Quorum Cyber

Threat Intelligence
Mirai Botnet

TLP Status: White

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1		01/02/2023	Initial Report
1.0		30/05/2023	Final PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Mirai Botnet

Overview

Mirai is a botnet malware variant that compromises smart devices that operate on ARC processors, the aim of which is to formulate a network of bot machines to carry out distributed denial-of-service (DDoS) attacks[1]. Mirai scans the internet for Internet of Things (IoT) devices that operate on the ARC processor. The malware has the capabilities of establishing a foothold on target systems if the username and password combination has not been reconfigured. Mirai initially infected and weaponised devices such as smart cameras and Realtek routers[2].

The botnet variant was created in a racketeering attempt by the cofounders of Protraf Solutions, an organisation offering DDoS mitigation services. The creators of Mirai originally leased out the Mirai Botnet variant for the implementation of DDoS attacks, as well as 'click fraud' attacks. The source code of Mirai was subsequently released into the wild, since when the code has constantly mutated and, as such, has led to the formation of more advanced botnet strains, such as: Okiru, Satori, Masuta and PureMasuta. These variants operate across the botnet model spectrum, namely those of: centralised botnets, tiered C&Cs and decentralised botnets.

In April 2023, the Mirari Botnet malware was detected to be actively exploiting a TP-Link Archer A21 (AX1800) WiFi router vulnerability.

Impact

The Mirai Botnet malware is particularly dangerous due to their abilities to implement DDoS attacks, which can prove difficult to remediate. Furthermore, IoT botnets have been documented to have implemented the following additional infection vectors on target systems:

- Denial-of-Service to legitimate traffic of Internet Service Providers
- Sending of spam email
- Launching of DDoS attacks to compromise websites and APIs
- Performance of click fraud attacks
- Disabling anti-virus software
- Solving weak CAPTCHA challenges on websites in order to imitate human behaviour during logins
- Theft of credit card information
- Hold companies to ransom with threats of DDoS attacks.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats such as the Mirai Botnet. EDRs can alert system users of potential breaches and stop the malware process during early signs of an attack attempt, therefore limiting the scope of damage.

[1] What is the Mirai Botnet? | Cloudflare
[2] What was the Mirai botnet | Malwarebytes

Affected Products

- Linux OS

Containment, Mitigations & Remediations

It is strongly recommended that the following mitigation steps are adhered to harden the network defences against all variations of botnet infections:

- Update IoT devices to the latest product versions
- Reconfigure the factory setting log-in keys, as well as the default username and password of IoT devices
- Implement network segmentation to ensure that all IoT devices are on a separate network from systems critical for daily operations
- Use and maintain anti-virus software
- Implement an official password policy.

Moreover, as previously stated, a main method of reducing the threat of the Mirai Botnet is to detect it in the early stages, whilst implementing an effective and monitored EDR solution. An effective EDR tool will increase detection of malicious attempts of Mirai Botnet compromise and halt the malware's progress if detected.

Indicators of Compromise

Mirai Associated File Hashes (SHA-256):

- 94b34225c084dba7db19725bc2aad74bcf85b9d0990a2c31b665faa4f42ec39a
- 076b8f462d0f38e96dcbb6c777169f3484104d011fad00df25d90b084e073404
- 275223305ebaa8383f05b36bfaf6c83aff0d0ac8ac3ec8584719f8716deefdc1
- 90a1b0edb95f9eb75402ac65073554a1c79011d7b3bfc3e9ee4cc7a532b4aff3
- 965d5ef911e5523bde2cad1dc259c52cbc80ae1f6901da8e15ff647d5e226bda
- af651f64efa4eb8eb72d494e999538cf8913ff4ebaeb6624ac245eca76b91e85
- c3e016cab6cf569300ceaef1bdeef56c282f5cc25b52577e45a5d33293af8455
- c7ff9eab4e6f1f3ba2c1ad24ed6bd2d261a4a556721faa8e41ba8ee207dcfd72
- da30e263d01e0a3cd95e29ac7e95c2674da40f35c438e6a4389e21c9d63ff8f4
- 501ba653527be5dc81cd5b5f4452dc90e108dc63e202a48fb26db83316a9e113
- 1ba51c1c22dfc2fda88da44ec8cab8ecb9670a1398ca4dfccefdc790a2c4da4e
- 29b409e7090613acbc528ea34d1905ae05e282423e97043c3cdc5f391af036ad
- 349c4b977fe2e9a89e5c36200846a0e8540f6006721133a69ba6be14765b281f
- 4eb63b9bec2e6996070125e809344cb9a7e38f1ba5062a558ace7bae15981095

- 54be7fe1c0f0d68e84d311c4a32e07029387a28307075849f87918b197f7eab0
- 658f77e7854641dd637c31b007166dea4ec7091d6a00f0cb00b417d2ba00cccd
- 7f62c5975b3c8cd99f84d52a7453307865b523e97685bc85b3bdbdbd11384143
- 809c8bafc1e07789a6487ac4e5274df8b4f0af68a85c780076114c7dc178a658

Mirai Associated IP Addresses:

- 179[.]43[.]175[.]5
- 185[.]216[.]71[.]112
- 204[.]76[.]203[.]6
- 45[.]95[.]55[.]214
- 101[.]109[.]242[.]42
- 180[.]117[.]224[.]253
- 223[.]13[.]70[.]225
- 121[.]227[.]226[.]166
- 27[.]43[.]119[.]75
- 61[.]53[.]72[.]55
- 101[.]108[.]64[.]115
- 111[.]242[.]240[.]115
- 112[.]80[.]116[.]27
- 113[.]221[.]26[.]207
- 118[.]121[.]188[.]128
- 125[.]44[.]233[.]214
- 175[.]11[.]66[.]136
- 182[.]122[.]108[.]50
- 220[.]186[.]169[.]99
- 45[.]95[.]55[.]202

Mirai Associated Domain:

- botnet[.]zu0x[.]com
- cdn2[.]duc3k[.]com
- pxp[.]softdetails[.]in
- cnc[.]chinesetable[.]us
- client[.]orxy[.]space
- fluu[.]badworldgama[.]xyz

- rigs[.]zu0x[.]com
- shop[.]loveday[.]cloud

Mirai Associated URLs:

- hxxp[://]112[.]80[.]116[.]27:50607/bin[.]sh
- hxxp[://]118[.]121[.]188[.]128:57199/bin[.]sh
- hxxp[://]175[.]11[.]66[.]136:37499/i
- hxxp[://]179[.]43[.]175[.]5/bins/sh4
- hxxp[://]182[.]122[.]108[.]50:47046/bin[.]sh
- hxxp[://]223[.]13[.]70[.]225:45488/i
- hxxp[://]45[.]95[.]55[.]202/reaper/reap[.]arm7
- hxxp[://]101[.]108[.]64[.]115:54349/bin[.]sh
- hxxp[://]101[.]109[.]242[.]42:35044/bin[.]sh
- hxxp[://]111[.]242[.]240[.]115:42206/i
- hxxp[://]112[.]80[.]116[.]27:50607/i
- hxxp[://]113[.]221[.]26[.]207:58992/Mozi[.]m
- hxxp[://]117[.]158[.]60[.]98:56639/Mozi[.]m
- hxxp[://]118[.]121[.]188[.]128:57199/i
- hxxp[://]121[.]227[.]226[.]166:33229/i
- hxxp[://]125[.]44[.]233[.]214:48455/bin[.]sh
- hxxp[://]176[.]97[.]210[.]166/Cherarm5
- hxxp[://]179[.]43[.]175[.]5/bins/arc
- hxxp[://]179[.]43[.]175[.]5/bins/arm6
- hxxp[://]179[.]43[.]175[.]5/bins/m68k

Exploited Vulnerabilities

The following IoT vulnerabilities have been disclosed in relation to the Mirai Botnet family[3]:

- CVE-2018-4068, CVE-2018-4070 and CVE-2018-4071: Information disclosure vulnerabilities impacting Sierra Wireless AirLink ES450 FW gateway version 4.9.3
- CVE-2019-12258, CVE-2019-12259, CVE-2019-12262 and CVE-2019-12264: DoS vulnerabilities impacting several versions of Wind River Systems' VxWorks real-time operating system (RTOS)

[3] Why Mirai is still a threat to the IoT ecosystem | Intel471

- CVE-2019-12255, CVE-2019-12260, CVE-2019-12261 and CVE-2019-12263: Memory corruption vulnerabilities impacting several versions of Wind River Systems' VxWorks RTOS
- CVE-2021-28372: An authentication bypass vulnerability impacting ThroughTek Kalay P2P Software Development Kit (SDK) versions 3.1.5 and earlier
- CVE-2021-31251: An improper authentication vulnerability impacting multiple firmwares from Chiyu Technology, for which an exploit and walk-through demonstration of an exploit were observed in open sources
- CVE-2023-1389: A command injection vulnerability affecting TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219

Threat Landscape

Regardless of the fact that the creators of the Mirai Botnet malware were apprehended, the source code of the malware was subsequently released into the wild and, as such, Mirai and other botnet variants pose a significant threat to unprotected IoT devices and the associated networks.

Since being released on the dark web, the Mirai source code is continuously being altered by threat actors to create more advanced versions of the malware. To date, these have included Okiru, Satori, Masuta and PureMasuta. Due to the open access nature of the source code as well as IoT markets continuing to develop in notoriety, it is highly likely that further variants will continue to emerge, leading to the potential of future attack efforts.

Threat Group

Due to the progressive development of additional variants, no specific threat actor has been associated with the Mirai Botnet malware. However, it should be noted that Russian-speaking threat actors have been linked to documented cases of attacks whilst using more advanced variants of the botnet[4].

Mitre Methodologies

Initial Access
T1566 - Phishing[5]

Execution
T1204.001 - User Execution: Malicious Link[6]
T1204.002 - User Execution: Malicious File[7]
T1059 - Command and Scripting Interpreter[8]
T1059.001 - Command and Scripting Interpreter: PowerShell[9]

Persistence
T1574 - Hijack Execution Flow[10]

[4] Why Mirai is still a threat to the IoT ecosystem | Intel471
[5] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®
[6] User Execution: Malicious Link, Sub-technique T1204.001 - Enterprise | MITRE ATT&CK®
[7] User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®
[8] Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®
[9] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[10] Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®

Privilege Escalation
T1574 - Hijack Execution Flow[11]

Defence Evasion
T1562 - Impair Defenses[12]
T1574 - Hijack Execution Flow[13]

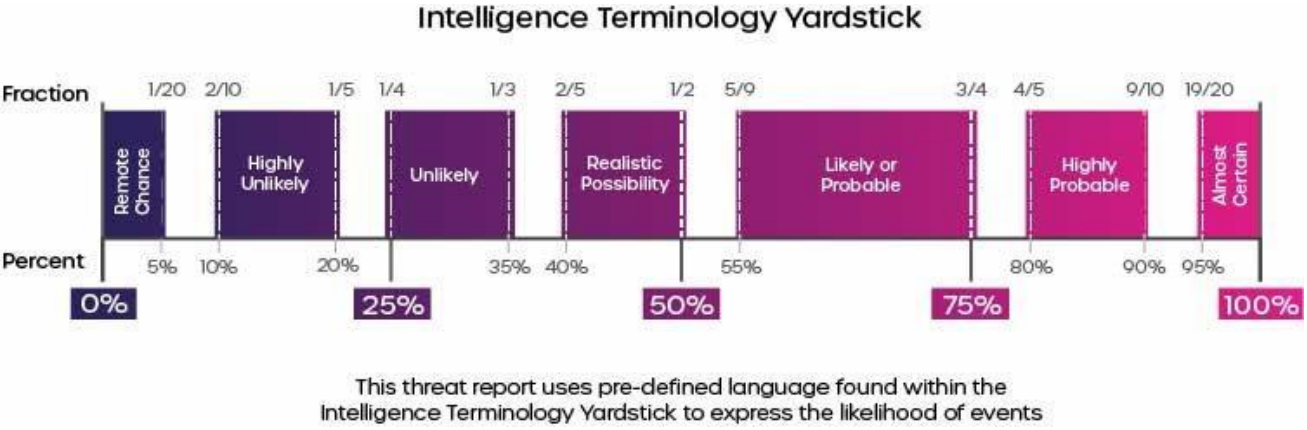
Discovery
T1046 - Network Service Discovery[14]
T1016 - System Network Configuration Discovery[15]
T1049 - System Network Connections Discovery[16]

Command and Control
T1071 - Application Layer Protocol[17]
T1071.001 - Web Protocols[18]

Further Information

- Avast Report
- CloudFlare Report
- Malwarebytes Report
- Intel471 Analysis
- CIS Security Blog

Intelligence Cut-off Date (ICoD): 30/05/2023 10:00 UTC



[11] Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®
[12] Impair Defenses, Technique T1562 - Enterprise | MITRE ATT&CK®
[13] Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®
[14] Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®
[15] System Network Configuration Discovery, Technique T1016 - Enterprise | MITRE ATT&CK®
[16] System Network Connections Discovery, Technique T1049 - Enterprise | MITRE ATT&CK®
[17] Application Layer Protocol, Technique T1071 - Enterprise | MITRE ATT&CK®
[18] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®