Dec 14 2023

NETMANAGEIT

Intelligence Report

Routers Roasting on an Open Firewall: the KV-botnet Investigation

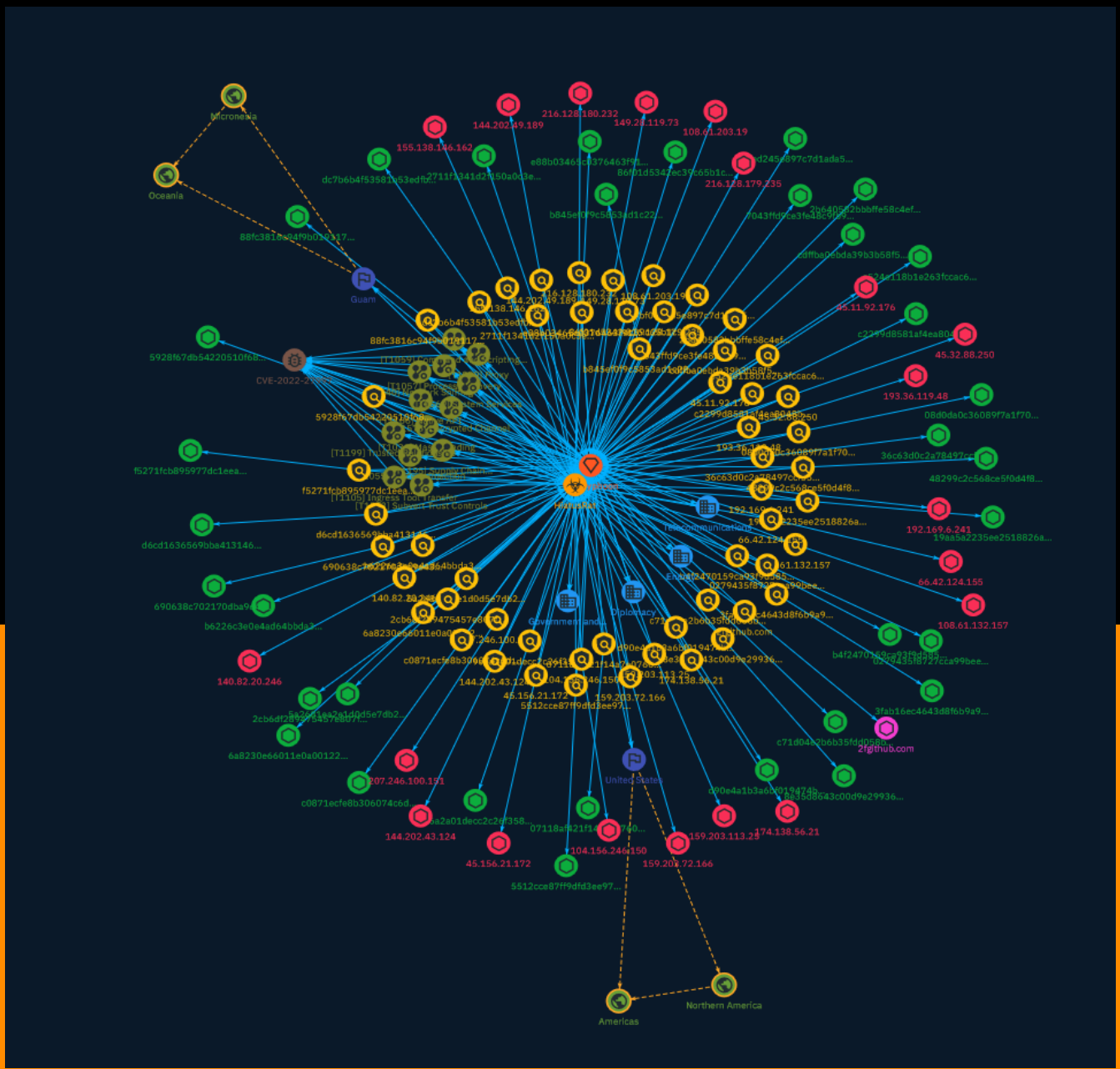

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A report on the “KV-botnet” - a network compromised by a state-sponsored actor based in China - reveals details of a multi-million dollar cyber-attack.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

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

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

Name

Network Sniffing

ID

T1040

Description

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for

subsequent Lateral Movement and/or Defense Evasion activities. In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring) On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture_embedded_packet_on_software)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well

as carrying out tasks and requests during routine operations. Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may use assembly to directly or in-directly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.(Citation: Redops Syscalls) Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001).

Name

System Services

ID

T1569

Description

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or Modify System Process](https://attack.mitre.org/techniques/T1543)), but adversaries can also abuse services for one-time or temporary execution.

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Supply Chain Compromise

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact

any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Trusted Relationship

ID

T1199

Description

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used. (Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

Sector

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name

108.61.132.157

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 108.61.132.157.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDNhXShTbArTWKVpbJQdLGVenxXoYlh9yk4erI76jlQUwS3 jRr98SEw1qM2xANZ8AmujbpfE2D/7KMSGh+aM04QJbSZxEcAIa0olUUap/fhrKSCsEqqgb85GC6n lQLFacASQqkgMcLrEYcaL5Mm9nLG7hQaKj/lXcLiBSamSs2CdwuYHDW3/VqgyWpxTqjCPH+bYpNU xLTp2wOmnGSh7DWmkghQTLOL5Et8nUyqggXIeGd9PLW1LYeEwgYq4mUmnNQmiae4Vg1Isj86jMGg /PHe3tHqgC5KPD3AQ8l4gqgN16vR66BfEAn9bS+8IiPqKUCQ33Tg21CEbUti4joh5K7j Fingerprint: 4e:56:85:10:66:f4:34:38:f6:0e:de:99:0d:73:0e:bd 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/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Sun, 19 Nov 2023 18:50:16 GMT Content-Type: text/html Content-Length: 169 Connection: keep-

alive Location: http://www.google.com/ ``` HEARTBLEED: 2023/11/19 18:50:30 108.61.132.157:443 - ERROR: write tcp 108.61.132.157:443: broken pipe ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '108.61.132.157']

Name

193.36.119.48

Description

CC=TW ASN=AS206804 EstNOC OY

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.36.119.48']

Name

88fc3816c94f9b0191179f4e933843ee4cfdbcb392968605491a387b1235ec12

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88fc3816c94f9b0191179f4e933843ee4cfdbcb392968605491a387b1235ec12']

Name

8e35d8643c00d9e2993625b03366a7cd1bd36e6a60bc0c6039a509fccf9df150

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e35d8643c00d9e2993625b03366a7cd1bd36e6a60bc0c6039a509fccf9df150']

Name

144.202.43.124

Description

CC=US ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.202.43.124']

Name

0279435f8727cca99bee575d157187787174d39f6872c2067de23afc681fe586

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0279435f8727cca99bee575d157187787174d39f6872c2067de23afc681fe586']

Name

140.82.20.246

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 140.82.20.246.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **21:** ``` 220 (vsFTPd 3.0.5) 530 Login incorrect. 530 Please login with USER and PASS. 211-Features: EPRT EPSV MDTM PASV REST STREAM SIZE TVFS 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCs8UA7kQ+NpspDqges3Hb/2CxbViR/5/ tiHKqnmTCGdKw7 DXojn/ 5U65Psjmhw6+tOYMHesN7s3rQXyQi7qLJJIJErLA0s4ARWzOrBTkTK3KXCha12zRbkiZZc + +xIETTbCDRLFQwuh9iQVniRIykB7iFQuGh0wpWB3RwUMiJhtHNaBOB+qqA8RgR1Ei/Ldv9fPsCG sIhpl9PrJxOwEKnHTXHLhvE7plmGUZHcG0OvTwD7SxDBZmSAWg03070M4fHp0q9L/ HTnVgIOjnUn nw882Ogg7KVlo2cmik5kNjNl6V/DCWXQb/xv1yN8lYhJR8qQ2bQ2wZ6m/ HqInAC1Fwf+Hf9ygeyg 6SM34PPhfKZdbdOqwdPLh1GBvaRZSntDISMt/ogs9Z/ 3Aelfo+FztoqGw3N6gO0dc1veiLljMTJH eqlbEv84KQ/dr3K39IwZkp3P4/82w22JB1R5hYywPRx31/ hsw5IT5Oq/NnKDk91kkGY375f8LehW 8mbL8LpUGXc= ``` Fingerprint: f2:8e:f0:1d: 95:30:f0:26:df:a3:92:f2:4f:da:cb:2e 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 ``` ---------- **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: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 29 Nov 2023 11:05:56 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '140.82.20.246']

Name

144.202.49.189

Description

Cobalt Strike botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.202.49.189']

Name

45.11.92.176

Description

ISP: CGI GLOBAL LIMITED **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **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 ``` ---------- **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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.11.92.176']

Name

159.203.72.166

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.0 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCLv9La5sRCpMlC8ePB/zcpfxTzHVCNicqF4nuoXs0+RBCLOG7ikJ3Ksd74j+8kKNBC9VDqf+1CiBm15RWCTuog= Fingerprint: 83:24:1c:55:21:0d:3b:07:83:f6:f8:ce:56:13:dd:0f 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 Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 Encryption Algorithms: aes256-gcm@openssh.com chacha20-

poly1305@openssh.com aes256-ctr MAC Algorithms: hmac-sha2-256-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.203.72.166']

Name

7043ffd9ce3fe48c9fb948ae958a2e9966d29afe380d6b61d5efb826b70334f5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7043ffd9ce3fe48c9fb948ae958a2e9966d29afe380d6b61d5efb826b70334f5']

Name

36c63d0c2a78497ccf555e84f0233a514943faeff38281d99d00baf5df23f184

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36c63d0c2a78497ccf555e84f0233a514943faeff38281d99d00baf5df23f184']

Name

f5271fcb895977dc1eead64415e525323cd412e3f2625aee2fafbb5674beea28

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5271fcb895977dc1eead64415e525323cd412e3f2625aee2fafbb5674beea28']

Name

c2299d8581af4ea8048bbf2bffd45c6ddca323c9c718c172355cc0df006ea6ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2299d8581af4ea8048bbf2bffd45c6ddca323c9c718c172355cc0df006ea6ca']

Name

d6cd1636569bba4131462bb8f45be1daa9a203aa343b6f2fd48a4847acfc29fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6cd1636569bba4131462bb8f45be1daa9a203aa343b6f2fd48a4847acfc29fa']

Name

e88b03465c0376463f912a5601a518cc697330dc3e5857068f3de0c434b52c9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e88b03465c0376463f912a5601a518cc697330dc3e5857068f3de0c434b52c9a']

Name

19aa5a2235ee2518826a48363cb603060ee73ddccdf7d93bf197f97d7402aa37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19aa5a2235ee2518826a48363cb603060ee73ddccdf7d93bf197f97d7402aa37']

Name

6a8230e66011e0a0012273f7d12110c23b1e33bd7232dc67a836662a3d1075c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a8230e66011e0a0012273f7d12110c23b1e33bd7232dc67a836662a3d1075c7']

Name

108.61.203.19

Description

CC=US ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '108.61.203.19']

Name

5a2681ea2e1d0d5e7db2a2499d2e6e27b2689830c638d5ee28c2eef9867ececf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a2681ea2e1d0d5e7db2a2499d2e6e27b2689830c638d5ee28c2eef9867ececf']

Name

5928f67db54220510f6863c0edc0343fdb68f7c7070496a3f49f99b3b545daf9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5928f67db54220510f6863c0edc0343fdb68f7c7070496a3f49f99b3b545daf9']

Name

174.138.56.21

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDUt3a/VT8q5bHezHzVEmFX1lsmikJDzdERUlUmSzMgrLBH V7GeOLBO1rmZioc+mh5aceyTuRT0XqHWP+N90oY9jSkraAPgQHwtjOlugAglEmP9ud+UqsInRdZl VwGET/ylk3EJ2CqHfZGy4e0Nkpg7REdlEab51lsVqXatqXLSo5WATcLkrEiWQrPFxy/DUA4igj6/ 8HpDumwrF/In7p8/ JibAKDsH9VfG0UsavODtJKDnRnHTIMeFAXbwhNVQhGAJOeyOx0J9NLITwecD UWh4TuV5g0wIzQopjwkYrk8LR7JI0+8dlvPfAu2tvDE82aaeDE482UbN/8t4/VYN0BwX Fingerprint: 48:7d:01:ad:fe:0a:83:f5:bc:17:cc:6a:cc:33:07:6b 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/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Fri, 01 Dec 2023 01:39:12 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: http://www.google.com/ ``` HEARTBLEED: 2023/12/01 01:39:20 174.138.56.21:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '174.138.56.21']

Name

07118af421f14a7e07601639f44a72f6782757ae74d2afffdb531b8209697e7f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07118af421f14a7e07601639f44a72f6782757ae74d2afffdb531b8209697e7f']

Name

cdffba0ebda39b3b58f59815be3829ca9c1cde957b46a6ad5ce4b31e405455bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cdffba0ebda39b3b58f59815be3829ca9c1cde957b46a6ad5ce4b31e405455bb']

Name

c71d04e2b6b35fdd058b4be5cf9ea3478697950378d4ee3c7fe0bf87e1e3730f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c71d04e2b6b35fdd058b4be5cf9ea3478697950378d4ee3c7fe0bf87e1e3730f']

Name

86f01d5342ec39c65b1cff716f19c334cec26a82b87492d783d5e8f4ff9cb63a

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86f01d5342ec39c65b1cff716f19c334cec26a82b87492d783d5e8f4ff9cb63a']

Name

207.246.100.151

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 207.246.100.151.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **443:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.246.100.151']

Name

2cb6df289475457e807fc202a2b4688b2e23a88c94a8431981780caf8b76acf7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2cb6df289475457e807fc202a2b4688b2e23a88c94a8431981780caf8b76acf7']

Name

149.28.119.73

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 149.28.119.73.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGMVGsdMMciYvRWUdkhgEgdI Lk1yQkNkzf40gGRqL7wDnKTtpb1mhPo+Xqahhk18lv+GM8AJLlCt//DPo2D9gqI= Fingerprint: 9c:07:82:81:59:4a:46:4c:99:97:3a:60:1d:4c:bd:08 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 ``` ---------- **443:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Thu, 16 Nov 2023 18:04:14 GMT Content-Length: 12 ``` HEARTBLEED: 2023/11/16 18:04:40 149.28.119.73:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.28.119.73']

Name

b4f2470159ca93f9d585ae2df1da972f6d14a0c418ebc202a324b9be5c877b61

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4f2470159ca93f9d585ae2df1da972f6d14a0c418ebc202a324b9be5c877b61']

Name

45.156.21.172

Description

CC=HK ASN=AS56971 Cgi Global Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.156.21.172']

Name

bf0ed245e897c7d1ada511db2939e8f3a879a96543f2651d5631339d5419bb75

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf0ed245e897c7d1ada511db2939e8f3a879a96543f2651d5631339d5419bb75']

Name

3fab16ec4643d8f6b9a99d85427322f7fb40e9ea3cd4de8318c6a52e29869d5a

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3fab16ec4643d8f6b9a99d85427322f7fb40e9ea3cd4de8318c6a52e29869d5a']

Name

b6226c3e0e4ad64bbda3e6a79eb464c7050faa25d1f5332dcac014d2e79dd87f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6226c3e0e4ad64bbda3e6a79eb464c7050faa25d1f5332dcac014d2e79dd87f']

Name

08d0da0c36089f7a1f700b989f2f7825c5ba2549a20735d0bd1e64ca9c4885bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '08d0da0c36089f7a1f700b989f2f7825c5ba2549a20735d0bd1e64ca9c4885bc']

Name

9e6a2a01decc2c26f3586a119b6fd3a886c4cf9c76aa452339d164fda40c63e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e6a2a01decc2c26f3586a119b6fd3a886c4cf9c76aa452339d164fda40c63e4']

Name

216.128.180.232

Description

CC=CA ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.128.180.232']

Name

45.32.88.250

Description

ISP: The Constant Company, LLC **OS:** Linux ---------- Hostnames: - 45.32.88.250.vultrusercontent.com - 1101.xyjlsp.org ---------- Domains: - vultrusercontent.com - xyjlsp.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC48FzJb1i4xpdzFy7aqRj1xjsHs3k11hIVmUsLMiqkdZ5A 4bUqKMaymdsgtUSXfHlwNVbBGtv+DbmjptdF9McsqHRV746XrUADhLONeVwFIz84mwydli66KA 9H 1s4T2KysAc3f/p/GnQFq+FJuXJIXgTWs4NKcBf59hSqOJyN+Sh0JY5ViMy+sH+ya0SHMSspylPE1 UFRxzZDK+3h++gjeAVv37hAa6GMVt3YNSdfgAHTZNGxXVUHMo+WAwNmRAt22/ gZP+WCcv4oX4aPc VjJppaO08CxLT+YBr9NmbACKnDTYhYHmd8X+xU4bQqYq/ FjPicLEp1EG92vfud6WVaGT Fingerprint: b4:cd:63:36:16:60:01:53:ce:10:d6:6d:04:5f:12:5b 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: 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 Server: Caddy Date: Fri, 08 Dec 2023 15:55:26 GMT Content-Length: 0 ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: Caddy Date: Sat, 02 Dec 2023 06:54:38 GMT Content-Length: 0 ``` HEARTBLEED: 2023/12/02 06:54:58 45.32.88.250:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.32.88.250']

Name

690638c702170dba9e43b0096944c4e7540b827218afbfaebc902143cda4f2a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '690638c702170dba9e43b0096944c4e7540b827218afbfaebc902143cda4f2a7']

Name

192.169.6.241

Description

ISP: QuadraNet Enterprises LLC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCdEpioiK43nStZdSwqb9kGcsa+puNkJjPFdTCjL1LlP2mHi7/lIhWzqPBn+hJ5aNNETX9JPkpo36XGzBd0Guwn6Ol1xYjsAVP6c9apFdQrDXgpYocC0xd3eK21+Xk47B5tp9u3H10BscmutGXIxHNu/Gy57SkPwbFCqM5IoJWyOiFnm5znNpsY2+wVFI7ygKy7fJP33Z0bNygHP9N+tkWNaCZDm8D+1wXkQzk5V5b1nD7nyIJymXeO1lPj0UVWo8SssAiPqa6gnVvz3UqQ nkeIwbmqOZ+KWmAXYS0B8XbFmtR1CGMrGUR+bNMA1/oFa6bmI+gMuuBNC0nTbnPH1s4J Fingerprint: c2:94:40:86:85:2b:62:c9:9b:f8:43:da:93:42:a6:75 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 = '192.169.6.241']

Name

5512cce87ff9dfd3ee9721eb29302d1700199ed7d625e09f9f779772ec06bdb0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5512cce87ff9dfd3ee9721eb29302d1700199ed7d625e09f9f779772ec06bdb0']

Name

dc7b6b4f53581b53edfbbc83d825cfa0450b2039f126cd62e8529189bb156033

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dc7b6b4f53581b53edfbbc83d825cfa0450b2039f126cd62e8529189bb156033']

Name

66.42.124.155

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2022 (build 10.0.20348) ---------- Hostnames: - 66.42.124.155.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- 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: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 03 Dec 2023 06:17:51 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.42.124.155']

Name

104.156.246.150

Description

CC=US ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.156.246.150']

Name

b845ef0f9c5853ad1c226ac0ae7bb91159d5bb132185c1bfd171696b755a9164

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b845ef0f9c5853ad1c226ac0ae7bb91159d5bb132185c1bfd171696b755a9164']

Name

159.203.113.25

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDEiel+htjKq3wy5MMb/3Loe87RhScnNm3ZXVpPUIVGrPCf

iGPHF10YgQmb4wr7xp+JvNrYa2C2UUMA369PdaH6In2S8pyWLFbuxMgSbhwp3wqAxapAbZ9sU Pxs glD4ozGOJLn9Tn53aiRv2TcTsS61NcEEbkJWSdwRVw3Lq3wo9OwKVKw1AClXFeofRDk/ roEXA4/q lgLkQ4IgDQWf+dkVPpn/ xZfiELCplPmVl8jiGBk15VPirA3MsDDVS9THN7G7g5lD7h6r2g1rH5CZ pr9uLoxEQandkn/ XCy5WyOi34SEG2KD7q1HAO0LKa3UbSRDLUpdHcwx2p9+hwV6W00TZ Fingerprint: 33:48:be: 0a:fd:26:c5:6c:c8:29:bb:78:83:c0:67:92 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 ``` ---------- **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 ``` ---------- **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 ``` ---------- **443:** ``` HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Tue, 12 Dec 2023 03:57:30 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: http://www.google.com/ ``` HEARTBLEED: 2023/12/12 03:58:05 159.203.113.25:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.203.113.25']

Name

2711f1341d2f150a0c3e2d596939805d66ba7c6403346513d1fc826324f63c87

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2711f1341d2f150a0c3e2d596939805d66ba7c6403346513d1fc826324f63c87']

Name

c524e118b1e263fccac6e94365b3a0b148a53ea96df21c8377ccd8ec3d6a0874

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c524e118b1e263fccac6e94365b3a0b148a53ea96df21c8377ccd8ec3d6a0874']

Name

d90e4a1b3a6bf019474b3be1703bf3211f1ebcca00b21bc252a39af274dc4fb0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd90e4a1b3a6bf019474b3be1703bf3211f1ebcca00b21bc252a39af274dc4fb0']

Name

216.128.179.235

Description

CC=CA ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.128.179.235']

Name

48299c2c568ce5f0d4f801b4aee0a6109b68613d2948ce4948334bbd7adc49eb

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48299c2c568ce5f0d4f801b4aee0a6109b68613d2948ce4948334bbd7adc49eb']

Name

c0871ecfe8b306074c6d376db14d966578a8511e5b5d355a4cf2c4d0b8c9deb9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0871ecfe8b306074c6d376db14d966578a8511e5b5d355a4cf2c4d0b8c9deb9']

Name

2b640582bbbffe58c4efb8ab5a0412e95130e70a587fd1e194fbcd4b33d432cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b640582bbbffe58c4efb8ab5a0412e95130e70a587fd1e194fbcd4b33d432cf']

Name

2fgithub.com

Pattern Type

stix

Pattern

[domain-name:value = '2fgithub.com']

Name

155.138.146.162

Description

ISP: The Constant Company, LLC **OS:** Windows (build 10.0.14393) ---------- Hostnames: - 155.138.146.162.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- 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 1607)/Windows Server 2016 (version 1607) OS Build: 10.0.14393 Target Name: WIN-76Q0A2QCBL4 NetBIOS Domain Name: WIN-76Q0A2QCBL4 NetBIOS Computer Name: WIN-76Q0A2QCBL4 DNS Domain Name: WIN-76Q0A2QCBL4 FQDN: WIN-76Q0A2QCBL4 ; Administrator SES ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '155.138.146.162']

Intrusion-Set

Name
Volt Typhoon

Description
[Volt Typhoon](https://attack.mitre.org/groups/G1017) is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021. [Volt Typhoon](https://attack.mitre.org/groups/G1017) typically focuses on espionage and information gathering and has targeted critical infrastructure organizations in the US including Guam. [Volt Typhoon](https://attack.mitre.org/groups/G1017) has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.(Citation: Microsoft Volt Typhoon May 2023)(Citation: Joint Cybersecurity Advisory Volt Typhoon June 2023)(Citation: Secureworks BRONZE SILHOUETTE May 2023)

Region

Name
Northern America
Name
Oceania
Name
Americas
Name
Micronesia

Country

Name
Guam

Name
United States

Malware

Name
HiatusRat

Vulnerability

Name
CVE-2022-27997

Domain-Name

Value
2fgithub.com

StixFile

Value
c524e118b1e263fccac6e94365b3a0b148a53ea96df21c8377ccd8ec3d6a0874
b6226c3e0e4ad64bbda3e6a79eb464c7050faa25d1f5332dcac014d2e79dd87f
d6cd1636569bba4131462bb8f45be1daa9a203aa343b6f2fd48a4847acfc29fa
cdffba0ebda39b3b58f59815be3829ca9c1cde957b46a6ad5ce4b31e405455bb
690638c702170dba9e43b0096944c4e7540b827218afbfaebc902143cda4f2a7
d90e4a1b3a6bf019474b3be1703bf3211f1ebcca00b21bc252a39af274dc4fb0
b845ef0f9c5853ad1c226ac0ae7bb91159d5bb132185c1bfd171696b755a9164
36c63d0c2a78497ccf555e84f0233a514943faeff38281d99d00baf5df23f184
2711f1341d2f150a0c3e2d596939805d66ba7c6403346513d1fc826324f63c87
88fc3816c94f9b0191179f4e933843ee4cfdbcb392968605491a387b1235ec12
e88b03465c0376463f912a5601a518cc697330dc3e5857068f3de0c434b52c9a
8e35d8643c00d9e2993625b03366a7cd1bd36e6a60bc0c6039a509fccf9df150
f5271fcb895977dc1eead64415e525323cd412e3f2625aee2fafbb5674beea28

19aa5a2235ee2518826a48363cb603060ee73ddccdf7d93bf197f97d7402aa37

6a8230e66011e0a0012273f7d12110c23b1e33bd7232dc67a836662a3d1075c7

dc7b6b4f53581b53edfbbc83d825cfa0450b2039f126cd62e8529189bb156033

2b640582bbbffe58c4efb8ab5a0412e95130e70a587fd1e194fbcd4b33d432cf

5512cce87ff9dfd3ee9721eb29302d1700199ed7d625e09f9f779772ec06bdb0

c2299d8581af4ea8048bbf2bffd45c6ddca323c9c718c172355cc0df006ea6ca

5928f67db54220510f6863c0edc0343fdb68f7c7070496a3f49f99b3b545daf9

c71d04e2b6b35fdd058b4be5cf9ea3478697950378d4ee3c7fe0bf87e1e3730f

7043ffd9ce3fe48c9fb948ae958a2e9966d29afe380d6b61d5efb826b70334f5

9e6a2a01decc2c26f3586a119b6fd3a886c4cf9c76aa452339d164fda40c63e4

bf0ed245e897c7d1ada511db2939e8f3a879a96543f2651d5631339d5419bb75

3fab16ec4643d8f6b9a99d85427322f7fb40e9ea3cd4de8318c6a52e29869d5a

5a2681ea2e1d0d5e7db2a2499d2e6e27b2689830c638d5ee28c2eef9867ececf

86f01d5342ec39c65b1cff716f19c334cec26a82b87492d783d5e8f4ff9cb63a

c0871ecfe8b306074c6d376db14d966578a8511e5b5d355a4cf2c4d0b8c9deb9

2cb6df289475457e807fc202a2b4688b2e23a88c94a8431981780caf8b76acf7

07118af421f14a7e07601639f44a72f6782757ae74d2afffdb531b8209697e7f

b4f2470159ca93f9d585ae2df1da972f6d14a0c418ebc202a324b9be5c877b61

08d0da0c36089f7a1f700b989f2f7825c5ba2549a20735d0bd1e64ca9c4885bc

0279435f8727cca99bee575d157187787174d39f6872c2067de23afc681fe586

48299c2c568ce5f0d4f801b4aee0a6109b68613d2948ce4948334bbd7adc49eb

IPv4-Addr

Value
144.202.43.124
216.128.180.232
216.128.179.235
159.203.113.25
149.28.119.73
45.156.21.172
140.82.20.246
155.138.146.162
174.138.56.21
45.32.88.250
66.42.124.155
207.246.100.151
193.36.119.48

192.169.6.241
108.61.203.19
104.156.246.150
108.61.132.157
144.202.49.189
159.203.72.166
45.11.92.176

External References

- https://otx.alienvault.com/pulse/657b0af55af290155cda7016
- https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
- https://github.com/blacklotuslabs/IOCs/blob/main/KVbotnet_IOCs.txt