Dec 19 2023

NETMANAGEIT

Intelligence Report

PikaBot distributed via malicious search ads

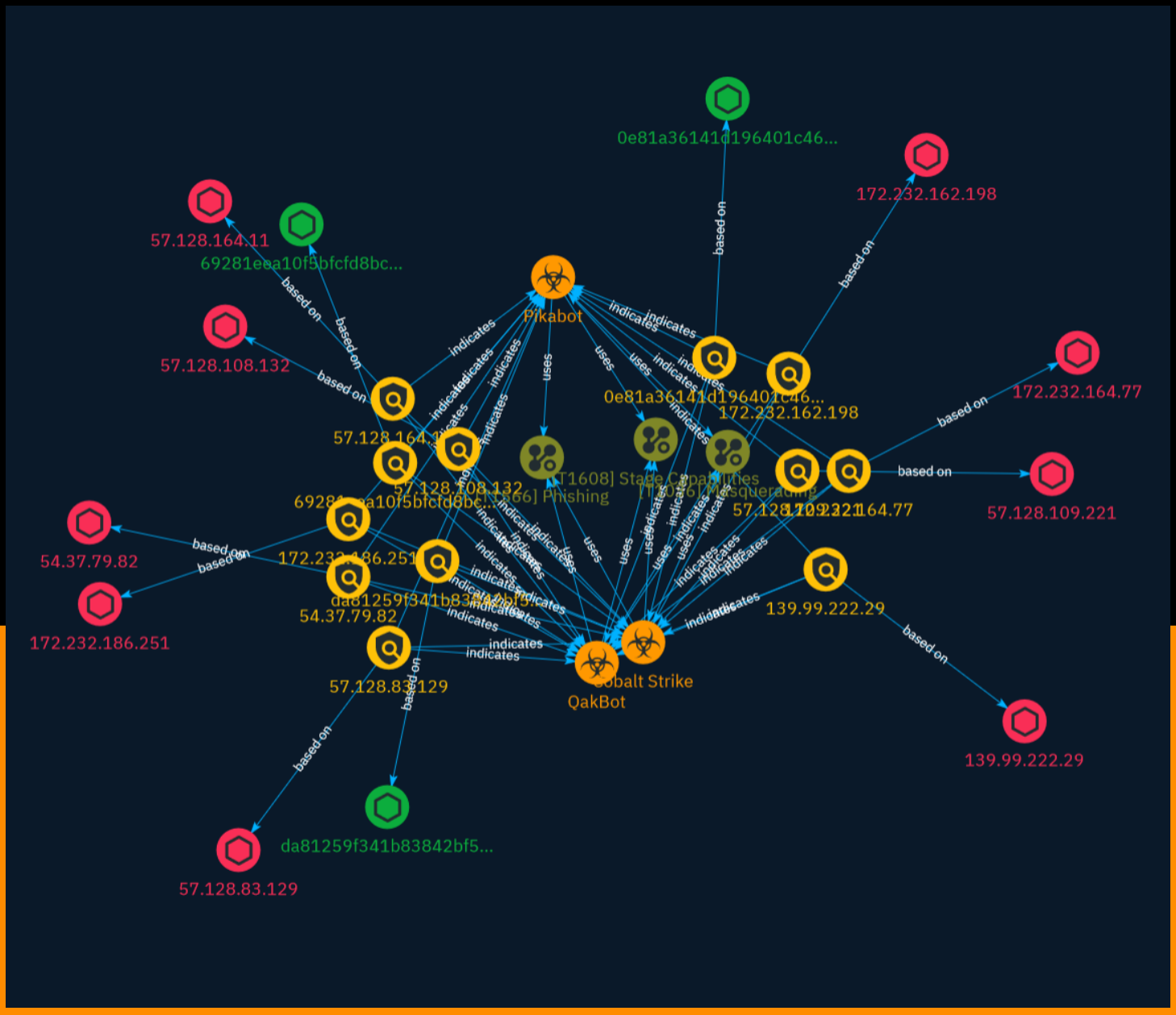

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Malwarebytes.com shares details of a new family of malware distributed via malvertising and web ad campaigns, as part of its 20th anniversary celebrations on 15 December 2023 and marks the launch of the company's Security Advisor.

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

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise

Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Indicator

Name

57.128.83.129

Description

ISP: OVH SAS **OS:** Windows Server 2022 (build 10.0.20348) ---------- Hostnames: - xbhxn.one ---------- Domains: - xbhxn.one ---------- Services: **53:** ``` 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 Resolver name: xbhxn.one ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **2525:** ``` 220 xbhxn.one ESMTP service ready\r\n ``` ---------- **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-C2RH9F7DBT0 NetBIOS Domain Name: WIN-C2RH9F7DBT0 NetBIOS Computer Name: WIN-C2RH9F7DBT0 DNS Domain Name: WIN-C2RH9F7DBT0 FQDN: WIN-C2RH9F7DBT0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '57.128.83.129']

Name

da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff']

Name

0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5']

Name

69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320']

Name

57.128.109.221

Description

ISP: OVH SAS **OS:** None ---------- Hostnames: - xnzrih.one ---------- Domains: - xnzrih.one ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCkXlRsZjgvPmJIN+fMlxIEN+W898cKLnmymPddFRR2SCvv zld2wJXus0MjO24Hcq8vUlF/mzAXplg/ v+BykPdtBw+PUygzGLp2MhvHO27+EdR89k04tOKpbAA/ nurya6Aaab2z9/ Kti4ZKdXUHP79EcrFGD9LZRE1MJf7thFWLe1Tnrl6vL1mf/Hc/tT+QuOpiLbTQ NiYLI9QR1V/ 0l3fFE7bqEDEz+sLyTUExc7ikYoUK/SvHrX7RF0Q4Gkay9dhj+XzL+82e5FRf6/NS lJxi7UrXP6Xpj17L8SFMZJf8hpoFxPxaahBDNH1La5KiUufP62OpOaC2T6G5JCMduyw5 Fingerprint: 06:77:32:b0:0b:fd:0f:52:29:4e:3b:38:c9:d1:e1:34 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ---------- **53:** ``` 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 Resolver name: xnzrih.one ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **8080:** ``` HTTP/1.0 403 Access denied while running with default configuration. Please correct any configuration file errors. Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '57.128.109.221']

Name

139.99.222.29

Description

CC=AU ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.99.222.29']

Name

57.128.164.11

Description

CC=FR ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '57.128.164.11']

Name

172.232.162.198

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - 172-232-162-198.ip.linodeusercontent.com ---------- Domains: - linodeusercontent.com ---------- Services: **25:** ``` 220 clv10159.com ESMTP service ready 250-clv10159.com says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.232.162.198']

Name

54.37.79.82

Description

ISP: OVH SAS **OS:** Linux ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC5wvKeN/G0nWnPA6lipc4F0ozt+Su+LR5Vhmbf57Tw1Dud QfOZ9w0Pmi83ZptKBwiT7gaCC8g/gXzCE/gdB2zZ9nWa5OQLfDACX30yTikZegrhDHjXJoALtXVP gdDnIGDUoDuT5mgCupB4ePpL9VOhlggyi8hq6tBtllUy2sZT8satpqIeQnmCVgna7FViKKX1jMmV QEF4s9hfP2A2ZV7wT4bdwhwsp4AG4UKHWDI6iW13GpUWmr8mIAIoCSVAbiCofOn3u6Gv89E3U D8e Zf14h2Ke0lAvH9eWCLsspTB6qr+0QHueIrIY+7ktmftF1bmMbRErNeeXZ39Sq02k8ax9KIdQqlfu p4J4DzhIpjHK9oYB9pXcEH7shBOtNVXXD0ZQbt8cw3qNml/TO5tpwt/Df+tPuCcrbTE/nKC5HGJx
```
```

9fGMbIri3wxm+ce/ eNHhIabkA+WQfpTZxhWI+QGHDUXnctLDc9TkD+SAVghHcxRzhEukIBwkMvuw +kaiaLV2gr0= Fingerprint: b3:3d:b5:f6:53:88:29:18:49:3d:21:f9:13:ca:7b:11 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '54.37.79.82']

Name

57.128.108.132

Description

ISP: OVH SAS **OS:** Windows Server 2022 (build 10.0.20348) ---------- Hostnames: ---------- Domains: ---------- 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 Server 2022 OS Build: 10.0.20348 Target Name: WIN-NOQ7JMK1B8T NetBIOS Domain Name: WIN-NOQ7JMK1B8T NetBIOS Computer Name: WIN-NOQ7JMK1B8T DNS Domain Name: WIN-NOQ7JMK1B8T FQDN: WIN-NOQ7JMK1B8T ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '57.128.108.132']

Name

172.232.164.77

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - 172-232-164-77.ip.linodeusercontent.com ---------- Domains: - linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCDGImODVnFqjOI8GLQD2Z Ei XD3HmSRWWNrg4cJ7cIkr4UquCvJZmeUTN07Q/GWbqRaKo301AF0lW2UOcUqsRLs= Fingerprint: 90:05:ce:6e:16:28:47:41:99:97:7f:a1:50:07:b9:f5 Kex Algorithms: sntrup761x25519-sha512@openssh.com 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 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 ``` ---------- **5357:** ``` HTTP/1.1 503 Service Unavailable Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 12 Dec 2023 23:03:38 GMT Connection: close Content-Length: 326 ``` ---------- **10250:** ``` HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Mon, 18 Dec 2023 16:17:17 GMT Content-Length: 19 ``` HEARTBLEED: 2023/12/18 16:17:28 172.232.164.77:10250 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.232.164.77']

Name

172.232.186.251

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - 172-232-186-251.ip.linodeusercontent.com ---------- Domains: - linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNh7m8um/ 0t2Cmm1MG86gLR0 RqqgXx8r7yIa+XXww+b6JSEC5OQZFjvKQ06AqsRSl/ BMDGTIChT4ex2RpgJhbT0= Fingerprint: a1:1e:ec:27:26:ef:f9:0d:a2:4f:8d:95:dc:17:d8:12 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com 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 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 ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 172.232.186.251:49664 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-C7BD8CD5A4\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 172.232.186.251:49664 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-C7BD8CD5A4\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 172.232.186.251:49664 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-C7BD8CD5A4\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: 172.232.186.251:49664 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-C7BD8CD5A4\pipe\lsass d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 172.232.186.251:49665 ncalrpc: WindowsShutdown ncacn_np: \\WIN-C7BD8CD5A4\PIPE\InitShutdown ncalrpc: WMsgKRpc063780 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-C7BD8CD5A4\PIPE\InitShutdown ncalrpc: WMsgKRpc063780 ncalrpc: WMsgKRpc067521 ncalrpc: WMsgKRpc0368632 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub ncalrpc: LRPC-ebf42fd7a6ca947a0f ncalrpc: LRPC-06245d22043e22d185 ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-ebf42fd7a6ca947a0f ncalrpc: LRPC-06245d22043e22d185 ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-06245d22043e22d185 ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-b440183abd2a161a1c ncalrpc: LRPC-78b63081426fb87024 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-ebf42fd7a6ca947a0f ncalrpc: LRPC-06245d22043e22d185 ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-06245d22043e22d185 ncalrpc: LRPC-61ef8288209c8fd3c8 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 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-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-49bca89e1c477cdd3d ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v2.0 ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v2.0 ncalrpc: OLEFB24966D5499745D4429C3E4CF34 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-8b3157c95f79324c87 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-8b3157c95f79324c87 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-56c9f0aab1c348e027 ncalrpc: LRPC-c3a8cdc205990edb29 ncalrpc: IUserProfile2 ncalrpc: LRPC-132eb21ca59ee27ba8 ncalrpc: senssvc ncalrpc: LRPC-f7d5a61f90eb5b1fea f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-f2320705194b6b6248 ncalrpc: LRPC-bebe6946de8934576a e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 ncalrpc: LRPC-f7d9d79164f807c515 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-4c462cb1f1bc6af4c6 ncalrpc: OLE5FD76EAA7B18FFFC82086EC162E0 ncalrpc: LRPC-b440183abd2a161a1c 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 ncalrpc: LRPC-610443fd6759445e2a a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-5ef05c2250d3a0d039 ncalrpc: LRPC-78b63081426fb87024 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 172.232.186.251:49666 ncacn_np: \\WIN-C7BD8CD5A4\pipe\eventlog ncalrpc: eventlog 7ea70bcf-48af-4f6a-8968-6a440754d5fa

version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-c35d178e5523f76968 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-6b380fd937a2833ad4 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 172.232.186.251:49667 ncalrpc: LRPC-bafe94fe8ce60a4199 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-C7BD8CD5A4\PIPE\atsvc ncalrpc: LRPC-ec23189fb4e9f6f463 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 172.232.186.251:49667 ncalrpc: LRPC-bafe94fe8ce60a4199 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-C7BD8CD5A4\PIPE\atsvc ncalrpc: LRPC-ec23189fb4e9f6f463 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-bafe94fe8ce60a4199 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-C7BD8CD5A4\PIPE\atsvc ncalrpc: LRPC-ec23189fb4e9f6f463 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-C7BD8CD5A4\PIPE\atsvc ncalrpc: LRPC-ec23189fb4e9f6f463 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-C7BD8CD5A4\PIPE\atsvc ncalrpc: LRPC-ec23189fb4e9f6f463 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-ec23189fb4e9f6f463 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-b3908b0c00e84c9eec ncalrpc: DNSResolver 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-C7BD8CD5A4\PIPE\wkssvc ncalrpc: LRPC-991a9ed6692f9f3585 eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-991a9ed6692f9f3585 f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-991a9ed6692f9f3585 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-9672c463d6a7bd75e4 3f787932-3452-4363-8651-6ea97bb373bb version: v1.0 annotation: NSP Rpc Interface ncalrpc: LRPC-2bb079afb75e889844 ncalrpc: OLEC8F21A92E57B8C5DF95FDF82569B 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 172.232.186.251:49668 ncacn_np: \\WIN-C7BD8CD5A4\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-f7d5a61f90eb5b1fea 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-65f191e6bed5d27119 ncalrpc: LRPC-210225c1064fcd22a2 ncalrpc: LRPC-d5fa97706bee5ec8da ncalrpc: LRPC-1b776e4717db63b07b f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-210225c1064fcd22a2 ncalrpc: LRPC-d5fa97706bee5ec8da ncalrpc: LRPC-1b776e4717db63b07b 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-d5fa97706bee5ec8da ncalrpc: LRPC-1b776e4717db63b07b dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-1b776e4717db63b07b 13560fa9-8c09-4b56-a1fd-04d083b9b2a1 version: v1.0 ncalrpc: LRPC-c90dbebdafabb2b932

ncalrpc: OLE47C742442542AB45E51E78E4117E c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-c90dbebdafabb2b932 ncalrpc: OLE47C742442542AB45E51E78E4117E f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-c90dbebdafabb2b932 ncalrpc: OLE47C742442542AB45E51E78E4117E b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-c90dbebdafabb2b932 ncalrpc: OLE47C742442542AB45E51E78E4117E abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-c90dbebdafabb2b932 ncalrpc: OLE47C742442542AB45E51E78E4117E a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-99cdbf90916695d566 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-49e9e42d53ff20b49f c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-49e9e42d53ff20b49f 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-49e9e42d53ff20b49f 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-49e9e42d53ff20b49f b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-f6c463c2ce67e35fdd 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.232.186.251:49669 ncalrpc: LRPC-428bb42e9f038ff7c4 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 172.232.186.251:49669 ncalrpc: LRPC-428bb42e9f038ff7c4 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.232.186.251:49669 ncalrpc: LRPC-428bb42e9f038ff7c4 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.232.186.251:49669 ncalrpc: LRPC-428bb42e9f038ff7c4 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 172.232.186.251:49669 ncalrpc: LRPC-428bb42e9f038ff7c4 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-49f6a2f3303990888b ncalrpc: OLE13565187A3E1FC10369960CCBB82 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-49f6a2f3303990888b ncalrpc: OLE13565187A3E1FC10369960CCBB82 509bc7ae-77be-4ee8-b07c-0d096bb44345 version: v1.0 ncalrpc: LRPC-4492e73f61fd42e1b4 ncalrpc: OLEAC07B6C02258E1BD40EEF8FE320F 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-555cd0c27d95b9dcf3 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-555cd0c27d95b9dcf3 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 172.232.186.251:49670 ncalrpc: ipsec 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 172.232.186.251:49671 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2

ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 d4051bde-9cdd-4910-b393-4aa85ec3c482 version: v1.0 ncalrpc: LRPC-5873c5fd23fe012de2 ncalrpc: OLE82B7564F6A2C7E6C267D110005C6 7df1ceae-de4e-4e6f-ab14-49636e7c2052 version: v1.0 ncalrpc: LRPC-4d5f2357a840057b52 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0368632 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-8f993f20149ea767a0 ncalrpc: OLE51CA94CD1CA3721686EC9EDE2420 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-8f993f20149ea767a0 ncalrpc: OLE51CA94CD1CA3721686EC9EDE2420 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-8f993f20149ea767a0 ncalrpc: OLE51CA94CD1CA3721686EC9EDE2420 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d14cefc4a3ed613bb1 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d14cefc4a3ed613bb1 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d14cefc4a3ed613bb1 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-d14cefc4a3ed613bb1 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-d14cefc4a3ed613bb1 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-cdf0457b30580c2023 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-b1d809ba4ebdd043bb ncalrpc: LRPC-b1d809ba4ebdd043bb ncalrpc: LRPC-b1d809ba4ebdd043bb d249bd56-4cc0-4fd3-8ce6-6fe050d590cb version: v0.0 ncalrpc: LRPC-a637f07b437800aac8 d8140e00-5c46-4ae6-80ac-2f9a76df224c version: v0.0 ncalrpc: LRPC-a637f07b437800aac8 a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-b466412e505be17779 ncalrpc: OLEA15CACC37D57E5F1405BF932486C 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncalrpc: 48fe1a25-3014-44ef-92a0-e062dd876e7b ncalrpc: LRPC-03b020254e74402acd ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ----------

Pattern Type

stix

Pattern
[ipv4-addr:value = '172.232.186.251']

Malware

Name
QakBot

Description
[QakBot](https://attack.mitre.org/software/S0650) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://attack.mitre.org/software/S0650) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://attack.mitre.org/software/S0654) and [Egregor](https://attack.mitre.org/software/S0554).(Citation: Trend Micro Qakbot December 2020)(Citation: Red Canary Qbot) (Citation: Kaspersky QakBot September 2021)(Citation: ATT QakBot April 2021)

Name
Pikabot

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition

to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

StixFile

Value
da81259f341b83842bf52325a22db28af0bc752e703a93f1027fa8d38d3495ff
0e81a36141d196401c46f6ce293a370e8f21c5e074db5442ff2ba6f223c435f5
69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320

IPv4-Addr

Value
57.128.164.11
57.128.83.129
172.232.162.198
139.99.222.29
57.128.108.132
54.37.79.82
57.128.109.221
172.232.186.251
172.232.164.77

External References

- https://otx.alienvault.com/pulse/65819f633436715278bf719e
- https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads?&web_view=true