Jun 10 2023

NETMANAGEIT

Intelligence Report

DynamicRAT — A full-fledged Java Rat

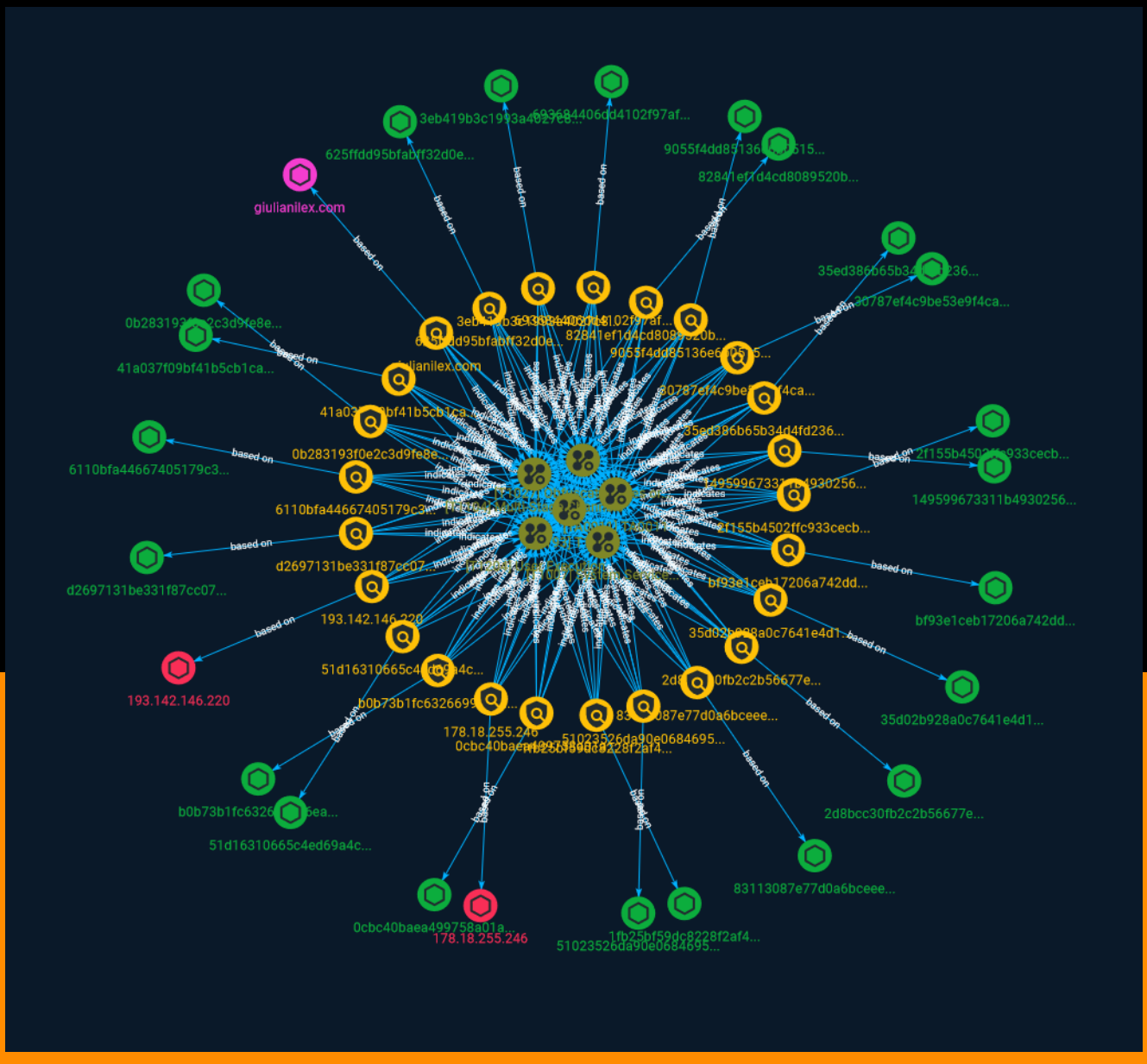

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On Tuesday, 06.06.2023, I was notified by one of my infosec colleagues, Fate, about a strange ".jar" file he had found in his network. While execution had been prevented through the AV, the file did stick out, because when looking at its strings, Fate had noticed several substrings that contained the word "attack" in it.

Confidence

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

15 / 100

Attack-Pattern

Name
T1193
ID
T1193
Name
User Execution
ID
T1204
Description
An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary,

or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

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

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup

first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name
TA0011

ID
TA0011

Indicator

Name
giulianilex.com
Pattern Type
stix
Pattern
[domain-name:value = 'giulianilex.com']
Name
2d8bcc30fb2c2b56677e29d7f3750ea7378869e992f3fefd3f4c4bb855185cfb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2d8bcc30fb2c2b56677e29d7f3750ea7378869e992f3fefd3f4c4bb855185cfb']
Name

193.142.146.220

Description

ISP: ColocationX Ltd. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 193.142.146.220:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \WINDOWS-1BBOQBP\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 193.142.146.220:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \WINDOWS-1BBOQBP\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 193.142.146.220:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \WINDOWS-1BBOQBP\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: 193.142.146.220:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \WINDOWS-1BBOQBP\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 193.142.146.220:49665 ncalrpc: WindowsShutdown ncacn_np: \ \WINDOWS-1BBOQBP\PIPE\InitShutdown ncalrpc: WMsgKRpc076FC0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WINDOWS-1BBOQBP\PIPE\InitShutdown ncalrpc: WMsgKRpc076FC0 ncalrpc: WMsgKRpc08A2D1 ncalrpc: WMsgKRpc04449822 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-590a697c5da72153b9 ncalrpc: LRPC-c1f53abcd1bbe8eef9 ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-590a697c5da72153b9 ncalrpc: LRPC-c1f53abcd1bbe8eef9 ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel

ncalrpc: umpo ncalrpc: LRPC-c1f53abcd1bbe8eef9 ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-e4845b0a2470355a7f ncalrpc: LRPC-1a0d585c1951381e3d 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-590a697c5da72153b9 ncalrpc: LRPC-c1f53abcd1bbe8eef9 ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-c1f53abcd1bbe8eef9 ncalrpc: LRPC-4ce1bf5fb19e0d12d7 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 0d47017b-b33b-46ad-9e18-fe96456c5078 version: v1.0 ncalrpc: umpo 95406f0b-b239-4318-91bb-cea3a46ff0dc version: v1.0 ncalrpc: umpo 4ed8abcc-f1e2-438b-981f-bb0e8abc010c version: v1.0 ncalrpc: umpo 0ff1f646-13bb-400a-ab50-9a78f2b7a85a version: v1.0 ncalrpc: umpo 6982a06e-5fe2-46b1-b39c-a2c545bfa069 version: v1.0 ncalrpc: umpo 082a3471-31b6-422a-b931-a54401960c62 version: v1.0 ncalrpc: umpo fae436b0-b864-4a87-9eda-298547cd82f2 version: v1.0 ncalrpc: umpo e53d94ca-7464-4839-b044-09a2fb8b3ae5 version: v1.0 ncalrpc: umpo 178d84be-9291-4994-82c6-3f909aca5a03 version: v1.0 ncalrpc: umpo 4dace966-a243-4450-ae3f-9b7bcb5315b8 version: v2.0 ncalrpc: umpo 1832bcf6-cab8-41d4-85d2-c9410764f75a version: v1.0 ncalrpc: umpo c521facf-09a9-42c5-b155-72388595cbf0 version: v0.0 ncalrpc: umpo 2c7fd9ce-e706-4b40-b412-953107ef9bb0 version: v0.0 ncalrpc: umpo 88abcbc3-34ea-76ae-8215-767520655a23 version: v0.0 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-c4bed6304254054b66 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc:

LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-28a83a72358b44116d ncalrpc: OLED33A3C0F6E08F4AEDC4A8E23E8AB ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 0361ae94-0316-4c6c-8ad8-c594375800e2 version: v1.0 ncalrpc: umpo 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 version: v1.0 ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-02858c3e0850fc3ef7 ncalrpc: IUserProfile2 ncalrpc: LRPC-bf8211781d4bd10b34 ncalrpc: LRPC-2580e865f2d32dde12 ncalrpc: senssvc ncalrpc: LRPC-575236a33981383c1c f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-ba711c03e753584b17 ncalrpc: LRPC-f82aa497c2655fefd3 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-e2cfa3a745bef2b1f0 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-51535c53a455fb5d6d ncalrpc: OLEB2F8B099E6D32159110F44C634CA ncalrpc: LRPC-e4845b0a2470355a7f 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-c08971bb9724fb4455 a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-5148d08acf88c490fc ncalrpc: LRPC-1a0d585c1951381e3d f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 193.142.146.220:49666 ncacn_np: \\WINDOWS-1BBOQBP\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-e92981ad1c4d16afe3 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-f03e10da30992aab41 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 193.142.146.220:49667 ncalrpc: LRPC-12780684ac72339c51 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WINDOWS-1BBOQBP\PIPE\atsvc ncalrpc: LRPC-cf260dabdb207c3724 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 193.142.146.220:49667 ncalrpc: LRPC-12780684ac72339c51 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WINDOWS-1BBOQBP\PIPE\atsvc ncalrpc: LRPC-cf260dabdb207c3724 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-12780684ac72339c51 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WINDOWS-1BBOQBP\PIPE\atsvc ncalrpc: LRPC-cf260dabdb207c3724 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WINDOWS-1BBOQBP\PIPE\atsvc ncalrpc: LRPC-cf260dabdb207c3724 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler

Service Remoting Protocol provider: taskcomp.dll ncacn_np: \
\WINDOWS-1BBOQBP\PIPE\atsvc ncalrpc: LRPC-cf260dabdb207c3724
0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-cf260dabdb207c3724 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-f75545e24922c3407d ncalrpc: DNSResolver 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-e1ca7afc40868307fc ncalrpc: OLED2B4D5EF131759D3573F81F15DE3
3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-02510cdfac03b6999a ncalrpc: OLEB3FCDE1962E153C477E5725F4D13 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-d01f55a3e8f9c27c0e ncalrpc: OLE0A019B30CD87294FBBEA55BD680C c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-d01f55a3e8f9c27c0e ncalrpc: OLE0A019B30CD87294FBBEA55BD680C f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-d01f55a3e8f9c27c0e ncalrpc: OLE0A019B30CD87294FBBEA55BD680C b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-d01f55a3e8f9c27c0e ncalrpc: OLE0A019B30CD87294FBBEA55BD680C abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-d01f55a3e8f9c27c0e ncalrpc: OLE0A019B30CD87294FBBEA55BD680C 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WINDOWS-1BBOQBP\PIPE\wkssvc ncalrpc: LRPC-821177e0e04630a9c1 eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-821177e0e04630a9c1 f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-821177e0e04630a9c1 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-7ecebf778c3d68a3f5 ncalrpc: OLE95047B73939EB181C1376A105D33 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-7ecebf778c3d68a3f5 ncalrpc: OLE95047B73939EB181C1376A105D33 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-8db8647370cc8bcc07 ncalrpc: LRPC-9745866baa6c1b6edc ncalrpc: LRPC-8de9d1f7c7b6a7dd71 ncalrpc: LRPC-8a7750cdd526ed34a5 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-9745866baa6c1b6edc ncalrpc: LRPC-8de9d1f7c7b6a7dd71 ncalrpc: LRPC-8a7750cdd526ed34a5 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-8de9d1f7c7b6a7dd71 ncalrpc: LRPC-8a7750cdd526ed34a5 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-8a7750cdd526ed34a5 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-3f4b588b3b64aea1dd 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 193.142.146.220:49668 ncacn_np: \
\WINDOWS-1BBOQBP\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-575236a33981383c1c 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 193.142.146.220:49669 ncalrpc: LRPC-851325e6cf1e10e498
4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 193.142.146.220:49669 ncalrpc: LRPC-851325e6cf1e10e498 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification

Protocol provider: spoolsv.exe ncacn_ip_tcp: 193.142.146.220:49669 ncalrpc: LRPC-851325e6cf1e10e498 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 193.142.146.220:49669 ncalrpc: LRPC-851325e6cf1e10e498 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 193.142.146.220:49669 ncalrpc: LRPC-851325e6cf1e10e498 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-dfceb87b6bcfb89a66 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-dfceb87b6bcfb89a66 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-dfceb87b6bcfb89a66 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-dfceb87b6bcfb89a66 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-915e5a0ee6bf7c0c83 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-5104b0be7952691fde 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 193.142.146.220:49670 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-c70a1904c6a4691ca3 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-c70a1904c6a4691ca3 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-e83802181932a341a9 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\WINDOWS-1BBOQBP\PIPE\ROUTER 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-b022266bb21432fc22 ncalrpc: OLE9EE7CB4E3D0035DD72241F4A6CEF 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-29e74a1d8d4f17c071 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: 193.142.146.220:49671 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-2354484fdebee2abe4 ncalrpc: LRPC-2354484fdebee2abe4 ncalrpc: LRPC-2354484fdebee2abe4 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-877cd777e5e4043f68 d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc:

LRPC-e48c5e46abc8b7e69a d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-e48c5e46abc8b7e69a 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc04449822 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-6250aeb6fbf9bc8085 ncalrpc: OLE81D722B4835EF75063AE9C45916C 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-6250aeb6fbf9bc8085 ncalrpc: OLE81D722B4835EF75063AE9C45916C 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-6250aeb6fbf9bc8085 ncalrpc: OLE81D722B4835EF75063AE9C45916C 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-ad476c2da9d449092c fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-ad476c2da9d449092c 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-ad476c2da9d449092c 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-ad476c2da9d449092c 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-ad476c2da9d449092c a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-0cbb2b362c0c0f15af ncalrpc: OLE0358D338D2D82A72736C323C3822 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: a78b54ea-586c-45cb-85d6-5c9f749b60e3 ncalrpc: LRPC-287c3db9738260c793 a111f1c5-5923-47c0-9a68-d0bafb577901 version: v1.0 annotation: NetSetup API ncalrpc: LRPC-3e54b8b16c1d30da6b ff9fd3c4-742e-45e0-91dd-2f5bc632a1df version: v1.0 annotation: appxsvc ncalrpc: LRPC-ea694ca0cd67d44d93 ae2dc901-312d-41df-8b79-e835e63db874 version: v1.0 annotation: appxsvc ncalrpc: LRPC-ea694ca0cd67d44d93 9435cc56-1d9c-4924-ac7d-b60a2c3520e1 version: v1.0 annotation: SPPSVC Default RPC Interface provider: sppsvc.exe ncalrpc: SPPCTransportEndpoint-00001 ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10/Windows Server 2022 OS Build: 10.0.20348 Target Name: WINDOWS-1BBOQBP NetBIOS Domain Name: WINDOWS-1BBOQBP NetBIOS Computer Name: WINDOWS-1BBOQBP DNS Domain Name: WINDOWS-1BBOQBP FQDN: WINDOWS-1BBOQBP ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 05 Jun 2023 02:41:37 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 10/Windows Server 2022 OS Build: 10.0.20348 Target Name: WINDOWS-1BBOQBP NetBIOS Domain Name: WINDOWS-1BBOQBP NetBIOS Computer Name: WINDOWS-1BBOQBP DNS Domain Name: WINDOWS-1BBOQBP FQDN: WINDOWS-1BBOQBP ``` ---------- **9098:** ``` {"packetID":0}\n ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.142.146.220']

Name

30787ef4c9be53e9f4caea0517e36b76a2e6aeddbeee1f5f5110c49518594020

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30787ef4c9be53e9f4caea0517e36b76a2e6aeddbeee1f5f5110c49518594020']

Name

0cbc40baea499758a01ad897cfc6beb54dc1cbbad56eedcf5197f42a141c0188

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0cbc40baea499758a01ad897cfc6beb54dc1cbbad56eedcf5197f42a141c0188']

Name

41a037f09bf41b5cb1ca453289e6ca961d61cd96eeefb1b5bbf153612396d919

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '41a037f09bf41b5cb1ca453289e6ca961d61cd96eeefb1b5bbf153612396d919']
Name
2f155b4502ffc933cecb3e1d182ba39b92498406b8084435114f9a27ea4a9825
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2f155b4502ffc933cecb3e1d182ba39b92498406b8084435114f9a27ea4a9825']
Name
b0b73b1fc6326699c6eaea17b05be9a26b1efd9f9ce66828e60de468c44aac74
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b0b73b1fc6326699c6eaea17b05be9a26b1efd9f9ce66828e60de468c44aac74']

Name

693684406dd4102f97af2cf276fcee80f85182b589281edd53c1da2570346364

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '693684406dd4102f97af2cf276fcee80f85182b589281edd53c1da2570346364']

Name

83113087e77d0a6bceeec33e6d043838e8f2bc5d0cc722e937b160ad0a1e9c79

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83113087e77d0a6bceeec33e6d043838e8f2bc5d0cc722e937b160ad0a1e9c79']

Name

6110bfa44667405179c3e15e12af1b62037e447ed59b054b19042032995e6c7e

Description

WinDivert_Driver

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6110bfa44667405179c3e15e12af1b62037e447ed59b054b19042032995e6c7e']

Name

35ed386b65b34d4fd2369039c916bacddafd7d1af5e5eb9fdc62a34a9ccd4dc0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35ed386b65b34d4fd2369039c916bacddafd7d1af5e5eb9fdc62a34a9ccd4dc0']

Name

1fb25bf59dc8228f2af4b181f39c24cee593bebfd09df5a7877c6b144a81637f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1fb25bf59dc8228f2af4b181f39c24cee593bebfd09df5a7877c6b144a81637f']

Name

625ffdd95bfabff32d0e8a95beabcd303c01c8bba73b90402d4e84d6e15dd8e5

Description

WinDivert_Driver

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '625ffdd95bfabff32d0e8a95beabcd303c01c8bba73b90402d4e84d6e15dd8e5']

Name

bf93e1ceb17206a742dd4f85700ef75f55ad76b04ca8a601c4d2a515151840aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf93e1ceb17206a742dd4f85700ef75f55ad76b04ca8a601c4d2a515151840aa']

Name

51d16310665c4ed69a4c18f07e927e4542520cf1c506b991776fc347757d26ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '51d16310665c4ed69a4c18f07e927e4542520cf1c506b991776fc347757d26ff']

Name

82841ef1d4cd8089520b4b57e6fc1f56b0e9dc39db814c5b3c5607fea5c4fd1e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82841ef1d4cd8089520b4b57e6fc1f56b0e9dc39db814c5b3c5607fea5c4fd1e']

Name

51023526da90e068469593de68a439be2c4f239c59f7f0314ef10825d079e8fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '51023526da90e068469593de68a439be2c4f239c59f7f0314ef10825d079e8fc']

Name

0b283193f0e2c3d9fe8e07ecb1716b869581d73fdf9b9fc18130fa15c244e48d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b283193f0e2c3d9fe8e07ecb1716b869581d73fdf9b9fc18130fa15c244e48d']

Name

149599673311b49302568fcde7dc7ef95e0d37bba1316b88cafb5c68f56e7f1c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '149599673311b49302568fcde7dc7ef95e0d37bba1316b88cafb5c68f56e7f1c']

Name

178.18.255.246

Description

ISP: Contabo GmbH **OS:** Windows (Build 10.0.14393) ---------- Hostnames: - vmi792829.contaboserver.net ---------- Domains: - contaboserver.net ---------- 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: 178.18.255.246:49664 ncalrpc: WindowsShutdown ncacn_np: \\VMI792829\PIPE\InitShutdown ncalrpc: WMsgKRpc07B980 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\VMI792829\PIPE\InitShutdown ncalrpc: WMsgKRpc07B980 ncalrpc: WMsgKRpc07F601 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc:

LRPC-b20205559a82fc2dc2 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-cbcf0f95c5dff86b72 ncalrpc: LRPC-0e490599ca8580f6d1 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-cbcf0f95c5dff86b72 ncalrpc: LRPC-0e490599ca8580f6d1 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-0e490599ca8580f6d1 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-a2049ebf2446430b6a ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 178.18.255.246:49665 ncacn_np: \\VMI792829\pipe\eventlog ncalrpc: eventlog ncalrpc: LRPC-97d4f237757da333bd ncalrpc: LRPC-40271383adc18cb701 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-cbcf0f95c5dff86b72 ncalrpc: LRPC-0e490599ca8580f6d1 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo b8cadbaf-e84b-46b9-84f2-6f71c03f9e55 version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 88abcbc3-34ea-76ae-8215-767520655a23 version: v0.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-7442284c6f64672066 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 4dace966-a243-4450-ae3f-9b7bcb5315b8 version: v1.0 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 1832bcf6-cab8-41d4-85d2-c9410764f75a version: v1.0 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-

cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo c521facf-09a9-42c5-b155-72388595cbf0 version: v0.0 ncalrpc: OLE811CCC1059200A4B1EC80B6C3741 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo 2c7fd9ce-e706-4b40-b412-953107ef9bb0 version: v0.0 ncacn_np: \\VMI792829\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-cbd9d9b0694757b0c6 ncalrpc: actkernel ncalrpc: umpo ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 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 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 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 f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-46074ef5d418b0ac40 a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-c5596f24f586bf4df0 ncalrpc: LRPC-a2049ebf2446430b6a ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 178.18.255.246:49665 ncacn_np: \\VMI792829\pipe\eventlog ncalrpc: eventlog ncalrpc: LRPC-97d4f237757da333bd 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 178.18.255.246:49665 ncacn_np: \\VMI792829\pipe\eventlog ncalrpc: eventlog ncalrpc: LRPC-97d4f237757da333bd 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncacn_ip_tcp: 178.18.255.246:49665 ncacn_np: \\VMI792829\pipe\eventlog ncalrpc: eventlog ncalrpc: LRPC-97d4f237757da333bd f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 178.18.255.246:49665 ncacn_np: \\VMI792829\pipe\eventlog ncalrpc: eventlog ncalrpc: LRPC-97d4f237757da333bd 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-97d4f237757da333bd bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-4283adcfbbcc8be5d1 ncalrpc: trkwks ncacn_np: \\VMI792829\pipe\trkwks ncalrpc: LRPC-09367cb169f972c1bd ncalrpc: TSUMRPD_PRINT_DRV_LPC_API ncalrpc: OLE3B70C3ACA5579C9F31E4570DBF3D ncalrpc: LRPC-0cc8e9ce5cdb7da2e5 ncalrpc: LRPC-40271383adc18cb701 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc:

LRPC-09367cb169f972c1bd ncalrpc: TSUMRPD_PRINT_DRV_LPC_API ncalrpc: OLE3B70C3ACA5579C9F31E4570DBF3D ncalrpc: LRPC-0cc8e9ce5cdb7da2e5 ncalrpc: LRPC-40271383adc18cb701 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 annotation: Network Connection Broker server endpoint ncalrpc: LRPC-09367cb169f972c1bd ncalrpc: TSUMRPD_PRINT_DRV_LPC_API ncalrpc: OLE3B70C3ACA5579C9F31E4570DBF3D ncalrpc: LRPC-0cc8e9ce5cdb7da2e5 ncalrpc: LRPC-40271383adc18cb701 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-09367cb169f972c1bd ncalrpc: TSUMRPD_PRINT_DRV_LPC_API ncalrpc: OLE3B70C3ACA5579C9F31E4570DBF3D ncalrpc: LRPC-0cc8e9ce5cdb7da2e5 ncalrpc: LRPC-40271383adc18cb701 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 annotation: Network Connection Broker server endpoint for NCB Reset module ncalrpc: LRPC-0cc8e9ce5cdb7da2e5 ncalrpc: LRPC-40271383adc18cb701 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-89e117ce045f89404e ncalrpc: LRPC-8f84b1d95740fc0484 ncalrpc: LRPC-95b35771d582565465 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-89e117ce045f89404e ncalrpc: LRPC-8f84b1d95740fc0484 ncalrpc: LRPC-95b35771d582565465 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-89e117ce045f89404e ncalrpc: LRPC-8f84b1d95740fc0484 ncalrpc: LRPC-95b35771d582565465 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-8f84b1d95740fc0484 ncalrpc: LRPC-95b35771d582565465 df4df73a-c52d-4e3a-8003-8437fdf8302a version: v0.0 annotation: WM_WindowManagerRPC\Server ncalrpc: LRPC-95b35771d582565465 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\VMI792829\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: OLEC5E5A51B19760C69E1AFD187C4D5 ncalrpc: LRPC-9a05012f282b519fcc 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-9a05012f282b519fcc fb9a3757-cff0-4db0-b9fc-bd6c131612fd version: v1.0 annotation: AppInfo ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 5f54ce7d-5b79-4175-8584-

cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2

b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-14d7566d22805e00e6 ncacn_np: \\VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_np: \ \VMI792829\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 178.18.255.246:49666 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-893571213dde9c0bf3 ncalrpc: ubpmtaskhostchannel ncacn_np: \ \VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \ \VMI792829\PIPE\atsvc ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: OLE92163CD960AE4A33069E7B4898A1 ncalrpc: senssvc ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-1333e6f3fd7af9dcf1 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-65b0f644d5e1fa1a44 ncalrpc: IUserProfile2 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\VMI792829\PIPE\wkssvc ncalrpc: nlaplg ncalrpc: LRPC-471cdce17e283bae0a eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-471cdce17e283bae0a f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-471cdce17e283bae0a 7aeb6705-3ae6-471a-882d-f39c109edc12 version: v1.0 ncalrpc: LRPC-14bc32b192a8ab27aa e7f76134-9ef5-4949-a2d6-3368cc0988f3 version: v1.0 ncalrpc: LRPC-14bc32b192a8ab27aa b3781086-6a54-489b-91c8-51d067172ab7 version: v1.0 ncalrpc: LRPC-14bc32b192a8ab27aa b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-14bc32b192a8ab27aa abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0

ncalrpc: LRPC-14bc32b192a8ab27aa 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 178.18.255.246:49668 ncalrpc: LRPC-8b4f8a0a52a23aa900 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 178.18.255.246:49668 ncalrpc: LRPC-8b4f8a0a52a23aa900 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 178.18.255.246:49668 ncalrpc: LRPC-8b4f8a0a52a23aa900 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 178.18.255.246:49668 ncalrpc: LRPC-8b4f8a0a52a23aa900 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 178.18.255.246:49668 ncalrpc: LRPC-8b4f8a0a52a23aa900 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-47f29c7cdd5ad82d41 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-47f29c7cdd5ad82d41 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: 178.18.255.246:49669 ncalrpc: ipsec 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 178.18.255.246:49670 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-227de7b6ce00febb97 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-227de7b6ce00febb97 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 178.18.255.246:49679 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\VMI792829\pipe\lsass 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\VMI792829\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\VMI792829\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \ \VMI792829\pipe\lsass 4b112204-0e19-11d3-b42b-0000f81feb9f version: v1.0 provider: ssdpsrv.dll ncalrpc: LRPC-494f531430c18446c4 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-4038960733fdca3a17 ncalrpc: LRPC-4038960733fdca3a17 ncalrpc:

LRPC-4038960733fdca3a17 ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 OS: Windows Server 2016 Datacenter 14393 Software: Windows Server 2016 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 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10/Windows Server 2016 OS Build: 10.0.14393 Target Name: VMI792829 NetBIOS Domain Name: VMI792829 NetBIOS Computer Name: VMI792829 DNS Domain Name: vmi792829 FQDN: vmi792829 ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 08 Jun 2023 20:28:53 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 10/Windows Server 2016 OS Build: 10.0.14393 Target Name: VMI792829 NetBIOS Domain Name: VMI792829 NetBIOS Computer Name: VMI792829 DNS Domain Name: vmi792829 FQDN: vmi792829 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '178.18.255.246']

Name

3eb419b3c1993a4027c88b2c7758067fe9040173782e00c8a94e7d3b7c6b9fab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3eb419b3c1993a4027c88b2c7758067fe9040173782e00c8a94e7d3b7c6b9fab']

Name

35d02b928a0c7641e4d128bb63c704116c5ee6b43c07eab0d24832eb98f5a165

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35d02b928a0c7641e4d128bb63c704116c5ee6b43c07eab0d24832eb98f5a165']

Name

d2697131be331f87cc0760e04bfebb7f116c16756110a311bb92e0bb271e4877

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2697131be331f87cc0760e04bfebb7f116c16756110a311bb92e0bb271e4877']

Name

9055f4dd85136e6b051569b8f7d039117af487e8ebba78fc484e4256b79746b7

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'9055f4dd85136e6b051569b8f7d039117af487e8ebba78fc484e4256b79746b7']
```

Domain-Name

Value
giulianilex.com

StixFile

Value
82841ef1d4cd8089520b4b57e6fc1f56b0e9dc39db814c5b3c5607fea5c4fd1e
b0b73b1fc6326699c6eaea17b05be9a26b1efd9f9ce66828e60de468c44aac74
1fb25bf59dc8228f2af4b181f39c24cee593bebfd09df5a7877c6b144a81637f
41a037f09bf41b5cb1ca453289e6ca961d61cd96eeefb1b5bbf153612396d919
bf93e1ceb17206a742dd4f85700ef75f55ad76b04ca8a601c4d2a515151840aa
149599673311b49302568fcde7dc7ef95e0d37bba1316b88cafb5c68f56e7f1c
51023526da90e068469593de68a439be2c4f239c59f7f0314ef10825d079e8fc
6110bfa44667405179c3e15e12af1b62037e447ed59b054b19042032995e6c7e
3eb419b3c1993a4027c88b2c7758067fe9040173782e00c8a94e7d3b7c6b9fab
625ffdd95bfabff32d0e8a95beabcd303c01c8bba73b90402d4e84d6e15dd8e5
30787ef4c9be53e9f4caea0517e36b76a2e6aeddbeee1f5f5110c49518594020
9055f4dd85136e6b051569b8f7d039117af487e8ebba78fc484e4256b79746b7
0b283193f0e2c3d9fe8e07ecb1716b869581d73fdf9b9fc18130fa15c244e48d

2d8bcc30fb2c2b56677e29d7f3750ea7378869e992f3fefd3f4c4bb855185cfb

2f155b4502ffc933cecb3e1d182ba39b92498406b8084435114f9a27ea4a9825

51d16310665c4ed69a4c18f07e927e4542520cf1c506b991776fc347757d26ff

0cbc40baea499758a01ad897cfc6beb54dc1cbbad56eedcf5197f42a141c0188

d2697131be331f87cc0760e04bfebb7f116c16756110a311bb92e0bb271e4877

83113087e77d0a6bceeec33e6d043838e8f2bc5d0cc722e937b160ad0a1e9c79

35ed386b65b34d4fd2369039c916bacddafd7d1af5e5eb9fdc62a34a9ccd4dc0

35d02b928a0c7641e4d128bb63c704116c5ee6b43c07eab0d24832eb98f5a165

693684406dd4102f97af2cf276fcee80f85182b589281edd53c1da2570346364

IPv4-Addr

Value
193.142.146.220
178.18.255.246

External References

- https://gi7w0rm.medium.com/dynamicrat-a-full-fledged-java-rat-1a2dabb11694
- https://otx.alienvault.com/pulse/64833c08dadf544c30e94298
- https://github.com/Gi7w0rm/MalwareConfigLists/blob/main/DynamicRAT/IoC.txt