Jun 10 2023

NETMANAGEIT

Intelligence Report

Asylum Ambuscade: crimeware or cyberespionage?

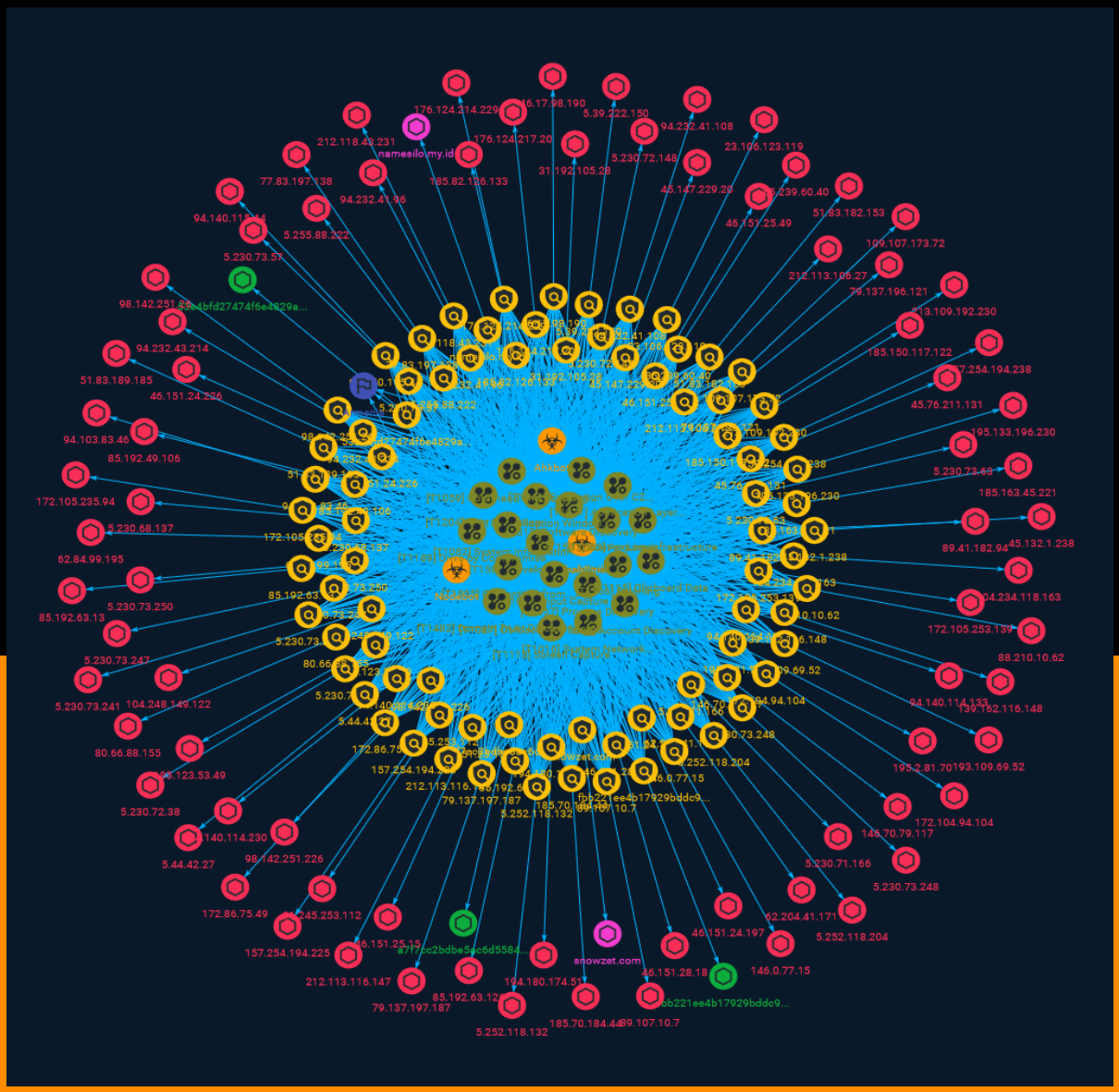

Table of contents

Overview

Entities

Observables

External References

Overview

Description

n this blogpost, welivesecurity provides details about the early 2022 espionage campaign and about multiple cybercrime campaigns in 2022 and 2023.

Confidence

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

15 / 100

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

Develop Capabilities

ID

T1587

Description

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020) As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending

features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Application Window Discovery

ID

T1010

Description

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020) Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features

such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Credentials from Password Stores

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

Software Discovery

ID

T1518

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

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

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing]

(https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

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

Account Discovery

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Name

Domain Trust Discovery

ID

T1482

Description

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets)(Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name

85.192.63.126

Description

ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - temporary-birth.aeza.netwo
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke
AAAAB3NzaC1yc2EAAAADAQABAAABgQCyRPPiOkxamwET6ZAmy29THbTFcZPsMMHAoc0P1PdnEbWa
BHZbgJvXvuHYw11yaDf4pHzcovp9ZHuO44dWNVSW18m2Yt6k8JsgzERwUHFORXxSmdB4VVXrJzG2 RI0r/bml/Rwy
756gWT11oU5GL0+XPXVSzy07/0YvTinko+T BEB8vYwpjD3K+m5lC5XsnFL/hgrRZYb79wQ82+PrCl1DtNTGviMnZNI6b
cE0U2tCmuX1glVdSJ3lCrWbs6+0TygU00DvE5ol4TUEYq6WVIcK+ifuw9+38a0RuhONtTgV9s6Hc ruie4BdYaci2+na/z
RgmHJp5DxbHIv+1L1jm88HZbN2lOkno02H3wKwJqkV4NIQ4GdsUaOzABsZLHWtWPEfjwfTxyTa+C Vl5J3X5kTO8= Fi
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp
sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.192.63.126']

Name

94.232.41.96

Description

ISP: XHOST INTERNET SOLUTIONS LP **OS:** Ubuntu ---------- Hostnames: ----------
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDsx
6yaWdOzsL0G3Avs4FklViT1Npa9YLEZwvR8wCivVz0FJa2Xsa9ZuTfRJ9HakfYNPONYmpSP4lpnF B/
L1exr3DcIAQLWGxEpqmQbkMrI3dqwhaJfPvU0jbC93HchbySi2supDdSLxAi3bm3UyreiUhMlh
lk4YM0kFQNJhx6oWLQce0caHf0Cqn1UUfGVns9Ea4FPpjWXzDnVi4Os4O8Fx97b3IwSfUPKYN5yf 3paqbHVJqbcilkK
Fingerprint: b4:8d:bb:c5:ce:40:26:82:76:f2:40:33:3c:7f:bd:cc Kex Algorithms: curve25519-sha256 curve25519-sha2
nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha
Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorit
ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com u
hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@ope
Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: E
GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.232.41.96']

Name

5.230.71.166

Description

CC=DE ASN=AS12586 GHOSTnet GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.71.166']

Name

104.248.149.122

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domai
Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 11

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.248.149.122']

Name

46.151.25.49

Description

ISP: Hosting technology LTD **OS:** Ubuntu ---------- Hostnames: - v1562195.hosted-by-v
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke
AAAAB3NzaC1yc2EAAAADAQABAAABgQDZmwIP6EahY4wyHFyhzSFoZlS9fa4njpscTU4GF/duhoTx gIeauSv5/
uUuCAXKqX5ifwWIt0wH9eNw67I5uxlVRrHv4VOxLAYGriAH0QrTa5F7zyOBxQFSqMuu YSqBgoA0ZQ/07Yht5x/Wqb
98T7SJIWUioKvM7GWfCpfJDtFz44mzS5jyCbUplSq0simvZpQH6pTfXODVGby8pDDwrDSk1TNwkj
XlD5MAcBKJ6zPqrhp8WAXCgGaC5x2KmbGOATAho+NAslWukg7oMhXg0dE1B66XId4kY5e9hwhgAA
qO7vnX5CePCl8rCvF9VD3NdSQZeenFuR2UxUUlfhm+4EbUi1v2BQSvzxMHJcgh3pSfpDGRgRmSyJ f/2PiIklEbh7UW
cegLNFiouOlqIQOoDGLWAJTmhhHnoZdi1eEnv5cNg2wrZlNMkd9 uyhj83/GHEs= Fingerprint: a9:2a:2c:81:b3:10:ec
curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-g
group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-r

poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh
etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm
hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.151.25.49']

Name

snowzet.com

Pattern Type

stix

Pattern

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

Name

53e4bfd27474f6e4829ac4d625d3d914452456baf5da2c1c51e2e6df35ab634a

Description

Cabinet_Archive SHA256 of 7db446b95d5198330b2b25e4ba6429c57942cfc9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '53e4bfd27474f6e4829ac4d625d3d914452456baf5da2c1c51e2e6df35ab634a']

Name

89.41.182.94

Description

CC=RO ASN=AS33911 Tennet Telecom Srl

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.41.182.94']

Name

98.142.251.226

Description

CC=EE ASN=AS62005 BlueVPS OU

Pattern Type

stix

Pattern

[ipv4-addr:value = '98.142.251.226']

Name

31.192.105.28

Description

ISP: HOSTKEY B.V. **OS:** Ubuntu ---------- Hostnames: - vision-cm-2.spotparking.ru ----- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLRT7QtljehhM44lPHxnQsQT hNWSMP8eFLL Fingerprint: cd:e7:ea:d9:83:ad:d1:bb:fa:24:f4:eb:ee:cf:68:3e Kex Algorithms: curve25519-sha256 curve25519-sha2 nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-grou sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh. sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` HTTP/1.1 200 OK Serv Type: application/json Content-Length: 28 Connection: keep-alive ``` HEARTBLEED: 2023/06/04 14:12:20 31.192 Cache-Control: no-cache Date: Wed, 10 May 2023 16:00:20 GMT Content-Length: 0 Docker Registry HTTP API:

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.192.105.28']

Name

195.2.81.70

Description

ISP: Hosting technology LTD **OS:** Ubuntu ---------- Hostnames: - host-195-2-81-70.host vdsina.ru ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: dpv8Yf9D4QdMqzhPhWlBTAOFeM7UT1x jX2BHDSfBNzidwM6lCd8ZM95MuIbXYy4iIDL7G7bscI41itWcwhuk29mtdo lH6V71D3hFD3nBinrZVqU9okLCLFDwW5QqOfr4h6gnMjWj8hUtOUosR2sEXC5+W BKrQiFmLWi4BoGPBr3igOTyA8c LSi7onObMtFOZNKp87Bjlx5qXWm+a1yu9Metgx/spOogxtpg8GA7pE/ae9KZFKrESmafVduQdKbA b/ZPc79D4NeAS s2hBtGN8R8AkxDEvMxORQVBy2Vavj5XgYCTkxmHSo queYxmYipXKtgSA8Rn2nYy0YprXDsbfde6j13aDhNfMheV8n

36:77:35:31:b8:56:ee:b1:94:66:86:47:c0 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-
group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group
rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr
gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha
sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512
---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 07 Jun 2023 02:19:09 GM
keep-alive Vary: Accept-Encoding X-Powered-By: Google Drive HLS Player Accept-Ranges: bytes CF-Cache-St
a.nel.cloudflare.com\/report\/v3?
s=BwILdlGd%2BKA0CAJJFUwvrWEi4s2GSHzdOLaMu938q2LyqgFRN%2FYDIMGes0rWfJIR71z4nFw3wYjl4jHGP%2Fx
nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} CF-RAY: 7d35689a4d

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.2.81.70']

Name

5.230.68.137

Description

ISP: GHOSTnet GmbH **OS:** Ubuntu ---------- Hostnames: - placeholder.noezserver.de -
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 Key type: ssh-rsa Ke
AAAAB3NzaC1yc2EAAAADAQABAAABgQC8sAuA+a6PE8qAnZYp812el7qNNbek8l0OHYgrFE2lLIV+ DIC81aPvN2eQlt
ResX49PaosQ4HTuhO3pkbsohqIU+EwRuREyj2h v9xLz+8UZf40wYtEciUE5TQLTvI8U8RBx1TX+V2m5L2wAsWKI2ZIE
CBCF+4sB6l+DZwRIPcc0Jj3psb2jJWA2ZAeIb8qGDGcI ZzENeMMzdAs/eJ9NGyggkBB81il3UkjYjm7iW6FxuqakJ+b/G
zucNtoVtdv9eGr39XUCeroYCjHRy8uJ5ETt2URGJC344eVQw/qgJAV6DmFnsw7ZBV0SlQoR6Va5R Lz9Ra9xT4YjwYEt
kOeKNEPVcSOuANK7mxJzf9C8uWFp9ZH1W8Pe w7bJyfX5GpU= Fingerprint: 7e:08:a3:c3:a2:c8:c0:fc:5c:0e:bd:c4:97
sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-excha
sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa
poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh
etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm
hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 Content-Length: 481 Content-Type: text/html;c
SAFE ---------- **2525:** ``` 220 mail.okibgunxqtvyfhavbyajqscd.com ESMTP service ready\r\n ``` -----

Pattern Type
stix
Pattern
[ipv4-addr:value = '5.230.68.137']
Name
45.76.211.131
Description
CC=JP ASN=AS20473 AS-CHOOPA
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.76.211.131']
Name
a7f7cc2bdbe5ac6d55841bcfb0ada2c0e55192af5f70dcdda68e7fd17112346a
Description
Delphi SHA256 of 3aa8a4554b175db9da5eeb7824b5c047638a6a9d
Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = 'a7f7cc2bdbe5ac6d55841bcfb0ada2c0e55192af5f70dcdda68e7fd17112346a']

Name

5.255.88.222

Description

ISP: Serverius **OS:** None ---------- Hostnames: - alphawolve.com - panel.followpolee.
followpolee.click ---------- Services: **8443:** ``` HTTP/1.1 200 OK Content-Type: text/html; cha
chunked ``` HEARTBLEED: 2023/05/24 09:46:58 5.255.88.222:8443 - SAFE ---------- **8880:** ``` HTTP/1.1
Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Tue, 30 May 2023 15:50:11 GMT Content-Length:

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.255.88.222']

Name

104.234.118.163

Description

ISP: RouterHosting LLC **OS:** Ubuntu ---------- Hostnames: ---------- Do
OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNT
VL2ZUUWk8HbeDKSMGWo00K1VyGFPMIOlIGmkEhVmrxYTTOsf0ynIAGT2uMSozVU= Fingerprint: 6e:e9:b1:40:af:e
curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519
hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Alg
Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@op

etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.234.118.163']

Name

185.123.53.49

Description

CC=EE ASN=AS62005 BlueVPS OU

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.123.53.49']

Name

45.147.229.20

Description

CC=DE ASN=AS30823 combahton GmbH

Pattern Type
stix
Pattern
[ipv4-addr:value = '45.147.229.20']
Name
46.151.24.197
Description
CC=NL ASN=AS207651 Hosting technology LTD
Pattern Type
stix
Pattern
[ipv4-addr:value = '46.151.24.197']
Name
46.151.24.226
Description
ISP: Hosting technology LTD **OS:** Ubuntu ---------- Hostnames: - v1913357.hosted-by-v ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJnktm13BG2bh1UnTVtOuask 1Rg1nR/FpyZeq 6a:88:59:a0:ee:8c:dc:3f:bb:05:af:51:f0:f6:4a:56 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.o sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha5 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorith

ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com u
hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@ope
Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.151.24.226']

Name

5.230.73.63

Description

ISP: GHOSTnet GmbH **OS:** None ---------- Hostnames: - ringbirdapp.com ----------
Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCboV+t
oAtgYMDp2mwDO1mYQz4bKNa0hV1kDCsyb0K0QWEXOVcxHP6iQZi3Me2OakcBtReyz8SJA8sH2S43 NUhIv2FBVar
oNw27VCV4OW BKI8Z5dTv3fNv5FO+MxTyIJVOj3NKouZdhC1TWYzRkJnvGlA+fNkqtzAKZYarm/ndMd4RtMifsbX 9oU
b59XZPWyAfU1OrDmLXi4If Fingerprint: f1:7b:6d:a9:1d:75:cf:2b:d4:ae:23:5e:58:65:f7:27 Kex Algorithms: curve2551
sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 di
diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Alg
ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-
aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm
etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac
zlib@openssh.com ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp
portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **7000:** ``` HTTP/1.0 302 Please use HTTPS
Options: nosniff Strict-Transport-Security: max-age=0 X-Content-Security-Policy: default-src 'self'; object-src
font-src https://fonts.gstatic.com 'self' X-WebKit-CSP: default-src 'self'; object-src 'self'; img-src data: 'self';
fonts.gstatic.com 'self' X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Content-Security-Pol
https://fonts.googleapis.com 'self'; font-src https://fonts.gstatic.com 'self' Location: https://5.230.73.63/ ``` -

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.63']

Name

91.245.253.112

Description

CC=SG ASN=AS9009 M247 Europe SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.245.253.112']

Name

185.82.126.133

Description

CC=LV ASN=AS52173 Sia Nano IT

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.82.126.133']

Name

146.70.79.117

Description

ISP: M247 Europe SRL **OS:** Windows ---------- Hostnames: ---------- Dor
Content-Type: text/html Last-Modified: Thu, 20 Oct 2022 03:00:02 GMT Accept-Ranges: bytes ETag: "4e137c30e
Content-Length: 701 ``` ---------- **1194:** ``` @}1\x96\x86\xf1$\xa1\xbb\x01\x00\x00\x00\x00\xd9\
4500: ``` VPN (IKE NAT-T) Initiator SPI: 2419177b2db0c3dd Responder SPI: 0000000000000000 Next Payloa
Encryption: False Commit: False Authentication: False Message ID: f95eb3a2 Length: 48 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.70.79.117']

Name

5.230.73.250

Description

ISP: GHOSTnet GmbH **OS:** Ubuntu ---------- Hostnames: ---------- Dom
OpenSSH_8.2p1 Ubuntu-4ubuntu0.1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCcotyCqUpu
XgWIVK1IBY2LdXmnGaKVhPMbfwsmB7tYubIarn8nR9rdXcHZZoOXRAAzZ5zwBdzRGWrfm483KFPT e0n2JHM58L1r8
EvSlL2+ 9WtOvP33SWbWQ/kMQP2OAQWt06lXOP41hL++jpK0hJaIWJzxU2srJ2yF/036sFWsafjjgaI96wfq
duiM8gxTozAe+t3gebR2EDRVNOK9oz3vCkDWnb55T2haxFHmkkaMPoLNcoUHMX4yqKsGw66XHlYg
sU538UIY1EN5OYgHWqOtAdGcTe+g8thNIUSTDxsWMh5JbaovRl9Uc7FjA4JjJ3+9D4VgZY1VymRQ +8kTE4axIbxVXufH
u08RnuhuJIE= Fingerprint: 09:1d:e6:5c:e9:bf:82:13:92:eb:e9:14:58:44:f0:32 Kex Algorithms: curve25519-sha256 cu
ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-g
Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: cha
aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac

sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.c
Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.250']

Name

212.113.106.27

Description

ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - childlike-nation.aeza.networ
---------- Domains: - aeza.network - sergeeva.photo ---------- Services: **22:**
nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO0Mo6G6KqcA+YVjDc2SXBe/
9uR7tN3giJxOu47XH56BucvCzMlALb+HXbjSuPgpSx6o9EqTAiYBiwfHVuGZ+X0= Fingerprint: cc:90:19:74:a0:89:c2:7
sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@o
group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms:
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op
nginx/1.18.0 (Ubuntu) Date: Sat, 03 Jun 2023 21:38:36 GMT Content-Type: text/html Content-Length: 612 Last-M
"6459e1c6-264" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.1
Connection: keep-alive ``` HEARTBLEED: 2023/05/26 09:17:54 212.113.106.27:443 - SAFE ---------- **5432:

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.113.106.27']

Name

194.180.174.51

Description

CC=MD ASN=AS39798 MivoCloud SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.180.174.51']

Name

5.230.73.57

Description

ISP: GHOSTnet GmbH **OS:** Debian ---------- Hostnames: ---------- Doma
OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDTbSmQvFihh
vPwFDxiTKviyp+4zU7fhMoR3UIGoVZOI0hazDOC4Dae9DSNx38xhkL4ONmx/vxy8IsI+5BqY0GEY wIhPWb4kyTY1rw
NL6v10B2G8S57WBrku j/xv5nVTayqI2V9lQetwOiAde0+1DraZD22uDcNsauF6D1+NWl58va88EkbF/keIZjxdxYh3z+3
SRvvOyYlQAQYaWHSOmkC6 n/EHhGz1NQ2k1+P3WMxN4zc5UOno4tHtAiVpt4+lKz2Z3t0iFs8L9H6qOqIZPme7oo6
y2UGjisS8L3VlOH5fDRGhTS7yosTusHzIoIVxLdAaJVzs8z8yTG+xe6Zo46CpzpOYkoFYdLan/A3 NXRLHIUihHU= Finge
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp
sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.57']

Name

172.105.253.139

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - www.zuventus.com - Domains: - zuventus.com - linodeusercontent.com ---------- Services: **80:** ``` HTTP/1.1 200 Tue, 02 May 2023 10:45:07 GMT ETag: "0-5fab3a1f81e20" Accept-Ranges: bytes Content-Length: 0 Content-Type Permanently Date: Sat, 27 May 2023 16:03:42 GMT Server: Apache X-Content-Type-Options: nosniff Location: h html; charset=iso-8859-1 ``` HEARTBLEED: 2023/05/27 16:04:20 172.105.253.139:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.105.253.139']

Name

94.140.114.230

Description

ISP: Sia Nano IT **OS:** None ---------- Hostnames: - n.sni-347-default.ssl.fastly.net ---- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key:

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE125R1Vnbea05vEbVqzcwwM CSsLSSE8pYSC
Fingerprint: b9:76:88:dd:50:a1:c5:60:c4:15:9f:bb:1f:60:c5:45 Kex Algorithms: curve25519-sha256 curve25519-sha25
nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-grou
sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption
aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh
etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.
sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` HTTP/1.1 500 Domain
Retry-After: 0 content-type: text/html Cache-Control: private, no-cache X-Served-By: cache-hel1410028-HEL
varnish ``` HEARTBLEED: 2023/06/05 14:49:09 94.140.114.230:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.140.114.230']

Name

5.230.72.148

Description

CC=DE ASN=AS12586 GHOSTnet GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.72.148']

Name

62.204.41.171

Description
CC=RU ASN=AS59425 Horizon LLC
Pattern Type
stix
Pattern
[ipv4-addr:value = '62.204.41.171']
Name
85.192.49.106
Description
CC=NL ASN=AS207651 Hosting technology LTD
Pattern Type
stix
Pattern
[ipv4-addr:value = '85.192.49.106']
Name
185.150.117.122
Description

ISP: UAB Cherry Servers **OS:** None ---------- Hostnames: ---------- Dom
Host: 185.150.117.122 Connection: keep-alive Cache-Control: no-cache Content-Type: text/html Content-Lengt
---

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.150.117.122']

Name

46.151.25.15

Description

ISP: Podolsk Electrosvyaz Ltd. **OS:** None ---------- Hostnames: - v1562193.hosted-by-v
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke
AAAAB3NzaC1yc2EAAAADAQABAAABgQC6q2iL4sjcmME5neFIc4wlA4FZrXIFWvmMUBFaAyqeugjA
tXT3mO4L06Yxgc2UL8cu+jCwXqmicDTkNAxRZzTyZzo9XlDDVwyyVYR0xOe+ksa96Wn75IjJPFvH EJH87gGhDIdetSnD
Et8MYTYNrNhnW/k9zgSLPFf7kbqc6CM92nh969xiVPGMjtZWw6GRx6zK+u2kfEaVbTLjOIL7FgHN 3uYHBPW/mvixd
aUg+AiD16fWJlQUrd8SnZiX3XTw103QbBBtfBeFk2H55qisALPc6tB3TY B4zq8hbObWAPRXnfGHL52xH2mN3YQUdn
1NUM4vk4vUe9GVG1VdjYmqQRItY4bbs0nE3aXhnZnvWwlE5TflpF56c6EjIe7rVH5bBptaP0JkBN Eh0M+x+oHf0= Fin
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp
sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op
Powered-By: Express Access-Control-Allow-Origin: * Date: Wed, 31 May 2023 16:24:25 GMT Connection: keep-a
3000: ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Thu, 01 Jun
Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.151.25.15']

Name

namesilo.my.id

Pattern Type

stix

Pattern

[domain-name:value = 'namesilo.my.id']

Name

94.140.114.133

Description

CC=LV ASN=AS43513 Sia Nano IT

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.140.114.133']

Name

5.230.73.247

Description

ISP: GHOSTnet GmbH **OS:** None ---------- Hostnames: ---------- Domai
Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDIbuMUdOXCpQ0B3SsPwh3ZYkgwGqylvembcTo5
DMMYIunrfzPPNvkHiJ2audd5uDbLa2dP5Ezfz2sj1yolOZgsOVbbGmxv5ZPcpT1ihiPgTNXsRwFp BCLckwcBfuvxKw7a
Hate9pqK3UHudGXad2M4WB5pQ6ZKT7kBvXLCIpCPSN 1rjjJewWEu1jrEEBkIXBut97FJ/yxAfeL/d8vOV7i5exR32EFzG
1zpChwqIGaNjdsMHVSTciKZXyUmuvUOH9E7AAw08lvznDn Fingerprint: c4:9e:ec:e2:6e:05:63:32:20:94:b8:b7:d1:1e:
sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-excha
sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 dif
sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@opens
aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algo
hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com uma
sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/
(CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 X-Powered-By: PHP/7.1.33 Transfer-Encoding: chunked Content-Type
OK Date: Fri, 26 May 2023 13:27:21 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 Content-
HEARTBLEED: 2023/05/26 13:27:40 5.230.73.247:443 - SAFE ---------- **2525:** ``` 220 mail.hfaehlrlyzvrfr

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.247']

Name

85.239.60.40

Description

ISP: Clouvider **OS:** None ---------- Hostnames: ---------- Domains: ----
Keep-Alive Content-Length: 1999 Content-Type: text/html Keep-Alive: timeout=15; max=19 ``` HEARTBLEED: 20

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.239.60.40']

Name

46.151.28.18

Description

ISP: Hosting technology LTD **OS:** None ---------- Hostnames: - v1630097.hosted-by-vds ---------- Services: **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-A alive Keep-Alive: timeout=5 Content-Length: 0 ``` ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Pow 2023 06:05:44 GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.151.28.18']

Name

94.232.43.214

Description

CC=RU ASN=AS208091 Xhost Internet Solutions Lp

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.232.43.214']

Name

185.163.45.221

Description

ISP: MivoCloud SRL **OS:** None ---------- Hostnames: - no-rdns.mivocloud.com -------- Services: **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Sat, timeout=5 Content-Length: 0 ``` ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.163.45.221']

Name

172.86.75.49

Description

ISP: BL Networks **OS:** Windows (Build 10.0.19041) ---------- Hostnames: - pedantic-hoo plesk.page ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI1Q5XAoMvtr3BwLxG4hRIjm qdjPYx8Pxm3tC e9:df:24:ef:45:96:5a:ed:eb:5c:e5:b0:96:f5:a7:46 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.c sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha5 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorith ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com ur hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@ope

Algorithms: none zlib@openssh.com ``` ---------- **53:** ``` none Resolver name: pedantic-hodgkin.1
name: pedantic-hodgkin.172-86-75-49.plesk.page ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx
Length: 432 Connection: keep-alive Last-Modified: Thu, 27 Apr 2023 10:21:14 GMT ETag: "1b0-5fa4eb758da80" A
443: ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 31 May 2023 11:36:28 GMT Content-Type: text/html; chars
Fri, 28 May 1999 00:00:00 GMT Last-Modified: Wed, 31 May 2023 11:36:28 GMT Cache-Control: no-store, no-cac
Pragma: no-cache P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA" X-Frame-Options: SAMEORIG
172.86.75.49:443 - SAFE ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID
AUTH=CRAM-MD5] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERA
OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID comp
Logging out A004 OK Logout completed. ``` HEARTBLEED: 2023/05/30 10:43:02 172.86.75.49:993 - SAFE ---------
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protoc
Build: 10.0.19041 Target Name: 6479F22C0805472 NetBIOS Domain Name: 6479F22C0805472 NetBIOS Compute
6479f22c0805472 ``` ---------- **4190:** ``` "IMPLEMENTATION" "Dovecot Pigeonhole"\r\n"SIEVE" "filein
comparator-i;ascii-numeric relational regex imap4flags copy include variables body enotify environment m
imapflags notify"\r\n"NOTIFY" "mailto"\r\n"SASL" "PLAIN LOGIN DIGEST-MD5 CRAM-MD5"\r\n"STARTTLS"\r\n
8443: ``` HTTP/1.1 200 OK Server: sw-cp-server Date: Wed, 24 May 2023 19:39:32 GMT Content-Type: text/ht
Expires: Fri, 28 May 1999 00:00:00 GMT Last-Modified: Wed, 24 May 2023 19:39:31 GMT Cache-Control: no-store
check=0 Pragma: no-cache P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA" X-Frame-Options: S
2023/05/24 19:39:42 172.86.75.49:8443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.86.75.49']

Name

176.124.217.20

Description

ISP: Hosting technology LTD **OS:** None ---------- Hostnames: - v1690497.hosted-by-vds
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke
AAAAB3NzaC1yc2EAAAADAQABAAABgQDMVeqVS7/4uQ2ITE43JyEzmEpK4mNgk70oXhYfIbwAvWXc
OysKjnXPnq6zEIaalZwLcjOqgZtwnvHyroLCS1ntYwbFiwxGoxOq2BbQkcbNlMVcMacl4QvIwaqV gZWB7QWM4Kgho
GtysvPtkpNtyoSyfQ1mjAIy6uXg9YFJ1Dtxo0zhxHW4gVNTchZ6g YpkRIBWJfHAFkOUjVFvlieZvmeObb3ahjXa1f35NV
RE4pMhJbf8qzdN1ChyYyXnuR0hdp6xcJI8iBRREGaa8H87ZUSsLcUJxqyDIUH nfas3QSEH26q3Xvy/c54YWZZhbxmF

eTrwcq9/5eU10+0NzFi6q8+xefQiIE4B8iFkLZk2rhSQGoYk4wAgN5duXF1eHI+GI1yJ+JM+hVtc 2Go5TIFuwdM= Finge
curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp
sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op
Powered-By: Express Access-Control-Allow-Origin: * Date: Wed, 07 Jun 2023 14:59:08 GMT Connection: keep-a
3000: ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Fri, 19 May
Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.124.217.20']

Name

5.230.73.248

Description

ISP: GHOSTnet GmbH **OS:** None ---------- Hostnames: ---------- Domai
Forbidden Date: Thu, 11 May 2023 10:52:09 GMT Server: Apache/2.4.56 (Debian) Content-Length: 279 Content-
HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request Prom
goversion: go1.17.3 revision: a2321e7b940ddcff26873612bccdf7cd4c42b6b6 version: 1.3.1 node_network_info: lo
operstate: unknown eth0: address: fa:30:df:36:e1:b8 broadcast: ff:ff:ff:ff:ff:ff device: eth0 duplex: unknown ope

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.248']

Name

62.84.99.195

Description

ISP: Hosting technology LTD **OS:** None ---------- Hostnames: - v1760235.hosted-by-vds ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke AAAAB3NzaC1yc2EAAAADAQABAAABgQCy5xxA9knTW09rBqamLou+YQClYLaMotE0p8tT9Sx5Zsrm E6OQ8WQfTFDrziuxbDHJpIIgCzMJG8rTqH5oNsy2PAX+qlaBm2X0bJ2lT3nb1c1NtZShyVULtEXn 3oee8E10f1jV1lR0bv gGR9c6PMymKW1oDTavMUgKdn/gxvMT/PC9lcOFZgJ72gUYvBbVvljJgxsm6/hHKUkql708BIhSyF BOP20pjZxenjHW PzDMbuXu+zLgLhw3c7vVM 5YHrpkcgcLYemGO3Qu1fte7/JMJ+Ow0H6fJh9aQzcVs0Asfc9V5hGRUAgvkifH31kCAavp sIqeAQDtSIaEh2gpAq5prMFTES4Qr8Tqi1c7rASqf008UpffQkOggSEgsBTlPTboPX1cCQYZ9CEp jklN/BUtMrs= Finge curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2- Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@ umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op Powered-By: Express Access-Control-Allow-Origin: * Date: Mon, 05 Jun 2023 10:18:51 GMT Connection: keep-a **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Thu, 08 Jun Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '62.84.99.195']

Name

79.137.196.121

Description

ISP: AEZA GROUP Ltd **OS:** Debian ---------- Hostnames: - stable-songs.aeza.network - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Ke

AAAAB3NzaC1yc2EAAAADAQABAAABAQCtB9sh1LpJ6wVogT1ifolraXFut7oeKNtci2+yRMI6bDS9 XuyEtO6Wi6XPl8Ue k84OQLtq8AjyQAQsvS7bWSZRixh28 cXKPchMkQP2x3IUOh8K/9CF+lIvWgHsC+zWqfYe3eqBRvIV+VMKLeT58djRvlc HEBwK3ziAf220xBOVX450pGUGuJ2tIaIH0EzsiTWOdzk3j+IcA6/ 83wbKBUAFY6Hd5AzcncDg4Silp+XVCvPlCXJOhHj+ a2:e8:e3:29:d4:c4:71:2c:ea:6a:85:42:e8:c8:40:88 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.o hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellm Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: cha aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.c Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` SSL Error: TLSV1_ALERT_PROTOCOL_VERS remote error: protocol version not supported ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.196.121']

Name

185.70.184.44

Description

CC=NL ASN=AS57043 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.70.184.44']

Name

212.118.43.231

Description

ISP: Hosting technology LTD **OS:** Ubuntu ---------- Hostnames: - v1708029.hosted-by-v ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke AAAAB3NzaC1yc2EAAAADAQABAAABgQDAKbInCAc3j2kZrDvOnEp1PV+YAg0S2vmXjPEcdncyDtwQ YHdyiUaU31Z549B+KGiLmY51JGlmu6AYGsQ5Hof9FZdOY94QP2lBj3614smk+FKTO+FhKleLBhxt szcTjAnz1M8t6JKqE IxQTbax64kbaf2txuy2QJgNr8sh48UNoR8eEJ6evbKpu7Fy06jmNl/IsT3bwOC0HzeX+5j1bWwd3 9SWv87uTNFsMT0Y zl9DIjAALC9FYAqY92vePe7SLQlZ8leV/O0b9IibzqeMTlb0JZ/PcZrw2IbV08SHesN20nnDENfJ B9EDGzhinZPGsCN0dvSFvOk2tzpaYF93P3RqgOnl4lFZuDs0lOFDGcPnDpkB4+WBQ3RB6v+VSa9H lv7RK2kI9Nc= Fi curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2- Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@ umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op Powered-By: Express Access-Control-Allow-Origin: * Date: Mon, 22 May 2023 13:56:22 GMT Connection: keep-a **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Tue, 23 May Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.118.43.231']

Name

88.210.10.62

Description

ISP: LLC KMS-KOM **OS:** Ubuntu ---------- Hostnames: - v1543306.hosted-by-vdsina.ru - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke AAAAB3NzaC1yc2EAAAADAQABAAABgQCbi0Egghu5xuRozCnkwnDUsNwBvy3hQkne+mhEW6sQjE9S LxO4co+IJxx5xJHomE7dw3QHIfsC0BAIQl5KQlJjrVo7EUe+psfuwd4bKlse821JgAVDT0btY1wn ZwUTHpUO9JoUCMpf

gXvW19KRQP1v1fjMOr4MtSL39hOdJdH0ylTpJ+iEZpzNpf4R811oKTGqtkPdlGE0SxRxnpc6KOu1 BuIGoMel0jE9EoySiy4ekhhEg8O26JKp2WWRzwqN7ab4ncKbDIx2O5BEUCAKcQfwGphwxt8DXF7/ gqV4LwOJkKvC/ WsO55ITEg4ERdnyPJ6InpGJL1kWjqJIAv6be4iK7VpT11kyW6MAHz7HOkCBaW2H unWDQyczKQOBrJKAEaMDr2OwLD dkzgu8gFjXk= Fingerprint: 96:11:2f:f9:34:b6:c5:8e:e5:87:1d:3e:31:4e:b9:70 Kex Algorithms: curve25519-sha256 cur ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-g Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: cha aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.c Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.210.10.62']

Name

5.230.72.38

Description

ISP: GHOSTnet GmbH **OS:** Windows (Build 10.0.17763) ---------- Hostnames: - placehol ---------- Services: **21:** ``` 220 Microsoft FTP Service 530 User cannot log in. 214-The follow ADAT * ALLO APPE AUTH CCC CDUP CWD DELE ENC * EPRT EPSV FEAT HELP HOST LANG LIST MDTM MIC * MKD REST RETR RMD RNFR RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD XPWD supported: LANG EN* UTF8 AUTH TLS;TLS-C;SSL;TLS-P; PBSZ PROT C;P; CCC HOST SIZE MDTM REST STREAM 211 html Last-Modified: Fri, 28 Apr 2023 22:06:13 GMT Accept-Ranges: bytes ETag: "593575a51d7ad91:0" Server: Mic 703 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x0 Info: OS: Windows 10/Windows Server 2019 OS Build: 10.0.17763 Target Name: VPS644C34091EBA NetBIOS Do VPS644C34091EBA DNS Domain Name: vps644c34091eba FQDN: vps644c34091eba ``` ---------- **5986 ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 07 Jun 2023 22:19:29 GMT Connection: close Content-Length: 3 10.0.17763 Target Name: VPS644C34091EBA NetBIOS Domain Name: VPS644C34091EBA NetBIOS Computer Na vps644c34091eba ``` HEARTBLEED: 2023/06/07 22:19:48 5.230.72.38:5986 - ERROR: write tcp 5.230.72.38:5986: br

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.72.38']

Name

94.232.41.108

Description

ISP: XHOST INTERNET SOLUTIONS LP **OS:** None ---------- Hostnames: ----------
OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDVi6JsOc4N
gXPU84iVAOCmDRHRue3Q4PgnKe1zdva9x8tMt0tjbZwUPD8Qz3eSfh6Uh0YIqSG6xuHfiBMWQMPr uPhJs0mt2YAF
IjEEp/SH VfIKgK4kCIgdH6gmgeU8PMnMxwE3JbtfjyT8Z7chljHF+ekKWc8LplyL9HeJc4vsJFVbIwbz9HKI F37x0HrAUC
OGgQgzgZCMYDbGfdRSoYF YDjuGRx5bf6fkJ+b9L05t3JWLcYCdxWVEELrlJdarmM8/P43J4+3RGgeC1cWtiGdodxzaJN
COGgZwuyW1NWDRVNyQtQxeMdcStiVhJ7CUV1kXgNz0pDh4Lt4yLLqMU DWKqRLrAkEs= Fingerprint: 32:54:ec:6e:
curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-
group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-r
poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh
etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm
hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------
Control-Allow-Origin: * Date: Mon, 29 May 2023 08:39:02 GMT Connection: keep-alive Keep-Alive: timeout=5
Found X-Powered-By: Express Access-Control-Allow-Origin: * Date: Sat, 03 Jun 2023 12:30:13 GMT Connection
----

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.232.41.108']

Name

146.0.77.15

Description

CC=NL ASN=AS57043 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.0.77.15']

Name

94.103.83.46

Description

ISP: Hosting technology LTD **OS:** None ---------- Hostnames: - host-94-103-83-46.host hosted-by-vdsina.ru - farmnet.ru ---------- Services: **8443:** ``` HTTP/1.1 302 Set-Cookie: JSE HttpOnly Location: https://farmbazis.ru/ Content-Type: text/html;charset=UTF-8 Content-Length: 0 Date: We 94.103.83.46:8443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.103.83.46']

Name

157.254.194.238

Description

CC=US ASN=AS29802 HVC-AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.254.194.238']

Name

212.113.116.147

Description

CC=DE ASN=AS210644 AEZA GROUP Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.113.116.147']

Name

176.124.214.229

Description

CC=NL ASN=AS207651 Hosting technology LTD

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.124.214.229']

Name

193.109.69.52

Description

CC=NL ASN=AS57043 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.109.69.52']

Name

5.230.73.241

Description

CC=DE ASN=AS12586 GHOSTnet GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.230.73.241']

Name

51.83.182.153

Description

ISP: OVH SAS **OS:** None ---------- Hostnames: ---------- Domains: ------ Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDBnTLjX7k1RgvUIkcdJhVZMg hRqoXfa7PZ9w/tSf5Icf6ZVyoY/j2JduylIcyhHC/I5L nTDmyk55iFBpkwiE9yKPNnUTNv+MFn9ukJ5jmqhWX9eyrk/rA gp5+jssC0D5pUYCJVNYG7CAhrkk6MMkFOk6DM+L6ZZV2Rm HqK8cyHdeYZU7tMK7dqGodTUNqBrXYolop3AZWWA 24:d1:be:fd:d2:68:d7:cf:c5:77:ff:1c Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2 group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2 sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.83.182.153']

Name

89.107.10.7

Description

CC=DE ASN=AS199785 Cloud Hosting Solutions, Limited.

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.107.10.7']

Name

94.140.115.44

Description

ISP: Sia Nano IT **OS:** None ---------- Hostnames: - charmainesshop.store ---------- Services: **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 udp 111 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.140.115.44']

Name

45.132.1.238

Description

ISP: Cloud Hosting Solutions, Limited. **OS:** None ---------- Hostnames: ---------- SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCd

Cq3IJ9hv1x3376EouRG4VROqUzLX9OEBSy6cMH03d2/PIwpWrP/hTLes8+NMHsbCG+X5Hzk3zDh3
O0kxNeoIB4waobJyVZ7S4OvG5vNfZDXBzXuUYjDCNitnp7qzlbEoNClOFqGL87kl29u+OPMcF8iy PIcX70jiLQJC1GhlSJ
iBEGuPf1qcZqrYwzPB1NbNGrumHpZFYbYg8YTL1hVUWeC/gwlje5pJ8h+O10PzG6y/xq4RpXWf09 KurtDYgfKnjf2/h
Q9p6BNPYQxp4vsk4O97xVumQY lKazeW/0BJgp65aErJeNvDnjBMwCLra4SbCeTkfK8CKYnSd4Q1zG2eaVhk9dE6A1
84:c2:41:b6:50:7b:46:4a:b8:cf Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-ni
exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha
ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes1
gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2
sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 h
---------- **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Da
timeout=5 Content-Length: 0 ``` ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express
Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.132.1.238']

Name

5.44.42.27

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** Ubuntu ---------- Hostnames: - mexomail-
---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10 Key type: ssh-rsa K
AAAAB3NzaC1yc2EAAAADAQABAAABAQDbY5sGmo5OYZUOXfV6TvyrB4tGEilk6SIvBY7b6E4kYJ5j DqNmPZBodzs2tZ
FPiwn15Sq3IkkqVs0ISFhEBl5GdfWKwdYgofLyLDkKZwHv0KAq 4FxjozqtqQXcUFrdeUDuUCmA7FDH5UaNtdbNckL0
k6z7I9ZiUG+WHMVdMqZOBvWEp1lu3Z7DVJXGOwGI2EzwRuqG+/VI+NW8m9p+/cyHBTLv9hos8SS6 a5eoem/Bzrh
Fingerprint: 80:98:1b:72:aa:38:23:6c:d3:5a:b6:82:22:a2:4d:a9 Kex Algorithms: curve25519-sha256@libssh.org ecd
hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2
Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op
(Ubuntu) 250-mexomail.com 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-STARTTLS 250-AUTH PLAIN LO
``` ---------- **465:** ``` 220 mexomail.com ESMTP (Ubuntu) 250-mexomail.com 250-PIPELINING 250-S
ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` HEARTBLEED: 2023/05/24 19:55:47 5.44.42.27:465 - SAFE ---
```

mexomail.com 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250
IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN AUTH=DIGEST-MD5
REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN AUTH=DIGEST-MD5 A001 OK Pre-login capabilities liste
ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout com
---

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.44.42.27']

Name

5.39.222.150

Description

CC=NL ASN=AS57043 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.39.222.150']

Name

5.252.118.204

Description

Simple indicator of observable {5.252.118.204}

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.118.204']

Name

172.105.235.94

Description

ISP: Akamai Connected Cloud **OS:** Ubuntu ---------- Hostnames: - 172-105-235-94.ip.lin
linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubunt
AAAAB3NzaC1yc2EAAAADAQABAAABgQCkP1VEinVkHOkOflJoXwQ4pcDS4sgGuscDzobrBgNJZQvx KKDmcoH+
+uGSm1qYLAO+gEvQgLVgnID5ABN5OZGPwMh4H3IptfzIpJPhbkmP+QfWS7SZxH14NOjy JiagZ+ubHZy/g19wvp7tzZ
mijhRWg4/XR4mG7a0Cv2jCDYh6ZmIcmy8vlE76nNUe/aC+Be5g9zEVfAd+tQ733TILilxtOLvSvR
TXUkm7jOC3COchKOW74utCpAb+OZEuyyde9TymybY26lZGIEPCAruiQw0MHpO+HxRVT2NZXdGWna
5XT9UoG1VH2boD9ugmXnCmtdZELxfS5eZQuYg5Dsf42IyRfy7Idcxs0MmT4zphIFS43Crd4NYIS9 qgdkmGBHjGkfWC
t6fugtIZcp8= Fingerprint: 1e:46:5d:c9:d4:17:45:04:4f:8c:7d:a3:c4:14:74:ce Kex Algorithms: curve25519-sha256 curv
ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-g
Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: cha
aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac
sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.c
Algorithms: none zlib@openssh.com ``` ---------- **5555:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.105.235.94']

Name
213.109.192.230
Description
CC=IT ASN=AS62005 BlueVPS OU
Pattern Type
stix
Pattern
[ipv4-addr:value = '213.109.192.230']
Name
79.137.197.187
Description
ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - broad-worm.aeza.network -- ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke AAAAB3NzaC1yc2EAAAADAQABAAABgQDu8KmHHS77hBGBwoE8OYHyurKPpcGgCWoJa0Szt4dylRG/ +ZqnvRZom F3IhWgn1rnMkgLqh5E4+Si5mmsBR6zFUfrFApF9ISBUC88R4S875Yww7yF hb4psLR40y9hTC2VX1IZFwV1waHV6ALij MCzHuOC6aGLaxAtvbfEtSxiyO2Ns9Os6G68JaXpF3LmhsOTpOvH9J7B3RZdyYY23yWri7tp0j6d5 lpkJnitGUci1627px vcmNCPZLCBU+mxDXpqH cLJF3abZ9a/1KES/0LZsczwwigN29P5nPuG5Bszkw6f1tQMFyhS0cD7K9Xbk1rh/9f0S55F MSU1rroJKSmJpQO3I9QY2IZkEr0dlKpsbL+qntOYjIGuwBS18nCkxq40xCxxhnUrpW8aJhuLyFrC KIOL24mxyr8= Fing curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2- Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@ umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op
Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.197.187']

Name

77.83.197.138

Description

CC=GB ASN=AS61046 HZ Hosting Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.83.197.138']

Name

139.162.116.148

Description

CC=JP ASN=AS63949 Akamai Connected Cloud

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.162.116.148']

Name

80.66.88.155

Description

ISP: XHOST INTERNET SOLUTIONS LP **OS:** None ---------- Hostnames: ----------
Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: R
80.66.88.155:49152 ncalrpc: WindowsShutdown ncacn_np: \\WIN-344VU98D3RU\PIPE\InitShutdown ncalrpc:
provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-344VU98D3RU\PIPE\InitShutdown nca
WMsgKRpc02FA732 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: dabrpc ncalrpc: LRPC-06c3
\WIN-344VU98D3RU\pipe\LSM_API_service ncalrpc: LSMApi ncalrpc: LRPC-99cf365252b73d737f ncalrpc: actke
v1.0 ncalrpc: LRPC-06c323216e3058d4cc ncacn_np: \\WIN-344VU98D3RU\pipe\LSM_API_service ncalrpc: LSM
umpo c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation: Impl friendly name provider: sysnt
umpo ncalrpc: LRPC-92550a7f542eb51593 ncacn_np: \\WIN-344VU98D3RU\PIPE\srvsvc ncacn_ip_tcp: 80.66.8
\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUse
ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 ncalrpc: IUserProfile2 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e v
a073-73560f8d9e3e version: v1.0 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 vers
af74-7c47cd0ade4a version: v1.0 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938
bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3b338d89-6cfa-44b8
8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: actkernel ncalrpc: umpo 085b0334-e454-4d9
4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: actkernel ncalrpc: umpo 3c4728c5-f0ab-448b-
Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc ncalrpc: dhcpcsvc6 ncalrpc: LRPC-f7cad88b99721bb322 nc
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0
ncalrpc: dhcpcsvc6 ncalrpc: LRPC-f7cad88b99721bb322 ncacn_ip_tcp: 80.66.88.155:49153 ncacn_np: \\WIN-344
abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 annotation: Wcm Service ncalrpc: LRPC-f7cad88b99721
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 a
f7cad88b99721bb322 ncacn_ip_tcp: 80.66.88.155:49153 ncacn_np: \\WIN-344VU98D3RU\pipe\eventlog ncalrpc
annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_
\WIN-344VU98D3RU\pipe\eventlog ncalrpc: eventlog 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57 version: v1.0 ar
LRPC-178ddbfb9338cbf945 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provid
\WIN-344VU98D3RU\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-92550a7f542eb51593
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss
fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: Dev
\WIN-344VU98D3RU\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-92550a7f542eb51593
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss
5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: Devi
\WIN-344VU98D3RU\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-92550a7f542eb51593
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss

201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: Devic
\WIN-344VU98D3RU\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-92550a7f542eb51593
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss
30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-92550a7f542eb5159
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss
1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncacn_ip_tcp: 80.66.88.155
\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUse
annotation: XactSrv service provider: srvsvc.dll ncacn_ip_tcp: 80.66.88.155:49154 ncalrpc: ubpmtaskhostchan
ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 ve
ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED8
e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncacn_ip_tcp:
\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUse
annotation: Proxy Manager provider server endpoint ncacn_ip_tcp: 80.66.88.155:49154 ncalrpc: ubpmtaskhos
ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 552d076a-cb29-4e44-8b6a-d15e59e2c0af
provider: iphlpsvc.dll ncacn_ip_tcp: 80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344
OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version:
80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senss
3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 80.66.88.155:49154 ncalrpc: ubpmtaskhos
ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 86d35949-83c9-4044-b424-db363231fd0c
Protocol provider: schedsvc.dll ncacn_ip_tcp: 80.66.88.155:49154 ncalrpc: ubpmtaskhostchannel ncacn_np: \
OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 378e52b0-c0a9-11cf-822d-00aa0051e40f version:
provider: taskcomp.dll ncacn_np: \\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED872C3D473
1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting
\WIN-344VU98D3RU\PIPE\atsvc ncalrpc: senssvc ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUse
schedsvc.dll ncalrpc: senssvc ncalrpc: OLED872C3D473910BC48EF01BC205A1 ncalrpc: IUserProfile2 2eb08e3e-
Interface provider: gpsvc.dll ncalrpc: LRPC-e7cd1226843849bcb9 b2507c30-b126-494a-92ac-ee32b6eeb039 ve
3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256 annotation: WinHttp Auto-Proxy Service ncacn_np:
ncalrpc: LRPC-20fc0d162007d62aa8 ncalrpc: OLE7AE0AD708B338717CDD2D0C4ECA3 7ea70bcf-48af-4f6a-8968-6
nsisvc.dll ncalrpc: LRPC-20fc0d162007d62aa8 ncalrpc: OLE7AE0AD708B338717CDD2D0C4ECA3 2fb92682-6599-4
MPSSVC.dll ncalrpc: LRPC-cff434ce27cd42435e ncalrpc: LRPC-3935cc6f25c7fae34b f47433c3-3e9d-4157-aad4-83
cff434ce27cd42435e ncalrpc: LRPC-3935cc6f25c7fae34b 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 a
cff434ce27cd42435e ncalrpc: LRPC-3935cc6f25c7fae34b dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 a
LRPC-3935cc6f25c7fae34b 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncac
LRPC-3cf26550817514c9c2 ncalrpc: DNSResolver eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annot
ncalrpc: DNSResolver f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upca
76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote
ncalrpc: LRPC-84a4b8178999fdbe92 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.e
ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notifi
ncalrpc: LRPC-84a4b8178999fdbe92 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]
spoolsv.exe ncacn_ip_tcp: 80.66.88.155:49155 ncalrpc: LRPC-84a4b8178999fdbe92 12345678-1234-abcd-ef00-01
Protocol provider: spoolsv.exe ncacn_ip_tcp: 80.66.88.155:49155 ncalrpc: LRPC-84a4b8178999fdbe92 367abb81
Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 80.66.88.155:49156 12345778-1
Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 80.66.88.155:49159 ncal
protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: lsacap

ncacn_np: \\WIN-344VU98D3RU\pipe\lsass 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: ncalrpc: LRPC-b60d80b256c651643c ncalrpc: LRPC-b60d80b256c651643c ncalrpc: LRPC-b60d80b256c651643c Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc02FA732 9435cc56-1d9c-4924-ac7d-b60a2c provider: sppsvc.exe ncalrpc: SPPCTransportEndpoint-00001 ``` ---------- **137:** ``` NetBIOS Respons \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 1 O 2012 R2 Standard 6.3 Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-write remote-api, unicode ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\ Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN- Computer Name: WIN-344VU98D3RU DNS Domain Name: WIN-344VU98D3RU FQDN: WIN-344VU98D3RU Admi settings to install them. am Windows Server 2012R2 0) ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.88.155']

Name

23.106.123.119

Description

CC=SG ASN=AS59253 Leaseweb Asia Pacific pte. ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.123.119']

Name

fbb221ee4b17929bddc95beac7d2736709cf1a5c161c3139a1cd90c3f2044420

Description

Cabinet_Archive SHA256 of 57157c5d3c1bb3eb3e86b24b1f4240c867a5e94f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fbb221ee4b17929bddc95beac7d2736709cf1a5c161c3139a1cd90c3f2044420']

Name

51.83.189.185

Description

CC=FR ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.83.189.185']

Name

195.133.196.230

Description

ISP: JSC Mediasoft ekspert **OS:** Ubuntu ---------- Hostnames: - ptr.ruvds.com --------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAA DVjFopD9cMfszYSxVKhzRYg vA3SmRLY23PALDQE+hfh/jIo25EzJfwmwLjxMLAuSo4r1260eUJ7N5gERb1JC2tZ5uj91K cJR9lVNglKmcQjbWV/yw1AP5XFvX6bJc+Bn WLGLvChlUnveLQlXX5/GUIJSwTQ8K7ZSpOX9R38TShD7uVIUrvsZwQd iBB6CEVjQNB8+y4wUBV27VEPQbo2cX9VuRcdRpl7/+yWwM7F7PV4feaj1EEBIs/hA2gvxrc50YOg cp+ETw7/ wNnfDxiDYepe9zFBIzvH5jZYrvYDvwUhe7mkc+nhrVem8tWu0r79Vv+UKBxlqTLgsVBe ClypggwCpyrUAB9671wr4Yje xq86ogWAtk= Fingerprint: b4:04:84:d3:01:8b:44:f3:1b:28:05:15:82:39:f2:b8 Kex Algorithms: curve25519-sha256 cu ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-g Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: cha aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.c Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.133.196.230']

Name

157.254.194.225

Description

CC=US ASN=AS29802 HVC-AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.254.194.225']

Name

46.17.98.190

Description

CC=NL ASN=AS57043 Hostkey B.v.

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.17.98.190']

Name

172.104.94.104

Description

ISP: Akamai Connected Cloud **OS:** Debian ---------- Hostnames: - 172-104-94-104.ip.lin
linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb1
AAAAB3NzaC1yc2EAAAADAQABAAABAQCrlN99W+vI3O6LW6WfKd+COcow6EiwWplhKllDYIQdqNfd
IX7rZ+VbYsaTDWI6GLSxVbbohuVCIkbvxNzNDkWZ6LFd8T+MdxNou4ejT3BISf8uk8LvL0EFA9OG nFtBW9JtsJHc8rA7
nYFteMQxGW HNqCyZq4Idbui//4G0ySc5Ewm355vo68pHOigpfO6ydREnHCNFCHap2+vEEEKYUlVbhh7ATRCo+h
Ojp04V7wQsoS+HJzjpw91FDCuf30VLMPF7cJntc6pRFGgumFLNqi0inF72jcwViWuaWP Fingerprint: fc:52:c6:82:a6:c
curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-
group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa
Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@op
etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@
umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@op

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.104.94.104']

Name

85.192.63.13

Description

ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - fusion-carnelian.aeza.netwo ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Ke AAAAB3NzaC1yc2EAAAADAQABAAABgQCkkSQuo+MgACDtrbv+6LSzrZ16u1rYEn26YcayQxJvJGP7 nVDIaHD1dO+wB 8+WyLE66kMSoOo61f+L2jLgbF3Ik8GzsxYc A6CLpEPxG1+g6NRcPwYTx7uSBOVfDahEZcjsJ7MJL8pmy5O40uLjM9xJF UWSQV9ta+Clz9HUoIWV4IrvkiOpL7c2jO+bTskyOkXKHMzHfwhP9+7q dymjQoGiwIRX1Cza4F799CVEqHLFhqrJIymz GmPVQVPPZ8MoD7axfkxyBNvRyXo49q6CkKrdP8zhc1LysGyD/3oKFFYkBqmarUcSZn04pcUbSQQ4 hjovVLQo0nY5 wyeKcuoMrspHCYWS7 eYtHF6yecTs= Fingerprint: 5c:2e:54:a6:08:63:55:e8:03:9a:99:b0:41:1e:37:be Kex Algorithms nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-gro sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Enc aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh. sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Serve Type: text/html Content-Length: 612 Last-Modified: Sun, 09 Apr 2023 21:55:43 GMT Connection: keep-alive ETa NTP protocolversion: 3 stratum: 0 leap: 3 precision: 0 rootdelay: 0.0 rootdisp: 0.0 refid: 1380013125 reftime: 0 Spigot 1.12.2 (Protocol 340) Description: A Minecraft Server Online Players: 0 Maximum Players: 20 ``` --------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.192.63.13']

Name

109.107.173.72

Description

ISP: Hosting technology LTD **OS:** None ---------- Hostnames: - v1600239.hosted-by-vd ---------- Services: **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-A alive Keep-Alive: timeout=5 Content-Length: 0 ``` ---------- **3000:** ``` HTTP/1.1 404 Not Found X-Pow 2023 02:15:15 GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.107.173.72']

Name

5.252.118.132

Description

CC=NL ASN=AS210644 AEZA GROUP Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.252.118.132']

Name

98.142.251.26

Description

CC=EE ASN=AS62005 BlueVPS OU

Pattern Type

stix

Pattern

[ipv4-addr:value = '98.142.251.26']

Country

Name
Armenia

Malware

Name
CobaltStrike

Name
Nodebot

Name
Ahkbot

Domain-Name

Value
namesilo.my.id
snowzet.com

StixFile

Value
a7f7cc2bdbe5ac6d55841bcfb0ada2c0e55192af5f70dcdda68e7fd17112346a
53e4bfd27474f6e4829ac4d625d3d914452456baf5da2c1c51e2e6df35ab634a
fbb221ee4b17929bddc95beac7d2736709cf1a5c161c3139a1cd90c3f2044420

IPv4-Addr

Value
5.255.88.222
5.230.73.250
98.142.251.26
46.151.25.49
5.39.222.150
79.137.197.187
212.118.43.231
146.70.79.117
5.252.118.204
5.230.73.241
77.83.197.138
193.109.69.52
172.86.75.49

104.248.149.122
45.147.229.20
98.142.251.226
85.192.49.106
85.192.63.126
79.137.196.121
94.140.115.44
212.113.116.147
94.232.41.108
5.230.72.148
172.104.94.104
195.2.81.70
176.124.217.20
62.204.41.171
62.84.99.195
94.232.41.96
94.232.43.214
5.230.73.57

45.132.1.238
157.254.194.225
46.151.24.197
46.151.25.15
45.76.211.131
85.192.63.13
185.70.184.44
5.44.42.27
91.245.253.112
212.113.106.27
46.151.28.18
51.83.189.185
157.254.194.238
185.123.53.49
109.107.173.72
5.230.72.38
194.180.174.51
5.230.73.63

88.210.10.62

89.107.10.7

146.0.77.15

104.234.118.163

85.239.60.40

172.105.253.139

195.133.196.230

89.41.182.94

139.162.116.148

94.140.114.230

23.106.123.119

80.66.88.155

5.230.73.248

5.230.71.166

94.140.114.133

51.83.182.153

213.109.192.230

185.163.45.221

46.151.24.226

185.82.126.133

94.103.83.46

185.150.117.122

5.230.73.247

5.252.118.132

31.192.105.28

5.230.68.137

172.105.235.94

46.17.98.190

176.124.214.229

External References

- https://www.welivesecurity.com/2023/06/08/asylum-ambuscade-crimeware-or-cyberespionage/
- https://otx.alienvault.com/pulse/648321ebdebe7ec1bfb04001