Jun 19 2023

NETMANAGEIT

Intelligence Report

Formbook from Possible ModiLoader (DBatLoader)

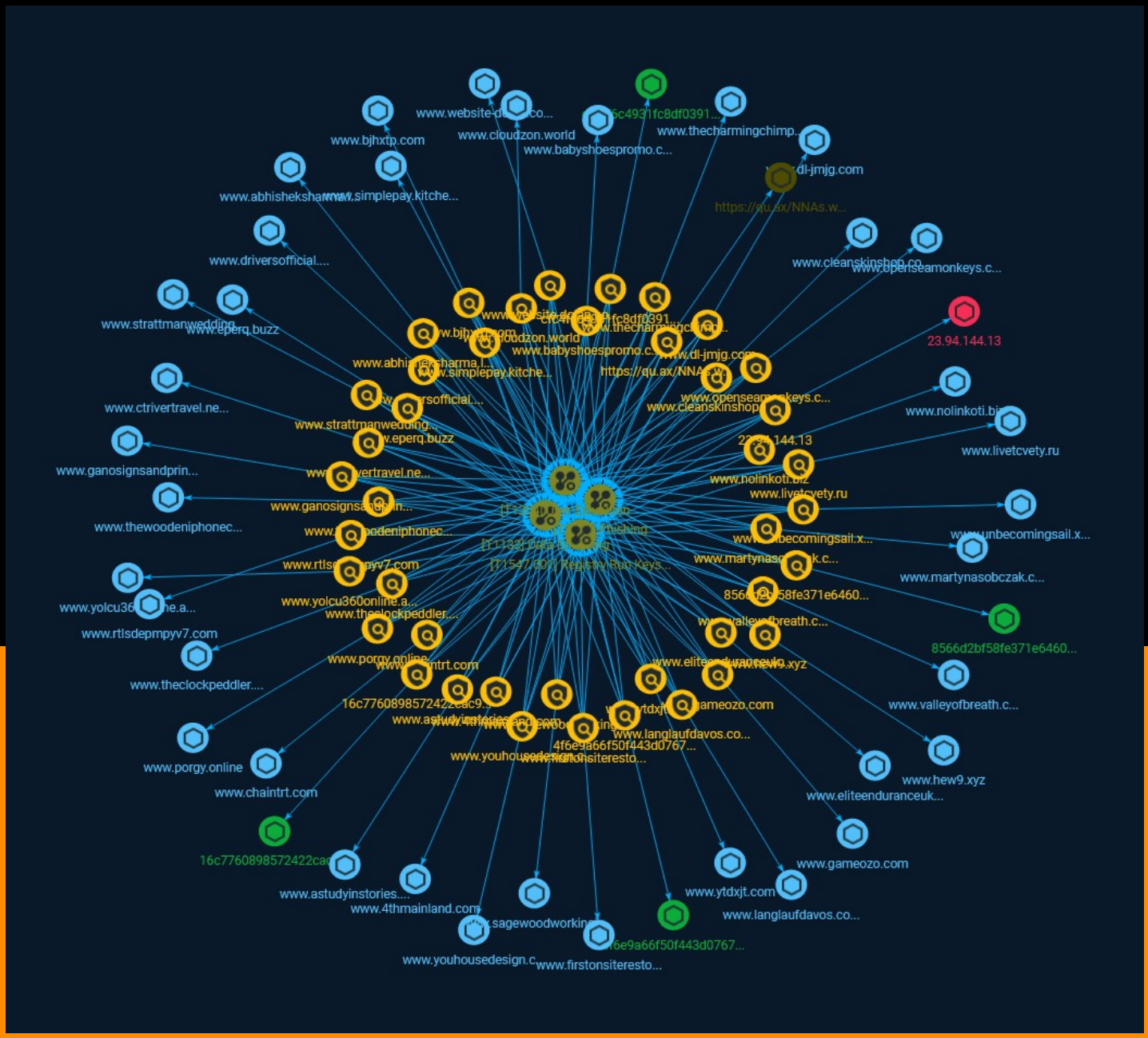

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Threat researcher Brad Duncan came across an example that kicks off with an Excel file exploiting CVE-2017-11882 to use what seems like ModiLoader (also known as DBatLoader).

Confidence

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

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

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

Registry Run Keys / Startup Folder

ID

T1547.001

Description

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level. Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`. The following run keys are created by default on Windows systems: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce` Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"` (Citation: Oddvar Moe RunOnceEx Mar 2018) The following Registry keys

can be used to set startup folder items for persistence: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` The following Registry keys can control automatic startup of services during boot: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices` Using policy settings to specify startup programs creates corresponding values in either of two Registry keys: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` subkeys can automatically launch programs. Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run when any user logs on. By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot. Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

Indicator

Name
www.unbecomingsail.xyz
Pattern Type
stix
Pattern
[hostname:value = 'www.unbecomingsail.xyz']
Name
www.porgy.online
Pattern Type
stix
Pattern
[hostname:value = 'www.porgy.online']
Name
www.dl-jmjg.com

Pattern Type
stix
Pattern
[hostname:value = 'www.dl-jmjg.com']
Name
www.sagewoodworkinginc.com
Pattern Type
stix
Pattern
[hostname:value = 'www.sagewoodworkinginc.com']
Name
www.driversofficial.com
Pattern Type
stix
Pattern
[hostname:value = 'www.driversofficial.com']
Name
www.cleanskinshop.com

Pattern Type
stix
Pattern
[hostname:value = 'www.cleanskinshop.com']
Name
www.youhousedesign.com
Pattern Type
stix
Pattern
[hostname:value = 'www.youhousedesign.com']
Name
www.simplepay.kitchen
Pattern Type
stix
Pattern
[hostname:value = 'www.simplepay.kitchen']
Name
www.valleyofbreath.com

Pattern Type
stix
Pattern
[hostname:value = 'www.valleyofbreath.com']
Name
www.eperq.buzz
Pattern Type
stix
Pattern
[hostname:value = 'www.eperq.buzz']
Name
www.openseamonkeys.com
Pattern Type
stix
Pattern
[hostname:value = 'www.openseamonkeys.com']
Name
www.4thmainland.com

Pattern Type
stix
Pattern
[hostname:value = 'www.4thmainland.com']
Name
www.bjhxtp.com
Pattern Type
stix
Pattern
[hostname:value = 'www.bjhxtp.com']
Name
www.eliteenduranceuk.com
Pattern Type
stix
Pattern
[hostname:value = 'www.eliteenduranceuk.com']
Name
www.theclockpeddler.com

Pattern Type
stix
Pattern
[hostname:value = 'www.theclockpeddler.com']
Name
www.babyshoespromo.com
Pattern Type
stix
Pattern
[hostname:value = 'www.babyshoespromo.com']
Name
www.ytdxjt.com
Pattern Type
stix
Pattern
[hostname:value = 'www.ytdxjt.com']
Name
www.thewoodeniphonecase.com

Pattern Type
stix
Pattern
[hostname:value = 'www.thewoodeniphonecase.com']
Name
www.livetcvety.ru
Pattern Type
stix
Pattern
[hostname:value = 'www.livetcvety.ru']
Name
www.astudyinstories.com
Pattern Type
stix
Pattern
[hostname:value = 'www.astudyinstories.com']
Name
www.abhisheksharma.life

Pattern Type
stix
Pattern
[hostname:value = 'www.abhisheksharma.life']
Name
www.gameozo.com
Pattern Type
stix
Pattern
[hostname:value = 'www.gameozo.com']
Name
www.rtlsdepmpyv7.com
Pattern Type
stix
Pattern
[hostname:value = 'www.rtlsdepmpyv7.com']
Name
www.thecharmingchimp.com

Pattern Type

stix

Pattern

[hostname:value = 'www.thecharmingchimp.com']

Name

4f6e9a66f50f443d07676ef43a7f2349fc713c96522058c1c4d425da7be4a4bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f6e9a66f50f443d07676ef43a7f2349fc713c96522058c1c4d425da7be4a4bf']

Name

www.ctrivertravel.net

Pattern Type

stix

Pattern

[hostname:value = 'www.ctrivertravel.net']

Name

www.martynasobczak.com

Pattern Type

stix

Pattern

[hostname:value = 'www.martynasobczak.com']

Name

www.chaintrt.com

Pattern Type

stix

Pattern

[hostname:value = 'www.chaintrt.com']

Name

cfc4f6c4931fc8df03919d96181178a903a6ccd39eb5268ac00b3a223c027b5b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cfc4f6c4931fc8df03919d96181178a903a6ccd39eb5268ac00b3a223c027b5b']

Name
www.hew9.xyz
Pattern Type
stix
Pattern
[hostname:value = 'www.hew9.xyz']
Name
www.ganosignsandprinting.com
Pattern Type
stix
Pattern
[hostname:value = 'www.ganosignsandprinting.com']
Name
www.nolinkoti.biz
Pattern Type
stix
Pattern
[hostname:value = 'www.nolinkoti.biz']

Name
www.firstonsiterestoration.com
Pattern Type
stix
Pattern
[hostname:value = 'www.firstonsiterestoration.com']
Name
www.cloudzon.world
Pattern Type
stix
Pattern
[hostname:value = 'www.cloudzon.world']
Name
8566d2bf58fe371e646076c60874a8fbb50de2fbf9b950c457804d316a3de89f
Description
DotNET_Reactor
Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = '8566d2bf58fe371e646076c60874a8fbb50de2fbf9b950c457804d316a3de89f']

Name

www.yolcu360online.autos

Pattern Type

stix

Pattern

[hostname:value = 'www.yolcu360online.autos']

Name

https://qu.ax/NNAs.wav

Pattern Type

stix

Pattern

[url:value = 'https://qu.ax/NNAs.wav']

Name

www.langlaufdavos.com

Pattern Type

stix

Pattern

[hostname:value = 'www.langlaufdavos.com']

Name

www.strattmanwedding.com

Pattern Type

stix

Pattern

[hostname:value = 'www.strattmanwedding.com']

Name

23.94.144.13

Description

ISP: ColoCrossing **OS:** Windows Server 2022 (build 10.0.20348) ---------- Hostnames: - 23-94-144-13-host.colocrossing.com ---------- Domains: - colocrossing.com ---------- Services: **21:** ``` 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ 530 Login or password incorrect! 214-The following commands are recognized: USER PASS QUIT CWD PWD PORT PASV TYPE LIST REST CDUP RETR STOR SIZE DELE RMD MKD RNFR RNTO ABOR SYST NOOP APPE NLST MDTM XPWD XCUP XMKD XRMD NOP EPSV EPRT AUTH ADAT PBSZ PROT FEAT MODE OPTS HELP ALLO MLST MLSD SITE P@SW STRU CLNT MFMT HASH 214 Have a nice day. 211-Features: MDTM REST STREAM SIZE MLST type*;size*;modify*; MLSD UTF8 CLNT MFMT 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCwfQRtv5JGm8PmDmi6ovJI/+CRPgpGVLOWZ7taaAb8740k kuGtRo1yplhSRnx8wAz5uHjdazHD5Ar2BQIr1/QdyZPZEdTLlBF7Bj278KMbkOIRBldmM6LEzLgN l/

4TbK0PZYhrRS0TcQQp2+KgGPIDyFcXlClCmCZ4aXTZT4MsA9w4vbM0yOzq7XSe7tzHigHYAEur vH9C2sPhAMx3KYtr6JOQT5mKCk84xwPkHpCP5c+dYV+Y0K9xfT+6y96B/r655QGk7N89+17u9Y0L PKwHPtMXmi7MYNjpGFrTNL/LQOxZqKWiGb2RQQRcVh0W0JK1/0w7hqdPldtqMt+GeMgjKh1Xf/ St UOpxenofbTAfZI9BmhQO1ZHjaTrfNikBN4J2LqGqNfjwS6tBWANPNbgillUybuVZIqvaPd3tXKkV eILWDNgjc60XnRIO8QwfkBrl1c6L9voxbhtHTK69BZoSntD7xAGAU9sDUXI9heFUg4cMJmyKMZVA XUb9R7cyleM= Fingerprint: a9:3d:2c:aa:2b:3c:20:74:79:ad:3a:06:76:cb:de:f9 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 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Sat, 17 Jun 2023 19:24:44 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17 Last-Modified: Thu, 06 Apr 2023 08:57:36 GMT ETag: "1443-5f8a719956000" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 23.94.144.13:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-JDPEQD10OQR\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 23.94.144.13:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-JDPEQD10OQR\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 23.94.144.13:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-JDPEQD10OQR\pipe\lsass 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 23.94.144.13:49664 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-JDPEQD10OQR\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 23.94.144.13:49665 ncalrpc: WindowsShutdown ncacn_np: \\WIN-JDPEQD10OQR\PIPE\InitShutdown ncalrpc: WMsgKRpc054D40 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-

JDPEQD10OQR\PIPE\InitShutdown ncalrpc: WMsgKRpc054D40 ncalrpc: WMsgKRpc057731 ncalrpc: WMsgKRpc04147F82 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-65186660bf16397885 ncalrpc: LRPC-f867e6bcb83cf8035a ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-65186660bf16397885 ncalrpc: LRPC-f867e6bcb83cf8035a ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-f867e6bcb83cf8035a ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-4c8a76e1b4a374bd6b ncalrpc: LRPC-ed7b77cb26594cd299 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-65186660bf16397885 ncalrpc: LRPC-f867e6bcb83cf8035a ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-f867e6bcb83cf8035a ncalrpc: LRPC-bd4ef11b23dfe8dd92 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e 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-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-d771327df4cf4948a7 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel

ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLE97C17D2788126F007015472355B5 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-2894669bed9f37659e ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-2894669bed9f37659e 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-2b579bcb49d0ab02b2 ncalrpc: LRPC-2685821f9064007f76 ncalrpc: IUserProfile2 ncalrpc: LRPC-81599f972ee9f11d91 ncalrpc: senssvc ncalrpc: LRPC-2d208ac5c7f85f33d4 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-c0685c706e62881ae4 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-40b7f59b251fbd8898 ncalrpc: OLEB41B384294BEB14AC498B2EB0340 ncalrpc: LRPC-4c8a76e1b4a374bd6b 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-02bf38a182929947dd a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-ad4ee74ed281e34e21 ncalrpc: LRPC-ed7b77cb26594cd299 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 23.94.144.13:49666 ncacn_np: \\WIN-JDPEQD10OQR\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-c4f5fcbb922d21a020 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-424f294e687ef05feb 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: 23.94.144.13:49667 ncalrpc: LRPC-12455dcb951372d887 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-3a8d70adc1f5da66c2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 23.94.144.13:49667 ncalrpc: LRPC-12455dcb951372d887 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-3a8d70adc1f5da66c2 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-12455dcb951372d887 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc:

LRPC-3a8d70adc1f5da66c2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-3a8d70adc1f5da66c2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-JDPEQD10OQR\PIPE\atsvc ncalrpc: LRPC-3a8d70adc1f5da66c2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-3a8d70adc1f5da66c2 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-d2fb5c59d414a7c00f ncalrpc: DNSResolver 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-JDPEQD10OQR\PIPE\wkssvc ncalrpc: LRPC-b19781b3de18706986 eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-b19781b3de18706986 f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-b19781b3de18706986 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 23.94.144.13:49668 ncacn_np: \\WIN-JDPEQD10OQR\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-2d208ac5c7f85f33d4 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-8756d741093d8cd90e 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-48c196f44abcc3ba57 c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-48c196f44abcc3ba57 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-48c196f44abcc3ba57 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-48c196f44abcc3ba57 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-48c196f44abcc3ba57 3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-4136452faeac831418 ncalrpc: OLE3F520055EA8F0056E647C9D8602E 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-3cca013c00dad56b98 ncalrpc: LRPC-a5e824dbbb9deb5761 ncalrpc: LRPC-47a59c1413d6da2754 ncalrpc: LRPC-ae1968d02ae377343d f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-a5e824dbbb9deb5761 ncalrpc: LRPC-47a59c1413d6da2754 ncalrpc: LRPC-ae1968d02ae377343d 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-47a59c1413d6da2754 ncalrpc: LRPC-ae1968d02ae377343d dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-ae1968d02ae377343d 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-a21d4464acbab810b3 ncalrpc: OLEB82FA2D6FF592E5A96F40ECC7FE7 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-30c6ba5213d9070bf7 ncalrpc: OLECB9A4B2D5DE5A136055F33FF7E56 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-30c6ba5213d9070bf7 ncalrpc: OLECB9A4B2D5DE5A136055F33FF7E56 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: OLE168D1E726AA1059A5218655EEB65 ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-80ba72622694557e95 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-80ba72622694557e95 2e6035b2-e8f1-41a7-

a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-80ba72622694557e95 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-80ba72622694557e95 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.94.144.13:49669 ncalrpc: LRPC-8f1af957be55a481bb 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 23.94.144.13:49669 ncalrpc: LRPC-8f1af957be55a481bb ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.94.144.13:49669 ncalrpc: LRPC-8f1af957be55a481bb 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.94.144.13:49669 ncalrpc: LRPC-8f1af957be55a481bb 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 23.94.144.13:49669 ncalrpc: LRPC-8f1af957be55a481bb b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-5340d70c9b4e3cbc75 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-07966ecf809b88fa4d 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-07966ecf809b88fa4d 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 23.94.144.13:49671 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-3072c6bcda0e8d107b ncalrpc: OLE12D702CF319B887FDC8FEE43B20B 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-75aa41c11803d8adcd 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-b7610e2069388baf57 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\WIN-JDPEQD10OQR\PIPE\ROUTER f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-6c0b4600f3ff5d5420 ncalrpc: LRPC-92ed4f29fe603eb9b4 d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-26682da8800f80d2df d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-26682da8800f80d2df a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-e858b5b2f602e31f93 ncalrpc: LRPC-e858b5b2f602e31f93 ncalrpc: LRPC-e858b5b2f602e31f93 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0

annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-2cdef086644bf538d1 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc04147F82 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d6268b917c70d63c3d fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d6268b917c70d63c3d 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d6268b917c70d63c3d 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d6268b917c70d63c3d 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-d6268b917c70d63c3d b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-d3fa380d99f7147ecc ncalrpc: OLE5B8C408A286482A71A56D94E83D5 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-d3fa380d99f7147ecc ncalrpc: OLE5B8C408A286482A71A56D94E83D5 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-d3fa380d99f7147ecc ncalrpc: OLE5B8C408A286482A71A56D94E83D5 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-fd080cbf0118548799 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 23.94.144.13:65227 bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-f3fa3c547973db3554 ncalrpc: OLEE8C56BFAA4CF0C8C6E06EE1498F8 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: e9c5b48e-95f4-4554-9c37-cac14465bf78 ncalrpc: LRPC-accf610400a151aad7 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Thu, 15 Jun 2023 18:34:41 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17 Last-Modified: Thu, 06 Apr 2023 08:57:36 GMT ETag: "1443-5f8a719956000" Accept-Ranges: bytes Content-Length: 5187 Content-Type: text/html ``` HEARTBLEED: 2023/06/15 18:34:59 23.94.144.13:443 - SAFE ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-JDPEQD10OQR NetBIOS Domain Name: WIN-JDPEQD10OQR NetBIOS Computer Name: WIN-JDPEQD10OQR DNS Domain Name: WIN-JDPEQD10OQR FQDN: WIN-JDPEQD10OQR ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sat, 17 Jun 2023 06:50:18 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 10/Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-JDPEQD10OQR NetBIOS Domain Name: WIN-JDPEQD10OQR NetBIOS Computer Name: WIN-JDPEQD10OQR DNS Domain Name: WIN-JDPEQD10OQR FQDN: WIN-JDPEQD10OQR ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.94.144.13']

Name

16c7760898572422cac97f705e9076c35610a07fbc40aaa91b5663af923cdca7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '16c7760898572422cac97f705e9076c35610a07fbc40aaa91b5663af923cdca7']

Name

www.website-dolap.com

Pattern Type

stix

Pattern

[hostname:value = 'www.website-dolap.com']

StixFile

Value
16c7760898572422cac97f705e9076c35610a07fbc40aaa91b5663af923cdca7
cfc4f6c4931fc8df03919d96181178a903a6ccd39eb5268ac00b3a223c027b5b
4f6e9a66f50f443d07676ef43a7f2349fc713c96522058c1c4d425da7be4a4bf
8566d2bf58fe371e646076c60874a8fbb50de2fbf9b950c457804d316a3de89f

Hostname

Value
www.openseamonkeys.com
www.martynasobczak.com
www.driversofficial.com
www.nolinkoti.biz
www.ganosignsandprinting.com
www.hew9.xyz
www.gameozo.com
www.unbecomingsail.xyz
www.bjhxtp.com
www.4thmainland.com
www.yolcu360online.autos
www.porgy.online
www.valleyofbreath.com

www.youhousedesign.com

www.website-dolap.com

www.eperq.buzz

www.thecharmingchimp.com

www.abhisheksharma.life

www.cloudzon.world

www.ctrivertravel.net

www.sagewoodworkinginc.com

www.dl-jmjg.com

www.cleanskinshop.com

www.theclockpeddler.com

www.thewoodeniphonecase.com

www.strattmanwedding.com

www.firstonsiterestoration.com

www.eliteenduranceuk.com

www.chaintrt.com

www.langlaufdavos.com

www.babyshoespromo.com

www.livetcvety.ru

www.simplepay.kitchen

www.ytdxjt.com

www.rtlsdepmpyv7.com

www.astudyinstories.com

IPv4-Addr

Value
23.94.144.13

External References

- https://isc.sans.edu/diary/rss/29958
- https://otx.alienvault.com/pulse/64907a0fed2b36310998d7ca