Jan 19 2024

NETMANAGEIT

Intelligence Report

Bigpanzi Exposed: The Hidden Cyber Threat Behind Your Set-Top Box

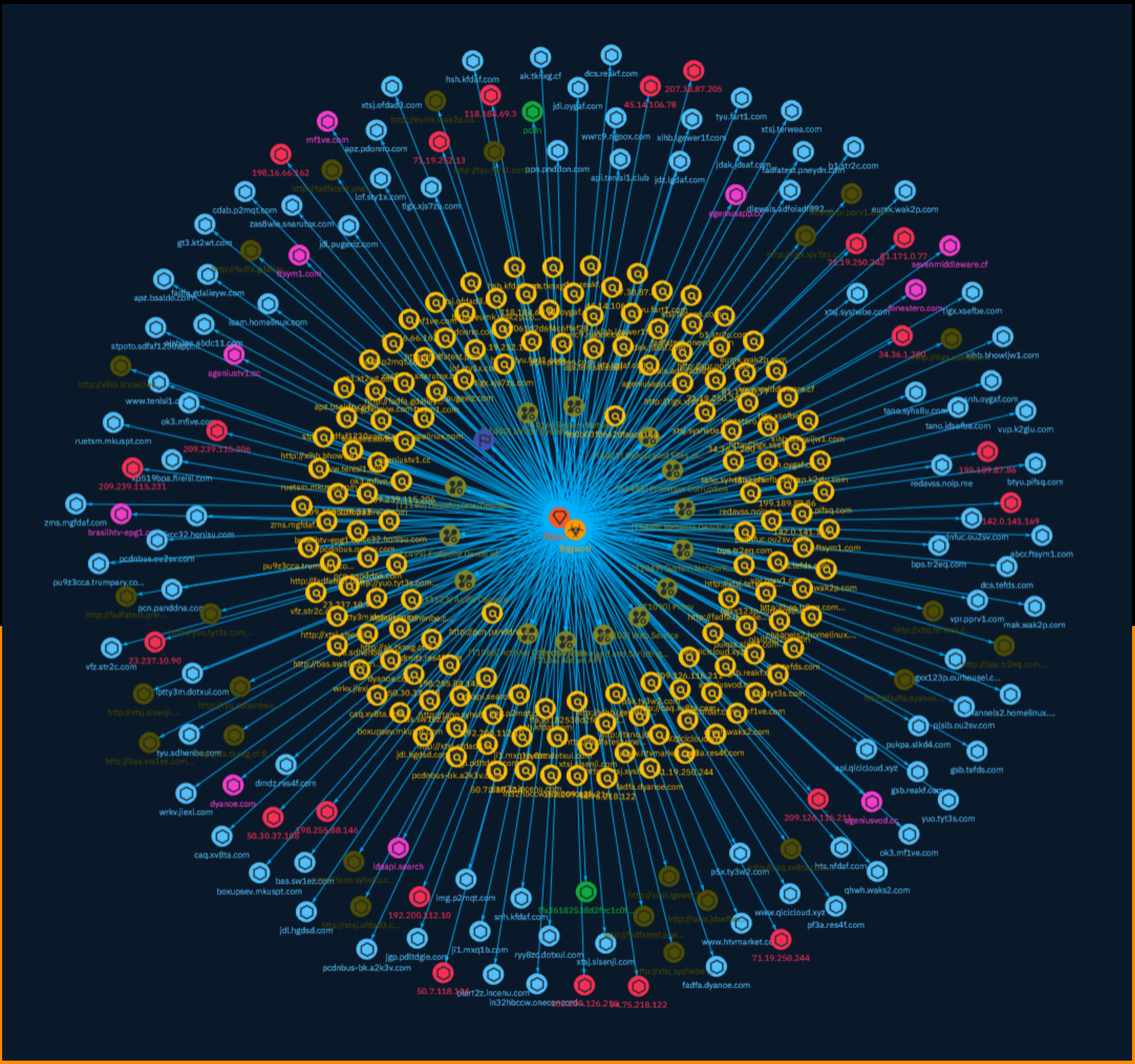

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 17
- Intrusion-Set 72
- Country 73
- Malware 74

Observables

- Domain-Name 75
- StixFile 76

- Hostname 77
- IPv4-Addr 83
- Url 85

External References

- External References 87

Overview

Description

A major cybercrime syndicate, known as Bigpanzi, is targeting Android set-top boxes and other devices with malicious software, as well as operating platforms such as Windows, Android and Windows. This botnet, which at its peak, Qianxin noted approximately 170,000 daily active bots, predominantly in Brazil has been mainly used for DDoS attacks. Additionally, the threat actors have used it to misuse controlled Android TVs, for example in a network attack on set-top boxes in the UAE on December 11, 2023, where regular broadcasts were substituted with footage of the Israel-Palestine conflict.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Network Denial of Service
ID
T1498
Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

Audio Capture

ID

T1123

Description

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Name

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

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
System Network Configuration Discovery

ID
T1016

Description
Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://

attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

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 indirectly 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

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection.

Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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

Endpoint Denial of Service

ID

T1499

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Name

Firmware Corruption

ID

T1495

Description

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.(Citation: Symantec Chernobyl W95.CIH) Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards. In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. For example, corruption of firmware responsible for loading the operating system for network devices may render the network devices inoperable.(Citation: dhs_threat_to_net_devices)(Citation: cisa_malware_orgs_ukraine) Depending on the device, this attack may also result in [Data Destruction](https://attack.mitre.org/techniques/T1485).

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation

Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Indicator

Name
71.19.252.13
Description
CC=CA ASN=AS11831 ESECUREDATA
Pattern Type
stix
Pattern
[ipv4-addr:value = '71.19.252.13']
Name
199.189.87.86
Description
CC=US ASN=AS30083 AS-30083-GO-DADDY-COM-LLC
Pattern Type
stix

Pattern

[ipv4-addr:value = '199.189.87.86']

Name

ok3.mf1ve.com

Pattern Type

stix

Pattern

[hostname:value = 'ok3.mf1ve.com']

Name

23.237.10.90

Description

CC=US ASN=AS174 COGENT-174

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.237.10.90']

Name

nikcc32.honisu.com

Pattern Type
stix
Pattern
[hostname:value = 'nikcc32.honisu.com']
Name
zas8wie.snarutox.com
Pattern Type
stix
Pattern
[hostname:value = 'zas8wie.snarutox.com']
Name
alchaes.abdc11.com
Pattern Type
stix
Pattern
[hostname:value = 'alchaes.abdc11.com']
Name
71.19.250.244

Description

ISP: eSecureData **OS:** None ------------------------- Hostnames: - angico.assuredwave.com ------------------------- Domains: - assuredwave.com ------------------------- Services: **123:** ``` NTP protocolversion: 3 stratum: 4 leap: 0 precision: -24 rootdelay: 0.448867797852 rootdisp: 93.8861236572 refid: 737586754 reftime: 3907708481.9 poll: 3 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '71.19.250.244']

Name

ji1.mxq1b.com

Pattern Type

stix

Pattern

[hostname:value = 'ji1.mxq1b.com']

Name

209.239.115.231

Description

CC=US ASN=AS30083 AS-30083-GO-DADDY-COM-LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.239.115.231']

Name

jgp.pdltdgie.com

Pattern Type

stix

Pattern

[hostname:value = 'jgp.pdltdgie.com']

Name

xtsj.syshebe.com

Pattern Type

stix

Pattern

[hostname:value = 'xtsj.syshebe.com']

Name

dmdz.res4f.com

Pattern Type

stix

Pattern

[hostname:value = 'dmdz.res4f.com']

Name

tyu.sdhenbe.com

Pattern Type

stix

Pattern

[hostname:value = 'tyu.sdhenbe.com']

Name

6ff061d2d6f4c6ffef28c433dd41c974801281ecc47f34ff19e76141fc8b09aa

Description

ELF:Lotoor-BD\ [Expl] SHA256 of 4338e9bd02b42eb458f8515caa3bab8e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ff061d2d6f4c6ffef28c433dd41c974801281ecc47f34ff19e76141fc8b09aa']

Name

jdl.hgdsd.com

Pattern Type

stix

Pattern

[hostname:value = 'jdl.hgdsd.com']

Name

hsh.kfdaf.com

Pattern Type

stix

Pattern

[hostname:value = 'hsh.kfdaf.com']

Name

plslb.ou2sv.com

Pattern Type

stix

Pattern
[hostname:value = 'plslb.ou2sv.com']

Name
http://xtsj.syshebe.com:8080

Pattern Type
stix

Pattern
[url:value = 'http://xtsj.syshebe.com:8080']

Name
ppn.pnddon.com

Pattern Type
stix

Pattern
[hostname:value = 'ppn.pnddon.com']

Name
http://xtsj.ofdad3.com:8080

Pattern Type
stix

Pattern

[url:value = 'http://xtsj.ofdad3.com:8080']

Name

http://fadfa.gdalieyw.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://fadfa.gdalieyw.com:8080']

Name

http://tigx.xsefbe.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://tigx.xsefbe.com:8080']

Name

ffa36182538d2fec1c0f16f53705d86cd6d6dc5b7c2185b8021976b6bc057459

Description

SHA256 of 606939075437b985bce0d46b080419d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffa36182538d2fec1c0f16f53705d86cd6d6dc5b7c2185b8021976b6bc057459']

Name

lof.sty1x.com

Pattern Type

stix

Pattern

[hostname:value = 'lof.sty1x.com']

Name

http://tano.jdsefbe.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://tano.jdsefbe.com:8080']

Name

vfz.str2c.com

Pattern Type

stix

Pattern

[hostname:value = 'vfz.str2c.com']

Name

dcs.reakf.com

Pattern Type

stix

Pattern

[hostname:value = 'dcs.reakf.com']

Name

94.75.218.122

Description

CC=NL ASN=AS60781 LeaseWeb Netherlands B.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.75.218.122']
Name
zms.mgfdaf.com
Pattern Type
stix
Pattern
[hostname:value = 'zms.mgfdaf.com']
Name
ageniusapp.cc
Pattern Type
stix
Pattern
[domain-name:value = 'ageniusapp.cc']
Name
iptty3m.dotxui.com
Pattern Type
stix
Pattern

[hostname:value = 'iptty3m.dotxui.com']
Name
dlewals.adfoiadf892.net
Pattern Type
stix
Pattern
[hostname:value = 'dlewals.adfoiadf892.net']
Name
pukpa.slkd4.com
Pattern Type
stix
Pattern
[hostname:value = 'pukpa.slkd4.com']
Name
http://tano.syhs8u.com:8080
Pattern Type
stix
Pattern

[url:value = 'http://tano.syhs8u.com:8080']

Name

btyu.pifsq.com

Pattern Type

stix

Pattern

[hostname:value = 'btyu.pifsq.com']

Name

50.30.37.108

Description

CC=US ASN=AS30083 AS-30083-GO-DADDY-COM-LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.30.37.108']

Name

ok3.mflve.com

Pattern Type

stix

Pattern

[hostname:value = 'ok3.mflve.com']

Name

snh.oygaf.com

Pattern Type

stix

Pattern

[hostname:value = 'snh.oygaf.com']

Name

tano.jdsefbe.com

Pattern Type

stix

Pattern

[hostname:value = 'tano.jdsefbe.com']

Name

bps.tr2eq.com

Pattern Type

stix

Pattern

[hostname:value = 'bps.tr2eq.com']

Name

pf3a.res4f.com

Pattern Type

stix

Pattern

[hostname:value = 'pf3a.res4f.com']

Name

xtsj.sisenji.com

Pattern Type

stix

Pattern

[hostname:value = 'xtsj.sisenji.com']

Name

api.tenlsi1.club

Pattern Type

stix

Pattern

[hostname:value = 'api.tenlsi1.club']

Name

209.126.116.211

Description

CC=US ASN=AS30083 AS-30083-GO-DADDY-COM-LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.126.116.211']

Name

9b0b03f06a2dfaacd1448466370101a9a7db47264af3326b87245369ede9068e

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b0b03f06a2dfaacd1448466370101a9a7db47264af3326b87245369ede9068e']

Name

www.qicicloud.xyz

Pattern Type

stix

Pattern

[hostname:value = 'www.qicicloud.xyz']

Name

198.16.66.162

Description

CC=NL ASN=AS174 COGENT-174

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.16.66.162']

Name

isam.homelinux.com

Pattern Type

stix

Pattern

[hostname:value = 'isam.homelinux.com']

Name

gsb.tefds.com

Pattern Type

stix

Pattern

[hostname:value = 'gsb.tefds.com']

Name

gt3.kt2wt.com

Pattern Type

stix

Pattern

[hostname:value = 'gt3.kt2wt.com']

Name

mak.wak2p.com

Pattern Type

stix

Pattern

[hostname:value = 'mak.wak2p.com']

Name

http://tyu.fart1.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://tyu.fart1.com:8080']

Name

xtsj.ofdad3.com

Pattern Type

stix

Pattern

[hostname:value = 'xtsj.ofdad3.com']

Name

gsb.reakf.com

Pattern Type
stix
Pattern
[hostname:value = 'gsb.reakf.com']
Name
pcdnbus.ou2sv.com
Pattern Type
stix
Pattern
[hostname:value = 'pcdnbus.ou2sv.com']
Name
ak.tknxg.cf
Pattern Type
stix
Pattern
[hostname:value = 'ak.tknxg.cf']
Name
p5x.ty3w2.com

Pattern Type

stix

Pattern

[hostname:value = 'p5x.ty3w2.com']

Name

redavss.noip.me

Pattern Type

stix

Pattern

[hostname:value = 'redavss.noip.me']

Name

ageniusvod.cc

Pattern Type

stix

Pattern

[domain-name:value = 'ageniusvod.cc']

Name

http://xihb.lgewer1f.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://xihb.lgewer1f.com:8080']

Name

jdl.pugexiz.com

Pattern Type

stix

Pattern

[hostname:value = 'jdl.pugexiz.com']

Name

fadfa.dyanoe.com

Pattern Type

stix

Pattern

[hostname:value = 'fadfa.dyanoe.com']

Name

apz.pdonno.com

Pattern Type

stix

Pattern

[hostname:value = 'apz.pdonno.com']

Name

fadfatest.pneydn.com

Pattern Type

stix

Pattern

[hostname:value = 'fadfatest.pneydn.com']

Name

50.7.118.114

Description

ISP: Cogent Communications **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 status 1 udp 44018 status 1 tcp 39295 ``` ------------------ **9096:** ``` \xb2\x80\xfc\xa7\x1dDq\xa0O6\xaf;\x90\x8d:\x97\xee3x\xb6w\xfa\x1d\xb3\x8c$IC\xa2\xd2\xff~u(\xfb,\xff\x19ri\x8d\x8f\xcc\xff ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.7.118.114']

Name

jdl.oygaf.com

Pattern Type

stix

Pattern

[hostname:value = 'jdl.oygaf.com']

Name

34.36.1.200

Description

ISP: Google LLC **OS:** None ------------------------- Hostnames: - 200.1.36.34.bc.googleusercontent.com ------------------------- Domains: - googleusercontent.com ------------------------- Services: **80:** ``` HTTP/1.1 404 Not Found Date: Wed, 03 Jan 2024 11:35:56 GMT Content-Length: 0 Server: istio-envoy Via: 1.1 google ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '34.36.1.200']

Name

http://ak.tknxg.cf:8080

Pattern Type

stix

Pattern

[url:value = 'http://ak.tknxg.cf:8080']

Name

abcr.ftsym1.com

Pattern Type

stix

Pattern

[hostname:value = 'abcr.ftsym1.com']

Name

http://fadfatest.pneydn.com:8080/stb-download/tool/$1

Pattern Type

stix

Pattern

[url:value = 'http://fadfatest.pneydn.com:8080/stb-download/tool/$1']

Name

http://yuo.tyt3s.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://yuo.tyt3s.com:8080']

Name

hgxx123p.ourhousei.com

Pattern Type

stix

Pattern

[hostname:value = 'hgxx123p.ourhousei.com']

Name

209.239.115.206

Description

ISP: GoDaddy.com, LLC **OS:** None ------------------------- Hostnames: - usloft5036.startdedicated.com ------------------------- Domains: - startdedicated.com ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Thu, 28 Dec 2023 08:56:04 GMT Content-Type: text/html Content-Length: 0 Last-Modified: Fri, 22

Jun 2018 09:35:49 GMT Connection: keep-alive ETag: "5b2cc2f5-0" Accept-Ranges: bytes ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.239.115.206']

Name

dcs.tefds.com

Pattern Type

stix

Pattern

[hostname:value = 'dcs.tefds.com']

Name

tano.syhs8u.com

Pattern Type

stix

Pattern

[hostname:value = 'tano.syhs8u.com']

Name

http://tigx.xjs7zu.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://tigx.xjs7zu.com:8080']

Name

118.184.69.3

Description

CC=CN ASN=AS137443 Anchnet Asia Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '118.184.69.3']

Name

ryy8zc.dotxui.com

Pattern Type

stix

Pattern

[hostname:value = 'ryy8zc.dotxui.com']

Name

71.19.250.242

Description

ISP: eSecureData **OS:** None -------------------------- Hostnames: - dabant.deliriousgrease.com -------------------------- Domains: - deliriousgrease.com -------------------------- Services: **21:** ``` 220 (vsFTPd 2.2.2) 530 Login incorrect. 530 Please login with USER and PASS. 211-Features: EPRT EPSV MDTM PASV REST STREAM SIZE TVFS UTF8 211 End ``` ------------------ **123:** ``` NTP protocolversion: 3 stratum: 2 leap: 0 precision: -23 rootdelay: 0.0558776855469 rootdisp: 0.0437774658203 refid: 3652506070 reftime: 3913926906.86 poll: 3 ``` ------------------ **8080:** ``` HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Tue, 09 Jan 2024 14:41:39 GMT Content-Type: text/html Content-Length: 3698 Last-Modified: Mon, 31 Oct 2016 12:37:31 GMT Connection: keep-alive ETag: "58173b0b-e72" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '71.19.250.242']

Name

jdz.lgdaf.com

Pattern Type

stix

Pattern

[hostname:value = 'jdz.lgdaf.com']

Name

http://pcn.panddna.com:8080/marketdatas/dns/hosts

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://pcn.panddna.com:8080/marketdatas/dns/hosts']

Name

http://eumk.wak2p.com:8080/marketdatas/dns/hosts

Pattern Type

stix

Pattern

[url:value = 'http://eumk.wak2p.com:8080/marketdatas/dns/hosts']

Name

192.200.112.10

Description

ISP: GorillaServers, Inc. **OS:** None ------------------------- Hostnames: - 192-200-112-10.static.gorillaservers.com ------------------------- Domains: - gorillaservers.com ------------------------- Services: **8080:** ``` HTTP/1.1 200 OK Server: nginx/1.13.9 Date: Wed, 17 Jan 2024 09:49:59 GMT Content-Type: text/html Content-Length: 0 Last-Modified: Fri, 22 Jun 2018 09:15:12 GMT ETag: "5b2cbe20-0" Accept-Ranges: bytes ``` ------------------ **8181:** ``` HTTP/1.0 503 Service Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html

503 Service Unavailable

No server is available to handle this request. ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.200.112.10']

Name

apz.bsaldo.com

Pattern Type

stix

Pattern

[hostname:value = 'apz.bsaldo.com']

Name

142.0.141.169

Description

ISP: PEG TECH INC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC6wOELPKJxhg1Jhyfe+BmGmTzm8dExv0J1vR9/+tmf4pjiGPtAydZKB8OTJI5iBEKAMs67u/pBEXmonHDK2r/ODx5vXhbWKWE7KlTma4zc1z1dLHd26P0yS703E8orQdb3TUOJOLpBtsLbJUXWOU4L41JgT0Sm3hf8iUQKHJA5oE8FeLIdyjxN9HldrhcfejwskAA1zCynCasYm+7RPTLq2Y6yk24Qu0vyidYPHCQG1z2/TStHZeIntOolqdDLtuieYeiFs0o22X+/3Hz49tWd7A/YsTV2L3TRT6lOUsbJmNqCExWECtFdxkq7lKGlATOmIVg3PW2veyR1c7PHITpt Fingerprint: ef:7a:46:43:3e:16:0c:0b:1a:d4:d8:52:d8:38:4e:cd 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 ``` ------------------ **80:** ``` HTTP/1.1 200 OK Server: nginx/1.22.1 Date: Tue, 16 Jan 2024 17:22:47 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Wed, 19 Oct 2022 10:48:27 GMT Connection: keep-alive ETag: "634fd5fb-267" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern
[ipv4-addr:value = '142.0.141.169']

Name
bas.sw1ez.com

Pattern Type
stix

Pattern
[hostname:value = 'bas.sw1ez.com']

Name
vup.k2glu.com

Pattern Type
stix

Pattern
[hostname:value = 'vup.k2glu.com']

Name
pcdnfuc.ou2sv.com

Pattern Type
stix

Pattern
[hostname:value = 'pcdnfuc.ou2sv.com']
Name
ageniustv1.cc
Pattern Type
stix
Pattern
[domain-name:value = 'ageniustv1.cc']
Name
tigx.xsefbe.com
Pattern Type
stix
Pattern
[hostname:value = 'tigx.xsefbe.com']
Name
img.p2mqt.com
Pattern Type
stix

Pattern

[hostname:value = 'img.p2mqt.com']

Name

http://fadfatest.pneydn.com:8080/stb-download/tool/na.sh

Pattern Type

stix

Pattern

[url:value = 'http://fadfatest.pneydn.com:8080/stb-download/tool/na.sh']

Name

channels2.homelinux.com

Pattern Type

stix

Pattern

[hostname:value = 'channels2.homelinux.com']

Name

kp519bpa.fireisi.com

Pattern Type

stix

Pattern

[hostname:value = 'kp519bpa.fireisi.com']

Name

http://xtsj.terwea.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://xtsj.terwea.com:8080']

Name

plart2z.incenu.com

Pattern Type

stix

Pattern

[hostname:value = 'plart2z.incenu.com']

Name

dyanoe.com

Pattern Type

stix

Pattern

[domain-name:value = 'dyanoe.com']

Name

b1.str2c.com

Pattern Type

stix

Pattern

[hostname:value = 'b1.str2c.com']

Name

www.htvmarket.com

Pattern Type

stix

Pattern

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

Name

207.38.87.205

Description

ISP: GoDaddy.com, LLC **OS:** None ------------------------- Hostnames: - condor3128.startdedicated.com ------------------------- Domains: - startdedicated.com ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.13.9 Date: Wed, 03 Jan 2024 12:25:21 GMT Content-Type: text/html Content-Length: 0 Last-Modified: Fri, 22 Jun 2018 09:15:12 GMT Connection: keep-alive ETag: "5b2cbe20-0" Accept-Ranges: bytes ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.38.87.205']

Name

yuo.tyt3s.com

Pattern Type

stix

Pattern

[hostname:value = 'yuo.tyt3s.com']

Name

fadfa.gdalieyw.com

Pattern Type

stix

Pattern
[hostname:value = 'fadfa.gdalieyw.com']

Name
eumk.wak2p.com

Pattern Type
stix

Pattern
[hostname:value = 'eumk.wak2p.com']

Name
api.qicicloud.xyz

Pattern Type
stix

Pattern
[hostname:value = 'api.qicicloud.xyz']

Name
www.tenlsi1.club

Pattern Type
stix

Pattern

[hostname:value = 'www.tenlsi1.club']

Name

81.171.0.77

Description

ISP: LeaseWeb Netherlands B.V. **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **1194:** ``` @\x9b\xd8\xac\xe5\xdes\x81\x98\x01\x00\x00\x00\x00\xd9\xce:\xbe\xf6\x98\xa5m\x00\x00\x00\x00 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '81.171.0.77']

Name

wrkv.jiexi.com

Pattern Type

stix

Pattern

[hostname:value = 'wrkv.jiexi.com']

Name
tigx.xjs7zu.com
Pattern Type
stix
Pattern
[hostname:value = 'tigx.xjs7zu.com']
Name
http://fadfatest.pneydn.com:8080/stb-download/tool/a.sh
Pattern Type
stix
Pattern
[url:value = 'http://fadfatest.pneydn.com:8080/stb-download/tool/a.sh']
Name
http://xtsj.sisenji.com:8080
Pattern Type
stix
Pattern
[url:value = 'http://xtsj.sisenji.com:8080']

Name
sevenmiddleware.cf
Pattern Type
stix
Pattern
[domain-name:value = 'sevenmiddleware.cf']
Name
pcdnbus-bk.a2k3v.com
Pattern Type
stix
Pattern
[hostname:value = 'pcdnbus-bk.a2k3v.com']
Name
pu9z3cca.trumpary.com
Pattern Type
stix
Pattern
[hostname:value = 'pu9z3cca.trumpary.com']

Name
45.14.106.78
Description
ISP: xTom **OS:** None ------------------------- Hostnames: - s22262.vps.hosting ------------------------- Domains: - vps.hosting ------------------------- Services: **1234:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAMZCmxkF8FFSdRHTrh3h347 ARpSbC9utIdmQuPYpTaX2cPWORPppHEkDSOdIK+FdXfXMX0zi8Adj/4eI1GHNhw= Fingerprint: 1c:f3:5c:c1:6a:0f:24:c6:16:51:63:5f:9a:15:67:b5 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 ``` ------------------ **8888:** ``` HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.10.12 Date: Fri, 29 Dec 2023 08:48:59 GMT Content-type: text/html; charset=utf-8 Content-Length: 297 ``` ------------------
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.14.106.78']
Name
pcn.panddna.com
Pattern Type

stix

Pattern

[hostname:value = 'pcn.panddna.com']

Name

xihb.lgewer1f.com

Pattern Type

stix

Pattern

[hostname:value = 'xihb.lgewer1f.com']

Name

in32hbccw.oneconcord.net

Pattern Type

stix

Pattern

[hostname:value = 'in32hbccw.oneconcord.net']

Name

ruetsm.mkuspt.com

Pattern Type

stix

Pattern

[hostname:value = 'ruetsm.mkuspt.com']

Name

xihb.bhowljw1.com

Pattern Type

stix

Pattern

[hostname:value = 'xihb.bhowljw1.com']

Name

http://tyu.sdhenbe.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://tyu.sdhenbe.com:8080']

Name

xtsj.terwea.com

Pattern Type

stix

Pattern

[hostname:value = 'xtsj.terwea.com']

Name

qhwh.waks2.com

Pattern Type

stix

Pattern

[hostname:value = 'qhwh.waks2.com']

Name

brasilhtv-epg1.cc

Pattern Type

stix

Pattern

[domain-name:value = 'brasilhtv-epg1.cc']

Name

tyu.fart1.com

Pattern Type

stix

Pattern

[hostname:value = 'tyu.fart1.com']

Name

http://caq.xv8ta.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://caq.xv8ta.com:8080']

Name

stpoto.sdfaf1230app.net

Pattern Type

stix

Pattern

[hostname:value = 'stpoto.sdfaf1230app.net']

Name

vpr.pprv1.com

Pattern Type

stix

Pattern

[hostname:value = 'vpr.pprv1.com']

Name

http://bas.sw1ez.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://bas.sw1ez.com:8080']

Name

mf1ve.com

Pattern Type

stix

Pattern

[domain-name:value = 'mf1ve.com']

Name

http://fadfa.dyanoe.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://fadfa.dyanoe.com:8080']

Name

http://xihb.bhowljw1.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://xihb.bhowljw1.com:8080']

Name

wwrc9.ngoox.com

Pattern Type

stix

Pattern

[hostname:value = 'wwrc9.ngoox.com']

Name

162.209.126.216

Description

CC=US ASN=AS27357 RACKSPACE

Pattern Type

stix

Pattern

[ipv4-addr:value = '162.209.126.216']

Name

cdab.p2mqt.com

Pattern Type

stix

Pattern

[hostname:value = 'cdab.p2mqt.com']

Name

http://vpr.pprv1.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://vpr.pprv1.com:8080']

Name

boxupsev.mkuspt.com

Pattern Type

stix

Pattern

[hostname:value = 'boxupsev.mkuspt.com']

Name

fonestero.com

Pattern Type

stix

Pattern

[domain-name:value = 'fonestero.com']

Name

hts.nfdaf.com

Pattern Type

stix

Pattern

[hostname:value = 'hts.nfdaf.com']

Name

198.255.88.146

Description

CC=CA ASN=AS174 COGENT-174

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.255.88.146']

Name

http://bps.tr2eq.com:8080

Pattern Type

stix

Pattern

[url:value = 'http://bps.tr2eq.com:8080']

Name

idaapi.search

Pattern Type

stix

Pattern

[domain-name:value = 'idaapi.search']
Name
ftsym1.com
Pattern Type
stix
Pattern
[domain-name:value = 'ftsym1.com']
Name
snh.kfdaf.com
Pattern Type
stix
Pattern
[hostname:value = 'snh.kfdaf.com']
Name
caq.xv8ta.com
Pattern Type
stix
Pattern

[hostname:value = 'caq.xv8ta.com']
Name
jdak.jdsaf.com
Pattern Type
stix
Pattern
[hostname:value = 'jdak.jdsaf.com']

Intrusion-Set

Name
Bigpanzi

Country

Name
Brazil

Malware

Name
Bigpanzi

Domain-Name

Value
ageniusvod.cc
mf1ve.com
ageniustv1.cc
ftsym1.com
sevenmiddleware.cf
dyanoe.com
brasilhtv-epg1.cc
idaapi.search
fonestero.com
ageniusapp.cc

StixFile

Value
9b0b03f06a2dfaacd1448466370101a9a7db47264af3326b87245369ede9068e
6ff061d2d6f4c6ffef28c433dd41c974801281ecc47f34ff19e76141fc8b09aa
ffa36182538d2fec1c0f16f53705d86cd6d6dc5b7c2185b8021976b6bc057459

Hostname

Value
pukpa.slkd4.com
ok3.mflve.com
hsh.kfdaf.com
caq.xv8ta.com
xtsj.ofdad3.com
p5x.ty3w2.com
bas.sw1ez.com
fadfa.gdalieyw.com
redavss.noip.me
nikcc32.honisu.com
eumk.wak2p.com
stpoto.sdfaf1230app.net
apz.bsaldo.com

xtsj.syshebe.com

pcdnbus-bk.a2k3v.com

zas8wie.snarutox.com

zms.mgfdaf.com

pcn.panddna.com

btyu.pifsq.com

jdak.jdsaf.com

b1.str2c.com

www.htvmarket.com

pcdnbus.ou2sv.com

apz.pdonno.com

ji1.mxq1b.com

kp519bpa.fireisi.com

abcr.ftsym1.com

jdl.hgdsd.com

fadfatest.pneydn.com

qhwh.waks2.com

plart2z.incenu.com

tigx.xsefbe.com
tyu.sdhenbe.com
tyu.fart1.com
vup.k2glu.com
ruetsm.mkuspt.com
lof.sty1x.com
bps.tr2eq.com
www.tenlsi1.club
gsb.tefds.com
ryy8zc.dotxui.com
pcdnfuc.ou2sv.com
yuo.tyt3s.com
alchaes.abdc11.com
dlewals.adfoiadf892.net
boxupsev.mkuspt.com
gt3.kt2wt.com
gsb.reakf.com
vfz.str2c.com

img.p2mqt.com
plslb.ou2sv.com
jdz.lgdaf.com
xtsj.terwea.com
pu9z3cca.trumpary.com
ak.tknxg.cf
ok3.mf1ve.com
dmdz.res4f.com
xihb.bhowljw1.com
www.qicicloud.xyz
wwrc9.ngoox.com
hts.nfdaf.com
in32hbccw.oneconcord.net
api.qicicloud.xyz
pf3a.res4f.com
jdl.pugexiz.com
tano.jdsefbe.com
tigx.xjs7zu.com

tano.syhs8u.com

dcs.tefds.com

jgp.pdltdgie.com

snh.oygaf.com

fadfa.dyanoe.com

snh.kfdaf.com

mak.wak2p.com

api.tenlsi1.club

dcs.reakf.com

hgxx123p.ourhousei.com

isam.homelinux.com

ppn.pnddon.com

channels2.homelinux.com

cdab.p2mqt.com

vpr.pprv1.com

wrkv.jiexi.com

xihb.lgewer1f.com

xtsj.sisenji.com

iptty3m.dotxui.com

jdl.oygaf.com

IPv4-Addr

Value
81.171.0.77
71.19.250.242
50.30.37.108
209.239.115.206
94.75.218.122
45.14.106.78
209.126.116.211
23.237.10.90
71.19.252.13
198.255.88.146
192.200.112.10
207.38.87.205
162.209.126.216

34.36.1.200
142.0.141.169
209.239.115.231
198.16.66.162
71.19.250.244
118.184.69.3
199.189.87.86
50.7.118.114

Url

Value
http://bas.sw1ez.com:8080
http://caq.xv8ta.com:8080
http://xtsj.terwea.com:8080
http://tyu.sdhenbe.com:8080
http://tigx.xjs7zu.com:8080
http://pcn.panddna.com:8080/marketdatas/dns/hosts
http://fadfa.gdalieyw.com:8080
http://xtsj.syshebe.com:8080
http://fadfatest.pneydn.com:8080/stb-download/tool/a.sh
http://tigx.xsefbe.com:8080
http://ak.tknxg.cf:8080
http://vpr.pprv1.com:8080
http://tano.syhs8u.com:8080

http://xtsj.ofdad3.com:8080

http://fadfa.dyanoe.com:8080

http://xtsj.sisenji.com:8080

http://fadfatest.pneydn.com:8080/stb-download/tool/$1

http://xihb.lgewer1f.com:8080

http://tano.jdsefbe.com:8080

http://fadfatest.pneydn.com:8080/stb-download/tool/na.sh

http://bps.tr2eq.com:8080

http://eumk.wak2p.com:8080/marketdatas/dns/hosts

http://tyu.fart1.com:8080

http://yuo.tyt3s.com:8080

http://xihb.bhowljw1.com:8080

External References

- https://otx.alienvault.com/pulse/65a905e6269453eec89db9c3
- https://blog.xlab.qianxin.com/bigpanzi-exposed-hidden-cyber-threat-behind-your-stb/