Oct 10 2023

NETMANAGEIT

Intelligence Report

IZ1H9 Campaign Enhances Its Arsenal with Scores of Exploits

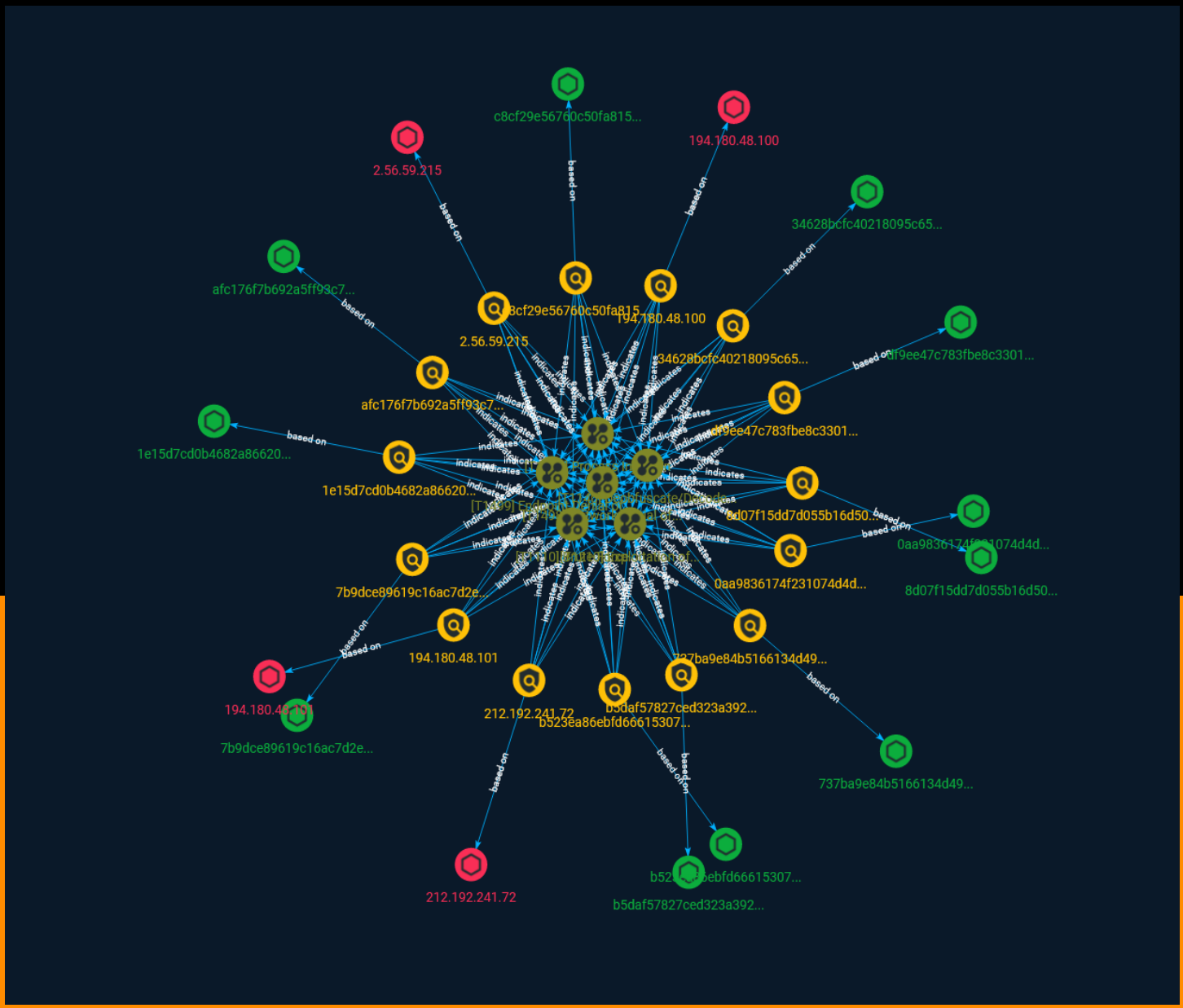

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In September 2023, our FortiGuard Labs team observed that the IZ1H9 Mirai-based DDoS campaign has aggressively updated its arsenal of exploits. Thirteen payloads were included in this variant, including D-Link devices, Netis wireless router, Sunhillo SureLine, Geutebruck IP camera, Yealink Device Management, Zyxel devices, TP-Link Archer, Korenix Jetwave, and TOTOLINK routers.

Confidence

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

15 / 100

Content

N/A

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

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a

victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Exploitation of Remote Services

ID

T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

Name

Endpoint Denial of Service

ID

T1499

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting 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) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the

system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may 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 DoS attacks against endpoint resources, 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. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

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
1e15d7cd0b4682a86620b3046548bdf3f39c969324a85755216c2a526d784c0d
Description
SUSP_ELF_LNX_UPX_Compressed_File
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1e15d7cd0b4682a86620b3046548bdf3f39c969324a85755216c2a526d784c0d']
Name
df9ee47c783fbe8c3301ed519033fc92b05d7fd272d35c64b424a7e46c6da43b
Description
Unix.Dropper.Mirai-7135858-0
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df9ee47c783fbe8c3301ed519033fc92b05d7fd272d35c64b424a7e46c6da43b']

Name

b523ea86ebfd666153078593476ca9bd069d6f37fa7846af9e53b1e01c977a17

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b523ea86ebfd666153078593476ca9bd069d6f37fa7846af9e53b1e01c977a17']

Name

2.56.59.215

Description

CC=US ASN=AS399471 AS-SERVERION

Pattern Type

stix

Pattern

[ipv4-addr:value = '2.56.59.215']

Name

0aa9836174f231074d4d55c819f6f1570a24bc3ed4d9dd5667a04664acb57147

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0aa9836174f231074d4d55c819f6f1570a24bc3ed4d9dd5667a04664acb57147']

Name

194.180.48.101

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDypwsxlt+/478EgV4Jn764y3ZizIsBFu5vDjeZaxc25STepCxEA+t1oWX7LaZNvU2b2rr4JTSikFsIysiZ0SLsvmiHGDKfGRrU4vqwZj3FDpLKXQ0eiexnlAhrSIcXs34U/Z3ETBL+5QvK0wooUPgjByai5P019YxxB99tDdz0l5cVZ5BwYgLxJNzbCbkKuwWWT8UIH3iRv5CoUGjeIPaxiP95w0YdR3SKNRm+VCrsM9pFHjjJj8q2gSuKwd+6pF85g90xmPqvXVIQFXCrmVe4s7zrmqY6oGQK7Q3cvtAsD+gU/A7DdEfdFiZ9iiH0foe+mDMyvOWDZnU4PbcwTuSXFingerprint: 93:21:32:01:e8:6e:58:14:b8:e8:d9:43:68:b8:0a:7f 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ---------- **3306:** ``` MySQL: Protocol Version: 10 Version: 5.6.51 Capabilities: 63487 Server Language: 8 Server Status: 2 Extended Server Capabilities: 32895 Authentication Plugin: mysql_native_password ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.180.48.101']

Name

194.180.48.100

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Date: Thu, 05 Oct 2023 19:02:55 GMT Server: Apache/2.4.6 (CentOS) Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.180.48.100']

Name

b5daf57827ced323a39261a7e19f5551071b5095f0973f1397d5e4c2fcc39930

Description

Backdoor:Linux/Mirai.YA!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b5daf57827ced323a39261a7e19f5551071b5095f0973f1397d5e4c2fcc39930']

Name

afc176f7b692a5ff93c7c66eee4941acf1b886ee9f4c070faf043b16f7e65c11

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afc176f7b692a5ff93c7c66eee4941acf1b886ee9f4c070faf043b16f7e65c11']

Name

8d07f15dd7d055b16d50cb271995b768fdd3ca6be121f6a35b61b917dfa33938

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8d07f15dd7d055b16d50cb271995b768fdd3ca6be121f6a35b61b917dfa33938']

Name

212.192.241.72

Description

CC=CZ ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.192.241.72']

Name

c8cf29e56760c50fa815a0c1c14c17641f01b9c6a4aed3e0517e2ca722238f63

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c8cf29e56760c50fa815a0c1c14c17641f01b9c6a4aed3e0517e2ca722238f63']

Name

737ba9e84b5166134d491193be3305afa273733c35c028114d8b1f092940b9a3

Description

SUSP_ELF_LNX_UPX_Compressed_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '737ba9e84b5166134d491193be3305afa273733c35c028114d8b1f092940b9a3']

Name

7b9dce89619c16ac7d2e128749ad92444fe33654792a8b9ed2a3bce1fee82e6a

Description

Unix.Trojan.Mirai-6981989-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b9dce89619c16ac7d2e128749ad92444fe33654792a8b9ed2a3bce1fee82e6a']

Name

34628bcfc40218095c65678b52ce13cea4904ce966d0fd47e691c3cb039871ec

Description

Unix.Trojan.Mirai-9936831-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34628bcfc40218095c65678b52ce13cea4904ce966d0fd47e691c3cb039871ec']

StixFile

Value
b5daf57827ced323a39261a7e19f5551071b5095f0973f1397d5e4c2fcc39930
0aa9836174f231074d4d55c819f6f1570a24bc3ed4d9dd5667a04664acb57147
8d07f15dd7d055b16d50cb271995b768fdd3ca6be121f6a35b61b917dfa33938
7b9dce89619c16ac7d2e128749ad92444fe33654792a8b9ed2a3bce1fee82e6a
b523ea86ebfd666153078593476ca9bd069d6f37fa7846af9e53b1e01c977a17
df9ee47c783fbe8c3301ed519033fc92b05d7fd272d35c64b424a7e46c6da43b
afc176f7b692a5ff93c7c66eee4941acf1b886ee9f4c070faf043b16f7e65c11
34628bcfc40218095c65678b52ce13cea4904ce966d0fd47e691c3cb039871ec
737ba9e84b5166134d491193be3305afa273733c35c028114d8b1f092940b9a3
1e15d7cd0b4682a86620b3046548bdf3f39c969324a85755216c2a526d784c0d
c8cf29e56760c50fa815a0c1c14c17641f01b9c6a4aed3e0517e2ca722238f63

IPv4-Addr

Value
194.180.48.100
194.180.48.101
2.56.59.215
212.192.241.72

External References

- https://otx.alienvault.com/pulse/65256889f90b0d9b7d871ed1
- https://www.fortinet.com/blog/threat-research/Iz1h9-campaign-enhances-arsenal-with-scores-of-exploits