Jun 12 2023

NETMANAGEIT

Intelligence Report

Zero Day Vulnerability in Barracuda Email Security Gateway Appliance (ESG) (CVE-2023-2868)

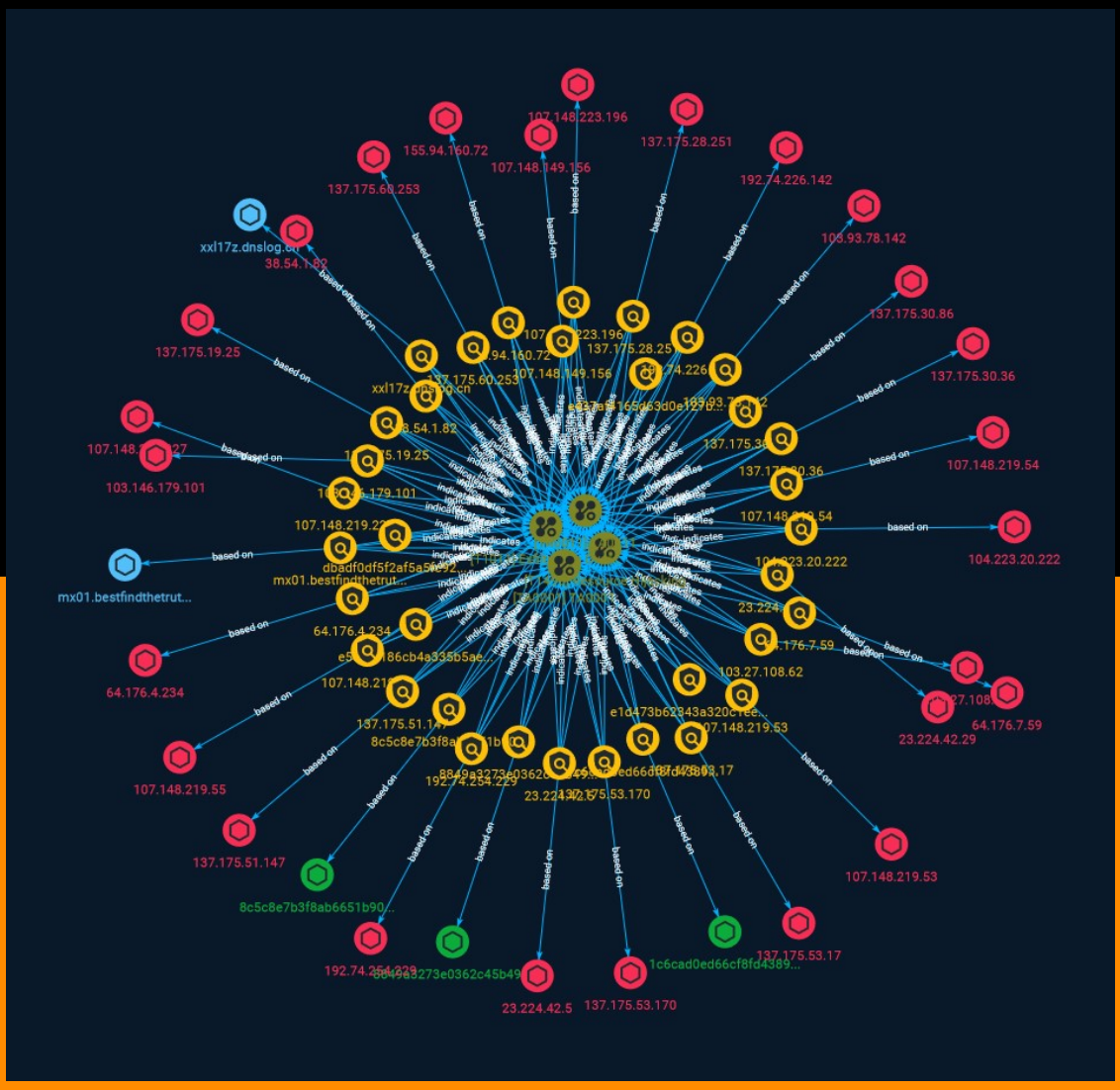

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The earliest identified evidence of exploitation of CVE-2023-2868 is currently October 2022. Barracuda also noted that malware was placed on a subset of vulnerable appliances to allow for persistence even if the vulnerability were patched. Additionally, evidence of data exfiltration was identified on a subset of impacted appliances. Because of this, on June 6, Barracuda updated its advisory, notifying customers to immediately replace ESG appliances regardless of patch version level. This issue is critical for every organization currently using the Barracuda Email Security Gateway Appliance.

Confidence

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

15 / 100

Attack-Pattern

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Name

TA0011

ID

TA0011

Name

TA0001

ID

TA0001

Indicator

Name

107.148.223.196

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDAZ25kl/65CXE2WXB2k5TnAxK4CUjQ1lOY/YqTHkO9511m tZrbEI0wMactZJ8eH4w7i/MF8zn4CZIlyYWMOJKi5obIysCtozkO35HeRnJRAMIufl4GftzlH+xY hx6/ygJXod01Uqs8w83xpRYnxpNPhEUlEMQMY0JIkGwF3yt1/iGMWNtyBP0nXeCoXQoWG6fY0IN+JHCly4pRnxPVmnKwYoY6DsPyqMuZDIndhbYMm/Aitz84lEk85pE96nUPiIHLJfdJH/NqFmL9g+WHe7CYxfShx/0m2idxpibyKw43DVSwy5GsOMf/RmAvyWql8i4hAgudyKK8rsw9W/sskVqN Fingerprint: 3e:a3:bf:39:6f:3c:20:22:72:f5:f8:69:45:35:60:b1 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.223.196']

Name

107.148.219.53

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDFxebF6X5cFj9IxO2p+nPYaIYXAkLj+wrolmfpXyGE0Q85e3wenMMgRHhAZ7v9f2pB/hHNjRvjj6QjtP8FyPC4i0u6EaFdCOXjUtmd10RgDUwRv8Dnf5U8eucTopjfXu2DzV1hxVLYDhFVcV+0eUJkmT8OeEfcJ/kwvVEyHu8XDEvBUGiT9dUxkWpgLdNi57rPOOHDt7PeZRatcn7h9PVZWVXqb+Qi6JPRgJpFSxflA+4nMxfsYzuZEDZyim3yP+PSKnH9KTzQhyirkwc679MEpSc5plCyg8A/g3l6Pv6a6ZXP8ifuyAUgARZ3xddUc+aeaA67BVk8g5jR0XuydzoX Fingerprint: f7:92:b6:b2:55:4d:20:e2:51:e3:9a:e6:7e:98:64:d8 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 ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Date: Mon, 22 May 2023 01:31:04 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/05/22 01:31:08 107.148.219.53:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.219.53']

Name

e588f4186cb4a335b5aec02f1cd9a8debf0e4c9b

Description

Looks for TAR archive with single quote/backtick as start of filename of enclosed files. CVE-2023-2868

Pattern Type

yara

Pattern

rule M_Hunting_Exploit_Archive_CVE_2023_2868 { meta: description = "Looks for TAR archive with single quote/backtick as start of filename of enclosed files. CVE-2023-2868" date_created = "2023-05-26" date_modified = "2023-05-26" md5 = "0d67f50a0bf7a3a017784146ac41ada0" version = "1.0" strings: $ustar = { 75 73 74 61 72 } $qb = "'`" condition: filesize < 1MB and $ustar at 257 and for any i in (0 .. #ustar) : ($qb at (@ustar[i] + 255)) }

Name

e437af4165d63d0e127bb7206172050efc255a68

Pattern Type

yara

Pattern

rule M_Hunting_Linux_Funchook { strings: $f = "funchook_" $s1 = "Enter funchook_create()" $s2 = "Leave funchook_create() => %p" $s3 = "Enter funchook_prepare(%p, %p, %p)" $s4 = "Leave funchook_prepare(..., [%p->%p],...) => %d" $s5 = "Enter funchook_install(%p, 0x%x)" $s6 = "Leave funchook_install() => %d" $s7 = "Enter funchook_uninstall(%p, 0x%x)" $s8 = "Leave funchook_uninstall() => %d" $s9 = "Enter funchook_destroy(%p)" $s10 = "Leave funchook_destroy() => %d" $s11 = "Could not modify already-installed funchook handle." $s12 = " change %s address from %p to %p" $s13 = " link_map addr=%p, name=%s" $s14 = " ELF type is neither ET_EXEC nor ET_DYN." $s15 = " not a valid ELF module %s." $s16 = "Failed to protect memory %p (size=%" $s17 = " protect memory %p (size=%" $s18 = "Failed to unprotect memory %p (size=%" $s19 = " unprotect memory %p (size=%" $s20 = "Failed to unprotect page %p (size=%" $s21 = " unprotect page %p (size=%" $s22 = "Failed to protect page %p (size=%" $s23 = " protect page %p (size=%" $s24 = "Failed to deallocate page %p (size=%" $s25 = " deallocate page %p (size=%" $s26 = " allocate page %p (size=%" $s27 = " try to allocate %p but %p (size=%" $s28 = " allocate page %p (size=%" $s29 = "Could not find a free region near %p" $s30 = " -- Use address %p or %p for function %p" condition: filesize < 15MB and uint32(0) == 0x464c457f and (#f > 5 or 4 of ($s*)) }

Name

8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347

Description

is__elf SHA256 of 177add288b289d43236d2dba33e65956

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347']

Name

107.148.219.227

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCvkO9T72A8U9/mdg/qseGeT8gCz0ybopCILrIyEHG+Vsv5 vPJiLiODnSE+eeYPNRczrcAbSeLqRl4wxu8m+pYcB1rtvXG4gGzFsufjU1wdidraJbVGbIC2bt6X BXoNCphvuzbeXcLebiy9OaJkzqHj38AsNCrpVNH2HrlxW+VjB909zCfI910SgZf8mfiW89AP623K Y17qUCeL0DVgqwru3cKvRIGaKrSFCQgfLJ7hmPWuyDqOSFnSPdSxGoA3JT9NfVpIxxhwkRectfW5 BNX5MP1lHQ42YqcwrHsy9IfhUZ1K0FFmOePLgV/MDamlO+bRbWmEbrfgYi148SHZDnG/ Fingerprint: 11:ad:43:0c:a6:93:3c:47:0f:14:eb:d6:a0:ed:c3:1a 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.219.227']

Name

137.175.30.86

Description

ISP: PEG TECH INC **OS:** Windows Server 2012 R2 ---------- Hostnames: ---------- Domains: ---------- Services: **135:** ``` Microsoft RPC

Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 137.175.30.86:49152 ncalrpc: WindowsShutdown ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\InitShutdown ncalrpc: WMsgKRpc059F80 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\InitShutdown ncalrpc: WMsgKRpc059F80 ncalrpc: WMsgKRpc05AB61 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-dd94b75e2914c03f2c ncacn_np: \\WIN-CLC0OFDKTMK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-4fca0674a7a0def326 ncalrpc: actkernel ncalrpc: umpo 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-dd94b75e2914c03f2c ncacn_np: \\WIN-CLC0OFDKTMK\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-4fca0674a7a0def326 ncalrpc: actkernel ncalrpc: umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-4fca0674a7a0def326 ncalrpc: actkernel ncalrpc: umpo ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: actkernel ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-a913f8c0469474b99e ncacn_ip_tcp: 137.175.30.86:49153 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: LRPC-a913f8c0469474b99e ncacn_ip_tcp: 137.175.30.86:49153 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\eventlog ncalrpc: eventlog abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-a913f8c0469474b99e ncacn_ip_tcp: 137.175.30.86:49153 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-a913f8c0469474b99e ncacn_ip_tcp: 137.175.30.86:49153 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\eventlog ncalrpc: eventlog f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 137.175.30.86:49153 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\eventlog ncalrpc: eventlog 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-6440f3834ea7ddcac6

ncacn_np: \\WIN-CLC0OFDKTMK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-6440f3834ea7ddcac6 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-6440f3834ea7ddcac6 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-6440f3834ea7ddcac6 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-6440f3834ea7ddcac6 ncacn_np: \\WIN-CLC0OFDKTMK\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: DeviceSetupManager ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\srvsvc ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 2e6035b2-e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-

CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 137.175.30.86:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: senssvc ncalrpc: OLEF4EFB6581F54838333676D0258EE ncalrpc: IUserProfile2 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-568a6d8a18fea38402 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\W32TIME_ALT ncalrpc: W32TIME_ALT ncalrpc: LRPC-f2bfcf0bc01fe30c5b ncalrpc: OLEFD7583B1F04A0DEE4501D5CF3AE4 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-f2bfcf0bc01fe30c5b ncalrpc: OLEFD7583B1F04A0DEE4501D5CF3AE4 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-f184fcd833917bdeb7 ncalrpc: LRPC-aa8056212d22d25068 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-f184fcd833917bdeb7 ncalrpc: LRPC-aa8056212d22d25068 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-f184fcd833917bdeb7 ncalrpc: LRPC-aa8056212d22d25068 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-aa8056212d22d25068 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-CLC0OFDKTMK\PIPE\wkssvc ncalrpc: LRPC-bedad1d59301dc4207 ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-bedad1d59301dc4207 ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-bedad1d59301dc4207 ncalrpc: DNSResolver 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote

Protocol provider: spoolsv.exe ncacn_ip_tcp: 137.175.30.86:49155 ncalrpc: LRPC-f406c37d7cd38ead55 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 137.175.30.86:49155 ncalrpc: LRPC-f406c37d7cd38ead55 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 137.175.30.86:49155 ncalrpc: LRPC-f406c37d7cd38ead55 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 137.175.30.86:49155 ncalrpc: LRPC-f406c37d7cd38ead55 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 137.175.30.86:49155 ncalrpc: LRPC-f406c37d7cd38ead55 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 137.175.30.86:49157 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 137.175.30.86:49158 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 137.175.30.86:49159 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-CLC0OFDKTMK\pipe\lsass b2507c30-b126-494a-92ac-ee32b6eeb039 version: v1.0 ncalrpc: LRPC-8375b79a47a09df533 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-6dd6675c057e606329 ncalrpc: LRPC-6dd6675c057e606329 ncalrpc: LRPC-6dd6675c057e606329 ``` ---------- **137:** ``` NetBIOS Response: MAC Address: 00:16:3C:A2:A6:21 ``` ---------- **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-CLC0OFDKTMK NetBIOS Domain Name: WIN-CLC0OFDKTMK NetBIOS Computer Name: WIN-CLC0OFDKTMK DNS Domain Name: WIN-CLC0OFDKTMK FQDN: WIN-CLC0OFDKTMK am Windows Server 2012R2 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 25 May 2023 22:06:37 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLC0OFDKTMK NetBIOS Domain Name: WIN-CLC0OFDKTMK NetBIOS Computer Name: WIN-CLC0OFDKTMK DNS Domain Name: WIN-CLC0OFDKTMK FQDN: WIN-CLC0OFDKTMK ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.30.86']

Name

8c5c8e7b3f8ab6651b906356535bf45992d6984d8ed8bd600a1a056a00e5afcb

Description

SHA256 of 0d67f50a0bf7a3a017784146ac41ada0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c5c8e7b3f8ab6651b906356535bf45992d6984d8ed8bd600a1a056a00e5afcb']

Name

155.94.160.72

Description

ISP: QuadraNet Enterprises LLC **OS:** Ubuntu ---------- Hostnames: - 155.94.160.72.static.greencloudvps.com ---------- Domains: - greencloudvps.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDxdTTqTzFYhlfCGbEFxaSZzIdEqg6BErSONgoeOZd0Ngkn KEVF7jU7W6WssO7EG8mXwqE5MYPLx50ltB3d1RZ1biuBzTfCy8dqJZyiDVQb/4dPXyQohl0Z50OF 5mGRcVgo6W1y5engiBSQID3ZFGmpPmwWDOoIPKqZaRRt5kxb+OX/ 7cQ8DwzE84CjFe7VMO42AIz8 Q/ QAIuH96xmic52cAgk9EnzOfysv6FMmctrHdJDZdZCpaUT8KpMV9esuKEdEJdyCpom3OJcg2Szi 7LKuMLl4OB025ean96wV5lEts8m4VQdD7qeY+k7NLyqJT96vDXQOZFqWdeO0bXbJVWTL Fingerprint: 14:c4:e9:f1:a4:f9:e6:61:7e:fb:29:20:43:88:4d:c5 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 = '155.94.160.72']

Name

103.27.108.62

Description

ISP: TOPWAY GLOBAL LIMITED **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDRqJ47stVb8UFoYfb3nkI/59wkhkr8jKFFEObNiCdyCW1oTe1Zhv91MXnxDnroerqv5tUoPYL9IJ+aeBYZzLCKMmgkBuEDxUDbKbQUOpJ7PwNUC1/l8b0hKDjmpP5h1aHWkGjq5HbHcckeQ2e0usMqrm8PxEYTXcMYK8vefkTp8l39zAP/u5TvsLBm4f87wNmjuYteMEHmOqX7uH4OeNADdt7vux+9ptXFgrG/r493SYbTnjKfMEMU5EJWpUotWGMuxd3tiyHuIqDj7QwKl2pK9lMTfBU+r1BR6GJUaSEbTDaNwcvhtvV6UaE743Dedu0o0No49FHwolUYMRYfJkzB Fingerprint: 4e:a8:89:ac:fc:ac:9d:5c:e8:cb:23:7a:4f:24:5f:79 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 diffie-hellman-group14-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 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 ``` ---------- **18245:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.27.108.62']

Name

137.175.19.25

Description

CC=US ASN=AS54600 PEGTECHINC

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.19.25']

Name

192.74.226.142

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: - xxl.fewrtewrzh.buzz ---------- Domains: - fewrtewrzh.buzz ---------- Services: **443:** ``` HTTP/1.1 404 Not Found Date: Fri, 09 Jun 2023

02:49:46 GMT Content-Length: 0 ``` HEARTBLEED: 2023/06/09 02:49:56 192.74.226.142:443 - SAFE ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.74.226.142']

Name

137.175.53.170

Description

ISP: PEG TECH INC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCh8hVAv+P9S5mPF+gI3kmuN0E4AF/Bc6jnN3cKrADXWZdn sDRdolP6gGq3ZsUIAHbpf/pRObwHxRR3LTkTIvem/kWgE3IbHZRY69ZnEWhCDLSRCDVqk9hSmJkC eGKSmNP1gIwghJAc8nkXKLza5CC8Q0nLHDHyWI17EeZ9AClWHoDAatYS/wv71z+5QJ4naNIa7FJF Ur/vrdpbXqsYNe8nOUcyCDqIxrSHE2M1ZSsR4jgzbG2Lxhprjd+DRLn8MZfA3gRkN7Seai8tHnD4 enRYa4hAybolWMK55WxMV/w/lgNNZ/4TqHobOs8Xn7SK7YPUSne7qEnr3hp/mX5KD9tb Fingerprint: 7f:7c:fe:2d:6c:28:64:36:2e:86:ca:ea:69:d7:43:68 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 ``` ------------------

Pattern Type
stix
Pattern
[ipv4-addr:value = '137.175.53.170']
Name
103.146.179.101
Description
CC=HK ASN=AS136933 Gigabitbank Global
Pattern Type
stix
Pattern
[ipv4-addr:value = '103.146.179.101']
Name
23.224.42.29
Description
ISP: CNSERVERS LLC **OS:** None ---------- Hostnames: - caomm1.com ---------- Domains: - caomm1.com ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 02:11. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421 Unable to read the indexed puredb file (or

old format detected) - Try pure-pw mkdb 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV SPSV ESTP 211 End. ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 31 May 2023 12:16:39 GMT Content-Type: text/html Content-Length: 138 Last-Modified: Fri, 24 Mar 2023 08:07:56 GMT Connection: keep-alive ETag: "641d5a5c-8a" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Sat, 10 Jun 2023 09:54:45 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Strict-Transport-Security: max-age=31536000 ``` HEARTBLEED: 2023/06/10 09:55:26 23.224.42.29:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.224.42.29']

Name

107.148.219.55

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDDOh/veuNTa6erPE/B7cq4pgsMcDTcXvgcoj1abDaZulOL d4DbxuBsgsanfQ1arxno+1lvaw5KGd5iT6z6/xF9sJ8LRSl3h36SB/fHlM+gI3WPgFMPblE/hx6m nMzwUhXGfnXCk7igIQvUCl9aTgyJiCke1xx8JUzziqqfa/6TB69RTGe7jy7FLN8rxPfLk070BIZF 9XC+V3p7Jw77sxFY59qI20k3a6NHYxscdulYzRONkc8q8n2g9y1qj55dvRBTeoq6Ri5BLAeb3bmR / UE+aRfbTz1S05Wz4lcITyDnhC1II7Xg6+7I/vaXTDJ+e/pXqBA/3/wtBpVJnh596NMH Fingerprint: 6e:64:48:38:b1:59:87:31:6c:7f:69:fb:c9:42:9c:85 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.219.55']

Name

107.148.149.156

Description

ISP: PEG TECH INC **OS:** Windows (Build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **137:** ``` NetBIOS Response: MAC Address: 00:16:3C:08:9F:D7 Names: WIN-CLC0OFDKTMK <0x0> ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 11 Jun 2023 00:34:16 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLC0OFDKTMK NetBIOS Domain Name: WIN-CLC0OFDKTMK NetBIOS Computer Name: WIN-CLC0OFDKTMK DNS Domain Name: WIN-CLC0OFDKTMK FQDN: WIN-CLC0OFDKTMK ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.149.156']

Name

137.175.53.17

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDZAKx5AsonUCkthKbw6/W+rFW+S/eIXhXMwTeWfb13fC9A5JrAPnsJ2m1k11jDA7FFcBjMoCuJ6CsTYJW5ZISWHQnwVxd1/Mib5MgFYDVzSJlO2DTNJrhTyrIht47DdibRM8azISUuZUK4h0b3EUx6v+gD8aSfI7YMDG3ormzGkCRCoLySUYcz61bX0y1+tPDnzWZyR541C3A3tGvQMxMUqssYird7up7WnTpg9ubXbZ+vgQtdKkZ9jph04sLLf+OOpuMtSyTy5g/PTqrEYN8q9YqgE6eKP1Nwywoo+utGB0NuSLWBpuLDaIbIRfHsO8PO8UPLhgzFsXdaXpKBg/Ar Fingerprint: f3:07:88:05:2a:34:e8:e9:52:2f:fa:2c:54:6b:8a:2b 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.53.17']

Name

mx01.bestfindthetruth.com

Pattern Type

stix

Pattern

[hostname:value = 'mx01.bestfindthetruth.com']

Name

137.175.30.36

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCt1yRPDMNUGi1ngk6NeM8Z7c+oVB6709c5UP1Tu3KBUABAdDA6xlj01mMCU+NIUFTcw77Q4hE13oF8xX4aHbXw60osM2Zs7gTGyqs00mz9tRfeArM613w3gdUuIfdVBkMofKb1ZqrD1hyx9UPbHL83WqqxPowa0Lc4Zz7FwWdHCTjGmCEeCH+YN/Zx8FG2biRYxEYbkglxb8pEJiAV8e4ojHnoFjumgUKFP3nTXQgYYHKsxxY64HiE4tERG6xVmiP9ngoc6nMEpSUbfSGkzpQOp+WK03YVXqz2vA8VtOa/+/A1cSonf7NEACOu5i56fArvUIPQkMmAbBI7ZlKCmOrv Fingerprint: 1c:ea:8d:0c:ff:fb:aa:f4:c4:fd:b5:28:d2:18:d5:0a 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.30.36']

Name

137.175.51.147

Description

ISP: PEG TECH INC **OS:** None ------------------------- Hostnames: - bing2.nqfgx.com ------------------------- Domains: - nqfgx.com ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC3CsvLufYu3Qezd5Rcp+6BZoBs3sItQyi6aNiO57G7hu0B eFCMWAxNZYwpdWLGVnBoV4msuCZQhIqvxzMqFbS9O7C2utlv9eIkihyHQsXkGItgspUTh/hpzQSq fzncXlAOvvWEW2AcE+chmz/CaW8+SW8t/ctGH8sjWI1LbgoRBUizhdWCDnknZf/4D9rtYLATZAb2 1mifsS4cSS4vFlZ/cIGzhstdWrH/xvz7pEc+pwhYvPkqFY7MknTZ/YJ6/Nd+HWQiPzloUU7e5H7Q 2f0E/Yclr0si2mXoEHIPEhBsG64XsRZEKSA989FebZm2ysr1Agt4ERfX8ZCNNaV5kXu5 Fingerprint: dc:47:4f:15:96:84:5d:40:7c:aa:8e:12:7d:02:9a:68 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.51.147']

Name
137.175.60.253
Description
CC=US ASN=AS54600 PEGTECHINC
Pattern Type
stix
Pattern
[ipv4-addr:value = '137.175.60.253']
Name
64.176.7.59
Description
ISP: The Constant Company, LLC **OS:** Ubuntu ---------- Hostnames: - 64.176.7.59.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu7.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEA99ARQRZcwt+9yTKOdQrDcynjKwLvQvyYwVh9Pdkmc5rmew1jNmNNsnB67Q++hHwS1lBAtEOZO2kbQ4Sg4SbI= Fingerprint: 94:71:06:98:b3:2b:76:e2:0e:12:15:29:f0:81:22:92 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.176.7.59']

Name

64.176.4.234

Description

CC=CL ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.176.4.234']

Name

103.93.78.142

Description

ISP: EDGENAP LTD **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key:

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFqnXEoA0YujDrA853fsYK2O V+4aE/4iDmlD6NsqB9Vc5CHukr99zztvlC1BOvPB3qolJaA2oPHBLWS6+7b56aA= Fingerprint: 98:20:ad:8d:58:e8:67:5c:c0:f7:e8:e7:a7:95:eb:31 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.93.78.142']

Name

1c6cad0ed66cf8fd438974e1eac0bc6dd9119f84892930cb71cb56a5e985f0a4

Description

is__elf SHA256 of 827d507aa3bde0ef903ca5dec60cdec8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c6cad0ed66cf8fd438974e1eac0bc6dd9119f84892930cb71cb56a5e985f0a4']

Name

38.54.1.82

Description

ISP: Kaopu Cloud HK Limited **OS:** Ubuntu ---------- Hostnames: - sgir01.ddns.net ---------- Domains: - ddns.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDBmsVc/iY9dpm0Kk2l7RE1T2aVxFKj0kX1xYtq1nzQb7XbPfCKb1GbO/l2Uc63JZae1deIQiEPLrJs20K81DuOEYXuL9gidF8RUizm9RzyX03si3V8Ixv5tlSwmb+f2KZpB/NL/RV2PWjNvCkoIhZFUAGRDPiMU6/XMyQbUjBkAcO3TPEdZa2PQUZwYbpujMGMdYSH vKOlyq9qg9igL+6gGIdOfcjjoB5Vvu7vCWVQRi/FyA5LLdLH0CxdBlEGOJSHyu2g62V8b1LiSOL6MppU8bfLi67f9jkue+6EHPZj61m9kMWhvpbyk7EFfr6h+D1v2G3uSEXoYh21nkeMZRlPZlzrGomHkJKvb6LbmDelS1Ri5mpLV62G005QvMzA4TopWBJC+mZw1oROnxpSNafscm4JWrO1KRuLbF3d+eJ0xkJCBU/oqFIcBMYV9bFA/KXC5EBPI08vDe6kzoxfHv55RrJkMzvGv0HSp2Un8gAs2k2KQv4ugwUk+eBaYYRD6uM= Fingerprint: 0a:f7:12:e1:fe:8e:6c:7f:b0:70:80:04:14:c3:5a:8e 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 ``` ---------- **2087:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Thu, 18 May 2023 08:23:43 GMT Content-Type: text/html Content-Length: 166 Connection: close

400 Bad Request

nginx

``` ------------------ **8443:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Tue, 16 May 2023 04:29:10 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 12 Connection: keep-alive Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff ``` HEARTBLEED: 2023/05/16 04:29:23 38.54.1.82:8443 - SAFE ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.54.1.82']

Name

104.223.20.222

Description

CC=US ASN=AS8100 ASN-QUADRANET-GLOBAL

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.223.20.222']

Name
```

192.74.254.229

Description

CC=US ASN=AS54600 PEGTECHINC

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.74.254.229']

Name

137.175.28.251

Description

ISP: PEG TECH INC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDLd+b0nzaEkB9cRMAdtfsvx+rOR3iNtxQesl7J5QbmeqM7aBcPxDU485h4YB1dTFgtlGlUaNOKlRnkwL0cpqLdFkl9Q4xPwLgWt/dc1Mc0PbKh2kXWFUItvFgjQrQ4oEU7jCNygFV6HPpa0uflsWZ0h47EXN+m1mMrVwdZ2WjPjTkJwFS3pk5GkmwUZtDY3UkrqbxRL7SCPiMRKZxUm9VoC44z5iDuwbmNdRQJFxLqm4wVfWfHGQ1xhEzjTUOSuYD1tuNoIzqkrotCKrUA9JguWM92xmCv/buCzdQKc+MGnWxSMM6ipk/bTPqIEgLqGJkhlmFkZCNi1XpFpYTRrNkL Fingerprint: 07:5c:f8:3d:00:b4:ea:cd:42:b7:ff:31:57:a6:6d:59 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.175.28.251']

Name

e1d473b62343a320c1eeee6853b90f9a63fe72c0

Pattern Type

yara

Pattern

rule M_Hunting_Linux_SALTWATER_2 { strings: $c1 = "TunnelArgs" $c2 = "DownloadChannel" $c3 = "UploadChannel" $c4 = "ProxyChannel" $c5 = "ShellChannel" $c6 = "MyWriteAll" $c7 = "MyReadAll" $c8 = "Connected2Vps" $c9 = "CheckRemoteIp" $c10 = "GetFileSize" $s1 = "[-] error: popen failed" $s2 = "/home/product/code/config/ssl_engine_cert.pem" $s3 = "libbindshell.so" condition: filesize < 15MB and uint32(0) == 0x464c457f and (2 of ($s*) or 4 of ($c*)) }

Name

dbadf0df5f2af5a5fc921c5d76d1c9c10d884621

Pattern Type

yara

Pattern

rule M_Hunting_Linux_SALTWATER_1 { strings: $s1 = { 71 75 69 74 0D 0A 00 00 00 33 8C 25 3D 9C 17 70 08 F9 0C 1A 41 71 55 36 1A 5C 4B 8D 29 7E 0D 78 } $s2 = { 00 8B D5 AD 93 B7 54 D5 00 33 8C 25 3D 9C 17 70 08 F9 0C 1A 41 71 55 36 1A 5C 4B 8D 29 7E 0D 78 } condition: filesize < 15MB and uint32(0) == 0x464c457f and any of them }

Name

107.148.219.54

Description

CC=US ASN=AS54600 PEGTECHINC

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.148.219.54']

Name

23.224.42.5

Description

CC=US ASN=AS40065 CNSERVERS

Pattern Type

stix

Pattern
[ipv4-addr:value = '23.224.42.5']
Name
xxl17z.dnslog.cn
Pattern Type
stix
Pattern
[hostname:value = 'xxl17z.dnslog.cn']

StixFile

Value
8849a3273e0362c45b4928375d196714224ec22cb1d2df5d029bf57349860347
1c6cad0ed66cf8fd438974e1eac0bc6dd9119f84892930cb71cb56a5e985f0a4
8c5c8e7b3f8ab6651b906356535bf45992d6984d8ed8bd600a1a056a00e5afcb

Hostname

Value
mx01.bestfindthetruth.com
xxl17z.dnslog.cn

IPv4-Addr

Value
107.148.223.196
137.175.53.17
107.148.219.227
103.93.78.142
107.148.219.53
137.175.30.86
107.148.219.55
192.74.226.142
137.175.19.25
23.224.42.29
38.54.1.82
137.175.53.170
107.148.149.156

137.175.30.36

107.148.219.54

64.176.4.234

192.74.254.229

23.224.42.5

137.175.51.147

137.175.28.251

103.146.179.101

103.27.108.62

104.223.20.222

155.94.160.72

64.176.7.59

137.175.60.253

External References

- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-action-response-zero-day-vulnerability-in-barracuda-email-security-gateway-appliance-esg-cve-2023-2868/
- https://otx.alienvault.com/pulse/648783b6e843ce3fe69a281a