Jul 24 2023

NETMANAGEIT

Intelligence Report

DDoS Botnets Target Zyxel Vulnerability CVE-2023-28771

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified and identified a number of botnets exploiting a critical vulnerability in the Zyxel firewall system, described as a "critical" vulnerability by the United States' cyber security agency.

Confidence

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

15 / 100

Indicator

Name
f82f5ec551f9ac3bb5a3b1ace5dd21c35239bd983fd9a36e0e7c07bfb48a3fdd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f82f5ec551f9ac3bb5a3b1ace5dd21c35239bd983fd9a36e0e7c07bfb48a3fdd']
Name
hoz.1337.cx
Pattern Type
stix
Pattern
[hostname:value = 'hoz.1337.cx']
Name

0c394849ce4f636cc79cc84389b66a0dbdaf14a61a6d87302e807f2153bc6c2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0c394849ce4f636cc79cc84389b66a0dbdaf14a61a6d87302e807f2153bc6c2b']

Name

171.22.136.15

Description

ISP: DediPath **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDxaRAEIfplkgM4P4vx3u2lDCtegY/VPVsWYe6Ct8DACDeC9RO5BJ+8QetUG4BxZHOPLM+NZDVQZ8DwKodwC1uPh0fr94AnLVWZ4z+CU0SYUk4cz45zCwnOuznG AGUUrNAHIX3j5qlDCptZpuc46DPjI3E3IHcEoQ9RwBELGkEX44ft2U6yNeqHRFd8GVh/56LTn+Rq BjQEurzjjGLsRWx3tMANtZyV5LkWRIuq1POEKxrFlQjbz3y9Ekn4HWgP1pbYZRWarNynl7EUCAGZ1cv5l3O6OUoBjUJFEmhwpR0OeQ36QJuECZ+iIg7C/MJ76crr4kQQFAmBuCXwRZMOpxUj Fingerprint: 98:f4:12:27:4e:d5:85:4c:4a:ac:b1:78:55:25:83:d5 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 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: Thu, 20 Jul 2023 16:49:15 GMT Content-Type: application/octet-stream Content-Length: 130 Last-Modified: Fri, 02 Jun 2023 04:50:55 GMT Connection: keep-alive ETag: "6479752f-82" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '171.22.136.15']

Name

92.118.39.16

Description

ISP: UNMANAGED LTD **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Thu, 20 Jul 2023 21:02:53 GMT Content-Length: 1 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.39.16']

Name

a6729c047d776294fa21956157eec0b50efa7447b8e2834b05be31080767006f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6729c047d776294fa21956157eec0b50efa7447b8e2834b05be31080767006f']

Name

79f69993110688372a5898d05f1141b7f44f3f5f55cd50b6a493c1d33af141c8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79f69993110688372a5898d05f1141b7f44f3f5f55cd50b6a493c1d33af141c8']

Name

2fe13ee992cf00778bcc92dc3732305114dca1700dedca7c29342216df236644

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2fe13ee992cf00778bcc92dc3732305114dca1700dedca7c29342216df236644']

Name

28fa9225db6d4208412398971231348 9e255376134f8e77f07b77c345a026304

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '28fa9225db6d4208412398971231348 9e255376134f8e77f07b77c345a026304']
Name
6137a30d8eb932d25664ced747424b15072e676b5d4d27d5b8f3b84f48344217
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6137a30d8eb932d25664ced747424b15072e676b5d4d27d5b8f3b84f48344217']
Name
928d8ccd71edda5891068d703603ba0b70687f746c9da73afa6692b274ea757c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '928d8ccd71edda5891068d703603ba0b70687f746c9da73afa6692b274ea757c']

Name

85d3d93910bfb8410a0e82810d05aa67a6702ce0cdfc38d1d01f2f9471d20150

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85d3d93910bfb8410a0e82810d05aa67a6702ce0cdfc38d1d01f2f9471d20150']

Name

171.22.136.18

Description

ISP: DediPath **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sun, 23 Jul 2023 15:19:16 GMT Content-Type: application/octet-stream Content-Length: 130 Last-Modified: Fri, 02 Jun 2023 04:50:55 GMT Connection: keep-alive ETag: "6479752f-82" Accept-Ranges: bytes ``` ---------- **5555:** ```
f0VMRgEBAQAAAAAAAAAAAAIAKAABAAAAlIEAADQAAADY3AAAAgAABDQAIAAFACgAEAAPAAEAAHBA
1wAAQFcBAEBXAQAgAQAAIAEAAAQAAAAEAAAAAQAAAAAAAAAAgAAAAIAAAGDYAABg2AAABQAAAACA
AAABAAAAYNgAAGDYAQBg2AEA3AMAAMQzAAAGAAAAAIAAAAcAAABk2AAAZNgBAGTYAQAAAAAACAAA
AAQAAAAEAAAAUeV0ZAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABwAAAAQAAAANwKDh8N8t6QSwTOLwrxvp AAAAAAAAAAAAAAAAAAEEAt6SxAn+UAMNTlAABT4wYAABogMJ/lAABT4xwAnxUP4KARE/8vEQEwoOMA MMTlEEC96B7/L+FA3AEAAAAAAGDYAQAE4C3lQDCf5QAAU+ME0E3iOACfFTgQnxUP4KARE/8vETAAn+UAMJDlAABT4wMAAAokMJ/lAABT4w/goBET/y8RBNCN4gTgneQe/y/hAAAAAGDYAQBE3AEAbNgB AAAAAAAAsKDjAOCg4wQQneQNIKDhBCAt5QQALeUQwJ/lBMAt5QwAn+UMMJ/lJyAA6tYaAOuQUQEA YLEAANSAAAAAIKDjAQAA6rIwUOEDIILgAQBR4wAwoOECEEHiAgCA4vj//4oAMNMFAiCDAAIIoOEg
```
```

CKDhQgiA4EAIgOAAAODhAAig4SAIoOEe/y/
hMEAt6QxAgOIQQJToAlCg4QDAoOMDIKDhAQAA6rIw UeEDwIzgAQBS4wEwoOECIELiAhCB4vj//
8oAMNMFBCig4QzAgwAOOKDhIiig4SM4oOECMIPgJDiD
4C44g+AFMIPgCSDQ5Qwwg+ACBIPgAgAA6gA4oOEjOKDhAgCD4CAosOH6//8aAADg4QAIoOEgC
KDh MEC96B7/
L+EQQC3pTDCf5QDAoOMAQJPlROCf5QwgoOEJAADqDjDS5wAAU+EOMILgCCCC4gMAABoB
MNPlAQBT4YwBjgADAAAKAcC ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '171.22.136.18']

Name

2c55674e938e7618f7c9273e3da61ce7aeab3dc5626b7b8b4e3fc7cc95d0436f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'2c55674e938e7618f7c9273e3da61ce7aeab3dc5626b7b8b4e3fc7cc95d0436f']

Name

d618c817e6a93193a499126156a1f7e888008dacdb247a769fd69ce4c0c87b67

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd618c817e6a93193a499126156a1f7e888008dacdb247a769fd69ce4c0c87b67']

Name

147.182.243.49

Description

CC=US ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '147.182.243.49']

Name

034cdcb42d1d7b921b4732230bbdcb4089107490a30b8cd7a62e67b657e33d26

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '034cdcb42d1d7b921b4732230bbdcb4089107490a30b8cd7a62e67b657e33d26']

Name

729f2fa4d037912a360cb7c4e2c37765da0c38725451600f0258109b672f615e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '729f2fa4d037912a360cb7c4e2c37765da0c38725451600f0258109b672f615e']

Name

109.207.200.47

Description

CC=UA ASN=AS43139 Maximum-Net LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.207.200.47']

Name

51becb81d6bdfe79111974c05f2e4a20a8825a872a92df86cbc98517100b031a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '51becb81d6bdfe79111974c05f2e4a20a8825a872a92df86cbc98517100b031a']

Name

3d69c780fefa0c3a34190989d43268a272004f0623d3e596bc0c92e1744832c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d69c780fefa0c3a34190989d43268a272004f0623d3e596bc0c92e1744832c9']

Name

42b4e116c5d2d3e9d4777c7eaa3c3835a126c02673583c2dfb1ae2bf0bf0db48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '42b4e116c5d2d3e9d4777c7eaa3c3835a126c02673583c2dfb1ae2bf0bf0db48']

Name

312022da42ab6df882c44d984f9aceea7f08e217a5ca8ca985c533a1af399cee

Description

Unix.Dropper.Mirai-7136015-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '312022da42ab6df882c44d984f9aceea7f08e217a5ca8ca985c533a1af399cee']

Name

routercontroller.geek

Pattern Type

stix

Pattern

[domain-name:value = 'routercontroller.geek']

Name

c68211116bbc43c2fe0aba8b598b88b218adc0d995311a4e7030de8acd48076e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c68211116bbc43c2fe0aba8b598b88b218adc0d995311a4e7030de8acd48076e']

Name

109.207.200.44

Description

ISP: Maximum-Net LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **500:** ``` VPN (IKE) Initiator SPI: 55656d6764527746 Responder SPI: 0000000000000000 Next Payload: RESERVED Version: 2.0 Exchange Type: DOI Specific Use Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 204 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.207.200.44']

Name

12c65cfd227d393fd338223eb50140571760de04ef0a21fe3c4636e1bfaf4966

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12c65cfd227d393fd338223eb50140571760de04ef0a21fe3c4636e1bfaf4966']

Name
babaroga.lib
Pattern Type
stix
Pattern
[domain-name:value = 'babaroga.lib']
Name
tempest.lib
Pattern Type
stix
Pattern
[domain-name:value = 'tempest.lib']
Name
109.205.213.30
Description
CC=AZ ASN=AS19318 IS-AS-1
Pattern Type
stix

Pattern

[ipv4-addr:value = '109.205.213.30']

Name

blacknurse.lib

Pattern Type

stix

Pattern

[domain-name:value = 'blacknurse.lib']

Name

193.32.162.190

Description

CC=RO ASN=AS47890 Unmanaged Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.32.162.190']

Name

dragon.lib

Pattern Type

stix

Pattern

[domain-name:value = 'dragon.lib']

Name

109.207.200.42

Description

ISP: Maximum-Net LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **3001:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8 Content-Length: 139 Date: Wed, 08 Feb 2023 02:14:11 GMT Connection: keep-alive Keep-Alive: timeout=5

Cannot GET /

``` ----------

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '109.207.200.42']
```

Vulnerability

Name
CVE-2023-28771

Malware

Name
Katana

Name
Mirai

Attack-Pattern

Name
Network Denial of Service
ID
T1498
Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.
Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for

adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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)

Domain-Name

Value
routercontroller.geek
dragon.lib
blacknurse.lib
babaroga.lib
tempest.lib

StixFile

Value
729f2fa4d037912a360cb7c4e2c37765da0c38725451600f0258109b672f615e
85d3d93910bfb8410a0e82810d05aa67a6702ce0cdfc38d1d01f2f9471d20150
2fe13ee992cf00778bcc92dc3732305114dca1700dedca7c29342216df236644
51becb81d6bdfe79111974c05f2e4a20a8825a872a92df86cbc98517100b031a
0c394849ce4f636cc79cc84389b66a0dbdaf14a61a6d87302e807f2153bc6c2b
79f69993110688372a5898d05f1141b7f44f3f5f55cd50b6a493c1d33af141c8
2c55674e938e7618f7c9273e3da61ce7aeab3dc5626b7b8b4e3fc7cc95d0436f
034cdcb42d1d7b921b4732230bbdcb4089107490a30b8cd7a62e67b657e33d26
42b4e116c5d2d3e9d4777c7eaa3c3835a126c02673583c2dfb1ae2bf0bf0db48
312022da42ab6df882c44d984f9aceea7f08e217a5ca8ca985c533a1af399cee
28fa9225db6d4208412398971231348 9e255376134f8e77f07b77c345a026304
928d8ccd71edda5891068d703603ba0b70687f746c9da73afa6692b274ea757c
c68211116bbc43c2fe0aba8b598b88b218adc0d995311a4e7030de8acd48076e

a6729c047d776294fa21956157eec0b50efa7447b8e2834b05be31080767006f

f82f5ec551f9ac3bb5a3b1ace5dd21c35239bd983fd9a36e0e7c07bfb48a3fdd

6137a30d8eb932d25664ced747424b15072e676b5d4d27d5b8f3b84f48344217

12c65cfd227d393fd338223eb50140571760de04ef0a21fe3c4636e1bfaf4966

3d69c780fefa0c3a34190989d43268a272004f0623d3e596bc0c92e1744832c9

d618c817e6a93193a499126156a1f7e888008dacdb247a769fd69ce4c0c87b67

Hostname

Value
hoz.1337.cx

IPv4-Addr

Value
147.182.243.49
171.22.136.15
109.207.200.44
171.22.136.18
109.207.200.47
92.118.39.16
193.32.162.190
109.205.213.30
109.207.200.42

External References

- https://otx.alienvault.com/pulse/64be7735f5c03be52e3d305c
- https://www.fortinet.com/blog/threat-research/ddos-botnets-target-zyxel-vulnerability-cve-2023-28771