Jun 27 2024

NETMANAGEIT

Intelligence Report

Armageddon is more than a Grammy-nominated album

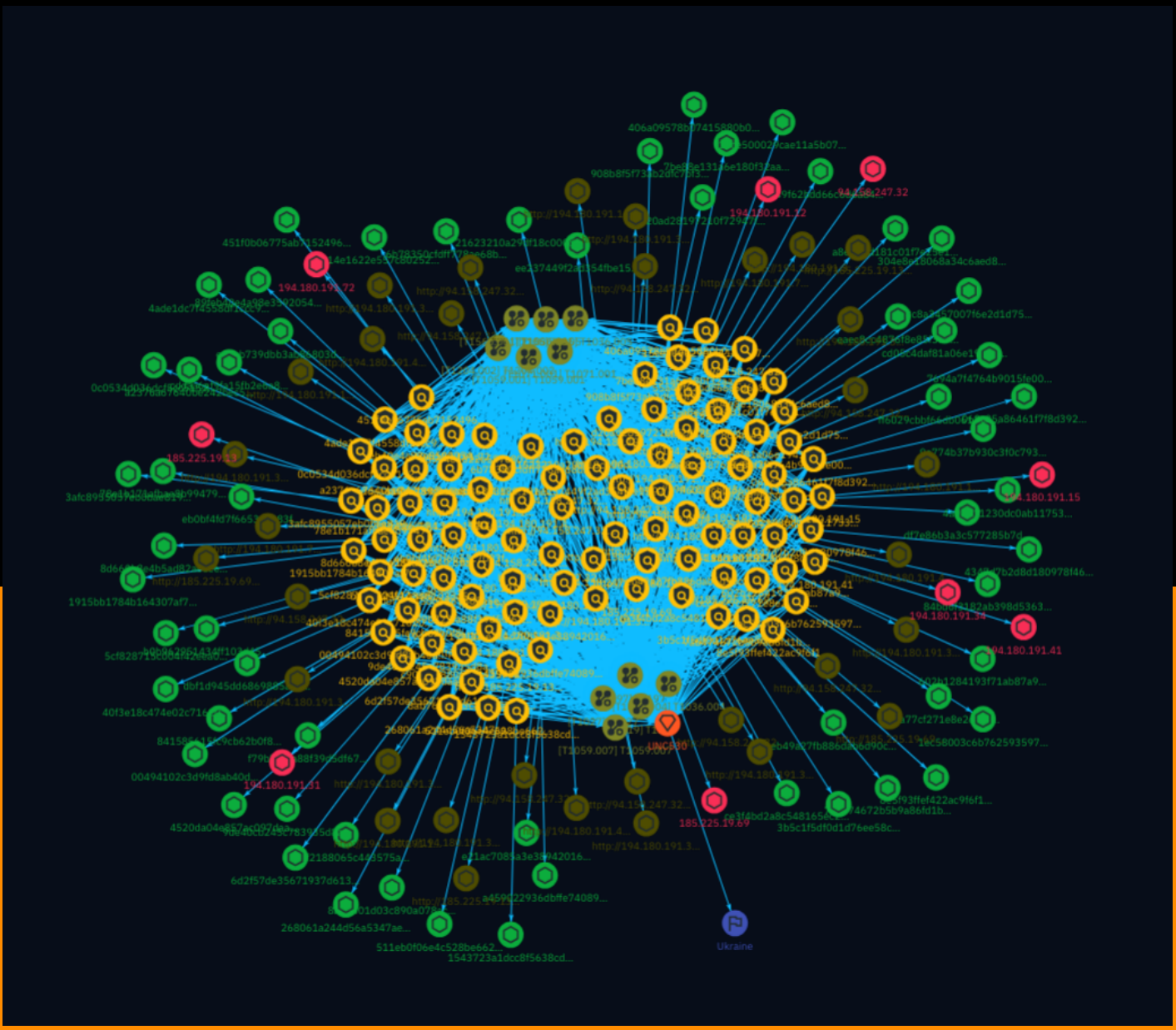

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details a Russia-linked threat actor targeting Ukraine, employing various obfuscation techniques. The malicious activity involves dropping a compressed file disguised as a RAR archive, which fetches a remote image likely for tracking execution. The payload employs mshta.exe to execute remote content and leverages LNK files with crafted filenames. The techniques suggest an effort to evade detection and hamper analysis.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1036.005
ID
T1036.005
Description
Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous. Adversaries may also use the same icon of the file they are trying to mimic.
Name
T1197
ID
T1197

Description

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM) (Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations. The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool. (Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin) Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)), execute, and even clean up after running malicious code (e.g. [Indicator Removal](https://attack.mitre.org/techniques/T1070)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots). (Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016) BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

Name

T1059.007

ID

T1059.007

Description

Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS) JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows

Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts) JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple's Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple's OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple's internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility `osascript`, they can be compiled into applications or script files via `osacompile`, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016)(Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode) Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

Name

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic 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. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1204.002

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) 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).

Name

T1027

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

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the

service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1560.001

ID

T1560.001

Description

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport. Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as `tar` on Linux and macOS or `zip` on Windows systems. On Windows, `diantz` or ` makecab` may be used to package collected files into a cabinet (.cab) file. `diantz` may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)). (Citation: diantz.exe_lolbas) `xcopy` on Windows can copy files and directories with a variety of options. Additionally, adversaries may use [certutil](https://attack.mitre.org/software/S0160) to Base64 encode collected data before exfiltration. Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities. (Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary-controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome’s Remote Desktop).(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

Name

T1036.004

ID

T1036.004

Description

Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description.(Citation: TechNet Schtasks)(Citation: Systemd Service Units) Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones. Tasks or services contain other fields, such as a description, that adversaries may attempt to make appear legitimate.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Fysbis Dr Web Analysis)

Indicator

Name
http://94.158.247.32/moh.17.04
Pattern Type
stix
Pattern
[url:value = 'http://94.158.247.32/moh.17.04']
Name
a2376a67640be242bec5c9ffe46822abab2361f7210a8d9ad6333df45e67117f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a2376a67640be242bec5c9ffe46822abab2361f7210a8d9ad6333df45e67117f']
Name
http://94.158.247.32/sb.15.04

Pattern Type
stix
Pattern
[url:value = 'http://94.158.247.32/sb.15.04']
Name
http://194.180.191.34/gps.19.04
Pattern Type
stix
Pattern
[url:value = 'http://194.180.191.34/gps.19.04']
Name
15ce500029cae11a5b07ed654faa371ef0bb0eb9add630a1e03c58606ea35eb9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '15ce500029cae11a5b07ed654faa371ef0bb0eb9add630a1e03c58606ea35eb9']
Name
http://94.158.247.32/odd.15.04

Pattern Type

stix

Pattern

[url:value = 'http://94.158.247.32/odd.15.04']

Name

185.225.19.69

Description

ISP: MivoCloud SRL **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDVem7yI7oLWbWXwB2UNi0YQ2eI+Vyqjv3mzQ3IUPHMyRJc VbbIJKyuCDZpu4U7u+dHoCGsf2rtaQDXoo80skP5eIIFdilQxapVIpcMwuyB+RjlNHZ0eS1eWbSm BqHy3ZYhmfdpMkWxSn+a8JycnazH+EBlg22uD+cpvDRvncE6NGpIA2wWtN7oB9SLKKMeK6O1h5/J lQHngz+E+s67ocK2x5IW2W5FCCiYg51YkDNw/AaAhQg36a1OpbdW6prm1JJ4RpBZ2xX4WJgmKoDj 5hx0PYLdypdip5EEYxWvL+qUyUrXv22zon+4CwRVUJ/30w4PaImWBwW2UEYYMGKXzUM3 Fingerprint: df:7d: 31:59:d7:35:79:68:1c:4f:24:cb:5a:2e:97:f8 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.c hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 17 Jun 2024 21:27:23 GMT Server: Apache/2.4.6 (CentOS OpenSSL/1.0.2k-fips PHP/7.1.33 X-Powered-By: PHP/7.1.33 Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` ---------- **111:** ``` Portmap Program Version Protocol Po portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 11 portmapper 2 udp 111 ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 t 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 u 111 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.225.19.69']

Name

http://194.180.191.12/od.04.06

Pattern Type

stix

Pattern

[url:value = 'http://194.180.191.12/od.04.06']

Name

1ec58003c6b7625935976bdfdf7d4a11228a57b32ce1eeece68a1ab48536bbc0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ec58003c6b7625935976bdfdf7d4a11228a57b32ce1eeece68a1ab48536bbc0']

Name

http://194.180.191.31/odes/relief.tmp

Pattern Type

stix

Pattern

[url:value = 'http://194.180.191.31/odes/relief.tmp']

Name

7694a7f4764b9015fe00f68cd75d06f7dae77fd64c58c9bcb83fd8196cc17d4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7694a7f4764b9015fe00f68cd75d06f7dae77fd64c58c9bcb83fd8196cc17d4b']

Name

http://194.180.191.31/zaliz.23.04

Pattern Type

stix

Pattern

[url:value = 'http://194.180.191.31/zaliz.23.04']

Name

8c8a3457007f6e2d1d75715d21b0423e9c6b90fd2e62f7b4398180017e3f768f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c8a3457007f6e2d1d75715d21b0423e9c6b90fd2e62f7b4398180017e3f768f']

Name

http://194.180.191.12/od/barren.7z

Pattern Type

stix

Pattern

[url:value = 'http://194.180.191.12/od/barren.7z']

Name

194.180.191.12

Description

ISP: MivoCloud SRL **OS:** Ubuntu ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDLtta0yxm7jWeJn6YwBZJpOcmQ9NF0gezvKM8tjsZSMsHF FSsppivnf56fMil3AMedpwJLqJMGJ0nCGeePVrXtCCP1/bBpj/GMYPGlZvJ5jBESdNk4V3iPvZrK hIaTvL7gY3Qqf4R0bOumyXtZfDQdAh8ulNGVj0seWnpylSnhvSMZ0Y4TcVu8yFomHcaQuTXXNK41 yZjC1vLQzU6M+MlBaJkZcPXJ8VdWR/OvQoRyCNR7kcj0EbARNswXoGKw5qPMq0zVOMPXouxV7XR1 NHL1PN6KI3Crhhd6kr09h0yzp0gt4tGJ3//dlm/bIY2JauelBabzgAbplK6tsrNRDSdv8mUED5PG rD7wrSuHak9FvaclnH9YoJtRm0nzn8gR0+VHh1oW7JOHVfl1/Rfe3K2qYSeIn2JoqfeLqQS0H0Sp H1GxnGT/ RL4DQzahR7F0D+WuEdvOXdVjffGU6wcNA4gIXWNtANxbeMSPbkFYpTDMI9WKifRzQBGh OT5FHidkCUE= Fingerpr a8:24:d8:fc:aa:9c:0a:19:0b:45:90:e2:19:0a:f2:76 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.o ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-

gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 (Ubuntu) Date: Tue, 25 Jun 2024 03:36:22 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://concurs.api.md/ ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Tue, 25 Jun 2024 03:36:25 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding link: ; rel=preload; as="font"; crossorigin=""; type="font/woff2" X-Powered-Next.js Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate Strict-Transport-Security: ma age=31536000; preload Access-Control-Allow-Origin: * Access-Control-Allow-Headers: Content-Type P3P: CP="NON CUR OTPi OUR NOR UNI" Content-Security-Policy: upgrade-insecure-requests ``` HEARTBLEED: 2024/06/25 03:36:31 194.180.191.12:443 - SAFE ---------- **5000:** ``` HTTP/1.1 404 NOT FOUND Server: gunicorn Date: Sun, 16 Jun 2024 20:05:56 GMT Connection: close Content-Type: text/html; charset=utf-8 Content-Length: 207 Access-Control-Allow-Origin: * ``` ---------- **5001:** ``` HTTP/1.1 200 OK Vary: RS Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding link: ; rel=preload; as="font"; crossorigin=""; type="font/woff2" X-Powered-By: Next.js Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate Content-Type: text/html; charset=utf-8 Date: Wed, 12 Jun 2024 09:39:20 GMT Connection: keep-aliv Keep-Alive: timeout=5 Transfer-Encoding: chunked 1cda

Concursuri Active

Concursuri Anteriaore

Regulamente

Concurs de ESEURI/POEZII, DESENE/ CARICATURI/POZE și VIDEO/ ANIMAȚII

În perioada 26 iulie–21 august 2022 lucrările elevilor și elevelor acceptate la concurs au fost afișate pe acea platformă online, iar orice vizitator a putut vota, la una sau mai multe secțiuni diferite, având posibilitatea acorde în decurs de 24 de ore cel mult câte un vot pentru fiecare din cele trei categorii.

Despre Concurs

Participa >

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industrys standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release o Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

+OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN DIGEST-MD5 CRAM-M . ``` HEARTBLEED: 2024/05/28 01:53:07 194.180.191.31:995 - SAFE ---------- **8443:** ``` HTTP/1.1 200 OK Server: sw-cp-server Date: Fri, 07 Jun 2024 11:46:10 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Expires: Fri, 28 May 1999 00:00:00 GMT Last-Modified: Fri, 07 Jun 2024 11:46:10 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA" X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff ``` HEARTBLEED: 2024/06/07 11:46:27 194.180.191.31:8443 - SAFE ---------- **8880:** ``` HTTP/1.1 303 See Other Server: sw-cp-server Date: Mon, 10 Jun 2024 07:30:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Expires: Fri, 28 May 1999 00:00:00 GMT Last-Modified: Mon, 10 Jun 2024 07:30:32 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache P3P: CP="NON COR CURa ADMa OUR NOR UNI COM NAV STA" X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Location: http://194.180.191.31/login.php X-Content-Type-Options: nosniff 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.180.191.31']

Name

4a98d11230dc0ab117534f78a9d626b754c0c9d7957a8d343a8f0e7a332f68ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a98d11230dc0ab117534f78a9d626b754c0c9d7957a8d343a8f0e7a332f68ce']

Name

451f0b06775ab715249635fc6930db45bfa4bd343f448b33a49f4941653a7315

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '451f0b06775ab715249635fc6930db45bfa4bd343f448b33a49f4941653a7315']

Name

194.180.191.15

Description

ISP: MivoCloud SRL **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC1eYznz5PjvQX5zwB4uiVMIEvF 3oTZxcmQbeUmu30T/ GwaI0hWUojTyQQLJ3c2B3kiipz7RsPokwvwHqhBs3NgzIgA0VR/3C959Mf5fwU/TBfZ0h+ +UFbcj W/kQHBJPG2zc6xMrUV4VcN1eSgzh1sfuJjR7zFKGIBXcKyDubZ1urIjAMsNyuVwE4WGae0J0SEoS 7ZABZhS4C00pTtmvVUNMDVufeW20SiOH287B9oeNVAz44ToosFgnMUPj9w+Z1hvuzum1lW46Dfcl rHB9APZIVfYc91FY7NzPyJCWWcKMMNO/dk1cyyiU6FDsgX2Yc4o9/jmh/eptqu/McIEK101yfTeC +1fPN6pJahxqV7QgBnPV4gK2Up31xh9BgJk0pvWPs4GT1qRitXpzJ0YuECpNzf1+fFEn5veMka3e / SeXWC6GhhkhY4r2/6VY4e0JbQoBXsXtWteuo6A4jxQ7B5IzMV7Kc4OgtVVLDGctygvvBh6n6mkj Us9Ngk2dV1E= Fingerprint: 02:f2:a2:bc:ef:75:30:f4:3d:d2:ff:02:79:a6:4c:45 Kex Algorithms: curve25519-sha256@libssh.org ecdh-

sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group-exchange-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-gcm@openssh.com aes256-ctr aes192-ctr aes128-ctr MAC Algorithms: hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512 hmac-sha2-256 umac-128@openssh.com Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jun 2024 03:07:25 GMT Content-Type: text/html Content-Length: 1658 Connection: keep-alive Last-Modified: Thu, 23 May 2024 19:04:22 GMT ETag: "67a-61923b802b980" Accept Ranges: bytes ``` ---------- **465:** ``` 220 interesting-cori.194-180-191-15.plesk.page ESMTP Postfix 250 interesting-cori.194-180-191-15.plesk.page 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING ``` HEARTBLEED 2024/06/11 20:23:55 194.180.191.15:465 - SAFE ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '194.180.191.15']
Name
ce3f4bd2a8c548165ec2a0f41d0bbd1ad5e87a2aebc026e82f15c956ba51ed3d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ce3f4bd2a8c548165ec2a0f41d0bbd1ad5e87a2aebc026e82f15c956ba51ed3d']
Name
185.225.19.13

Description

ISP: MivoCloud SRL **OS:** Linux ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC6k/ L3ZQT2fkhpzgZl0grZLKyp7aqtoCB33lgk6xMr4E2v iCWVRYeq1qiNxthLAsZBp2rAeZmqD3WssN6Uieqgaln4Y56NBaseouTgbFtmUBnUVcZURGD5pJ9r 7OC2jVGJUlCGhLRf11A8CXjvaAUgHawVoqNzWQWm9PqscWhqg0bKHKbO9VFcpHrgXqjsBhRUxsi/ A10ET2gwnsXl1wZ/oXMCxtXRkCYMxxVbylv7IMLOop6yih/Xfc3w6DUC+SsyaRyO6M0IHzlJxeHk OBf+io7fIelFtp4am00JB43E0cTFgr5ikBfIOrV8bjb/ybc+wlKzlHPi40zLozPEHrhjccQ2u/E/ Rx/ A+heVqJDnsqMrcjW2jf5ucmI8EP99SSh4uHkOn6mR2w/t7BeMVE4WBdzkJEVg106RO8IpH1ch 5R2x6IfaPkQ7+z/ hdy1JKI2XlnIZ00m9acAHXoTzb+Ui4V2iOxFQ9LlJ04NXpqG5KqcZfD6QQu+0 oKLaDH9+HeU= Fingerprint: 68:3b:fd 40:3a:78:c0:6b:e1:01:53:1d:9a:4c:99:45 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp521 ecdh sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group-exchange-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-gcm@openssh.com aes2 ctr aes192-ctr aes128-ctr MAC Algorithms: hmac-sha2-512-etm@openssh.com hmac-sha2-256-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512 hmac-sha2-256 umac-128@openssh.com Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, Jun 2024 20:17:00 GMT Server: Apache/2.4.59 (Debian) Content-Length: 0 Content-Type: text/html; charset=UTF-8 ``` ---------- **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 1 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.225.19.13']

Name

406a09578b07415880b035cb8afd688465ffd28a9c7c46680987295ce50d8840

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '406a09578b07415880b035cb8afd688465ffd28a9c7c46680987295ce50d8840']

StixFile

Value
89feb40e4a98e3592054dbd8c4d47a9edbeb308659cf4d1ef9e3deba6f38a698
6b78350cfdff778ae68b47980deeb8841d0a8a2488eb3cb6ce500758df66544e
eb0bf4fd7f6653c7083f3e691d566cecc0049e94308f54c8d64af34a54bc78a1
3afc8955057eb0bae819ead1e7f534f6e5784bbd5b6aa3a08af72e187b157c5b
8c8a3457007f6e2d1d75715d21b0423e9c6b90fd2e62f7b4398180017e3f768f
908b8f5f73ab2dfc7bf3070868d219d1b45f8e2d1f560162dddfd6ce19ed7592
6d2f57de35671937d6134bf4d2fdbfe6310a6b184dceecdeaa7f4583eb0ab6f6
451f0b06775ab715249635fc6930db45bfa4bd343f448b33a49f4941653a7315
df7e86b3a3c577285b7d00671b93c759cf973a90f2cce0cbff1ace7247015c30
00494102c3d9fd8ab40d8e7b3f8a1d4e30876257c18c45761922edf938970719
eb49a27fb886dab6d90cb5f68e9c753ae408ee656aa942bebe7ac5b2fc68891a
cddaa6af9fa15fb2e6a8bfffab0fade552331cedac28a179ee9f49dfef37aea1
3b5c1f5df0d1d76ee58cf859557f03df35692f2a57d10c111ebdec9f69ac4b34

dbf1d945dd6869885a5effcda12e81a626079fb9bb66ede8bb58c3e5539465d2

8ab7601d03c890a078ac9f8763c950b24b5908cb76559110a65dc1d2e4385097

9e774b37b930c3f0c79311f6de448bc5602e16edfef92f4ff09645f27217cdea

1ec58003c6b7625935976bdfdf7d4a11228a57b32ce1eeece68a1ab48536bbc0

4520da04e857ac097daa03500ed553ed49ec00e6fc0f349b977a11bbe1ec0924

0c0534d036dcf5cc5152b2dcb03e837b5bf8c66481d283bd637373cd49b66f7f

55a49f62bdd66c6d6a84f476aa0f64a9b27376164ae1875e273ce9bec2eb7f43

cd05c4daf81a06e1941833734b20c1b2427e9cbf9b86c1c7fc6515f27932970b

841585615fc9cb62b0f8410f1a4df38e7d11cc4b48c54e75dcdc051e9308257e

1543723a1dcc8f5638cd43c5882f132b554c248b334473098fc49ae007e8ee4e

268061a244d56a5347ae66364f6a1cf6ab5654d19086fae6d5607b95d8fc793c

21623210a29df18c000dbf3fcc5bb4885e8a03915f47b152a93a07f66eb2e90f

406a09578b07415880b035cb8afd688465ffd28a9c7c46680987295ce50d8840

ee237449f2ad354fbe15e9505a96f6682dd66ca8277e93c7424c751d6da201ff

8e5f93ffef422ac9f6f19b840509aba5ae88aa39d846c1e40f04b26c4d20cf79

304e8e18068a34c6aed82d0ad744f94687c08842a51e525a87d22a65db2334e5

bd514e1622e557c80252bd000060e8221c651e485a43e795fce47ab60a1d8468

9de40cb245c783935d8a7c809262f91f6a511baed67d758b7c48de7b3505e7b0

a459022936dbffe74089f1ed8160303f1fe909ff459842397d507c0b198a5ee1

4a98d11230dc0ab117534f78a9d626b754c0c9d7957a8d343a8f0e7a332f68ce

e18cb739dbb3ab86803db71bf93d407a8bbabfa836eabc85a3133dfc126eb94b

c901f2188065c443575a84249ce012faa735657b79e6dd5dc6697358d59fb574

ff6029cbbf66db06113a576533d2fdca734c4a44338625cbf58929c9ee87e26a

eaec8cc4876f8e85f387cee5f1443ae48858f7b5b36be395ea0c139c1367d8de

78e1b171afbae8b994792bb33a0bf41f39d596def43a6b3e1ac28d7dd27bb8ca

15ce500029cae11a5b07ed654faa371ef0bb0eb9add630a1e03c58606ea35eb9

bccaa77cf271e8e2c4aaf9982154e8166445c05274d3f58a8352b5daf0ffa3c9

40f3e18c474e02c71620c611e2e3827793d7f07d26cc49396be500baa37dc872

511eb0f06e4c528be6627d537b118bf4932f5a90adc81a3e986beea90f14fe77

5cf828715c004f42eea066b4935511ecb42a4e150235faee482b06904af83cc7

7ab474672b5b9a86fd1b00ab6ec5d2164ecab9cf846ebccb65202ed68d65eaf1

602b1284193f71ab87a9b8d656bfd858f113e2f1a9d85d8331740d2c852a075b

4ade1dc7f4558df1ccc96433e5b26872ab283fcd39e4a3f070480ea62d3e9f30

8d660b8e4b5ad82aeeee594545d400483662630d301e832ee35627695a746f95

4347d7b2d8d180978f4646ccc457be2de0d0c7db84896e1bcd250d2d834a37b1

84bd6f3182ab398d5363fd6b8a375641e08c57318225714a618ffb6b6b10aefb

a2376a67640be242bec5c9ffe46822abab2361f7210a8d9ad6333df45e67117f

a8e291d181c01f7e25e14910b60755d0d439ab1d8616ce0e122514b3fed3dc52

1915bb1784b164307af70a70e3264cfe3bc3c82c43e49da59c0c592d4d29af43

b0b962951434ff103d45db66096e04d468c757379081e6ef534da800ed6a6cef

7694a7f4764b9015fe00f68cd75d06f7dae77fd64c58c9bcb83fd8196cc17d4b

062c25a86461f7f8d392e93bd97836773a889adbdbac9d2ce11e65860a4f2af2

f79b723fa88f39d5df67f2517b088a12b490673fa07d6a2b35275f7dc573172e

e21ac7085a3e38942016f3cb8db4d2f3ba0e7846c7ffb0cc7eb1d2bc0953d6d4

ce3f4bd2a8c548165ec2a0f41d0bbd1ad5e87a2aebc026e82f15c956ba51ed3d

d20ad28197210f72947f4f14e6a5dd6aafcbf4309d46e8a1bf7f18d107784b77

7be88e131a6e180f32aab59734be70ac57d773c5b68bd7919dd32f6f6f9b3de1

External References

- https://blog.strikeready.com/blog/armageddon-is-more-than-a-grammy-nominated-album/
- https://otx.alienvault.com/pulse/667bceea6851fd16532946b9