Jan 11 2024

NETMANAGEIT

Intelligence Report

Black Basta-Affiliated Water Curupira's Pikabot Spam Campaign

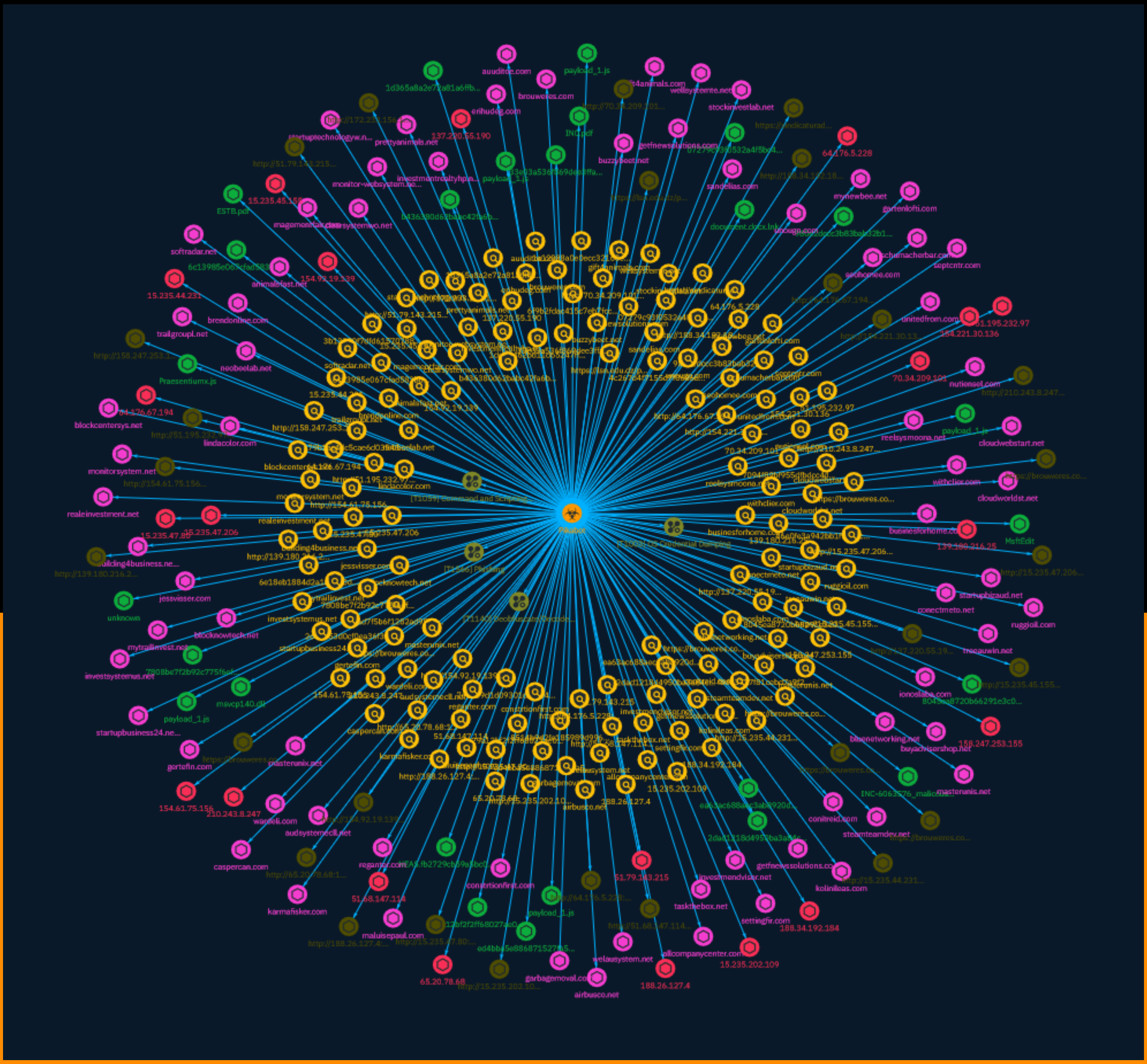

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Pikabot is a type of loader malware that was actively used in spam campaigns by a threat actor we track under the Intrusion set Water Curupira in the first quarter of 2023, followed by a break at the end of June that lasted until the start of September 2023. Other researchers have previously noted its strong similarities to Qakbot, the latter of which was taken down by law enforcement in August 2023. An increase in the number of phishing campaigns related to Pikabot was recorded in the last quarter of 2023, coinciding with the takedown of Qakbot — hinting at the possibility that Pikabot might be a replacement for the latter (with DarkGate being another temporary replacement in the wake of the takedown).

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

OS Credential Dumping

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

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

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

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)

Indicator

Name

1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a']

Name

mynewbee.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'mynewbee.net']

Name

http://15.235.202.109:2226

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://15.235.202.109:2226']

Name

animalsfast.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'animalsfast.net']

Name

980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753']

Name

15.235.47.206

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.47.206']

Name

lindacolor.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8']

Name

blocknowtech.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'blocknowtech.net']

Name

maluisepaul.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

https://brouweres.com:443/vvs49/0.6515179055030298.dat

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'https://brouweres.com:443/vvs49/0.6515179055030298.dat']

Name

magementfair.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

bluenetworking.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'bluenetworking.net']

Name

eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a']

Name

auuditoe.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name
steamteamdev.net
Description
Cobalt Strike botnet C2 domain (confidence level: 100%)
Pattern Type
stix
Pattern
[domain-name:value = 'steamteamdev.net']
Name
gift4animals.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'gift4animals.com']
Name
51.79.143.215

Description
Pikabot botnet C2 server (confidence level: 100%)

Pattern Type
stix

Pattern
[ipv4-addr:value = '51.79.143.215']

Name
businesforhome.com

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[domain-name:value = 'businesforhome.com']

Name
4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b']

Name

clearsystemwo.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'clearsystemwo.net']

Name

210.243.8.247

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '210.243.8.247']

Name

monitor-websystem.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'monitor-websystem.net']

Name

7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7']

Name

gartenlofti.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

unitedfrom.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe']

Name

septcntr.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21']

Name

64.176.67.194

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2022 (build 10.0.20348) -------------------------- Hostnames: - 64.176.67.194.vultrusercontent.com -------------------------- Domains: - vultrusercontent.com -------------------------- Services: **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 20 Nov 2023 22:58:08 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-C49ADB459A NetBIOS Domain Name: WIN-C49ADB459A NetBIOS Computer Name: WIN-C49ADB459A DNS Domain Name: WIN-C49ADB459A FQDN: WIN-C49ADB459A ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.176.67.194']

Name

ruggioil.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1701890238, 'iso': '2023-12-06T14:17:18-05:00'} - **IPQS: Domain:** ruggioil.com - **IPQS: IP Address:** 173.44.141.202

Pattern Type

stix

Pattern

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

Name

wardeli.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

startupbizaud.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'startupbizaud.net']

Name

https://lsn.edu.dz/pqis/?aWDzZBatBsyv

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'https://lsn.edu.dz/pqis/?aWDzZBatBsyv']

Name

karmafisker.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3']

Name

caspercan.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

http://158.247.253.155:2225

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://158.247.253.155:2225']

Name

139.180.216.25

Description

ISP: The Constant Company, LLC **OS:** None ------------------------- Hostnames: - 139.180.216.25.vultrusercontent.com ------------------------- Domains: - vultrusercontent.com ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCvzHr5W2OouIO7rWJVQJ6Ws9FyKuJ6Atr8nOloshLHs3YUer2qZDcW82gQX8RdrMMBY7NKUl+bYCG6djrqyHbPFwyCVqfEjmk84C8Noe6uoEOvZ13sVbt3n3R

F ASsa23y+i9l00J3EjDJqBen/C1ObK770AvPd5IW7SWtNqWOohI7E7Bm3hUxc9xSlTtTCB76PylzE sjds3OuFjTtvHBL9Mk8g8+biUQiP/2w0tNjJLWWZnR7BDPTk3xD8Oj3Qwi8cqScP3WlyIFu7c9xQ E3vv6gtxBy1WT0C7zhbd6vHm9EE/Bv8/gplyz2N1+248/1pTpTZz46+xiC596dD8ZzcmmSnT9fED D64t5Bj5yXp2cEZbZ/qlZMxr0BtmyglUTDXJZKqz6qWdJHa8lS3zfqcAIPYb24euVEbZhD3ZbT3n 8WaLvs/c6uGMuG7So4EyqMFjaH+Z8FauERQDwDnxums4x2OrdKDbUUPiWiZkSzOdZxareoJE/ 6hD vKfTDzyQX68= Fingerprint: 57:0b:d0:85:3c:6c:1e:9a:25:e7:bd:a0:ab:d7:24:92 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-group14-sha256 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 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.180.216.25']

Name

treeauwin.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'treeauwin.net']

Name

startuptechnologyw.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'startuptechnologyw.net']

Name

188.34.192.184

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ------------------------- Hostnames: - static.184.192.34.188.clients.your-server.de - www.api.checksum.ch - api.checksum.ch ------------------------- Domains: - your-server.de - checksum.ch ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDwGnvUXdFfMr69vON/39rmq Rvd9FXlBXa9ALXoRJbsJeNJFSgAJnajv31s218yHdZaa4bjtyW/RxnbKnwHUhKQ= Fingerprint: ae:0b:a5:33:d5:cf:b9:e1:b3:8f:5a:a1:67:9a:98:67 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 kex-strict-s-v00@openssh.com 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/1.18.0 (Ubuntu) Date: Mon, 08 Jan 2024 04:49:09 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Mon, 25 Dec 2023 16:27:48 GMT Connection: keep-alive ETag: "6589ad84-264" Accept-Ranges: bytes ``` ------------------ **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Sat, 06 Jan 2024 08:30:59 GMT Content-Length: 0 Connection: keep-alive ``` HEARTBLEED: 2024/01/06 08:31:33 188.34.192.184:443 - SAFE ------------------ **5000:** ``` HTTP/1.1 404 Not Found Content-Length: 0 Date: Sat, 06 Jan 2024 14:38:30 GMT Server: Kestrel ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.34.192.184']

Name

http://172.233.156.100:13721

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://172.233.156.100:13721']

Name

withclier.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

masterunix.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'masterunix.net']

Name

15.235.45.155

Description
Pikabot botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '15.235.45.155']
Name
investmendvisor.net
Description
Cobalt Strike botnet C2 domain (confidence level: 100%)
Pattern Type
stix
Pattern
[domain-name:value = 'investmendvisor.net']
Name
constrtionfirst.com
Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

15.235.44.231

Description

Pikabot botnet C2 server (confidence level: 50%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.44.231']

Name

15.235.202.109

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.202.109']

Name

https://brouweres.com:443/vvs49/0.15313287608559223.dat

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'https://brouweres.com:443/vvs49/0.15313287608559223.dat']

Name

http://15.235.45.155:2221

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://15.235.45.155:2221']

Name

154.61.75.156

Description

Pikabot botnet C2 server (confidence level: 50%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.61.75.156']

Name

6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193']

Name

ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d']

Name

realeinvestment.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'realeinvestment.net']

Name

investmentrealtyhp.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'investmentrealtyhp.net']

Name

settingfir.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

blockcentersys.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern
[domain-name:value = 'blockcentersys.net']

Name
http://15.235.44.231:5938

Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 15.235.44.231

Pattern Type
stix

Pattern
[url:value = 'http://15.235.44.231:5938']

Name
b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7']

Name
stockinvestlab.net

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[domain-name:value = 'stockinvestlab.net']

Name
http://15.235.47.80:23399

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[url:value = 'http://15.235.47.80:23399']

Name
15.235.47.80

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '15.235.47.80']

Name

64.176.5.228

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: - 64.176.5.228.vultrusercontent.com ------------------------- Domains: - vultrusercontent.com ------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: ALERO5 NetBIOS Domain Name: ALERO5 NetBIOS Computer Name: ALERO5 DNS Domain Name: alero5 FQDN: alero5 ``` ----------------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 19 Nov 2023 12:56:38 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: ALERO5 NetBIOS Domain Name: ALERO5 NetBIOS Computer Name: ALERO5 DNS Domain Name: alero5 FQDN: alero5 ``` -----------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.176.5.228']

Name

http://51.195.232.97:13782

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 51.195.232.97

Pattern Type

stix

Pattern

[url:value = 'http://51.195.232.97:13782']

Name

taskthebox.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'taskthebox.net']

Name

51.68.147.114

Description

Pikabot botnet C2 server (confidence level: 50%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.68.147.114']

Name

conectmeto.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'conectmeto.net']

Name

buyadvisershop.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'buyadvisershop.net']

Name

fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de']

Name

sandelias.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

http://210.243.8.247:23399

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 210.243.8.247

Pattern Type

stix

Pattern

[url:value = 'http://210.243.8.247:23399']

Name

allcompanycenter.com

Pattern Type

stix

Pattern

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

Name

cloudwebstart.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'cloudwebstart.net']

Name

158.247.253.155

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: - 158-247-253-155.constant.com ------------------------- Domains: - constant.com ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAACAQDalulLb4e8ucFk5y2MWCA+YgTwAsmzYDHyA3jSTuDGxpUf QoB0f65wi/cLqE9J70C2zGgYziCR30HELuEdKnw9706sd94Qy5D04TbcoMIf8lQywL0gtad5QZSg vzmdwZ3+qUv81FBIeAD2WWqgNyQiUpWMlWxawJZUBgBsKn8/521L8skIDEEEcNTlTYJsTIJ/Brj0 +o+MKg0/gPIVLSE0vXksWDxm2f/bGSuBHCfS1ES++CdumCGEva2xzZf22DY6JFfWBMYB5cQHSvQv Gt0w9isTnR7oKi7oWFIo75zB7xlVIEtBi947p0F6SjgeAswoZYPJe5cxx01IpDlGzZuqH0/W29Zf m7M/ puM9G+cJV/R3ulVXPgwCS+gJbL7cudRoM2F/1cQfRXeQ254qvOYAXKivcdDQStJjMa9ewcjT Ug55YMeQgYYgKc2Xm6yOvr2r57xpTIzqxxLefsqn1HDHLWKli+BJ077jgY7ONiCsZyGs12YXCdXh OPO4Y5HBgS5YwCRT0aFGimFSAWNBBZMiBbwpnvCAPRY6EtPcj2fJTIdO+U/ 7k6yNSodYV20xg1nQ WQ5druPIZuZPjryki8iJ/ HazmeRGnzaqR0Wb1q6LI9f5aFz41v1ETXlXSQQs1LOSy9mKo96wPL1y WyKM47FAci/ oJ8UKEA+LR2N5YWhpXQ== Fingerprint: 06:d0:c6:28:ca:78:d1:fb:f9:9f:73:3e:bc:1b:b7:9d Kex Algorithms: curve25519-sha256@libssh.org diffie-hellman-group-exchange-sha256 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes256-gcm@openssh.com aes128-gcm@openssh.com aes256-ctr aes128-ctr MAC Algorithms: umac-128-etm@openssh.com hmac-sha2-512 hmac-sha2-256 Compression Algorithms: none zlib@openssh.com ``` ------------------ **500:** ``` VPN (IKE) Initiator SPI: 77316a6767777471 Responder SPI: 326e336a6c646a31 Next Payload: RESERVED Version: 2.0 Exchange Type: DOI Specific Use Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 36 ``` ------------------ **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 19 Nov 2023 21:17:22 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: ALERO1 NetBIOS Domain Name: ALERO1 NetBIOS Computer Name: ALERO1 DNS Domain Name: alero1 FQDN: alero1 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '158.247.253.155']

Name

http://139.180.216.25:2967

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://139.180.216.25:2967']

Name

07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632']

Name

garbagemoval.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

monitorsystem.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'monitorsystem.net']

Name

cloudworldst.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'cloudworldst.net']

Name

building4business.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'building4business.net']

Name

wellsystemte.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'wellsystemte.net']

Name

http://65.20.78.68:13721

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://65.20.78.68:13721']

Name

trailgroupl.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'trailgroupl.net']

Name

https://sindicaturadetecate.gob.mx/pe/?IDbHJCMofpEIzDQjrcwNcDqHoiQRnSKZQcA

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'https://sindicaturadetecate.gob.mx/pe/?IDbHJCMofpEIzDQjrcwNcDqHoiQRnSKZQcA']

Name

8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df']

Name

getfnewsolutions.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

reelsysmoona.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'reelsysmoona.net']

Name

prettyanimals.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'prettyanimals.net']

Name

http://188.34.192.184/76DKN6/Wheez

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://188.34.192.184/76DKN6/Wheez']

Name

http://64.176.5.228:13783

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://64.176.5.228:13783']

Name
http://154.92.19.139:2222
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[url:value = 'http://154.92.19.139:2222']
Name
unougn.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'unougn.com']
Name
brendonline.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

http://70.34.209.101:13720

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://70.34.209.101:13720']

Name

8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004']

Name
154.92.19.139

Description
Pikabot botnet C2 server (confidence level: 100%)

Pattern Type
stix

Pattern
[ipv4-addr:value = '154.92.19.139']

Name
https://brouweres.com:443/vvs49/0.8450027286577588.dat

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern

[url:value = 'https://brouweres.com:443/vvs49/0.8450027286577588.dat']

Name

29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8']

Name

33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34']

Name

46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66']

Name

6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e']

Name

buzzybeet.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'buzzybeet.net']

Name

http://154.221.30.136:13724

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://154.221.30.136:13724']

Name

6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8']

Name

erihudeg.com

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[domain-name:value = 'erihudeg.com']

Name
http://51.68.147.114:2083

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[url:value = 'http://51.68.147.114:2083']

Name
brouweres.com

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[domain-name:value = 'brouweres.com']

Name
http://15.235.47.206:13783

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[url:value = 'http://15.235.47.206:13783']

Name
neobeelab.net

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern

[domain-name:value = 'neobeelab.net']

Name

seohomee.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

65.20.78.68

Description

ISP: The Constant Company, LLC **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: - 65.20.78.68.vultrusercontent.com ------------------------- Domains: - vultrusercontent.com ------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: ALERO1 NetBIOS Domain Name: ALERO1 NetBIOS Computer Name: ALERO1 DNS Domain Name: alero1 FQDN: alero1 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '65.20.78.68']

Name

3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624']

Name

nutiensel.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

startupbusiness24.net

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 weeks ago', 'timestamp': 1703326400, 'iso': '2023-12-23T05:13:20-05:00'} - **IPQS: Domain:** startupbusiness24.net - **IPQS: IP Address:** 95.179.128.84

Pattern Type

stix

Pattern

[domain-name:value = 'startupbusiness24.net']

Name

mytrailinvest.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'mytrailinvest.net']

Name

welausystem.net

Description

Cobalt Strike botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'welausystem.net']

Name

investsystemus.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'investsystemus.net']

Name

154.221.30.136

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.221.30.136']

Name

http://64.176.67.194:2967

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://64.176.67.194:2967']

Name

1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b']

Name

https://brouweres.com:443/vvs49/0.9900618798908114.dat

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'https://brouweres.com:443/vvs49/0.9900618798908114.dat']

Name

7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2']

Name

http://51.79.143.215:13783

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://51.79.143.215:13783']

Name

conitreid.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1702457006, 'iso': '2023-12-13T03:43:26-05:00'} - **IPQS: Domain:** conitreid.com - **IPQS: IP Address:** 45.155.249.7

Pattern Type

stix

Pattern

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

Name

79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21']

Name

masterunis.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'masterunis.net']

Name

reganter.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1702290674, 'iso': '2023-12-11T05:31:14-05:00'} - **IPQS: Domain:** reganter.com - **IPQS: IP Address:** 5.39.221.36

Pattern Type

stix

Pattern

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

Name

137.220.55.190

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.220.55.190']

Name

188.26.127.4

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.26.127.4']

Name

softradar.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'softradar.net']

Name

getfnewssolutions.com

Pattern Type

stix

Pattern

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

Name

http://137.220.55.190:2223

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://137.220.55.190:2223']

Name

http://154.61.75.156:2078

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://154.61.75.156:2078']

Name

51.195.232.97

Description

Pikabot botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.195.232.97']

Name

gertefin.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

70.34.209.101

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[ipv4-addr:value = '70.34.209.101']

Name

airbusco.net

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'airbusco.net']
Name
jessvisser.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'jessvisser.com']
Name
schumacherbar.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'schumacherbar.com']
Name

http://188.26.127.4:13785

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 188.26.127.4 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://188.26.127.4:13785']

Name

1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469']

Name
kolinileas.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'kolinileas.com']

Name
audsystemecll.net
Description
Cobalt Strike botnet C2 domain (confidence level: 100%)
Pattern Type
stix
Pattern
[domain-name:value = 'audsystemecll.net']

Name
ionoslaba.com

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix

Pattern
[domain-name:value = 'ionoslaba.com']

Malware

Name
Pikabot

Domain-Name

Value
karmafisker.com
building4business.net
treeauwin.net
maluisepaul.com
brendonline.com
steamteamdev.net
startupbusiness24.net
prettyanimals.net
welausystem.net
startuptechnologyw.net
conectmeto.net
wardeli.com
wellsystemte.net

withclier.com
unougn.com
gartenlofti.com
reganter.com
buzzybeet.net
settingfir.com
investsystemus.net
nutiensel.com
ionoslaba.com
clearsystemwo.net
bluenetworking.net
gertefin.com
neobeelab.net
masterunis.net
monitorsystem.net
conitreid.com
airbusco.net
auuditoe.com

allcompanycenter.com

caspercan.com

mynewbee.net

buyadvisershop.net

magementfair.com

businesforhome.com

blocknowtech.net

brouweres.com

ruggioil.com

masterunix.net

stockinvestlab.net

getfnewssolutions.com

reelsysmoona.net

getfnewsolutions.com

lindacolor.com

softradar.net

constrtionfirst.com

blockcentersys.net

septcntr.com
investmendvisor.net
trailgroupl.net
cloudwebstart.net
investmentrealtyhp.net
gift4animals.com
kolinileas.com
realeinvestment.net
sandelias.com
mytrailinvest.net
schumacherbar.com
startupbizaud.net
monitor-websystem.net
seohomee.com
garbagemoval.com
animalsfast.net
audsystemecll.net
jessvisser.com

unitedfrom.com
taskthebox.net
erihudeg.com
cloudworldst.net

StixFile

Value
6f9b2fdac415c7eb7fcc31c5ff9aac7e6347ddf4747985b7bac4f76a6f9da193
1dd66462bd11d65247fff82ae81358c9e1b5e1024a953478b8a5de8f5fc5443a
7808be7f2b92c775f6ef047ffc857d8731e75bf486a45fec1c4d199b43c5a6c2
6e18eb1884d2a1a20a0d6a4dcdaf1b7ab342271b2de0d0327848f37eb45e785e
79b1ac4dc5cae6d03548c2ab570e98f9cfb7e4da24480ce3d513b1abdd13bf21
7e85b9d1d09301d8b3f48df44159347d89cb3c798d0436b5e9b060df4072b8c7
6c13985e067cfad583bb1f5751821e649a61a41171a5f95ee9dfd254c04f71a8
4c267d4f7155d7f0686d1ac2ea861eaa926fd41a9d71e8f6952caf24492b376b
ea63ac688aec3ab8920d83617f214922c16aedee341edbe3a18469179555fb21
1a12028a0e0ecc32160e5372a45d95e3045421906f2c807b7c4c8f4a85d47469
eead7f5b6f1282ad988238cc8c39292fa99ea416f7793038a20e5caabe93112a
8514b9d2fe185989d996a2669788910405af5e8fd7102ab3decdd4d727af35df
7094f89bf955dfbdcc4de8943af2328aa7475c2fb6af305c76a6df73aff8b1c3

2c49ff53d0cf0ea36f34148598b8eacca12a1a654bfc09c4e00d6b60a8ad57fe
8045ea8720b66291e3c00f6fd1925de11241410421851b7cabe4a707875a1004
2dad1218d4950ba3a84cfce17af2d8d4ece92f623338d49b357ec9d973ecf8a8
1d365a8a2e72a81a6ffbc6c0c32b28e580872e57df184c270b4fa47ac8b8bf2b
46e0fe3a942bb1f9aa9cd1b460ca7efa9acddb3c5b2d2bc3b42a87d8463f1c66
ed4bba5e886871527fa56beb280f222ef0fde97686db00a74ee02c1a44a0094d
980e2dccc3b83bab32b13f82091f37a2ffcf302c7fb7e87532c7c618f68c0753
33e03a536f869dee3ffa0b1bc8c885f77c50d0a7974b6e9b4041a5a254255c34
3b13380f7dfd615707887f3e8904f432aacdbb111822dd596a44366cb5526624
b436380d62babc42fa6b3adc592e1b6b0bd05c5cb1b0c08aa5c55eae738729e7
29a12bf2f2ff68027ae042a24f1c1285c6bc4b7a495d3d2a8f565ef67141eca8
07279c93f0532a4f5bc4617ab3cb30b7c336f71f587e934a5a0e35ce88fbf632
fbd63777f81cebd7a9f2f1c7f2a8982499fe4d18b9f4aa4e7ed589ceefac47de

IPv4-Addr

Value
51.79.143.215
137.220.55.190
188.34.192.184
15.235.44.231
154.92.19.139
210.243.8.247
15.235.47.206
139.180.216.25
154.61.75.156
64.176.5.228
15.235.202.109
15.235.47.80
154.221.30.136

65.20.78.68

15.235.45.155

70.34.209.101

51.68.147.114

51.195.232.97

188.26.127.4

64.176.67.194

158.247.253.155

Url

Value
https://sindicaturadetecate.gob.mx/pe/?IDbHJCMofpEIzDQjrcwNcDqHoiQRnSKZQcA
http://154.92.19.139:2222
http://51.79.143.215:13783
http://188.34.192.184/76DKN6/Wheez
https://brouweres.com:443/vvs49/0.15313287608559223.dat
http://51.195.232.97:13782
http://51.68.147.114:2083
http://15.235.47.80:23399
http://172.233.156.100:13721
http://15.235.44.231:5938
http://158.247.253.155:2225
http://15.235.47.206:13783
http://188.26.127.4:13785

http://70.34.209.101:13720

https://brouweres.com:443/vvs49/0.6515179055030298.dat

http://65.20.78.68:13721

http://137.220.55.190:2223

http://64.176.5.228:13783

https://lsn.edu.dz/pqis/?aWDzZBatBsyv

https://brouweres.com:443/vvs49/0.8450027286577588.dat

http://154.61.75.156:2078

http://64.176.67.194:2967

https://brouweres.com:443/vvs49/0.9900618798908114.dat

http://139.180.216.25:2967

http://210.243.8.247:23399

http://15.235.202.109:2226

http://154.221.30.136:13724

http://15.235.45.155:2221

External References

- https://otx.alienvault.com/pulse/659e657578d730b29e7590e5
- https://www.trendmicro.com/en_us/research/24/a/a-look-into-pikabot-spam-wave-campaign.html