Jun 11 2023

NETMANAGEIT

Intelligence Report

Ukraine remains Russia's biggest cyber focus in 2023

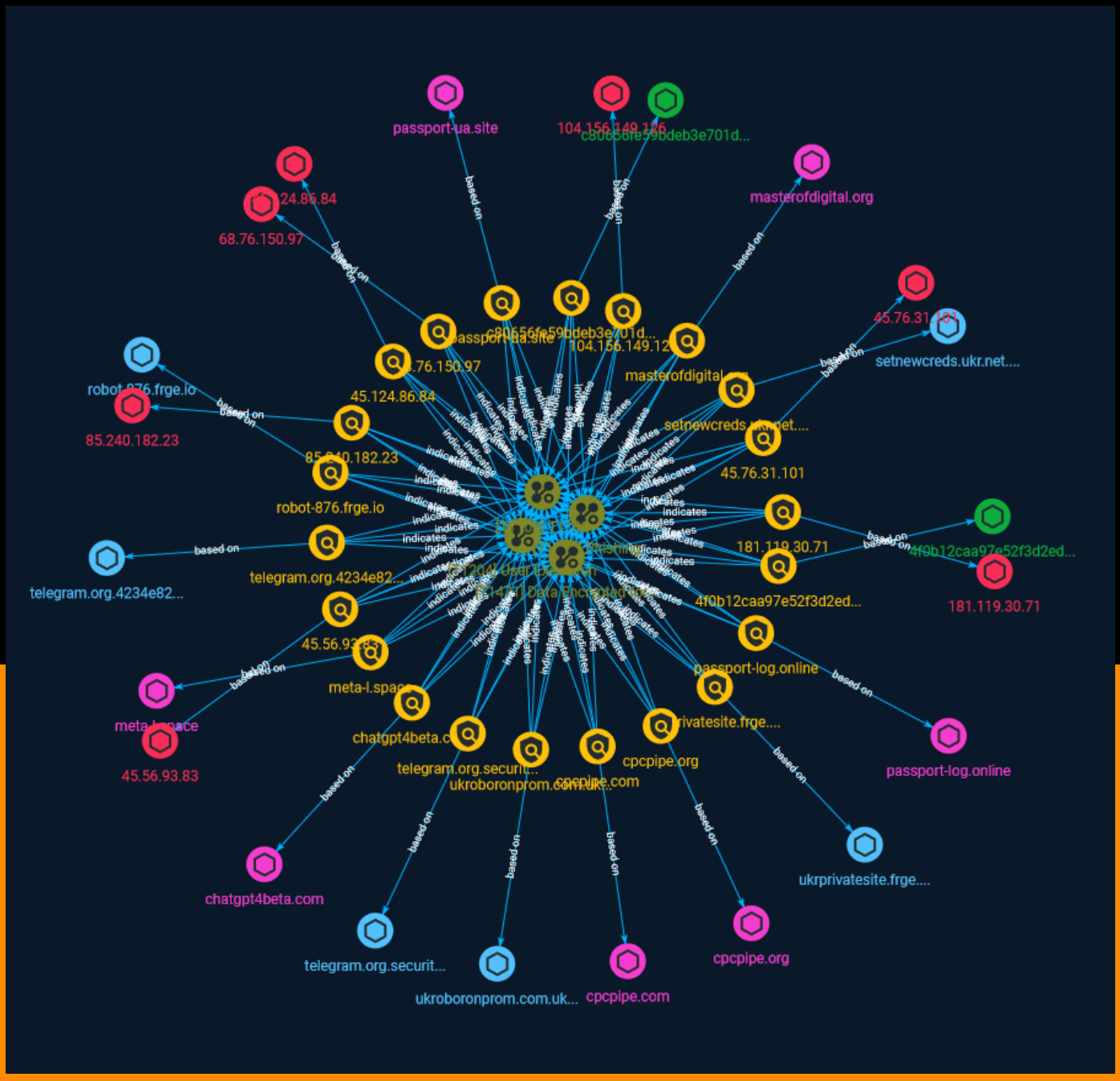

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In the first quarter of 2023, Russian government-backed phishing campaigns targeted users in Ukraine the most, with the country accounting for over 60% of observed Russian targeting. Looking at information operations (IO).

Confidence

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

15 / 100

Attack-Pattern

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

User Execution

ID

T1204

Description

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

Name

T1100

ID

T1100

Name

Data Encrypted for Impact

ID

T1471

Description

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Sector

Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Indicator

Name
chatgpt4beta.com
Pattern Type
stix
Pattern
[domain-name:value = 'chatgpt4beta.com']
Name
68.76.150.97
Description
ISP: AT&T Services, Inc. **OS:** None ---------- Hostnames: - 68-76-150-97.lightspeed.hstntx.sbcglobal.net ---------- Domains: - sbcglobal.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_6.7p2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCpwKXoVAm75kPxHMjTfNnIF+Vg9DluNsSFml0PlyDStJCs 36gMsmgD5KUfGmWXgq692Lfm9aGYmL3sDSFw4t/ikg6dHkwLR7SoYikNpmQg8MFyp88hTALtGkrW tIOHBSalWAaNdhqAYSrJZbNBLrGgoGeWPGTsqMKWRQTOubVo0GtNrmSzHMViih1QJTzvpQ87OveO Y2eagRixHD8FsbJmEXKjrGzMmbmYAWXBEDOwy1Dde8MnXmVABPWyrtE2/IEufq9+DPX3q0mJDm+o L2QShu5IYjWXDLI7gSoCGTYYM9fd490+4isD7elYhaF2UWPoDSZTgSuCDNwqz8lvNpbv Fingerprint: 69:22:25:e8:cf: 96:40:bc:ea:36:d6:75:f8:b4:e6:7e Kex Algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss ecdsa-sha2-nistp256 Encryption

Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-256-96 hmac-sha2-512 hmac-sha2-512-96 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **53:** ``` ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 17 Apr 2023 06:33:58 GMT Server: Webs X-Frame-Options: SAMEORIGIN ETag: "413f-1e0-5f598ef3" Content-Length: 480 Content-Type: text/html Connection: keep-alive Keep-Alive: timeout=60, max=99 Last-Modified: Thu, 10 Sep 2020 02:26:59 GMT Hikvision IP Camera: Web Version: 4.0.51 build 200909 Plugin Version: 3.0.6.46 Custom Version: DZP20200827163 ActiveX Files: AudioIntercom.dll: 1.4.0.6 LTSWebVideoActiveX.ocx: 3.0.7.1002 NetStream.dll: 1.0.5.50 npLTSWebVideoPlugin.dll: 3.0.7.1002 PlayCtrl.dll: 7.3.6.80 StreamTransClient.dll: 1.1.3.15 SystemTransform.dll: 2.5.3.7 Hikvision IP Camera: Web Version: 4.0.51 build 200909 Plugin Version: 3.0.6.46 Custom Version: DZP20200827163 ActiveX Files: AudioIntercom.dll: 1.4.0.6 LTSWebVideoActiveX.ocx: 3.0.7.1002 NetStream.dll: 1.0.5.50 npLTSWebVideoPlugin.dll: 3.0.7.1002 PlayCtrl.dll: 7.3.6.80 StreamTransClient.dll: 1.1.3.15 SystemTransform.dll: 2.5.3.7 ``` ---------- **81:** ``` HTTP/1.1 200 OK Date: Thu, 13 Apr 2023 17:59:26 GMT Server: Webs ETag: "0-d5c-1e0" Content-Length: 480 Content-Type: text/html Connection: keep-alive Keep-Alive: timeout=60, max=99 Last-Modified: Thu, 09 May 2019 03:57:16 GMT Hikvision IP Camera: Web Version: 4.0.51 build 190509 Plugin Version: 3.0.6.43 Device Version: 4.1.50 Custom Version: DZP20190319045 ActiveX Files: AudioIntercom.dll: 1.4.0.6 NetStream.dll: 1.0.5.44 npWebVideoPlugin.dll: 3.0.6.43 PlayCtrl.dll: 7.3.5.31 StreamTransClient.dll: 1.1.3.8 SystemTransform.dll: 2.5.2.15 WebVideoActiveX.ocx: 3.0.6.43 Hikvision IP Camera: Web Version: 4.0.51 build 190509 Plugin Version: 3.0.6.43 Device Version: 4.1.50 Custom Version: DZP20190319045 ActiveX Files: AudioIntercom.dll: 1.4.0.6 NetStream.dll: 1.0.5.44 npWebVideoPlugin.dll: 3.0.6.43 PlayCtrl.dll: 7.3.5.31 StreamTransClient.dll: 1.1.3.8 SystemTransform.dll: 2.5.2.15 WebVideoActiveX.ocx: 3.0.6.43 ``` ---------- **82:** ``` HTTP/1.1 200 OK Date: Wed, 19 Apr 2023 02:53:41 GMT Server: Webs X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1;mode=block ETag: "0-1c7-1e1" Content-Length: 481 Content-Type: text/html Connection: keep-alive Keep-Alive: timeout=60, max=99 Last-Modified: Fri, 17 Apr 2020 02:35:32 GMT Hikvision IP Camera: Web Version: 4.0.51 build 200413 Plugin Version: 3.0.7.21 Custom Version: DZP20200121045 ActiveX Files: AudioIntercom.dll: 1.4.0.8 localServiceControl: 1.0.0.8 NetStream.dll: 1.0.5.57 npWebVideoPlugin.dll: 3.0.7.21 PlayCtrl.dll: 7.3.7.39 StreamTransClient.dll: 1.1.3.17 SystemTransform.dll: 2.5.3.13 WebVideoActiveX.ocx: 3.0.7.21 Hikvision IP Camera: Web Version: 4.0.51 build 200413 Plugin Version: 3.0.7.21 Custom Version: DZP20200121045 ActiveX Files: AudioIntercom.dll: 1.4.0.8 localServiceControl: 1.0.0.8 NetStream.dll: 1.0.5.57 npWebVideoPlugin.dll: 3.0.7.21 PlayCtrl.dll: 7.3.7.39 StreamTransClient.dll: 1.1.3.17 SystemTransform.dll: 2.5.3.13 WebVideoActiveX.ocx: 3.0.7.21 ``` ---------- **443:** ``` HTTP/1.1 200 OK X-Frame-Options: SAMEORIGIN X-Xss-Protection: 1; mode=block Content-Length: 8442 X-Content-Type-Options: nosniff Content-Type: text/html; charset=UTF-8 Date: Fri, 31 Mar 2023 00:29:52 GMT Server: Server ``` HEARTBLEED: 2023/03/31 00:30:07 68.76.150.97:443 - SAFE ---------- **1701:** ``` \xc8\x02\x00\x0c\x00\x00\x00\x00\x00\x00\x00\x01 ``` ----------

Pattern Type
stix

Pattern

[ipv4-addr:value = '68.76.150.97']

Name

passport-log.online

Pattern Type

stix

Pattern

[domain-name:value = 'passport-log.online']

Name

robot-876.frge.io

Pattern Type

stix

Pattern

[hostname:value = 'robot-876.frge.io']

Name

masterofdigital.org

Pattern Type

stix

Pattern

[domain-name:value = 'masterofdigital.org']

Name

ukroboronprom.com.ukr.pm

Pattern Type

stix

Pattern

[hostname:value = 'ukroboronprom.com.ukr.pm']

Name

85.240.182.23

Description

ISP: MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A. **OS:** None ---------- Hostnames: - bl7-182-23.dsl.telepac.pt ---------- Domains: - telepac.pt ---------- Services: **22:** ``` SSH-2.0-OpenSSH_6.7p2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDeufiaqchgLg3db1KKta2fZmh90I91B0KKCXKD+jlQ7QrE 8QCKEPFj37i9t5vSyrl7a7s5ZdLATxnxLe093VMd7o8DGseuXjc6eMpVnvT0pPGOQdb/AwOE7Zr7 K2WunY4ENAUzjTDExRxyFtcM8I5byHN5FChAC616tcfYk69IZRD2zS0lfkIYFXYKfMbfBrVgDByw P/ OTQgDWs19E0FAIr9cb2Dpitu74EjTbE7Dl6mQwvyXQwa8F2eaKText6RXZyJlq284eutTp603n XxBz8xLImPNcpe7BUSed+LhXQvCZy1e1ISMysewDDgBnruVf+uiXYkuZ/MmvifuOkTAn Fingerprint: 69:e6:88:76:3f:ef:e4:2b:ac:31:a6:94:e9:be:7d:a8 Kex Algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss ecdsa-sha2-nistp256 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-256-96 hmac-sha2-512 hmac-sha2-512-96 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **53:** ``` ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Location: https://85.240.182.23:443/ Content-Length: 0 Date: Sat, 11 Feb 2023 17:17:51 GMT Server Server ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -21 rootdelay:

0.0480804443359 rootdisp: 0.0344390869141 refid: 860707310 reftime: 3884460379.69 poll: 3 ``` ---------- **443:** ``` HTTP/1.1 200 OK X-Frame-Options: SAMEORIGIN X-Xss-Protection: 1; mode=block Content-Length: 8469 X-Content-Type-Options: nosniff Content-Type: text/html; charset=UTF-8 Set-cookie: beaker.session.id=314e4e46ab65446aa68c6504a3df61ba; httponly; Path=/; secure Date: Wed, 15 Feb 2023 11:06:26 GMT Server: Server ``` HEARTBLEED: 2023/02/15 11:06:58 85.240.182.23:443 - ERROR: heartbleed: timeout ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.240.182.23']

Name

45.76.31.101

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - vi-sh.010.us.vm.virtio.cloud ---------- Domains: - virtio.cloud ---------- Services: **21: ``` 220 ProFTPD Server ready. 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD XRMD MKD XMKD PWD XPWD SIZE SYST HELP NOOP FEAT OPTS HOST CLNT AUTH CCC* CONF* ENC* MIC* PBSZ PROT TYPE STRU MODE RETR STOR STOU APPE REST ABOR RANG USER PASS ACCT* REIN* LIST NLST STA SITE MLSD MLST 214 Direct comments to root@45.76.31.101 211-Features: AUTH TLS CCC CLNT EPRT EPSV HOST LANG en-US.UTF-8* MDTM MFF modify;UNIX.group;UNIX.mode; MFMT MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.groupname*;UNIX.mode*;UNIX.owner*;UNIX.ownername PBSZ PROT RANG STREAM REST STREAM SIZE SSCN TVFS UTF8 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_5.3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAABIwAAAQEArAbUB8tEDZIq+yuQkM1sc9l35pa6czAL7RwBRyRwuVuxaj54 g6xq39YJicPFAdV2/W1Gi3sFoD/vMTeXd6/qJWJlB243rT16uDNPRYoltwab7u7rXWMmIFOsYqs3 KkOD5OJG79aRmhs61DXcx1rZ/Riw0I0xcxQtdvZXGfEDFCbVmFo1vCvAVbczo3AplfT1v4F7oai8 b0D3iFb6ncykY99HceOvwOpEI3abAzYd8w54Juc7CIZhZBVFm7RKbgrjARLdpnIBpYMqOCGD4PSX kKw+UCdTE6n1wyRQMjCAlgLeU5zi23rAw+fclvcL8G5F4Ee3E2K7jke6xtUxZfgo5w== Fingerprint: a8:8e:da:2b:f2:7c:b1:37:51:44:d7:79:1e:8a:aa:2c Kex Algorithms: diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc

3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **25:** ``` 220 vi-sh.010.us.vm.virtio.cloud ESMTP Exim 4.96 Fri, 31 Mar 2023 05:15:27 +0200 250-vi-sh.010.us.vm.virtio.cloud Hello 224.169.191.178 [224.169.191.178] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP ``` ---------- **53:** ``` 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 Resolver name: vi-sh.010.us.vm.virtio.cloud ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 11 Apr 2023 17:27:45 GMT Server: Apache/2 X-Powered-By: PHP/7.0.33 P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" Permissions-Policy: interest-cohort=() Expires: Wed, 17 Aug 2005 00:00:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: 0067e9ee4561c256249da0f8a32e1f02=td7fppsgalisvtohc3c1hsk814; path=/; HttpOnly Last-Modified: Tue, 11 Apr 2023 17:27:45 GMT Vary: Accept-Encoding,User-Agent Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 ``` ---------- **110:** ``` +OK Dovecot DA ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL PLAIN . ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sat, 15 Apr 2023 20:52:52 GMT Server: Apache/2 Last-Modified: Sun, 12 Jun 2022 02:24:13 GMT ETag: "2c-5e136de1055db" Accept-Ranges: bytes Content-Length: 44 Vary: User-Agent Content-Type: text/html ``` HEARTBLEED: 2023/04/15 20:53:01 45.76.31.101:443 - SAFE ---------- **465:** ``` 220 vi-sh.010.us.vm.virtio.cloud ESMTP Exim 4.96 Sat, 08 Apr 2023 20:24:44 +0200 250-vi-sh.010.us.vm.virtio.cloud Hello 224.164.94.23 [224.164.94.23] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 250 HELP ``` HEARTBLEED: 2023/04/08 18:24:52 45.76.31.101:465 - SAFE ---------- **587:** ``` 220 vi-sh.010.us.vm.virtio.cloud ESMTP Exim 4.96 Tue, 28 Mar 2023 13:46:53 +0200 250-vi-sh.010.us.vm.virtio.cloud Hello 224.138.30.29 [224.138.30.29] 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 LITERAL+ AUTH=PLAIN] Dovecot DA ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN 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: 2023/04/02 06:01:32 45.76.31.101:993 - SAFE ---------- **995:** ``` +OK Dovecot DA ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN . ``` HEARTBLEED: 2023/04/17 09:31:14 45.76.31.101:995 - SAFE ---------- **2222:** ``` HTTP/1.0 400 Bad Request x-use-https: yes Conent-Type: text/html ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '45.76.31.101']

Name
meta-l.space
Pattern Type
stix
Pattern
[domain-name:value = 'meta-l.space']
Name
c80656fe59bdeb3e701d1f7eeaaba2ef673368b2c4947945f598e3e84a6cb7f8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c80656fe59bdeb3e701d1f7eeaaba2ef673368b2c4947945f598e3e84a6cb7f8']
Name
ukrprivatesite.frge.io
Pattern Type
stix
Pattern
[hostname:value = 'ukrprivatesite.frge.io']

Name
telegram.org.4234e8234ad0f.24o1.com
Pattern Type
stix
Pattern
[hostname:value = 'telegram.org.4234e8234ad0f.24o1.com']
Name
setnewcreds.ukr.net.frge.io
Pattern Type
stix
Pattern
[hostname:value = 'setnewcreds.ukr.net.frge.io']
Name
cpcpipe.com
Pattern Type
stix
Pattern
[domain-name:value = 'cpcpipe.com']

Name
passport-ua.site
Pattern Type
stix
Pattern
[domain-name:value = 'passport-ua.site']
Name
4f0b12caa97e52f3d2edada9133f2e4a3442953d14c8ed12deb7219c722ea197
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4f0b12caa97e52f3d2edada9133f2e4a3442953d14c8ed12deb7219c722ea197']
Name
45.56.93.83
Description
ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - sakurablinds.com - li895-83.members.linode.com - www.sakurablinds.com ---------- Domains: - linode.com - sakurablinds.com ---------- Services: **25:** ``` 220 li895-83.members.linode.com ESMTP Exim 4.92.3 Wed, 29 Mar 2023 13:54:25 +0800 250-li895-83.members.linode.com Hello 5zdu5k7c8yzju.org [224.99.95.116] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-CHUNKING 250-STARTTLS 250-PRDR 250 HELP ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Sun, 09 Apr 2023 03:39:16 GM

Content-Type: text/html Content-Length: 564 Connection: keep-alive ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Apr 2023 01:16:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Powered-By: PHP/7.0.7 Link: ; rel="https:api.w.org/" Link: ; rel="alternate"; type="application/json" Link: ; rel=shortlink ``` HEARTBLEED: 2023/04/12 01:19:09 45.56.93.83:443 - SAFE ---------- **465:** ``` 220 li895-83.members.linode.com ESMTP Exim 4.92.3 Mon, 17 Apr 2023 11:18:44 +0800 250-li895-83.members.linode.com Hello 224.44.82.87 [224.44.82.87] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-CHUNKING 250-PRDR 250 HELP ``` HEARTBLEED: 2023/04/1 03:21:28 45.56.93.83:465 - SAFE ---------- **587:** ``` 220 li895-83.members.linode.com ESMTP Exim 4.92.3 Fri, 14 Apr 2023 20:49:26 +0800 250-li895-83.members.linode.com Hello 224.16.186.63 [224.16.186.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-CHUNKING 250-STARTTLS 250-PRDR 250 HELP ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.56.93.83']

Name

104.156.149.126

Description

ISP: HIVELOCITY, Inc. **OS:** None ---------- Hostnames: ---------- Domain ---------- Services: **443:** ``` HTTP/1.1 404 Not Found Content-Type: text/html Server: nginx/1.11.13 Date: Sat, 25 Mar 2023 14:28:49 GMT Content-Length: 162

404 Not Found

nginx/1.11.13
``` ----------

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '104.156.149.126']

**Name**

cpcpipe.org

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'cpcpipe.org']

**Name**

45.124.86.84

**Description**

**ISP:** VIETNAM POSTS AND TELECOMMUNICATIONS GROUP **OS:** None ----------
Hostnames: - evatest.vn - ungthudaitructrang.com - thinprep.vn - sv-86084.bkns.vn ----------
Domains: - ungthudaitructrang.com - bkns.vn - evatest.vn - thinprep.vn ---------- Services:
**80:** ``` HTTP/1.1 200 OK Server: nginx Date: Sun, 09 Apr 2023 16:18:35 GMT Content-Type: text/html Conten
Length: 4358 Last-Modified: Mon, 23 Apr 2018 01:55:27 GMT Connection: keep-alive Vary: Accept-Encoding ETa
"5add3d0f-1106" Accept-Ranges: bytes ``` ---------- **222:** ``` SSH-2.0-OpenSSH_5.3 Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEA8k1sKpT1Npc1sOdnMVnLE20AaUeA908Fp/F6TvN3bwbcnh9Y
IBAKGSlV83m6AMDmUJoWNSSrlD032OUU+Y6HJ7dzme4XrKSmJLvISWzEzS+p9ls89L85QDKseBcB CPdOaOuC/
```

p+Ur6yS/FuEyQXS09UkIMWNfmytdg1FtPRLsChp0TwgB7Y+UTorOlYlKpIdok/LvUGX P/ 1wCDgEno3vK9Tp7QJE3NlU3ZsNUaOxFVQ/LWl65mDQG5Nl2oDYOAQSWaGmXB3dyT1I3g+oITrr OjsuJQyBCqT8NHuky79+nwa6ZuNIDoN+W720bZQVFgJMDKsaPIt7X0GU/SrhuNbKzQ== Fingerprint: 11:14:0d:6e: 72:3f:52:fe:fc:41:7e:52:f3:61:13:11 Kex Algorithms: diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 17 Apr 2023 01:58:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Set-Cookie: steven_session=27deaa64302a07abd17218ad5ae3df889a002ec5; expires=Mon, 17-Apr-2023 03:58:13 GM Max-Age=7200; path=/; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block ``` HEARTBLEED: 2023/04/17 01:58:36 45.124.86.84:443 - SAFE ---------- **465:** ``` 220 sv-86084.bkns.vn ESMTP Exim 4.92.3 Sun, 16 Apr 2023 14:14:55 +0700 250-sv-86084.bkns.vn Hello 224.39.12.42 [224.39.12.42] 250-SIZE 52428800 250-8BITMIM 250-PIPELINING 250-CHUNKING 250-PRDR 250 HELP ``` HEARTBLEED: 2023/04/16 07:15:04 45.124.86.84:465 - SAFE ---------- **587:** ``` 220 sv-86084.bkns.vn ESMTP Exim 4.92.3 Thu, 23 Mar 2023 11:18:14 +0700 250 sv-86084.bkns.vn Hello 224.217.138.35 [224.217.138.35] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-CHUNKING 250-STARTTLS 250-PRDR 250 HELP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.124.86.84']

Name

181.119.30.71

Description

CC=CO ASN=AS18747 IFX18747

Pattern Type

stix

Pattern

[ipv4-addr:value = '181.119.30.71']

Name

telegram.org.security.ohsxy.com

Pattern Type

stix

Pattern

[hostname:value = 'telegram.org.security.ohsxy.com']

Country

Name
Ukraine

Domain-Name

Value
chatgpt4beta.com
masterofdigital.org
passport-log.online
meta-l.space
cpcpipe.com
cpcpipe.org
passport-ua.site

StixFile

Value
4f0b12caa97e52f3d2edada9133f2e4a3442953d14c8ed12deb7219c722ea197
c80656fe59bdeb3e701d1f7eeaaba2ef673368b2c4947945f598e3e84a6cb7f8

Hostname

Value
telegram.org.4234e8234ad0f.24o1.com
telegram.org.security.ohsxy.com
setnewcreds.ukr.net.frge.io
ukroboronprom.com.ukr.pm
robot-876.frge.io
ukrprivatesite.frge.io

IPv4-Addr

Value
68.76.150.97
45.76.31.101
85.240.182.23
45.56.93.83
45.124.86.84
181.119.30.71
104.156.149.126

External References

- https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/
- https://otx.alienvault.com/pulse/64403596d7a47d80451657c3