Oct 04 2023

NETMANAGEIT

Intelligence Report

EvilProxy Phishing Attack Strikes Indeed

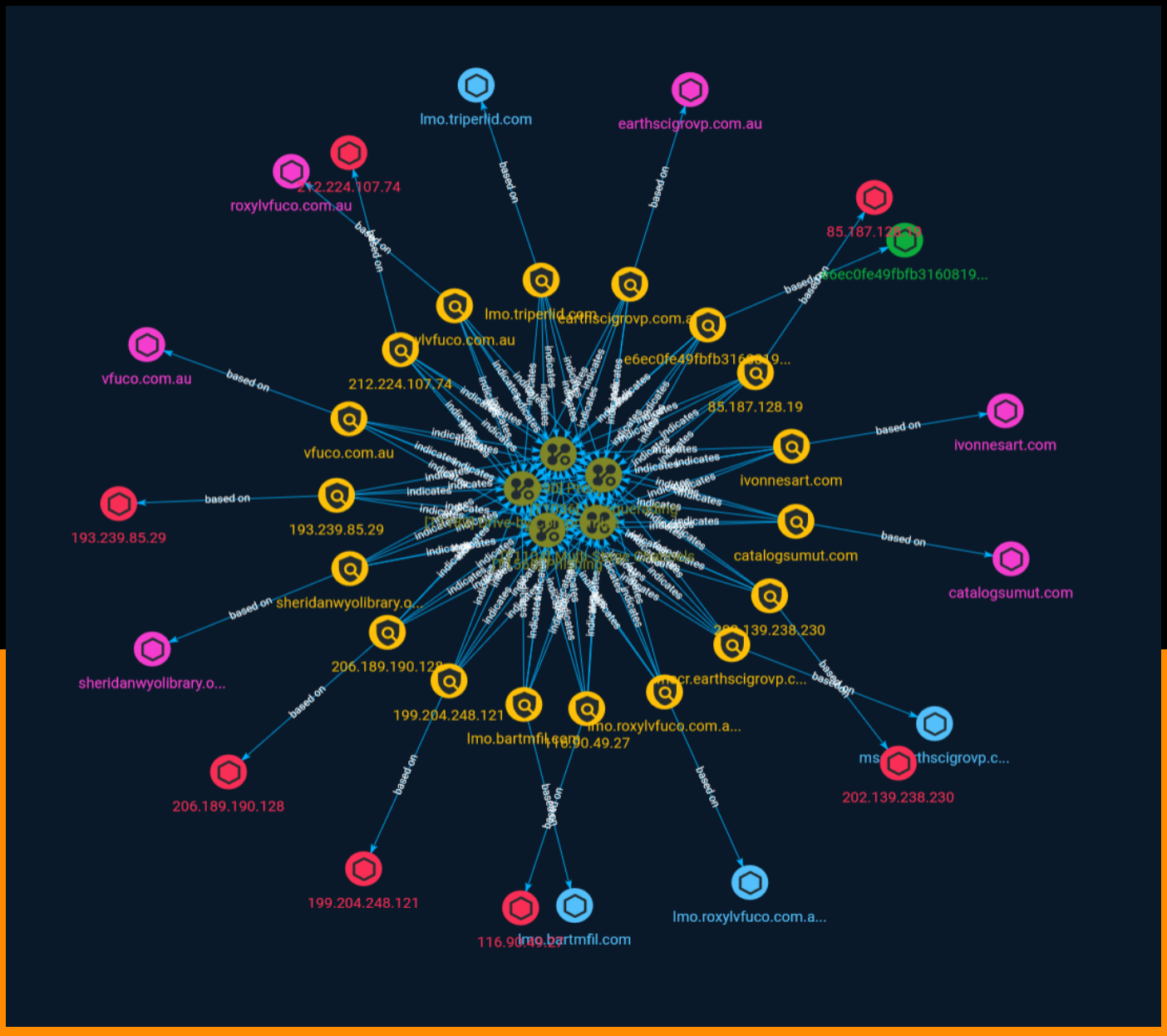

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A sophisticated phishing campaign targeting C-suite employees and other key executives has been identified by Menlo Labs. The infection vector was a phishing email delivered with a link that is deceptively crafted in such a way that it comes from a trusted source, in this case, ‘indeed.com’. Upon clicking the link the victim is redirected to a fake Microsoft Online login page.

Confidence

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

15 / 100

Content

N/A

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
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

Proxy

ID

T1090

Description

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

source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

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

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)

Indicator

Name
lmo.bartmfil.com
Pattern Type
stix
Pattern
[hostname:value = 'lmo.bartmfil.com']
Name
roxylvfuco.com.au
Pattern Type
stix
Pattern
[domain-name:value = 'roxylvfuco.com.au']
Name
202.139.238.230

Description
CC=AU ASN=AS834 IPXO
Pattern Type
stix
Pattern
[ipv4-addr:value = '202.139.238.230']
Name
sheridanwyolibrary.org
Pattern Type
stix
Pattern
[domain-name:value = 'sheridanwyolibrary.org']
Name
lmo.triperlid.com
Pattern Type
stix
Pattern
[hostname:value = 'lmo.triperlid.com']

Name
lmo.roxylvfuco.com.au
Pattern Type
stix
Pattern
[hostname:value = 'lmo.roxylvfuco.com.au']
Name
vfuco.com.au
Pattern Type
stix
Pattern
[domain-name:value = 'vfuco.com.au']
Name
ivonnesart.com
Pattern Type
stix
Pattern
[domain-name:value = 'ivonnesart.com']

Name

199.204.248.121

Description

ISP: Jumpline Inc **OS:** None ---------- Hostnames: - www.abbysdad.com - cp11.machighway.com - mail.abbysdad.com - abbysdad.com - webmail.abbysdad.com - webdisk.abbysdad.com - cpcontacts.abbysdad.com - cpanel.abbysdad.com - machighway.com - autodiscover.abbysdad.com - cpcalendars.abbysdad.com ---------- Domains: - machighway.com - abbysdad.com ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 00:17. 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: EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD AUTH TLS PBSZ PROT UTF8 TVFS ESTA PASV EPSV SPSV 211 End. ``` ---------- **26:** ``` 220-cp11.machighway.com ESMTP Exim 4.93 #2 Tue, 26 Sep 2023 21:09:52 -0400 \r\n220-We do not authorize the use of this system to transport unsolicited, \r\n220 and/or bulk e-mail. \r\n ``` ---------- **53:** ``` 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 Resolver name: cp11.machighway.com ``` ---------- **53:** ``` 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 Resolver name: cp11.machighway.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Wed, 04 Oct 2023 01:13:26 GMT Server: Apache/2.4.52 (cPanel) OpenSSL/1.1.1m mod_bwlimited/1.4 Transfer-Encoding: chunked Content-Type: text/html ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN . ``` ---------- **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 Date: Wed, 04 Oct 2023 09:40:20 GMT Server: Apache/2.4.52 (cPanel) OpenSSL/1.1.1m mod_bwlimited/1.4 Content-Length: 2924 Content-Type: text/html;charset=ISO-8859-1 ``` HEARTBLEED: 2023/10/04 09:40:01 199.204.248.121:443 - SAFE ---------- **465:** ``` 220-cp11.machighway.com ESMTP Exim 4.93 #2 Fri, 22 Sep 2023 19:29:26 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-cp11.machighway.com Hello 224.90.79.28 [224.90.79.28] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250 HELP ``` HEARTBLEED: 2023/09/22 23:29:05

199.204.248.121:465 - SAFE ---------- **587:** ``` 220-cp11.machighway.com ESMTP Exim 4.93 #2 Sat, 16 Sep 2023 08:28:13 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-cp11.machighway.com Hello 224.38.45.207 [224.38.45.207] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 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: 2023/09/28 19:04:56 199.204.248.121:993 - SAFE ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/09/23 02:47:10 199.204.248.121:995 - SAFE ---------- **2082:** ``` HTTP/1.1 301 Moved Content-length: 117 Location: https://cp11.machighway.com:2083/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2083:** ``` HTTP/1.1 301 Moved Content-length: 116 Location: https://cp11.machighway.com:2083 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache ``` ---------- **2086:** ``` HTTP/1.1 301 Moved Content-length: 117 Location: https://cp11.machighway.com:2087/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2087:** ``` HTTP/1.1 301 Moved Content-length: 116 Location: https://cp11.machighway.com:2087 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache ``` ---------- **2096:** ``` HTTP/1.1 301 Moved Content-length: 116 Location: https://cp11.machighway.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 '224.228.214.165' is not allowed to connect to this MySQL server Error Code: 1130 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '199.204.248.121']

Name

earthscigrovp.com.au

Pattern Type

stix

Pattern

[domain-name:value = 'earthscigrovp.com.au']

Name

mscr.earthscigrovp.com.au

Pattern Type

stix

Pattern

[hostname:value = 'mscr.earthscigrovp.com.au']

Name

193.239.85.29

Description

CC=RO ASN=AS9009 M247 Europe SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.239.85.29']

Name

85.187.128.19

Description

ISP: A2 Hosting, Inc. **OS:** None ---------- Hostnames: - webdisk.targetmarketing.ae - autodiscover.targetmarketing.ae - www.targetmarketing.ae - sg1-sr4.supercp.com - webmail.targetmarketing.ae - targetmarketing.ae - cpcalendars.targetmarketing.ae - mail.targetmarketing.ae - cpcontacts.targetmarketing.ae - cpanel.targetmarketing.ae ---------- Domains: - supercp.com - targetmarketing.ae ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Tue, 03 Oct 2023 22:13:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Set-Cookie: cl-bypass-cache=yes; Expires=Tue, 03-Oct-23 23:13:00 GMT; Domain=wingsbd.com; Path=/; HttpOnly; SameSite=Lax Server: imunify360-webshield/1.21 Last-Modified: Tuesday, 03-Oct-2023 22:13:00 GMT Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0 cf-edge-cache: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 04 Oct 2023 05:26:44 GMT Server: Apache X-Powered-By: PHP/7.4.33 X-UA-Compatible: IE=edge Link: ; rel="https://api.w.org/", ; rel="alternate"; type="application/json", ; rel=shortlink Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/10/04 05:27:12 85.187.128.19:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.187.128.19']

Name

116.90.49.27

Description

ISP: Hostopia Australia Web Pty Ltd **OS:** None ---------- Hostnames: - www.canningcollege.wa.edu.au - stealth-servers.com.au - canningcollege.wa.edu.au - vmcp05.stealth-servers.com.au ---------- Domains: - stealth-servers.com.au - canningcollege.wa.edu.au ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDSklL6ZwyPZTBXNVbBlK83xObMS9Q/dQFQ2xdh7LbLwIWX 06kcRvWqIeeWdVQwUTQsY5x0VUQbRjssFh3jxk3xhQcWV6rZSEn9Kec9j3Jo3sEOiyYsOkhKp1Lpg6anxbN55QBJXude5/GeCVssHU9FQ32U2UwzaqcQ2QZExX1R4Cgk7JQ7NqUzrRcfSLx5bPZ4vhG1Rfkg7QKTARRdbc07A0R2wAoFkHEeOiM/l76S8NIKuapyqrhQipW34Snrn6/6J6VVsRHTpf8tuD1sAUv8xyDjkLvspK6paxwTwuwI74fgIM5S0i2XzHdHsW4LiYHzybbshgDQZhnyPxH3SchT Fingerprint: 89:3a:d2:a9:28:fb:30:c4:dc:60:23:e1:c7:a2:15:11 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 ssh-dss ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **53:** ``` 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 Resolver name: vmcp05.stealth-servers.com.au ``` ---------- **53:** ``` 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 Resolver name: vmcp05.stealth-servers.com.au ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Keep-Alive: timeout=5, max=100 x-powered-by: PHP/7.3.33 expires: Wed, 04 Oct 2023 01:33:00 GMT cache-control: max-age=3600 x-redirect-by: WordPress location: https://www.rmcg.com.au/ content-type: text/html; charset=UTF-8 content-length: 1 date: Wed, 04 Oct 2023 00:33:00 GMT server: LiteSpeed vary: User-Agent referrer-policy: no-referrer-when-downgrade ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN LOGIN . ``` ---------- **443:** ``` HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html last-modified: Tue, 03 Oct 2023 06:10:14 GMT accept-ranges: bytes content-length: 283956 date: Wed, 04 Oct 2023 02:59:50 GMT server: LiteSpeed vary: User-Agent,User-Agent cache-control: max-age=0, no-cache, no-store, must-revalidate pragma: no-cache expires: Mon, 29 Oct 1923 20:30:00 GMT 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: 2023/10/04 03:00:30 116.90.49.27:443 - SAFE ---------- **465:** ``` 220-vmcp05.stealth-servers.com.au ESMTP Exim 4.96 #2 Mon, 25 Sep 2023 02:29:30 +1000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-vmcp05.stealth-servers.com.au Hello b7pxdmkl11qoyie.org [224.253.0.179] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 250 HELP ``` HEARTBLEED: 2023/09/24 16:29:38 116.90.49.27:465 - SAFE ---------- **587:** ```

220-vmcp05.stealth-servers.com.au ESMTP Exim 4.96 #2 Tue, 03 Oct 2023 12:29:44 +1100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail. 250-vmcp05.stealth-servers.com.au Hello 88val6oh7gp.com [224.38.186.116] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 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: 2023/09/23 03:39:09 116.90.49.27:993 - SAFE ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/09/13 22:33:39 116.90.49.27:995 - SAFE ---------- **2082:** ``` HTTP/1.1 301 Moved Content-length: 127 Location: https://vmcp05.stealth-servers.com.au:2083/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2083:** ``` HTTP/1.1 301 Moved Content-length: 126 Location: https://vmcp05.stealth-servers.com.au:2083 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache ``` ---------- **2086:** ``` HTTP/1.1 301 Moved Content-length: 127 Location: https://vmcp05.stealth-servers.com.au:2087/ Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private ``` ---------- **2087:** ``` HTTP/1.1 301 Moved Content-length: 126 Location: https://vmcp05.stealth-servers.com.au:2087 Content-type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.90.49.27']

Name

212.224.107.74

Description

ISP: firstcolo GmbH **OS:** None ---------- Hostnames: - mihanmob.mehranistore.com ---------- Domains: - mehranistore.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJh14twuj2aFUFn0x4bPkPRYLl6+F9ID3fYNrErihaSzsGroTu6tDykQr7W1H3iBamPB7SgQQbQbBT793R4cD+c= Fingerprint: dc:9a:52:39:4f:fb:ed:ee:dd:ed:fd:d6:d0:1e:fb:4b Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.24.0 Date: Thu, 21 Sep 2023 14:38:19 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive x-ua-compatible: IE=edge link: ; rel="https://api.w.org/" link: ; rel="alternate"; type="application/json" link: ; rel=shortlink vary: Accept-Encoding,Accept-Encoding,Accept-Encoding 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" ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.24.0 Date: Sun, 24 Sep 2023 02:32:54 GMT Content-Type: text/html Content-Length: 20433 Connection: keep-alive Set-Cookie: cl-bypass-cache=yes; Expires=Sun, 24-Sep-23 03:32:54 GMT; Domain=hivsti.com; Path=/; HttpOnly; SameSite=Lax Last-Modified: Sunday, 24-Sep-2023 02:32:54 GMT Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0 cf-edge-cache: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT ``` HEARTBLEED: 2023/09/24 02:33:11 212.224.107.74:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.224.107.74']

Name

catalogsumut.com

Pattern Type

stix

Pattern

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

Name

206.189.190.128

Description

ISP: DigitalOcean, LLC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_9.2p1 Debian-2 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAUHuIOXCf6R6VHV0h3icA9IpvrWPuUJhTQY3Byo4GuIYuCswCY9fbqZV3WxSkm0vOTVaofwRNqkY++fJNxd+b4= Fingerprint: 7e:13:41:9d:b2:f1:2b:c8:db:4b:bb:16:1c:6a:51:cc Kex Algorithms: sntrup761x25519-sha512@openssh.com curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 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/1.1 302 Found Location: https://206.189.190.128/ Date: Mon, 02 Oct 2023 06:46:31 GMT Content-Length: 5 Content-Type: text/plain; charset=utf-8 ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Mon, 02 Oct 2023 06:49:06 GMT Content-Length: 19 ``` HEARTBLEED: 2023/10/02 06:49:27 206.189.190.128:443 - SAFE ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '206.189.190.128']
Name
e6ec0fe49fbfb31608198b22eaa2d00fe6ec0fe49fbfb31608198b22eaa2d00f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e6ec0fe49fbfb31608198b22eaa2d00fe6ec0fe49fbfb31608198b22eaa2d00f']

Domain-Name

Value
catalogsumut.com
roxylvfuco.com.au
earthscigrovp.com.au
sheridanwyolibrary.org
vfuco.com.au
ivonnesart.com

StixFile

Value
e6ec0fe49fbfb31608198b22eaa2d00fe6ec0fe49fbfb31608198b22eaa2d00f

Hostname

Value
lmo.triperlid.com
mscr.earthscigrovp.com.au
lmo.bartmfil.com
lmo.roxylvfuco.com.au

IPv4-Addr

Value
212.224.107.74
206.189.190.128
85.187.128.19
193.239.85.29
116.90.49.27
199.204.248.121
202.139.238.230

External References

- https://otx.alienvault.com/pulse/651d8320c33e63ab09baa409
- https://www.menlosecurity.com/blog/evilproxy-phishing-attack-strikes-indeed/