THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Mirai

Threat Actor Malware

Description

MIRAI

CATEGORY

Malware

SEVERITY

High

Platforms

Linux

IMPACT

- Massive DDoS Attacks
- Compromised IoT Devices
- Global Disruptions
- Evolving Threat Variants

Mirai is a prominent botnet that was first uncovered in August 2016 by MalwareMustDie, targeting Linux-based devices and IoT systems such as IP cameras, routers, and other embedded devices. It spreads by exploiting devices with weak or default credentials, integrating them into a botnet capable of launching large-scale Distributed Denial-of-Service (DDoS) attacks. The name "Mirai," meaning "future" in Japanese, reflects its enduring significance in the cybersecurity landscape. After its source code was publicly released on "Hack Forums," countless variants have surfaced, continuing to infect networks worldwide and demonstrating the botnet's adaptability over time.

Mirai remains active to this day, with its evolving variants targeting new devices and vulnerabilities in IoT systems. The botnet's operators, often referred to as the Mirai Group, use it to execute disruptive DDoS campaigns, causing significant harm to businesses and critical infrastructure globally. Mitigation strategies include securing devices with strong, unique credentials, keeping firmware up-to-date, monitoring network traffic for anomalies, and implementing network segmentation and firewall protections. Despite these defenses, Mirai persists as a dynamic and ongoing threat, underscoring the need for constant vigilance in IoT security.

Kill Chain

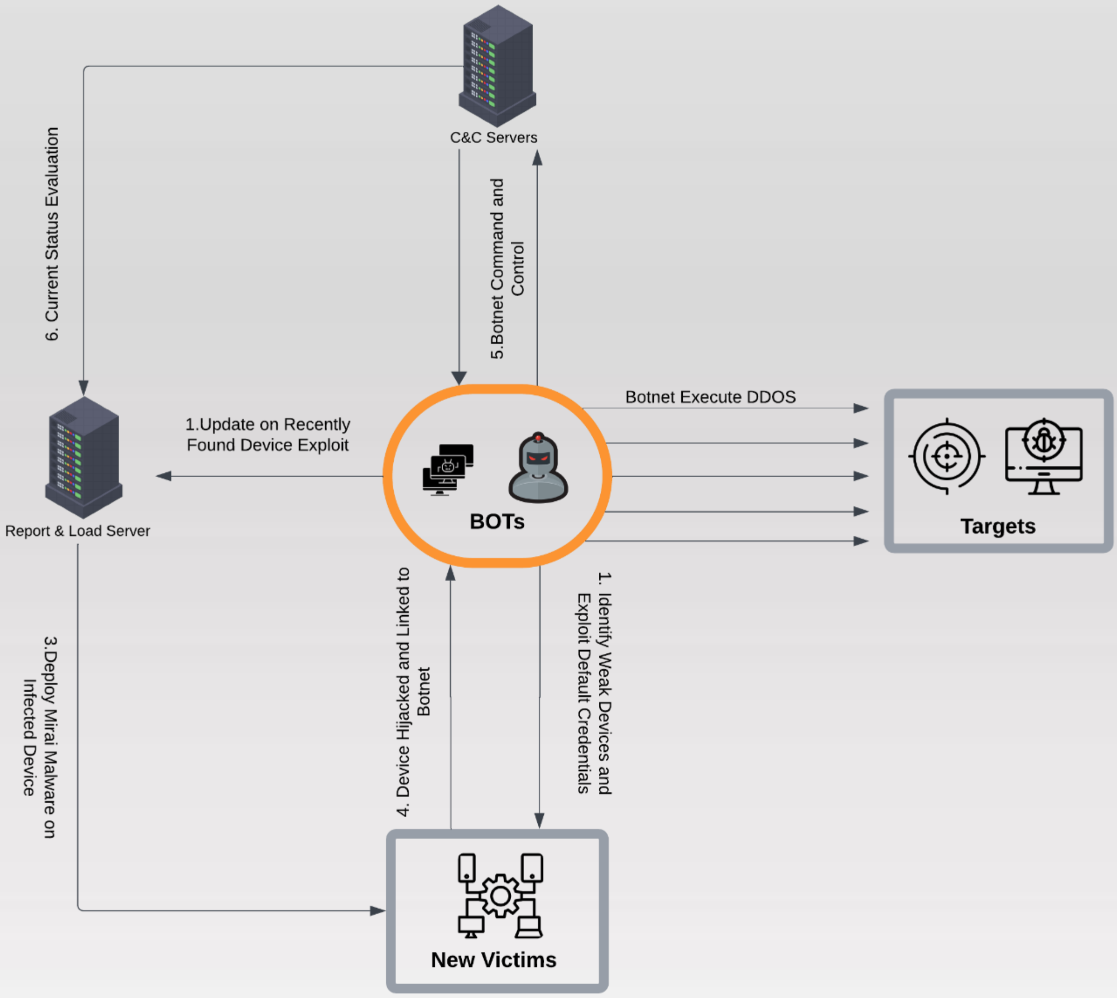
C&C Servers
6. Current Status Evaluation
5.Botnet Command and Control
Report & Load Server
1.Update on Recently Found Device Exploit
BOTs
Botnet Execute DDOS
Targets
3.Deploy Mirai Malware on Infected Device
4. Device Hijacked and Linked to Botnet
1. Identify Weak Devices and Exploit Default Credentials
New Victims

Figure 1 Kill Chain

Indicator of Compromise

SHA256

```
70f771acd4001552c5d52e094d81e8182999aea36a8da9408986dafcafd4108b
cc39d4f5323db2ee8f3f429ac735ee31ed5bccfd1f85d9ad30969d0ff310e953
aa949b446142cfe846fae5807bd1926e27413d4ed159f0d64e229e16405db877
38c6186a6fecf95119db02642066425ea032a548c047109d2f95a5bb57b93c14
4d3aced5ba022dfb56457b0b542d928ee51494a2617e93d9b0b11cdf73b28ece
e9443c9839e44b26721c53e21c46a4962d48a17ff157a7613dbd37f057f3ca2c
842c5aa3d5f89619982040c7b219b5bd94747795429944eca74c95cc51ac09ff
894d7d18d48c6209b1364e79a33f08a1f422a3eaf8ce45d12c34925fa22a9b37
c7d3f9322b1df4367a776ed5450fe89b64e3fa03fb737c63660fb9a3771e0515
507c78d68af86d5cac722485d716aeb6b56ad497b80b5acbb4f72656c8975628
840f71bd9511687d213b34f5897782402bd1874a67d732540d08b85be32a3e62
5361bcacfe99af180093639c55d4492cfa41c67e9d47294a479a5f84737fd756
5a83a114618b3ff9218749032e0db52284af78173721dcb01693d032c3f39db6
ad5b1001a96dc0bcb196d7d36ea286fdc000e3bdd6c7ec20c81f4476653556d1
ed852379c284be21d3d291bf28d0f337fba1df6e271913f770b0f2b16723869b
bc1e3631919954989eacfa536b5e81f9b95c753dc93efcebfb1783465303c32a
6c568bd265a5c182913cd277c88a151c797dfeb05244edaf156dea1b389a0baa
27d13d2f3ecfa851961cceee52850b9a1a18a0acd72cd9a6c0e1d1ee13ff3715
9d7bcbd227ddec00a4fd7b3892eba60d55f72d379d2031e459097f025d7c1792
7aead7f883ad2f95d7924111f5c35349ee8b250bc0d3846b34ff148f2a081ebc
1cd3e59c61ea3c704a1a5a173802106636a6d3aa20339f3811a20cc0ff89c2d5
a1dbee4731197745736293298688861fbea713564a85b1a00d2bdc0f457c1cf93
0fe42c6bace1aafe91e7320d353c1ca482aca127bb11cef80a374eb7fb92c1df
d1eb6155452f3ab97e2df1311a93514c6c4be839810a31307404b22a21ca400f
1f8dd777f2b7d73d80edd4838c967ecbda52329a4655a88232bc99c4d9938765
```

Indicator of Compromise

MD5

561ccfd5b0ebe406d0b12df2e891e162
a4ea0982ea775fbc4557052cf1613b46
65d6d4897e9c295144450b2cf27d4cfd
7e1c6b650321cf8c4d478efef84809ba
42dd0dd5a0d798b589d95dc36f1cbd99
5623e3d922a8b4a86e37f832d8dc1723
e96e55c5a8ffad62537f7478dc0c0108
9f6bf2d1851e1aa00574e898b286a828
c029e40e274644b7a5e12cbedf829d64
e4c8fd03b5000066b3d9287923cb4633
232b002e8b9b8f3f4564962c029076ef
5d960b87f9e7c9b5744b9e4dac86bc02
bd827c8352a04573804d21482a13085d
d0ae1b5c5bb0a21598513af1c24241db
1a18318a911cb02d42cc08e0966cb7f1
e2f4e02895958be4c0ce38865719fc04
50728716bbb3316434121160f54a0457
ffe59b766a0bce1e3801e1d121591ddd
863d42556b9959a21f17a42ded62abf4
533f9b0a0b39795fc283c93337c09636
0c2f9c2a0adef69479c517fcf0d987ab
18c6ee92c7637a8a4e4c036381f19954
939406d5d370d1a039a9b0829d910b05
51209b0209e9874b27699a62f313c7db

Remediation

- Change Default Credentials
- Update and Patch Devices Regularly
- Network Segmentation
- Implement Intrusion Detection and Prevention Systems (IDPS)
- Device Firewall and Access Control
- Disable Unnecessary Services and Ports
- Network Traffic Analysis and Monitoring
- Block Known Mirai IPs and Domains
- User Education
- Incident Response Plan

ThreatCure

Cyber Threat Advisory

Secure your byte world

Marai

Threat Actor Malware