Jun 10 2023

NETMANAGEIT

Intelligence Report

Stealth Soldier Backdoor Used in Targeted Espionage Attacks in North Africa

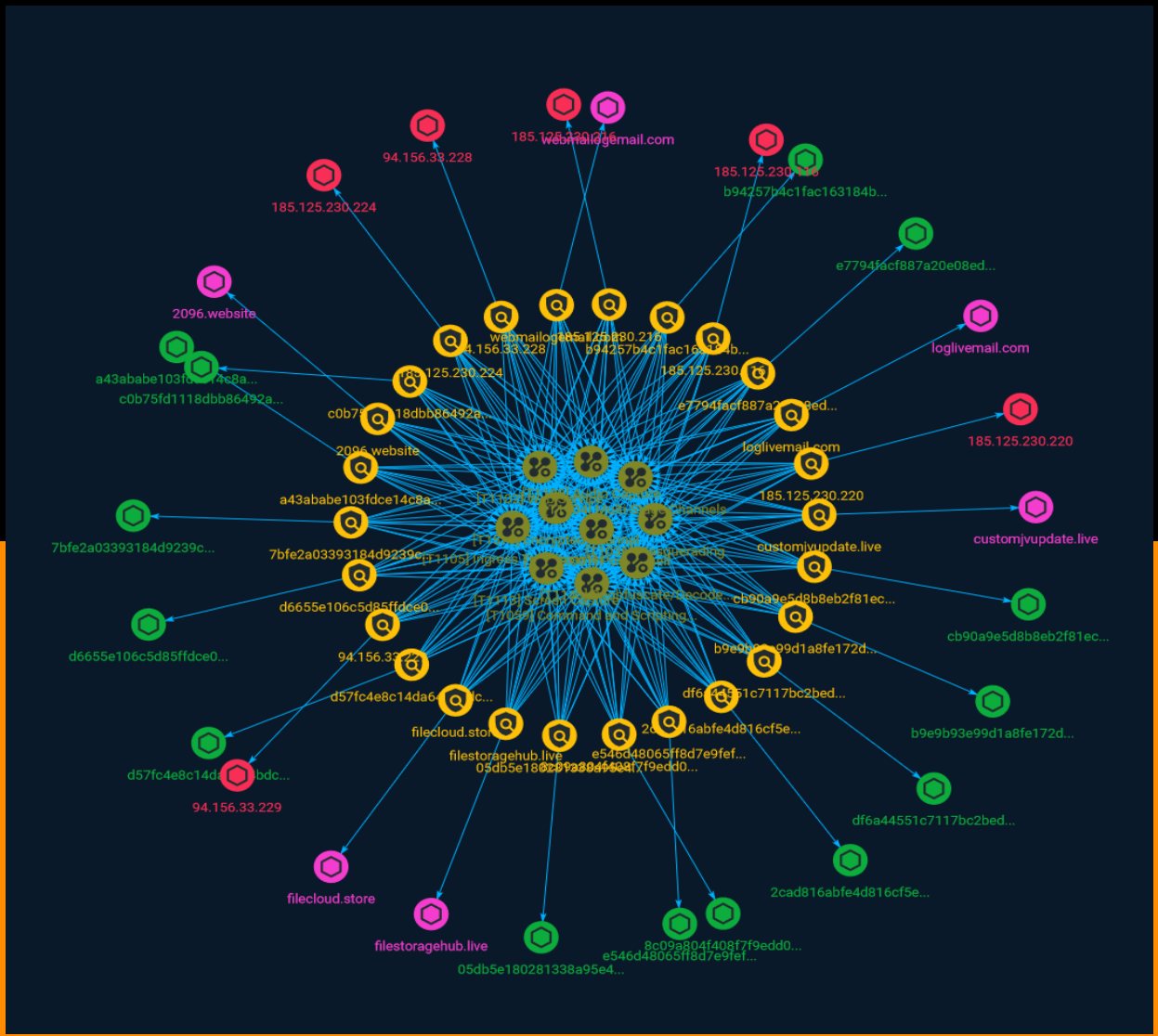

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers identified an ongoing operation against targets in North Africa involving a previously undisclosed multi-stage backdoor called Stealth Soldier. The malware Command and Control (C&C) network is part of a larger set of infrastructure, used at least in part for spear-phishing campaigns against government entities. Based on what they observed in the phishing website themes and VirusTotal submissions, the campaign appears to target Libyan organizations.

Confidence

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

15 / 100

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
Name
Encrypted Channel
ID
T1573
Description

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

Name

Audio Capture

ID

T1123

Description

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

Name

PowerShell

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

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). 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) 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)

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

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

Web Service

ID

T1102

Description

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

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

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)

Indicator

Name

2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb']

Name

a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974']

Name

e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f']

Name

filestoragehub.live

Pattern Type

stix

Pattern

[domain-name:value = 'filestoragehub.live']

Name

94.156.33.228

Description

ISP: Amarutu Technology Ltd **OS:** None ---------- Hostnames: - zetfilmeonline.net - cpcontacts.zetfilmeonline.net - mail.zetfilmeonline.net - webdisk.zetfilmeonline.net - mail.94-156-33-190.cprapid.com - cpanel.zetfilmeonline.net - webmail.zetfilmeonline.net - cpcalendars.zetfilmeonline.net - zetfilmeonline.net.voxfilmeonline.net - 94-156-33-190.cprapid.com - www.zetfilmeonline.net.voxfilmeonline.net - www.94-156-33-190.cprapid.com - www.zetfilmeonline.net ---------- Domains: - zetfilmeonline.net - voxfilmeonline.net - cprapid.com ---------- Services: **21:** ``` 220----------

Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 22:43. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 530 Login authentication failed 214-The following SITE commands are recognized ALIAS CHMOD IDLE UTIME 214 Pure-FTPd - http://pureftpd.org/ 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV ESTP 211 End. ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCmgzNO2tKI3F5mEtwwZPzl7AKkGPviUYrAfU8VDxA8ExApHphc2lQU9RbCLUexcPNRgGY5oyG6NVHnYqd70AyI4LSKBMaaAgeWvXiKefGWDD3x9cvF2VPwyjYUH6GpFlQzAuW7WVZu21z2nZd4wTZ9B8oew2dEZ4fqGzCcJrDvQnEBAKOrQkdMeawR/lebAyMzfTCBCtg0iwBDLKRUat8Hj5il+aUaYqpuiX4dFuLb4u2dUmIOxpN9xvGcrZQ6R9qL4bnmadVIbxTV4wf15xhGHrsw4yh3YRPlb1ApjB2NslrRpUY1iby2gebXQVYKulO0vqg+CsFRzp9eZtACIchsnsadg9Arc+oc2gqppCY3nl1sWJrQt6csEHlx7Hx3PWYPsIp+mCC4uSieDKcxXjfs3UXyKM+hny4pRzV6AabBbhVkz5AxJLTThj7pgmPWmR65BvflA1o1eAGrHRfENyuuWxd6AU3lDSjHw02QxSz9VvOsOEAaiDtfpzdf1mZgGCk= Fingerprint: b3:f2:2c:40:76:c5:08:fc:c2:d6:93:31:1b:81:ea:a8 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **53:** ``` PowerDNS Authoritative Server 4.7.2 (built Dec 9 2022 10:19:47 by root@bh-centos-8.dev.cpanel.net) Resolver ID: 94-156-33-190.cprapid.com ``` ---------- **53:** ``` PowerDNS Authoritative Server 4.7.2 (built Dec 9 2022 10:19:47 by root@bh-centos-8.dev.cpanel.net) Resolver ID: 94-156-33-190.cprapid.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html; charset=UTF-8 link: ; rel="https://api.w.org/" etag: "12918-1685585799;;;" x-litespeed-cache: hit transfer-encoding: chunked date: Thu, 01 Jun 2023 07:13:58 GMT server: LiteSpeed ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN . ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ```

---------- **443:** ``` HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html; charset=UTF-8 link: ; rel="https://api.w.org/" etag: "14468-1685759128;;;" x-litespeed-cache: hit transfer-encoding: chunked date: Sat, 03 Jun 2023 10:44:00 GMT server: LiteSpeed alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" ``` HEARTBLEED: 2023/06/03 10:44:04 94.156.33.228:443 - SAFE ---------- **587:** ``` 220-94-156-33-190.cprapid.com ESMTP Exim 4.96 #2 Wed, 07 Jun 2023 02:15:08 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-94-156-33-190.cprapid.com Hello 224.48.158.159 [224.48.158.159] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-STARTTLS 250 HELP ``` ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` HEARTBLEED: 2023/05/24 12:43:17 94.156.33.228:993 - SAFE ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/05/28 18:31:55 94.156.33.228:995 - SAFE ---------- **2077:** ``` HTTP/1.1 302 Moved Date: Mon, 05 Jun 2023 05:50:56 GMT Server: cPanel Persistent-Auth: false Host: 94.156.33.228:2077 Cache-Control: no-cache, no-store, must-revalidate, private Connection: close Location: https://94-156-33-190.cprapid.com:2078/ Vary: Accept-Encoding Expires: Fri, 01 Jan 1990 00:00:00 GMT X-Redirect-Reason: requiressl ``` ---------- **2082:** ``` HTTP/1.1 301 Moved Content-length: 123 Location: https://94-156-33-190.cprapid.com:2083/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2083:** ``` HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Wed, 31 May 2023 22:17:28 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: cpsession=%3avDpK5lBkNMS7814f%2c77ef671e3ee027ab60fc47f55d399a60; HttpOnly; path=/; port=2083; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2083; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: imp_key=expired; HttpOnly; domain=94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970

00:00:01 GMT; path=/; port=2083 Cache-Control: no-cache, no-store, must-revalidate, private X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 37216 ``` HEARTBLEED: 2023/05/31 22:17:40 94.156.33.228:2083 - SAFE ---------- **2086:** ``` HTTP/1.1 301 Moved Content-length: 123 Location: https://94-156-33-190.cprapid.com:2087/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2087:** ``` HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Fri, 09 Jun 2023 01:58:34 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: whostmgrsession=%3a_E7DYftc7_iOGjue%2ccc4bcb88457589f0eb9fafdbeb5c1484; HttpOnly; path=/; port=2087; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2087; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: imp_key=expired; HttpOnly; domain=94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.228; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Cache-Control: no-cache, no-store, must-revalidate, private X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 36883 ``` HEARTBLEED: 2023/06/09 01:58:42 94.156.33.228:2087 - SAFE ---------- **2095:** ``` HTTP/1.1 301 Moved Content-length: 123 Location: https://94-156-33-190.cprapid.com:2096/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2096:** ``` HTTP/1.1 301 Moved Content-length: 122 Location: https://94-156-33-190.cprapid.com:2096 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache ``` ---------- **3306:** ``` MySQL: Error Message: Host '224.133.106.32' is not allowed to connect to this MySQL server Error Code: 1130 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.156.33.228']

Name

b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e']

Name

d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885']

Name

185.125.230.116

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.125.230.116']

Name

8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946']

Name

c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6']

Name

customjvupdate.live

Pattern Type

stix

Pattern

[domain-name:value = 'customjvupdate.live']

Name

d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db']

Name

185.125.230.216

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.125.230.216']

Name

df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4']

Name

7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd']

Name

loglivemail.com

Pattern Type

stix

Pattern

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

Name

05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc']

Name

185.125.230.224

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.125.230.224']

Name

cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a']

Name

94.156.33.229

Description

ISP: Amarutu Technology Ltd **OS:** None ---------- Hostnames: - topfilmeonline.net - 94-156-33-190.cprapid.com - www.topfilmeonline.net - www.94-156-33-190.cprapid.com - mail.94-156-33-190.cprapid.com ---------- Domains: - cprapid.com - topfilmeonline.net ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 21:56. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 530 Login authentication failed 214-The following SITE commands are recognized ALIAS CHMOD IDLE UTIME 214 Pure-FTPd - http://pureftpd.org/ 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV ESTP 211 End. ``` ---------- **53:** ``` PowerDNS Authoritative Server 4.7.2 (built Dec 9 2022 10:19:47 by root@bh-centos-8.dev.cpanel.net) Resolver ID: 94-156-33-190.cprapid.com ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Tue, 30 May 2023 11:28:59 GMT server: LiteSpeed location: http://topfilmeonline.biz/ ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` ---------- **443:** ``` HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Wed, 07 Jun 2023 18:35:46 GMT server: LiteSpeed location: http://topfilmeonline.biz/ alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" ``` HEARTBLEED: 2023/06/07 18:35:56 94.156.33.229:443 - SAFE ---------- **465:** ``` 220-94-156-33-190.cprapid.com ESMTP Exim 4.96 #2 Wed, 07 Jun 2023 07:13:12 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-94-156-33-190.cprapid.com Hello 224.48.112.59 [224.48.112.59] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 250 HELP ``` HEARTBLEED: 2023/06/07 11:13:20 94.156.33.229:465 - SAFE ---------- **587:** ``` 220-94-156-33-190.cprapid.com ESMTP Exim 4.96 #2 Tue, 23 May 2023 22:12:24 -0400 220-We

do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-94-156-33-190.cprapid.com Hello 224.28.147.158 [224.28.147.158] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-STARTTLS 250 HELP ``` ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/06/01 10:06:27 94.156.33.229:995 - SAFE ---------- **2082:** ``` HTTP/1.1 301 Moved Content-length: 123 Location: https://94-156-33-190.cprapid.com:2083/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2083:** ``` HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Wed, 07 Jun 2023 06:47:28 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: cpsession=%3aEsD9gubwhamNX6Sq%2c326067f3e71d976ac8b47471f759a0a3; HttpOnly; path=/; port=2083; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2083; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: imp_key=expired; HttpOnly; domain=94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083 Cache-Control: no-cache, no-store, must-revalidate, private X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 37216 ``` HEARTBLEED: 2023/06/07 06:47:32 94.156.33.229:2083 - SAFE ---------- **2086:** ``` HTTP/1.1 301 Moved Content-length: 123 Location: https://94-156-33-190.cprapid.com:2087/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2087:** ``` HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset="utf-8" Date: Tue, 06 Jun 2023 08:54:45 GMT Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: whostmgrsession=%3a77j7jZizMAmaqOI0%2c8df71ae3bec6abcb776e9c87ca73ea9a; HttpOnly; path=/; port=2087; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;

secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2087; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: imp_key=expired; HttpOnly; domain=94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure Set-Cookie: Horde=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.94.156.33.229; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087 Cache-Control: no-cache, no-store, must-revalidate, private X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 36883 ``` HEARTBLEED: 2023/06/06 08:54:50 94.156.33.229:2087 - SAFE ---------- **3306:** ``` MySQL: Error Message: Host '224.48.158.159' is not allowed to connect to this MySQL server Error Code: 1130 ``` ---------- **7080:** ``` HTTP/1.0 301 Moved Permanently Location: https://94.156.33.229/ Cache-Control: private, no-cache, max-age=0 Pragma: no-cache Server:LiteSpeed Content-Length: 0 Connection: Close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.156.33.229']

Name

b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723']

Name

e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f']

Name

2096.website

Pattern Type

stix

Pattern

[domain-name:value = '2096.website']

Name

185.125.230.220

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.125.230.220']

Name
filecloud.store
Pattern Type
stix
Pattern
[domain-name:value = 'filecloud.store']
Name
webmailogemail.com
Pattern Type
stix
Pattern
[domain-name:value = 'webmailogemail.com']

Country

Name
Libya

Domain-Name

Value
loglivemail.com
customjvupdate.live
2096.website
filestoragehub.live
webmailogemail.com
filecloud.store

StixFile

Value
7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd
8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946
e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f
a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974
2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb
b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e
c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6
d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885
05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc
b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723
cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a
df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4
e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f

d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db

IPv4-Addr

Value
185.125.230.116
185.125.230.224
94.156.33.229
94.156.33.228
185.125.230.220
185.125.230.216

External References

- https://otx.alienvault.com/pulse/64834366fe4bc8b938137732
- https://research.checkpoint.com/2023/stealth-soldier-backdoor-used-in-targeted-espionage-attacks-in-north-africa/