Jan 25 2024

NETMANAGEIT

Intelligence Report

Letters allegedly from the State Special Communications Service and the State Emergency Service - UAC-0050 attack using RemoteUtilities

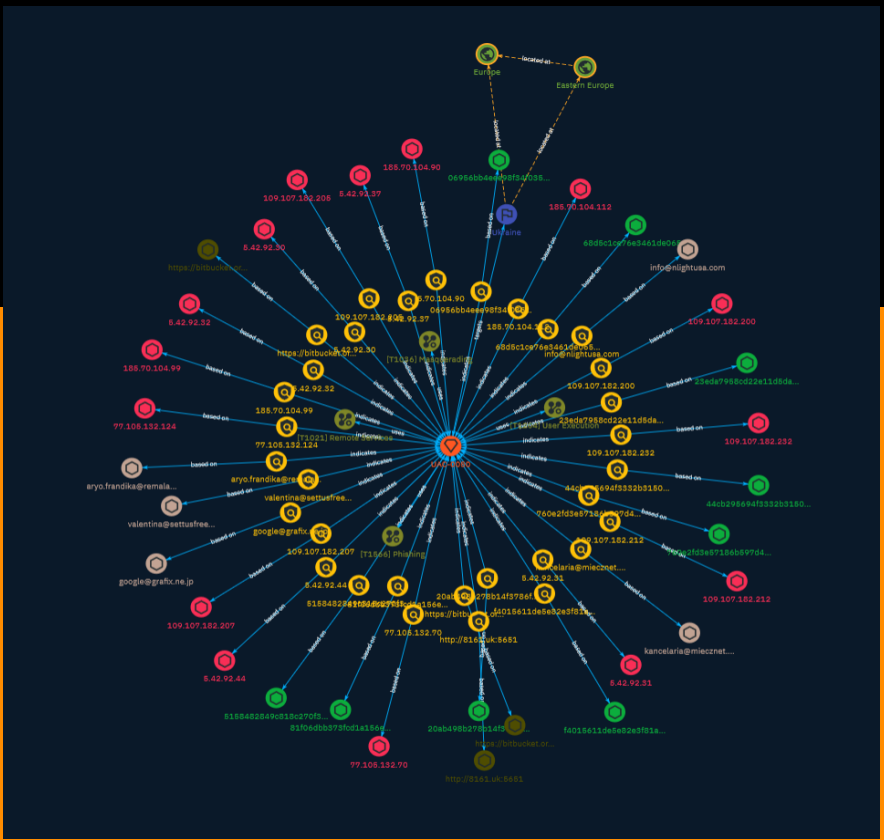

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On 22.01.2024, the Government Computer Emergency Response Team of Ukraine CERT-UA detected mass distribution of emails, allegedly on behalf of the State Special Communications Service and the State Emergency Service of Ukraine, containing a RAR archive or a link to Bitbucket and dedicated to "virus removal" and "evacuation", respectively.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.
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

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

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In

versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Indicator

Name

109.107.182.212

Description

ISP: Daniil Yevchenko **OS:** None ---------- Hostnames: - hosted-by.yeezyhost.net ---------- Domains: - yeezyhost.net ---------- Services: **135:** ```
\x05\x00\x0c\x03\x10\x00\x00\x00<\x00\x00\x00\x01\x00\x00\x00\xb8\x10\xb8\x10\xc3&\x00\x00\x04\x00135\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x04]\x88\x8a\xeb\x1c\xc9\x11\x9f\xe8\x08\x00+\x10H`\x02\x00\x00\x00 ``` ---------- **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.182.212']

Name

109.107.182.207

Description

ISP: Daniil Yevchenko **OS:** None ------------------------- Hostnames: - hosted-by.yeezyhost.net ------------------------- Domains: - yeezyhost.net ------------------------- Services: **135:** ``` Microsoft RPC Endpoint Mapper 04eeb297-cbf4-466b-8a2a-bfd6a2f10bba version: v1.0 annotation: EFSK RPC Interface provider: efssvc.dll ncacn_np: \\DESKTOP-TCRDU4C\pipe\efsrpc ncalrpc: LRPC-c89cb5681b4b4694e7 df1941c5-fe89-4e79-bf10-463657acf44d version: v1.0 annotation: EFS RPC Interface provider: efssvc.dll ncacn_np: \\DESKTOP-TCRDU4C\pipe\efsrpc ncalrpc: LRPC-c89cb5681b4b4694e7 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 109.107.182.207:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 109.107.182.207:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 109.107.182.207:49664 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: \\DESKTOP-TCRDU4C\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: 109.107.182.207:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 109.107.182.207:49665 ncalrpc: WindowsShutdown ncacn_np: \\DESKTOP-TCRDU4C\PIPE\InitShutdown ncalrpc: WMsgKRpc05EEE0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\DESKTOP-TCRDU4C\PIPE\InitShutdown ncalrpc: WMsgKRpc05EEE0 ncalrpc: WMsgKRpc061821 ncalrpc: WMsgKRpc01A3A8212 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-1d173f1adb776de9d1 ncalrpc: LRPC-44493256f7a9dec5e4 ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel

ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-1d173f1adb776de9d1 ncalrpc: LRPC-44493256f7a9dec5e4 ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-44493256f7a9dec5e4 ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-f8de4e29fc207c071f ncalrpc: LRPC-8b4f1301a78fb11c67 ncalrpc: LRPC-ae9b01f4b4ad033f4f 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-1d173f1adb776de9d1 ncalrpc: LRPC-44493256f7a9dec5e4 ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-44493256f7a9dec5e4 ncalrpc: LRPC-1e9706a1830cd761ce ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 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-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-8fefb109e7d6ec2426 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLEFF28E5B0C7DB43DCA5872B7304A7 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel

ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-0b1f53d1f238e80e09 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-0b1f53d1f238e80e09 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-9f60f942d716940a9f ncalrpc: LRPC-5497e54456a52fae23 ncalrpc: IUserProfile2 ncalrpc: LRPC-6c02069bb88777a465 ncalrpc: senssvc a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-b9625475def081e2cc ncalrpc: LRPC-f8de4e29fc207c071f e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-4b606f20993667e6c3 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-ece15ce6153bf22d7d ncalrpc: OLE50B6E8367696364E2048A8FFC489 ncalrpc: LRPC-8b4f1301a78fb11c67 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-abfc45e0ec96748c7c f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 109.107.182.207:49666 ncacn_np: \\DESKTOP-TCRDU4C\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-8b090542b738c8dc54 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: 109.107.182.207:49667 ncalrpc: LRPC-8c657ec4f24d30b050 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-45795f48b5752ac59a 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 109.107.182.207:49667 ncalrpc: LRPC-8c657ec4f24d30b050 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-45795f48b5752ac59a 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-8c657ec4f24d30b050 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-45795f48b5752ac59a 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-45795f48b5752ac59a 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-45795f48b5752ac59a 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-45795f48b5752ac59a

4c8d0bef-d7f1-49f0-9102-caa05f58d114 version: v1.0 ncalrpc: nlaapi ncalrpc: nlaplg 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-64f3b2da11c84a6ee5 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\DESKTOP-TCRDU4C\PIPE\wkssvc ncalrpc: LRPC-adc5dc1dc31e8e088f eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-adc5dc1dc31e8e088f f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-adc5dc1dc31e8e088f 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 109.107.182.207:49668 ncacn_np: \\DESKTOP-TCRDU4C\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-5497e54456a52fae23 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: e824f61c-49e9-4b47-9ef9-b8cd760917a4 ncalrpc: LRPC-cbd261d5e4f0865f0d 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-f6504b8cacd00b0443 ncalrpc: OLE124E21A51A094860B252A3642F11 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-f6504b8cacd00b0443 ncalrpc: OLE124E21A51A094860B252A3642F11 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-1269d13ddedac058fb ncalrpc: DNSResolver c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 7aeb6705-3ae6-471a-882d-f39c109edc12 version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 e7f76134-9ef5-4949-a2d6-3368cc0988f3 version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-93f242a559ef127479 ncalrpc: OLE75A7A200F2B83F8B75B8908BD028 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 109.107.182.207:49669 ncalrpc: LRPC-accd4eb6bcffa01553 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 109.107.182.207:49669 ncalrpc: LRPC-accd4eb6bcffa01553 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 109.107.182.207:49669 ncalrpc: LRPC-accd4eb6bcffa01553 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 109.107.182.207:49669 ncalrpc: LRPC-accd4eb6bcffa01553 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 109.107.182.207:49669 ncalrpc: LRPC-accd4eb6bcffa01553 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-4546b7c4b74e574a27 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-8c76eeb6406cbf637c ncalrpc: LRPC-8d29e70b5d49790168 ncalrpc: LRPC-b9b4dcef7c2d5bd55b ncalrpc: LRPC-4d30fc3b966cf88ff4 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation:

Fw APIs ncalrpc: LRPC-8d29e70b5d49790168 ncalrpc: LRPC-b9b4dcef7c2d5bd55b ncalrpc: LRPC-4d30fc3b966cf88ff4 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-b9b4dcef7c2d5bd55b ncalrpc: LRPC-4d30fc3b966cf88ff4 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-4d30fc3b966cf88ff4 e7a216af-1ec1-447f-8d3f-a87278db564d version: v1.0 ncalrpc: LRPC-10c3fa199824577263 e64b9aee-f372-4312-9a14-8f1502b5c8e3 version: v1.0 ncalrpc: LRPC-7451022c8532ff65e4 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: OLE70A3B0947B7111B2508E8CA167E6 ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-98676d587d8060fa5e c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-98676d587d8060fa5e 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-98676d587d8060fa5e 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-98676d587d8060fa5e 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-d20499fe4410678397 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-d20499fe4410678397 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-bb42be8466812bada1 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-6299f9938480a919d9 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\DESKTOP-TCRDU4C\PIPE\ROUTER f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-8f448ac9b2e5799c4d ncalrpc: LRPC-5c889c89de557f8592 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: 109.107.182.207:49670 ncalrpc: ipsec 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-77e8bc0839f1565f97 ncalrpc: OLE5E945B9AAD2140D02EF19623CA46 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 109.107.182.207:49671 4b112204-0e19-11d3-b42b-0000f81feb9f version: v1.0 provider: ssdpsrv.dll ncalrpc: LRPC-0f603c99863156a672 c27f3c08-92ba-478c-b446-b419c4cef0e2 version: v1.0 ncalrpc: LRPC-4e6c878140a011311f 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-6d61fb31409c7ea1a7 ncalrpc: OLE02726566297F2D899000551B3BCB 26268c86-

e770-433e-86ef-5f3ba6731fba version: v1.0 ncalrpc: LRPC-909fdca5b2834f274e ncalrpc: OLEAEF569E24E281F4CB7F27FD02DFD 54b4c689-969a-476f-8dc2-990885e9f562 version: v0.0 ncalrpc: LRPC-1644b361ae6e50e7da be6293d3-2827-4dda-8057-8588240124c9 version: v0.0 ncalrpc: LRPC-1644b361ae6e50e7da 7a20fcec-dec4-4c59-be57-212e8f65d3de version: v1.0 ncalrpc: LRPC-024adff5f8a41de506 06bba54a-be05-49f9-b0a0-30f790261023 version: v1.0 annotation: Security Center provider: wscsvc.dll ncalrpc: LRPC-3a4be214f0aee4bac9 ncalrpc: OLEA06BBDC5ADEA74D8FF60ADC5D6B6 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-4db1b50f4c3a9e9198 bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-67a8292a26eeb2caab ncalrpc: OLEF251B925C85237508F70A443CF03 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc01A3A8212 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-9d8afef5a624695175 ncalrpc: OLEF233AD05C6521BFB89BE68F35E56 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-9d8afef5a624695175 ncalrpc: OLEF233AD05C6521BFB89BE68F35E56 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-9d8afef5a624695175 ncalrpc: OLEF233AD05C6521BFB89BE68F35E56 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint 923c9623-db7f-4b34-9e6d-e86580f8ca2a version: v1.0 ncalrpc: OLE31D6638C4A71626175E22BA6E0DD ncalrpc: LRPC-28081ad76b0b72f7db 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd version: v1.0 ncalrpc: OLE31D6638C4A71626175E22BA6E0DD ncalrpc: LRPC-28081ad76b0b72f7db d2716e94-25cb-4820-bc15-537866578562 version: v1.0 ncalrpc: OLE31D6638C4A71626175E22BA6E0DD ncalrpc: LRPC-28081ad76b0b72f7db 43890c94-bfd7-4655-ad6a-b4a68397cdcb version: v0.0 ncalrpc: LRPC-28081ad76b0b72f7db c8ba73d2-3d55-429c-8e9a-c44f006f69fc version: v0.0 ncalrpc: LRPC-28081ad76b0b72f7db e8748f69-a2a4-40df-9366-62dbeb696e26 version: v0.0 ncalrpc: LRPC-28081ad76b0b72f7db 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-900dedbf9e858367da fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-900dedbf9e858367da 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-900dedbf9e858367da 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-900dedbf9e858367da 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-900dedbf9e858367da 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-a7ac388b2c677e7184 ncalrpc: OLEECD00F81A839D4A6A2986E344567 ncalrpc: LRPC-d9ddfa691dd953b605 ncalrpc: LRPC-d9ddfa691dd953b605 ncalrpc: LRPC-d9ddfa691dd953b605 ba4aa15a-be94-47fb-9bfb-fef110e7efad version: v1.0 annotation: DevQueryBroker client query RPC interface ncalrpc: LRPC-2c6ddf6710d5837d7a ``` ---------- **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-

TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.182.207']

Name

kancelaria@miecznet.com.pl

Pattern Type

stix

Pattern

[email-addr:value = 'kancelaria@miecznet.com.pl']

Name

5158482849c818c270f302c1dfa06d770ed2b5056cf393d60fd56817636866da

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5158482849c818c270f302c1dfa06d770ed2b5056cf393d60fd56817636866da']

Name

https://bitbucket.org/dsnsgovua/dsns/downloads/plan_dsns.gov.ua.rar

Pattern Type

stix

Pattern

[url:value = 'https://bitbucket.org/dsnsgovua/dsns/downloads/plan_dsns.gov.ua.rar']

Name

44cb295694f3332b31500c7d8408e6f93bb34a56617ae6850a205ed16c2a42a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44cb295694f3332b31500c7d8408e6f93bb34a56617ae6850a205ed16c2a42a8']

Name

5.42.92.44

Description

ISP: Daniil Yevchenko **OS:** Windows (build 10.0.19041) ---------- Hostnames: - hosted-by.yeezyhost.net ---------- Domains: - yeezyhost.net ---------- Services: **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 (version 2004)/Windows Server (version 2004)

OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.92.44']

Name

valentina@settusfree.org.uk

Pattern Type

stix

Pattern

[email-addr:value = 'valentina@settusfree.org.uk']

Name

5.42.92.31

Description

ISP: Daniil Yevchenko **OS:** Windows (build 10.0.19041) ---------- Hostnames: - hosted-by.saltu-cloud.pro ---------- Domains: - saltu-cloud.pro ---------- Services: **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-

TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.92.31']

Name

5.42.92.30

Description

ISP: Daniil Yevchenko **OS:** None ---------- Hostnames: - hosted-by.saltu-cloud.pro ---------- Domains: - saltu-cloud.pro ---------- Services: **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 Server 2022 OS Build: 10.0.20348 Target Name: WIN-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 19 Jan 2024 00:26:48 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.92.30']

Name

185.70.104.90

Description

ISP: HOSTKEY B.V. **OS:** Windows Server 2012 R2 ---------- Hostnames: ---------- Domains: ---------- Services: **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: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP am Windows Server 2012R2 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.70.104.90']

Name

185.70.104.99

Description

CC=RU ASN=AS50867 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.70.104.99']

Name

5.42.92.37

Description

ISP: Daniil Yevchenko **OS:** Windows (build 10.0.19041) ---------- Hostnames: - hosted-by.yeezyhost.net ---------- Domains: - yeezyhost.net ---------- Services: **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.92.37']

Name

68d5c1ce76e3461de065e61ade5428ab10eb1962aa9f2e89199823a033d5cbca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '68d5c1ce76e3461de065e61ade5428ab10eb1962aa9f2e89199823a033d5cbca']

Name

aryo.frandika@remala.id

Pattern Type

stix

Pattern

[email-addr:value = 'aryo.frandika@remala.id']

Name

info@nlightusa.com

Pattern Type

stix

Pattern

[email-addr:value = 'info@nlightusa.com']

Name

f4015611de5e82e3f81a77b896af259d120f1ca956035378a3d9e51fba010669

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4015611de5e82e3f81a77b896af259d120f1ca956035378a3d9e51fba010669']

Name

https://bitbucket.org/ccleaners/ccleaner/downloads/ccleaner.zip

Pattern Type

stix

Pattern

[url:value = 'https://bitbucket.org/ccleaners/ccleaner/downloads/ccleaner.zip']

Name

760e2fd3e57186b597d40b996811768e6c4a28ca54685e029104fcf82f68238d

Description

blowfish_constants

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '760e2fd3e57186b597d40b996811768e6c4a28ca54685e029104fcf82f68238d']

Name

77.105.132.70

Description

ISP: Valery Smoliar **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 77.105.132.70:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 77.105.132.70:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 77.105.132.70:49664 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: \\DESKTOP-TCRDU4C\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: 77.105.132.70:49664 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: \\DESKTOP-TCRDU4C\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 77.105.132.70:49665 ncalrpc: WindowsShutdown ncacn_np: \\DESKTOP-TCRDU4C\PIPE\InitShutdown ncalrpc: WMsgKRpc062AC0 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\DESKTOP-TCRDU4C\PIPE\InitShutdown ncalrpc: WMsgKRpc062AC0 ncalrpc: WMsgKRpc065171 ncalrpc: WMsgKRpc0264A4852 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-1151e320afd128a89f ncalrpc: LRPC-c09999ab4ed6d86bd8 ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-1151e320afd128a89f ncalrpc: LRPC-c09999ab4ed6d86bd8 ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel

ncalrpc: umpo ncalrpc: LRPC-c09999ab4ed6d86bd8 ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-5d8655207b663086a7 ncalrpc: LRPC-6132f41de2decd5585 ncalrpc: LRPC-f05f327607e50853d5 ncalrpc: LRPC-af33a2314252c5c5ef ncalrpc: OLE93A32280BDAD3C70A645D3DCF1F4 ncalrpc: LRPC-af33a2314252c5c5ef ncalrpc: OLE93A32280BDAD3C70A645D3DCF1F4 ncalrpc: LRPC-91dac9b1929d460c4e 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-1151e320afd128a89f ncalrpc: LRPC-c09999ab4ed6d86bd8 ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-c09999ab4ed6d86bd8 ncalrpc: LRPC-890e6b8ba436c2654d ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 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-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-7f17d47201937e5f9b ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLEEEBEBFDBB9EAD4922DAB37633031 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-

c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-c1ec7f9fd3e92ab388 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-c1ec7f9fd3e92ab388 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-17372745d924db81d6 ncalrpc: IUserProfile2 ncalrpc: LRPC-c8337ae1a1ad3114f7 ncalrpc: senssvc ncalrpc: LRPC-9a56612ed633a9e5a9 a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-c1eb6097af9b684f76 ncalrpc: LRPC-5d8655207b663086a7 e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-3d6bc0d3b65f76e63e 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-9a148a983d764cab9f ncalrpc: OLE2334F933B3E1BB3BE6778AF65D44 ncalrpc: LRPC-6132f41de2decd5585 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-d8079f00d2319b2b42 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 77.105.132.70:49666 ncacn_np: \\DESKTOP-TCRDU4C\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-da9f756dc63c667ff4 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 4c8d0bef-d7f1-49f0-9102-caa05f58d114 version: v1.0 ncalrpc: nlaapi ncalrpc: nlaplg 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 77.105.132.70:49667 ncalrpc: LRPC-44452d778f31fe2b68 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-fee9420a6d9ec67a21 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 77.105.132.70:49667 ncalrpc: LRPC-44452d778f31fe2b68 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-fee9420a6d9ec67a21 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-44452d778f31fe2b68 ncalrpc: ubpmtaskhostchannel ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-fee9420a6d9ec67a21 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-fee9420a6d9ec67a21 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\DESKTOP-TCRDU4C\PIPE\atsvc ncalrpc: LRPC-fee9420a6d9ec67a21 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-fee9420a6d9ec67a21

30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-3141bf5b0480e55668 8833d1d0-965f-4216-b3e9-fbe58cad3100 version: v1.0 provider: SCardSvr.dll ncalrpc: LRPC-bcf6d4bb2637dee8c8 ncalrpc: LRPC-f05f327607e50853d5 c6b5235a-e413-481d-9ac8-31681b1faaf5 version: v1.256 ncalrpc: LRPC-bcf6d4bb2637dee8c8 ncalrpc: LRPC-f05f327607e50853d5 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\DESKTOP-TCRDU4C\PIPE\wkssvc ncalrpc: LRPC-3956b433977846595a eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-3956b433977846595a f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-3956b433977846595a 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 77.105.132.70:49668 ncacn_np: \\DESKTOP-TCRDU4C\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-9a56612ed633a9e5a9 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: 588a315f-d133-4b62-b37d-c5a665b5d4ad ncalrpc: LRPC-496cdd3307863e8add 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-23030f989be9b6ea02 ncalrpc: DNSResolver 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-bd564c4d9d8e2ad28a ncalrpc: OLED3342793EFEBE784914D1055FC01 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-bd564c4d9d8e2ad28a ncalrpc: OLED3342793EFEBE784914D1055FC01 c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 7aeb6705-3ae6-471a-882d-f39c109edc12 version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 e7f76134-9ef5-4949-a2d6-3368cc0988f3 version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-04bdd6c2ccc15808af ncalrpc: OLEE0B76A02FB99E0E0981C96720394 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-2728bdf78392e3b284 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-e9f26b7122a429d6a1 ncalrpc: LRPC-9486038c4cf18cfda5 ncalrpc: LRPC-173731c58dd95007a4 ncalrpc: LRPC-e712ad6d4f645bb4e1 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-9486038c4cf18cfda5 ncalrpc: LRPC-173731c58dd95007a4 ncalrpc: LRPC-e712ad6d4f645bb4e1 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-173731c58dd95007a4 ncalrpc: LRPC-e712ad6d4f645bb4e1 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-e712ad6d4f645bb4e1 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-05db368b4f38b797ea c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: OLEA8B3174972D8570ECE3A46412B81 ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f1e303cea174513ac9 c36be077-e14b-4fe9-8abc-

e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f1e303cea174513ac9 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-f1e303cea174513ac9 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-f1e303cea174513ac9 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-d195272401bc665f14 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-d195272401bc665f14 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 77.105.132.70:49672 650a7e26-eab8-5533-ce43-9c1dfce11511 version: v1.0 annotation: Vpn APIs ncalrpc: LRPC-de3787caa64631be54 ncalrpc: VpnikeRpc ncalrpc: RasmanLrpc ncacn_np: \\DESKTOP-TCRDU4C\PIPE\ROUTER 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: 77.105.132.70:49673 4b112204-0e19-11d3-b42b-0000f81feb9f version: v1.0 provider: ssdpsrv.dll ncalrpc: LRPC-54fb7840063134a983 f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-92266f94cd3c06e830 c27f3c08-92ba-478c-b446-b419c4cef0e2 version: v1.0 ncalrpc: LRPC-0d075696811ed4da34 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-7d52d4bd16cb0ec53a ncalrpc: OLEC14D532FC6555F9F022058386DE0 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-0fd2a467f287019d90 ncalrpc: OLE711F9BF79D17ACD7CA8342B44C17 54b4c689-969a-476f-8dc2-990885e9f562 version: v0.0 ncalrpc: LRPC-37053d51069e7b3913 be6293d3-2827-4dda-8057-8588240124c9 version: v0.0 ncalrpc: LRPC-37053d51069e7b3913 7a20fcec-dec4-4c59-be57-212e8f65d3de version: v1.0 ncalrpc: LRPC-181be5a2583a9b9a26 06bba54a-be05-49f9-b0a0-30f790261023 version: v1.0 annotation: Security Center provider: wscsvc.dll ncalrpc: LRPC-6d30ae279c7c8e0c44 ncalrpc: OLEA78905FD15E49DE8611C8646C4F1 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-8c4ed98ada2e8e4ae0 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-5629cbee85454d986c ncalrpc: OLEACC1F0B054D97BD170103B3855B3 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0264A4852 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-f67d71243cba754ac3 ncalrpc: OLE84962D7E9CAB1DAF77EA3E1FD1F1 0fc77b1a-95d8-4a2e-a0c0-

cff54237462b version: v0.0 ncalrpc: LRPC-f67d71243cba754ac3 ncalrpc: OLE84962D7E9CAB1DAF77EA3E1FD1F1 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-f67d71243cba754ac3 ncalrpc: OLE84962D7E9CAB1DAF77EA3E1FD1F1 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-4507eedf7d8306708e fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-4507eedf7d8306708e 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-4507eedf7d8306708e 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-4507eedf7d8306708e 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-4507eedf7d8306708e 43890c94-bfd7-4655-ad6a-b4a68397cdcb version: v0.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 c8ba73d2-3d55-429c-8e9a-c44f006f69fc version: v0.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 e8748f69-a2a4-40df-9366-62dbeb696e26 version: v0.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 923c9623-db7f-4b34-9e6d-e86580f8ca2a version: v1.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd version: v1.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 d2716e94-25cb-4820-bc15-537866578562 version: v1.0 ncalrpc: LRPC-8652a8f69eb35356f2 ncalrpc: OLE4144F4CCE0FF69CEF2959E347C02 ba4aa15a-be94-47fb-9bfb-fef110e7efad version: v1.0 annotation: DevQueryBroker client query RPC interface ncalrpc: LRPC-947cc0016cdfac40a0 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-96fcd5d5e7fbc3a48b ncalrpc: OLE59875C01E289B3DBC8D2026BD62D ncalrpc: LRPC-954bf11817419fb26c ncalrpc: LRPC-954bf11817419fb26c ncalrpc: LRPC-954bf11817419fb26c 4be96a0f-9f52-4729-a51d-c70610f118b0 version: v1.0 annotation: wbiosrvc provider: wbiosrvc.dll ncalrpc: LRPC-dd91bcd2401f5a4059 c0e9671e-33c6-4438-9464-56b2e1b1c7b4 version: v1.0 annotation: wbiosrvc provider: wbiosrvc.dll ncalrpc: LRPC-dd91bcd2401f5a4059 169c453b-5955-4672-be44-21f61e9ef18f version: v1.0 annotation: INgcContainerEnum ncalrpc: LRPC-59bc378e385f845182 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 77.105.132.70:62784 ncalrpc: LRPC-b57a567be061d23f7f 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 77.105.132.70:62784 ncalrpc: LRPC-b57a567be061d23f7f ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 77.105.132.70:62784 ncalrpc: LRPC-b57a567be061d23f7f 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 77.105.132.70:62784 ncalrpc: LRPC-b57a567be061d23f7f 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 77.105.132.70:62784 ncalrpc: LRPC-b57a567be061d23f7f ``` ---------- **137:** ``` NetBIOS Response: Server Name: DESKTOP-TCRDU4C MAC Address: 52:54:00:79:97:DB Names: DESKTOP-TCRDU4C <0x0> WORKGROUP <0x0> DESKTOP-TCRDU4C <0x20> ``` ---------- **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.105.132.70']

Name

109.107.182.205

Description

ISP: Daniil Yevchenko **OS:** Windows (build 10.0.19041) ---------- Hostnames: - hosted-by.yeezyhost.net ---------- Domains: - yeezyhost.net ---------- Services: **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.182.205']

Name
109.107.182.232

Description
ISP: Daniil Yevchenko **OS:** None ------------------------- Hostnames: - hosted-by.yeezyhost.net ------------------------- Domains: - yeezyhost.net ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDNYp6W8ozpsWzsrIe0QoXLSFDRRe4d29g6e28V4s2AMeFj wslHJuKWlMC0HhVT/UQ6fiENqqLfQYjtk+xcrYQCvRPzLuzEOybO/ NbWfGdM8btQDJ1gSVWY4K6J WGCX7l6CqQnMHkD70eZVx9p4BmxzYZFrlR6PY7XNtD62xz88nou9V59rL9fs91EPdQC/Snb7ji+6VnO4B6c1Nuw1QmCHUKcnGuaw5KdYz3Xk/9FT4fihEkgtERX1TGREUpVK/dxp0LIUX6Dudi4a71x1jlUR5gc5O7oJMuSoJiGc4r27Lzl+XcoYe/LdS6X8/3QqPZzMrZBc8nbCTpCVSx2wo3mqIqhNphN8hz9sz+QQxDV4csNFMe8sbd/Ms+Xw50nhhzHbAXMkDUBeJJYEtaw8IHMMT7js1mr5HpKtFfIUfd8z1UgD8duR415e9QGaM/G9CirvkIlnsnu6djQVlwkz1KxTzLd+Fk2INbmbBa0THRw3qYupYCRNWxNDZ7X0yroAo4s= Fingerprint: 67:03:a0:14:36:14:f2:0a:d0:71:3a:3f:c1:bc:49:6a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------------- **80:** ``` HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Fri, 12 Mar 2021 09:48:13 GMT Accept-Ranges: bytes ETag: "a5e7f1d12417d71:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 22 Jan 2024 01:11:02 GMT Content-Length: 7099 ``` ----------------- **1433:** ``` MS-SQL NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ----------------- **1801:** ``` \x10Z\x0b\x00LIOR<\x02\x00\x00\xff\xff\xff\xff\x00\x00\x12\x00\x06U=Q6\xdf\xc7@\x96C\x17\ \<\xe7l\xaa2\xf0\x07\x06\t\x87\xadN\x8co\x9b\xbf\xb46\xb9{\x00\x00\x00\x00\x10\x02\x00\x00ZZZ

ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ ``` ------------------ **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-BS656MOF35Q NetBIOS Domain Name: WIN-BS656MOF35Q NetBIOS Computer Name: WIN-BS656MOF35Q DNS Domain Name: WIN-BS656MOF35Q FQDN: WIN-BS656MOF35Q ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.182.232']

Name

20ab498b278b14f3786f634778a04d219c74e9fd8517b98f4aca313c9934b7f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20ab498b278b14f3786f634778a04d219c74e9fd8517b98f4aca313c9934b7f2']

Name

5.42.92.32

Description

CC=SE ASN=AS203727 Daniil Yevchenko

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.92.32']

Name

81f06dbb373fcd1a156e6076d13a76088715dafaf1ee80ba3adddd1b973b65a2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '81f06dbb373fcd1a156e6076d13a76088715dafaf1ee80ba3adddd1b973b65a2']

Name

77.105.132.124

Description

ISP: Valery Smoliar **OS:** Windows (build 10.0.19041) ---------- Hostnames: ---------- Domains: ---------- Services: **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **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 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found

Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 29 Dec 2023 12:22:10 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-LIVFRVQFMKO NetBIOS Domain Name: WIN-LIVFRVQFMKO NetBIOS Computer Name: WIN-LIVFRVQFMKO DNS Domain Name: WIN-LIVFRVQFMKO FQDN: WIN-LIVFRVQFMKO ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.105.132.124']

Name

109.107.182.200

Description

Agressive IP known malicious on AbuseIPDB - countryCode: FI - abuseConfidenceScore: 100 - lastReportedAt: 2024-01-24T20:47:10+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.182.200']

Name

http://8161.uk:5651

Pattern Type

stix

Pattern

[url:value = 'http://8161.uk:5651']

Name

185.70.104.112

Description

CC=RU ASN=AS50867 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.70.104.112']

Name

23eda7958cd22e11d5daa39d5a82e5740512c9435a138214b98d1925520bf8e8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23eda7958cd22e11d5daa39d5a82e5740512c9435a138214b98d1925520bf8e8']

Name
google@grafix.ne.jp
Pattern Type
stix
Pattern
[email-addr:value = 'google@grafix.ne.jp']
Name
06956bb4eee98f34f035af11666459b2f9fc5f7485b2cf16f6afb17bfa15a061
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '06956bb4eee98f34f035af11666459b2f9fc5f7485b2cf16f6afb17bfa15a061']

Intrusion-Set

Name
UAC-0050

Region

Name
Europe

Name
Eastern Europe

Country

Name
Ukraine

Email-Addr

Value
kancelaria@miecznet.com.pl
google@grafix.ne.jp
info@nlightusa.com
valentina@settusfree.org.uk
aryo.frandika@remala.id

StixFile

Value
06956bb4eee98f34f035af11666459b2f9fc5f7485b2cf16f6afb17bfa15a061
20ab498b278b14f3786f634778a04d219c74e9fd8517b98f4aca313c9934b7f2
f4015611de5e82e3f81a77b896af259d120f1ca956035378a3d9e51fba010669
68d5c1ce76e3461de065e61ade5428ab10eb1962aa9f2e89199823a033d5cbca
44cb295694f3332b31500c7d8408e6f93bb34a56617ae6850a205ed16c2a42a8
5158482849c818c270f302c1dfa06d770ed2b5056cf393d60fd56817636866da
23eda7958cd22e11d5daa39d5a82e5740512c9435a138214b98d1925520bf8e8
760e2fd3e57186b597d40b996811768e6c4a28ca54685e029104fcf82f68238d
81f06dbb373fcd1a156e6076d13a76088715dafaf1ee80ba3adddd1b973b65a2

IPv4-Addr

Value
109.107.182.207
109.107.182.200
5.42.92.31
109.107.182.205
109.107.182.232
77.105.132.70
185.70.104.99
109.107.182.212
5.42.92.44
5.42.92.37
5.42.92.32
185.70.104.90
185.70.104.112

77.105.132.124

5.42.92.30

Url

Value
http://8161.uk:5651
https://bitbucket.org/dsnsgovua/dsns/downloads/plan_dsns.gov.ua.rar
https://bitbucket.org/ccleaners/ccleaner/downloads/ccleaner.zip

External References

- https://otx.alienvault.com/pulse/65b19b7584b073db3e0c3236
- https://cert.gov.ua/article/6277285