Jun 10 2023

NETMANAGEIT

Intelligence Report

Old Wine in the New Bottle: Mirai Variant Targets Multiple IoT Devices

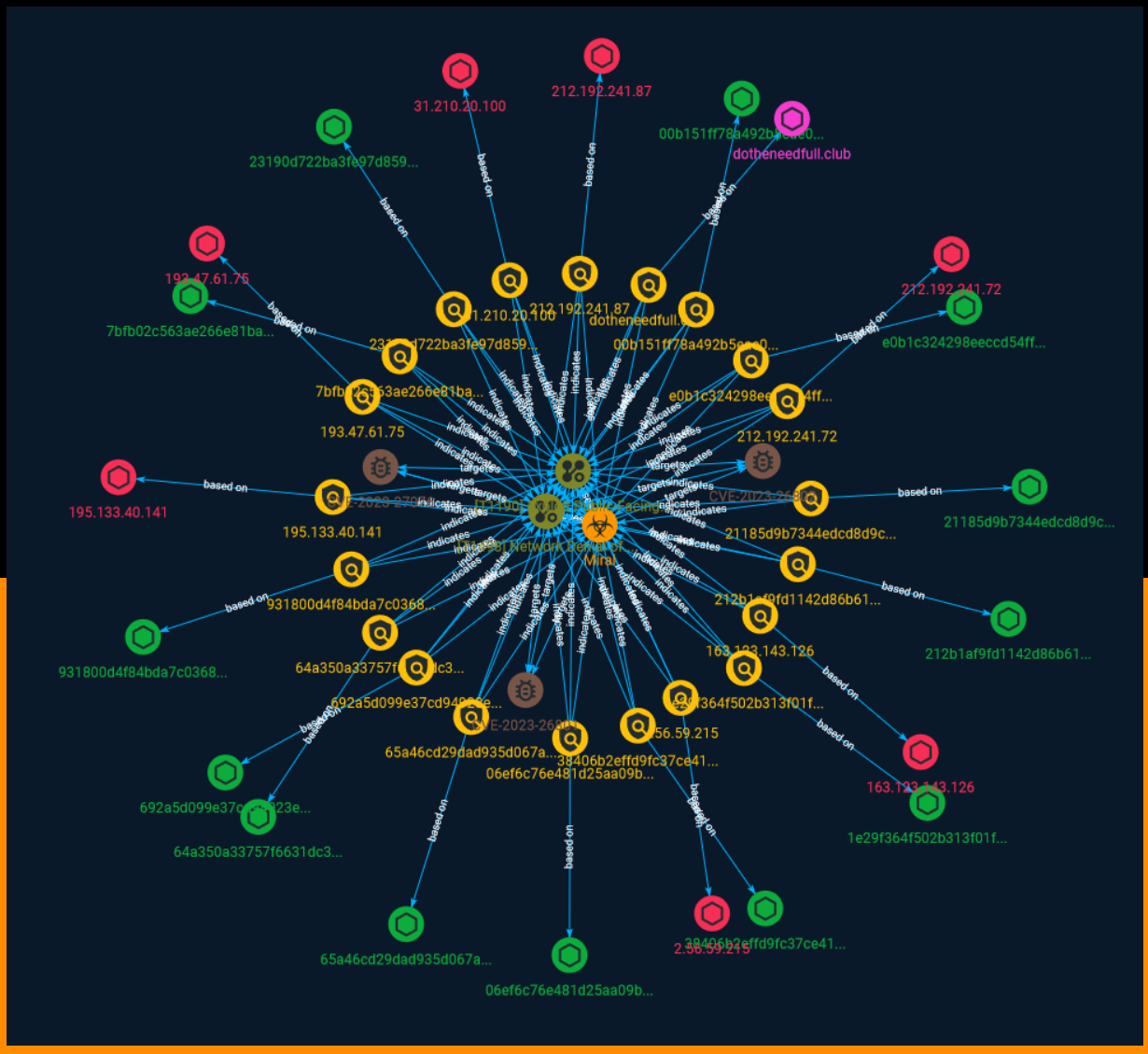

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On April 10, Unit 42 researchers observed a Mirai variant called IZ1H9, which used several vulnerabilities to spread itself.

Confidence

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

15 / 100

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

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending

on the flaw being exploited this may also involve [Exploitation for Defense Evasion] (https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Indicator

Name
2.56.59.215
Description
CC=NL ASN=AS399471 AS-SERVERION
Pattern Type
stix
Pattern
[ipv4-addr:value = '2.56.59.215']
Name
195.133.40.141
Description
CC=DE ASN=AS15731 InterLIR GmbH
Pattern Type
stix

Pattern

[ipv4-addr:value = '195.133.40.141']

Name

e0b1c324298eeccd54ffc2ff48288ec51fbec44f5f82229537508785a9bda6de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0b1c324298eeccd54ffc2ff48288ec51fbec44f5f82229537508785a9bda6de']

Name

06ef6c76e481d25aa09b3b15959d702be29c22d63bd35524766397e3d36d0d2e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '06ef6c76e481d25aa09b3b15959d702be29c22d63bd35524766397e3d36d0d2e']

Name

31.210.20.100

Description

CC=MX ASN=AS14178 Megacable Comunicaciones de Mexico, S.A. de C.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.210.20.100']

Name

163.123.143.126

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '163.123.143.126']

Name

64a350a33757f6631dc375632de191967ae59c876b4718a087e299bd54f23844

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64a350a33757f6631dc375632de191967ae59c876b4718a087e299bd54f23844']

Name

dotheneedfull.club

Pattern Type

stix

Pattern

[domain-name:value = 'dotheneedfull.club']

Name

1e29f364f502b313f01f28f1ae85bf27114fae5eede6550809fe5bca58f59174

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e29f364f502b313f01f28f1ae85bf27114fae5eede6550809fe5bca58f59174']

Name

193.47.61.75

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type
stix
Pattern
[ipv4-addr:value = '193.47.61.75']
Name
212.192.241.72
Description
CC=DE
Pattern Type
stix
Pattern
[ipv4-addr:value = '212.192.241.72']
Name
65a46cd29dad935d067a4289445d2efb2710d44d789bf1bf0efb29f94d20e531
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '65a46cd29dad935d067a4289445d2efb2710d44d789bf1bf0efb29f94d20e531']

Name

23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14']

Name

212b1af9fd1142d86b61956ac1198623f9017153153cfc20bfeab6a9fd44004a

Description

ELF:Mirai-GH\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '212b1af9fd1142d86b61956ac1198623f9017153153cfc20bfeab6a9fd44004a']

Name

931800d4f84bda7c0368c915dfd27721d63ed0ce6a9bc9f13e1417d4c2fe88f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '931800d4f84bda7c0368c915dfd27721d63ed0ce6a9bc9f13e1417d4c2fe88f3']

Name

00b151ff78a492b5eae0c8d3c769857f171f8424cf36c3b2505f7d7889109599

Description

Unix.Dropper.Mirai-7135858-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00b151ff78a492b5eae0c8d3c769857f171f8424cf36c3b2505f7d7889109599']

Name

38406b2effd9fc37ce41ee914fda798de9c9b0e239a0cc94b1464dc2a9984fe9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '38406b2effd9fc37ce41ee914fda798de9c9b0e239a0cc94b1464dc2a9984fe9']

Name

7bfb02c563ae266e81ba94a745ea7017f12010d5491708d748296332f26f04f5

Description

Unix.Trojan.Mirai-6981989-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7bfb02c563ae266e81ba94a745ea7017f12010d5491708d748296332f26f04f5']

Name

21185d9b7344edcd8d9c4af174e468c38cb3b061e6bd6bd64a4be9bd3fa27ff5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21185d9b7344edcd8d9c4af174e468c38cb3b061e6bd6bd64a4be9bd3fa27ff5']

Name

692a5d099e37cd94923ea2b2014d79e6e613fb061a985069736dd3d55d4330c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '692a5d099e37cd94923ea2b2014d79e6e613fb061a985069736dd3d55d4330c4']

Name

212.192.241.87

Description

CC=DE

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.192.241.87']

Malware

Name
Mirai

Vulnerability

Name
CVE-2023-26801
Name
CVE-2023-27076
Name
CVE-2023-26802

Domain-Name

Value
dotheneedfull.club

StixFile

Value
65a46cd29dad935d067a4289445d2efb2710d44d789bf1bf0efb29f94d20e531
00b151ff78a492b5eae0c8d3c769857f171f8424cf36c3b2505f7d7889109599
212b1af9fd1142d86b61956ac1198623f9017153153cfc20bfeab6a9fd44004a
931800d4f84bda7c0368c915dfd27721d63ed0ce6a9bc9f13e1417d4c2fe88f3
21185d9b7344edcd8d9c4af174e468c38cb3b061e6bd6bd64a4be9bd3fa27ff5
1e29f364f502b313f01f28f1ae85bf27114fae5eede6550809fe5bca58f59174
7bfb02c563ae266e81ba94a745ea7017f12010d5491708d748296332f26f04f5
06ef6c76e481d25aa09b3b15959d702be29c22d63bd35524766397e3d36d0d2e
38406b2effd9fc37ce41ee914fda798de9c9b0e239a0cc94b1464dc2a9984fe9
23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14
e0b1c324298eeccd54ffc2ff48288ec51fbec44f5f82229537508785a9bda6de
64a350a33757f6631dc375632de191967ae59c876b4718a087e299bd54f23844
692a5d099e37cd94923ea2b2014d79e6e613fb061a985069736dd3d55d4330c4

IPv4-Addr

Value
163.123.143.126
195.133.40.141
212.192.241.87
193.47.61.75
31.210.20.100
2.56.59.215
212.192.241.72

External References

- https://otx.alienvault.com/pulse/64712ddfa559e42b1ee4bf5c
- https://unit42.paloaltonetworks.com/mirai-variant-iz1h9/