NETMANAGEIT

Intelligence Report

Peeling Back the Layers of RemcosRat Malware

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Malware 13
- Attack-Pattern 14

Observables

- StixFile 19
- IPv4-Addr 20

External References

- External References 21

Overview

Description

Remcos is a sophisticated RAT which provides an attacker with backdoor access to the infected system and collects a variety of sensitive information. Remcos incorporates different obfuscation and anti-debugging techniques to evade detection. It regularly updates its features and makes this malware a challenging adversary.

Confidence

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

15 / 100

Indicator

Name

172.96.14.18

Description

ISP: UnReal Servers, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **135:** ``` Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 172.96.14.18:49152 ncalrpc: WindowsShutdown ncacn_np: \\H-18691\PIPE\InitShutdown ncalrpc: WMsgKRpc056730 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\H-18691\PIPE\InitShutdown ncalrpc: WMsgKRpc056730 ncalrpc: WMsgKRpc0570F1 ncalrpc: WMsgKRpc02DB1A72 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-36bd3a2b4c1e040a9f ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-36bd3a2b4c1e040a9f ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncacn_np: \ \H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncacn_np: \

\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncacn_np: \\H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncacn_np: \ \H-18691\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-9b4a4aa0ef397a8acf ncalrpc: actkernel ncalrpc: umpo ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 172.96.14.18:49153 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: \\H-18691\pipe\lsass abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-d0f3ac94ca357644c9 ncacn_ip_tcp: 172.96.14.18:49154 ncacn_np: \\H-18691\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-d0f3ac94ca357644c9 ncacn_ip_tcp: 172.96.14.18:49154 ncacn_np: \\H-18691\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: LRPC-d0f3ac94ca357644c9 ncacn_ip_tcp: 172.96.14.18:49154 ncacn_np: \\H-18691\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: 172.96.14.18:49154 ncacn_np: \\H-18691\pipe\eventlog ncalrpc: eventlog 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-675d62e3c501490b42 ncacn_np: \\H-18691\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-675d62e3c501490b42 ncacn_np: \\H-18691\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 5f54ce7d-5b79-4175-8584-

cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-675d62e3c501490b42 ncacn_np: \\H-18691\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-675d62e3c501490b42 ncacn_np: \\H-18691\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-675d62e3c501490b42 ncacn_np: \\H-18691\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_np: \\H-18691\PIPE\srvsvc ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 172.96.14.18:49155 ncalrpc: ubpmtaskhostchannel ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc:

OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\H-18691\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLECA2C7DBD4973BD4BB570BECD11C7 ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-ed189507ba5654d747 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: LRPC-9a3f576034a233badc ncalrpc: OLEB4AEA4ADE0E92EAB8F57681EB664 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-9a3f576034a233badc ncalrpc: OLEB4AEA4ADE0E92EAB8F57681EB664 b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-fd9ab59ae3fa5136ef 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-dc962b78d9b9c4d94f ncalrpc: LRPC-289211b9cf27d27394 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-dc962b78d9b9c4d94f ncalrpc: LRPC-289211b9cf27d27394 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-dc962b78d9b9c4d94f ncalrpc: LRPC-289211b9cf27d27394 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-289211b9cf27d27394 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\H-18691\PIPE\wkssvc ncalrpc: LRPC-dad68d776e54014646 ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-dad68d776e54014646 ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-dad68d776e54014646 ncalrpc: DNSResolver 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.96.14.18:49156 ncalrpc: LRPC-6be85aa459082f6ce7 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 172.96.14.18:49156 ncalrpc: LRPC-6be85aa459082f6ce7 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.96.14.18:49156 ncalrpc: LRPC-6be85aa459082f6ce7 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.96.14.18:49156 ncalrpc: LRPC-6be85aa459082f6ce7 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.96.14.18:49156 ncalrpc: LRPC-6be85aa459082f6ce7 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 172.96.14.18:49157 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: 172.96.14.18:49158 f763c91c-2ab1-47fa-868f-7de7efd42194 version: v1.0 annotation: VM Allow-List Provider RPC ncalrpc: RdvVmAllowListRpc ncalrpc: OLE5451DE63C610694A58335BA9E25A 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-75dba3bbc3ed3d18a3 ncalrpc: LRPC-75dba3bbc3ed3d18a3 ncalrpc: LRPC-75dba3bbc3ed3d18a3 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc02DB1A72 ``` ---------- **137:** ``` NetBIOS Response: Server Name: H-18691 MAC Address: 00:15:5D:0E:02:27 Names: WORKGROUP <0x0> H-18691 <0x0> H-18691 <0x20> ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2012 R2 Datacenter Evaluation 9600 Software: Windows Server 2012 R2 Datacenter 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 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 am Windows Server 2012R2 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 15 Aug 2023 09:10:52 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.96.14.18']

Name

32c8993532bc4e1f16e86c70c0fac5d51439556b8dcc6df647a2288bc70b8abf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '32c8993532bc4e1f16e86c70c0fac5d51439556b8dcc6df647a2288bc70b8abf']

Name

1035dbc121b350176c06f72311379b230aaf791b01c7091b45e4c902e9aba3f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1035dbc121b350176c06f72311379b230aaf791b01c7091b45e4c902e9aba3f4']

Name

0b3d65305edc50d3882973e47e9fbf4abc1f04eaecb13021f434eba8adf80b67

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b3d65305edc50d3882973e47e9fbf4abc1f04eaecb13021f434eba8adf80b67']

Name

212.192.219.52

Description

ISP: Serverion LLC **OS:** Windows (build 6.3.9600) ---------- Hostnames: - sur-more.dolphintask.com ---------- Domains: - dolphintask.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Tue, 20 Jun 2023 15:15:20 GMT Accept-Ranges: bytes ETag: "b2f3178aa3d91:0" Server: Microsoft-IIS/8.5 Date: Mon, 31 Jul 2023 15:32:47 GMT Content-Length: 701 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: FIREVPS-RDP NetBIOS Domain Name: FIREVPS-RDP NetBIOS Computer Name: FIREVPS-RDP DNS Domain Name: FireVPS-RDP FQDN: FireVPS-RDP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.192.219.52']

Name

3ed5729dc3f12a479885e434e0bdb7722f8dd0c0b8b27287111564303b98036c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ed5729dc3f12a479885e434e0bdb7722f8dd0c0b8b27287111564303b98036c']

Name

61c72e0dd15ea3de383e908fdb25c6064a5fa84842d4dbf7dc49b9a01be30517

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '61c72e0dd15ea3de383e908fdb25c6064a5fa84842d4dbf7dc49b9a01be30517']

Malware

Name
RemcosRat
Name
SykCrypter
Name
Remcos

Attack-Pattern

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
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

Encrypted Channel

ID

T1573

Description

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

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control

mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

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)

StixFile

Value
1035dbc121b350176c06f72311379b230aaf791b01c7091b45e4c902e9aba3f4
3ed5729dc3f12a479885e434e0bdb7722f8dd0c0b8b27287111564303b98036c
0b3d65305edc50d3882973e47e9fbf4abc1f04eaecb13021f434eba8adf80b67
32c8993532bc4e1f16e86c70c0fac5d51439556b8dcc6df647a2288bc70b8abf
61c72e0dd15ea3de383e908fdb25c6064a5fa84842d4dbf7dc49b9a01be30517

IPv4-Addr

Value
172.96.14.18
212.192.219.52

External References

- https://otx.alienvault.com/pulse/64ef403008890b7b5795b0c7
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/peeling-back-the-layers-of-remcosrat-malware/