgvzvRwE3oF7papYI3xAQ8IG8ZrjJY+QoI7RAOxKI6tlzYKv0AjYpcs7awheI21G1/K37vzilcvo/PhfjeiF4rNMOyT9Y+Acx6/jJqYCLi6/uu3H2xQuGZhXWPU0ylhCM9BjeUGJNDKs52ZHKCkRUKD5zWYnjA8Hwu8hZuoFhKgbZxSmUJHYeJA9g/hTuLwqt3vN3mw8OkT3T/5E+Fw/SgTrskHsIVfxLlV8wE6vigtcpS/opbmk8+crXKiEMeCl8oFYw9ElZD++bTFPeQr7BnjpIpw46FUt+e4Tn6agEfl2Q85MnDdCZHRPERvVoHIIo0JQ4ok0O0Y6OKMmz0cSYt7WWLmD4f8XXmcsEKNwg2MlKJ/RKraeDOmjORRA56qBEvo0J/yCWSFIwEUPs6N jfr/XRydrvzZJqxAbL2s0PukG5Xm3nOQ2hQd9fGnzT335N88TAIm/Nr6+cisE1pBWoCd0/k3a3sc gscth+8/J0WPiTCd8LM37TC512l+W5YWviqJ04zFXl33pNgBQjUAtx9Z2+ZOzNIAYcJCoQImW1B8Rxt4vKIEM0CPBxK0J8/0edNCUOnaKw== Fingerprint: d4:57:1f:b7:2d:

5a:e6:d0:ee:c4:a1:63:b9:c2:b5:bf 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 = '89.117.55.149']

Name

9a3050007e1c46e226e7c2c27d4703f6396280386329044919 3a0d0ca9661b3b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a3050007e1c46e226e7c2c27d4703f6396280386329044919 3a0d0ca9661b3b']

Name

9ee35c6eb97230cd9b61ba32dba7befea4122f89b3747d2389970050a1d019f9

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9ee35c6eb97230cd9b61ba32dba7befea4122f89b3747d2389970050a1d019f9']
Name
342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c937b28a53e4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c937b28a53e4']
Name
ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3cfade9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3cfade9']

Name

53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b8187c95c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b8187c95c']

Name

6c109d098a1f44017f3937a71628d9dbd4d2ca8aa266656ee4720c37cc31558e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c109d098a1f44017f3937a71628d9dbd4d2ca8aa266656ee4720c37cc31558e']

Name

060ed94db064924a90065a5f4efb50f938c52619ca003f096482353e444bd096

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '060ed94db064924a90065a5f4efb50f938c52619ca003f096482353e444bd096']

Name

87.251.67.92

Pattern Type

stix

Pattern

[ipv4-addr:value = '87.251.67.92']

Name

4ed74a205fad15c843174d7d8b30ae60a181e79f31cc30ebc683072f187e4cdd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4ed74a205fad15c843174d7d8b30ae60a181e79f31cc30ebc683072f187e4cdd']

Name

3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4']

Name

b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851']

Name

189c9c4603defb14fa8c942f5ff7814804654269917640478686530f91c4b66c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '189c9c4603defb14fa8c942f5ff7814804654269917640478686530f91c4b66c']

Name

9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc30d3335458a97

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc30d3335458a97']

Name

4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2']

Name

b03f94c61528c9f3731a2e8da4975c072c9ed4e5372d3ec6b0939eebe01e54a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b03f94c61528c9f3731a2e8da4975c072c9ed4e5372d3ec6b0939eebe01e54a4']

Name

d81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961cfa62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961cfa62']

Name

36269d1892283991a9db23492cd8efcd68af74060384b9686219a97f76a9989e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36269d1892283991a9db23492cd8efcd68af74060384b9686219a97f76a9989e']

Name

80.66.75.55

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.55']

Name

b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b']

Name

90be90ad4fb906574f9e7afe587f0826a71152bfc32cfc665a58877562f2edd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90be90ad4fb906574f9e7afe587f0826a71152bfc32cfc665a58877562f2edd4']

Name

0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39']

Name

10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880']

Name

121.4.69.26

Pattern Type

stix

Pattern

[ipv4-addr:value = '121.4.69.26']

Name

2a549489e2455a2d84295604e29c727dd20d65f5a874209840ce187c35d9a439

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a549489e2455a2d84295604e29c727dd20d65f5a874209840ce187c35d9a439']

Name

5.181.86.241

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.86.241']

Name

a9543bc9612276863fc77b663fa3ff6efb85db69a01baa86c6dfabf73684b5c1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a9543bc9612276863fc77b663fa3ff6efb85db69a01baa86c6dfabf73684b5c1']

Name

dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb33f6a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb33f6a']

Name

124.223.11.169

Pattern Type

stix

Pattern

[ipv4-addr:value = '124.223.11.169']

Name

777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899']

Name

5c34f6fa6eada3197404bf95eced9d288688537598629158a4f4e18d6882cb9b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5c34f6fa6eada3197404bf95eced9d288688537598629158a4f4e18d6882cb9b']

Name

603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e']

Name

4e00f3e0e09d13e76da56009173098eefafc4ad50806583d5333990fa44e6420

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e00f3e0e09d13e76da56009173098eefafc4ad50806583d5333990fa44e6420']

Name

62.122.184.113

Description

ISP: Chang Way Technologies Co. Limited **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.24.0 Date: Mon, 03 Jul 2023 09:35:12 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Sat, 03 Jun 2023 10:34:46 GMT Connection: keep-alive ETag: "647b1746-267" Accept-Ranges: bytes ``` ---------- **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: 62.122.184.113:49152 ncalrpc: WindowsShutdown ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\InitShutdown ncalrpc: WMsgKRpc09FF00 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\InitShutdown ncalrpc: WMsgKRpc09FF00 ncalrpc: WMsgKRpc0F07F1 ncalrpc: WMsgKRpc03823E03 ncalrpc: WMsgKRpc03B8C3A2 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6

ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo 5c9a4cd7-ba75-45d2-9898-1773b3d1e5f1 version: v1.0 annotation: Device Install Service RPC Interface ncalrpc: LRPC-25856165c3de1bfc43 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-7ffba8bd511e8c9394 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-f1843e5db120e07ef6 ncalrpc: actkernel ncalrpc: umpo ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-236c04c1ef91a08b77 ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 62.122.184.113:49153 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-236c04c1ef91a08b77 ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 62.122.184.113:49153 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 62.122.184.113:49153 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 62.122.184.113:49153 ncacn_np: \\WIN-IFE1ME1KNVK\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: 62.122.184.113:49153 ncacn_np: \\WIN-IFE1ME1KNVK\pipe\eventlog ncalrpc: eventlog 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: OLE56166967D2C9D0758DF5DBC35CFA ncalrpc: LRPC-5cdd8ff6b115942709 ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-5cdd8ff6b115942709 ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT 8c7daf44-

b6dc-11d1-9a4c-0020af6e7c57 version: v1.0 annotation: Group Policy RPC Interface provider: appmgmts.dll ncalrpc: LRPC-d0c0636be0e275efee 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncacn_np: \\WIN-IFE1ME1KNVK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncacn_np: \\WIN-IFE1ME1KNVK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncacn_np: \\WIN-IFE1ME1KNVK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncacn_np: \\WIN-IFE1ME1KNVK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_np: \\WIN-IFE1ME1KNVK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-9326d054b4ecb7fb32 ncalrpc: DeviceSetupManager ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\srvsvc ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server

endpoint ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \
\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc:
senssvc ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0
annotation: Adh APIs ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc: ubpmtaskhostchannel
ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5
ncalrpc: senssvc ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0
annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 62.122.184.113:49154
ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc:
OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 552d076a-
cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration
endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc:
OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2
3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 62.122.184.113:49154
ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc:
OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2
86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler
Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 62.122.184.113:49154 ncalrpc:
ubpmtaskhostchannel ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc ncalrpc:
OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2 378e52b0-
c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service
Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-IFE1ME1KNVK\PIPE\atsvc
ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc: IUserProfile2
1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler
Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-
IFE1ME1KNVK\PIPE\atsvc ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc
ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider:
schedsvc.dll ncalrpc: OLE381026A30DCA3E7D7E427626FFC5 ncalrpc: senssvc ncalrpc:
IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy
RPC Interface provider: gpsvc.dll ncalrpc: LRPC-58aeea38bf46b82afd 2fb92682-6599-42dc-
ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc:
LRPC-6ca3635ac752969f5a ncalrpc: LRPC-5a95b7ec2757ed93ec f47433c3-3e9d-4157-
aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-6ca3635ac752969f5a
ncalrpc: LRPC-5a95b7ec2757ed93ec 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0
annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-6ca3635ac752969f5a ncalrpc:
LRPC-5a95b7ec2757ed93ec dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation:
Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-5a95b7ec2757ed93ec
7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \
\WIN-IFE1ME1KNVK\PIPE\wkssvc ncalrpc: OLEE2ECEC48307513440EE666F7C32B ncalrpc:
DNSResolver ncalrpc: nlaapi ncalrpc: nlaplg ncalrpc: keysvc eb081a0d-10ee-478a-
a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc:
OLEE2ECEC48307513440EE666F7C32B ncalrpc: DNSResolver ncalrpc: nlaapi ncalrpc: nlaplg
ncalrpc: keysvc f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness
Client Upcall Server ncalrpc: OLEE2ECEC48307513440EE666F7C32B 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: 62.122.184.113:49155 ncalrpc: LRPC-408bdca0920090ea92 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 62.122.184.113:49155 ncalrpc: LRPC-408bdca0920090ea92 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 62.122.184.113:49155 ncalrpc: LRPC-408bdca0920090ea92 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 62.122.184.113:49155 ncalrpc: LRPC-408bdca0920090ea92 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 62.122.184.113:49155 ncalrpc: LRPC-408bdca0920090ea92 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 62.122.184.113:49156 b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 62.122.184.113:49157 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-IFE1ME1KNVK\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: 62.122.184.113:49157 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-IFE1ME1KNVK\pipe\lsass 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-ccb884b4fc46767607 ncalrpc: LRPC-ccb884b4fc46767607 ncalrpc: LRPC-ccb884b4fc46767607 ncalrpc: LRPC-b0d909dbb23c1db933 ncalrpc: OLE1DCFE6CD0C998AC8CDE20AF7BCC4 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0F07F1 ncalrpc: WMsgKRpc03B8C3A2 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: 62.122.184.113:49158 b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-1ac791ce6eda306e55 ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Standard Evaluation 9600 Software: Windows Server 2012 R2 Standard Evaluation 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 02 Jul 2023 21:02:33 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-IFE1ME1KNVK NetBIOS Domain Name: WIN-IFE1ME1KNVK NetBIOS Computer Name:

WIN-IFE1ME1KNVK DNS Domain Name: WIN-IFE1ME1KNVK FQDN: WIN-IFE1ME1KNVK ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.122.184.113']

Name

185.170.144.153

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.170.144.153']

Name

0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f6dae2f2020c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f6dae2f2020c4']

Name

ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b8fe949

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b8fe949']

Name

fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a']

Name

df30d74ab6600c1532a14c53a7f08f1afd41ec63cf427a4b91b99c3c2524caba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df30d74ab6600c1532a14c53a7f08f1afd41ec63cf427a4b91b99c3c2524caba']

Name

8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbbd05e83e22

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbbd05e83e22']

Name

49.235.255.219

Pattern Type

stix

Pattern

[ipv4-addr:value = '49.235.255.219']

Name

586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0']

Name

1f793f973fd906f9736aa483c613b82d5d2d7b0e270c5c903704f9665d9e1185

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f793f973fd906f9736aa483c613b82d5d2d7b0e270c5c903704f9665d9e1185']

Name

77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5

Description

Filecoder SHA256 of d215d4166dfa07be393459c99067319036eb80ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5']

Name

7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48']

Name

80.66.75.116

Description

ISP: Kakharov Orinbassar Maratuly **OS:** Windows Server 2012 R2 (build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Standard 9600 Software: Windows Server 2012 R2 Standard 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwio, nt-find, nt-smb, nt-status, rpc-remote-api, unicode ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 20 Jun 2023 17:14:35 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.75.116']

Name

e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295cb8435836a

Description

Win32:RansomX-gen\ [Ransom]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295cb8435836a']

Malware

Name
Mallox

Attack-Pattern

Name

XSL Script Processing

ID

T1220

Description

Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages. (Citation: Microsoft XSLT Script Mar 2017) Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control. Similar to [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127), the Microsoft common line transformation utility binary (msxsl.exe) (Citation: Microsoft msxsl.exe) can be installed and used to execute malicious JavaScript embedded within local or remote (URL referenced) XSL files. (Citation: Penetration Testing Lab MSXSL July 2017) Since msxsl.exe is not installed by default, an adversary will likely need to package it with dropped files. (Citation: Reaqta MSXSL Spearphishing MAR 2018) Msxsl.exe takes two main arguments, an XML source file and an XSL stylesheet. Since the XSL file is valid XML, the adversary may call the same XSL file twice. When using msxsl.exe adversaries may also give the XML/XSL files an arbitrary file extension.(Citation: XSL Bypass Mar 2019) Command-line examples:(Citation: Penetration Testing Lab MSXSL July 2017) (Citation: XSL Bypass Mar 2019) * `msxsl.exe customers[.]xml script[.]xsl` * `msxsl.exe script[.]xsl script[.]xsl` * `msxsl.exe script[.]jpeg script[.]jpeg` Another variation of this technique, dubbed “Squiblytwo”, involves using [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) to invoke JScript or VBScript within an XSL file. (Citation: LOLBAS Wmic) This technique can also execute local/remote scripts and, similar

to its [Regsvr32](https://attack.mitre.org/techniques/T1218/010)/ "Squiblydoo" counterpart, leverages a trusted, built-in Windows tool. Adversaries may abuse any alias in [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) provided they utilize the /FORMAT switch.(Citation: XSL Bypass Mar 2019) Command-line examples: (Citation: XSL Bypass Mar 2019)(Citation: LOLBAS Wmic) * Local File: `wmic process list /FORMAT:evil[.]xsl` * Remote File: `wmic os get /FORMAT:"https[:]//example[.]com/evil[.]xsl"`

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or

gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas)

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)

StixFile

Value
cb47327c7cce30cff8962c48fa3b51e57e331e1592ea78b21589164c5396ccd9
d6c51935d0597b44f45f1b36d65d3b01b6401593f95cb4c2786034072ad89b63
9e3684be0b4c2dc93f962c03275e050fed57d9be6411396f51bdf8d4bb5e21c0
1276786fc51f3b7e987aa95ebff0a3e1e358ee4e86e2302e472f84710271af7b
e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf8cf4f
342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c937b28a53e4
603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e
e7178a4bad4407316b85894307df32fdf85b597455364eb8ec4d407749e852ce
9a3050007e1c46e226e7c2c27d4703f6396280386329044919 3a0d0ca9661b3b
0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f6dae2f2020c4
ebdcf54719cceddffc3c254b0bfb1a2b2c8a136fa207293dbba8110f066d9c51
1e2515efb64200258752d785863fd35df6039441a80cb615dfff4fbdffb484ec
10eea0c13fd1a782c065627e23e7051edc1622f2eae5fbe138725369c12f4b6d

d81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961cfa62

b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b

2a549489e2455a2d84295604e29c727dd20d65f5a874209840ce187c35d9a439

05194b34f8ff89facdd7b56d05826b08edaec9c6e444bdc32913e02cab01afd4

f730e83049c7fe81f6e4765ab91efbb7a373751d51fdafe697a4977dc7c1ea11

d22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8bca

36269d1892283991a9db23492cd8efcd68af74060384b9686219a97f76a9989e

ee6fd436bf5aff181e3d4b9a944bf644076e902a1bbf622978b5e005522c1f77

10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880

1f793f973fd906f9736aa483c613b82d5d2d7b0e270c5c903704f9665d9e1185

2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d54cb014

189c9c4603defb14fa8c942f5ff7814804654269917640478686530f91c4b66c

df30d74ab6600c1532a14c53a7f08f1afd41ec63cf427a4b91b99c3c2524caba

0463277782f9e98b0e7a028cea0f689a81cf080fa0d64d4de8ef4803bb1bf03a

dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb33f6a

7f8f1afa1390246409263e606aa05e2896b8d1da7018c534e67ca530a59ebda1

b03f94c61528c9f3731a2e8da4975c072c9ed4e5372d3ec6b0939eebe01e54a4

4ed74a205fad15c843174d7d8b30ae60a181e79f31cc30ebc683072f187e4cdd

e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009

8e54c38bc3585c3163c3e25d037bcf55695c274aaea770f2f59f0a0910a4b572

f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bdb1a

6c743c890151d0719150246382b5e0158e8abc4a29dd4b2f049ce7d313b1a330

4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2

ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b8fe949

cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a

724aa6dae72829e9812b753d188190e16fb64ac6cd39520897d917cfdccc5122

e284ad63a832123240bd40b6c09565fae8525c00ddf308d5b8f5c8ce69ed6b09

d15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570

0901a9920c9f0c74fb2170524477693d62c8493715520ae95143abd8055e7a39

7c84eafb3b05f0d5316fae610d9404c54ef39383d0fe0e3c07407a26bb9f6750

586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0

90be90ad4fb906574f9e7afe587f0826a71152bfc32cfc665a58877562f2edd4

9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc30d3335458a97

9ee35c6eb97230cd9b61ba32dba7befea4122f89b3747d2389970050a1d019f9

8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbbd05e83e22

1b2727af9fc187cd5c932c6defe50b983ad7508b4196ad6c5ff5e96686277c56

777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899

c599bebc9ae54a54710008042361293d71475e5fbe8f0cbaceb6ee4565a72015

a9543bc9612276863fc77b663fa3ff6efb85db69a01baa86c6dfabf73684b5c1

060ed94db064924a90065a5f4efb50f938c52619ca003f096482353e444bd096

4e00f3e0e09d13e76da56009173098eefafc4ad50806583d5333990fa44e6420

fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a

53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b8187c95c

3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4

5c34f6fa6eada3197404bf95eced9d288688537598629158a4f4e18d6882cb9b

fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be65ab176

5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552

ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3cfade9

c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c

de9d3e17555e91072919dc700dc7e588cd52617debcad2f764ef9c7fbf6c9f7b

6c109d098a1f44017f3937a71628d9dbd4d2ca8aa266656ee4720c37cc31558e

a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d3f22e33ed636525

1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13

0e1c7ea4148e7473e15a8e55413d6972eec6e24ef365e9f629884f89645de71a

b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851

7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48

e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295cb8435836a

77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5

IPv4-Addr

Value
80.66.75.135
49.235.255.219
87.251.67.92
121.4.69.26
80.66.75.36
124.223.11.169
92.118.148.227
89.117.55.149
185.170.144.153
103.96.72.140
80.66.75.55
5.181.86.241
119.3.125.197

80.66.75.37
194.26.135.44
87.251.64.245
80.66.75.126
62.122.184.113
45.93.201.74
80.66.75.51
80.66.75.116

Url

Value
http://80.66.75.36/aRX.exe

External References

- https://otx.alienvault.com/pulse/64ba4d9c546bd878d60f0c8c
- https://unit42.paloaltonetworks.com/mallox-ransomware/