Mar 20 2024

NETMANAGEIT

Intelligence Report

Mirai Nomi: A Botnet Leveraging DGA

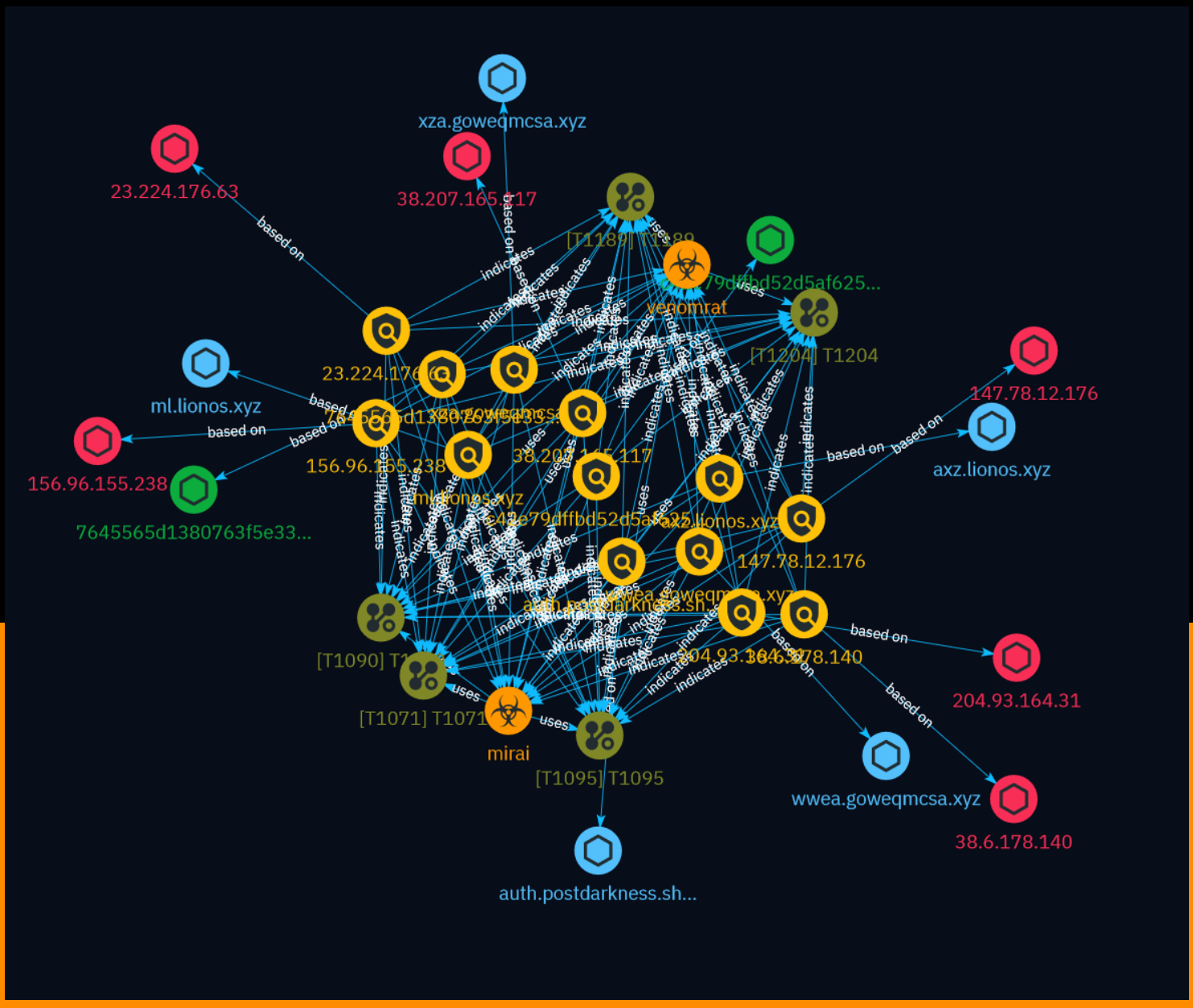

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report provides an analysis of a new Mirai botnet variant named Mirai Nomi that utilizes domain generation algorithm (DGA) for command and control. The variant employs multiple encryption algorithms and introduces persistent functions. It fetches time seeds from NTP servers for DGA and connects to decrypted C2 servers after verifying availability. The botnet is currently not very active but exhibits concerning capabilities.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
xza.goweqmcsa.xyz
Pattern Type
stix
Pattern
[hostname:value = 'xza.goweqmcsa.xyz']
Name
wwea.goweqmcsa.xyz
Pattern Type
stix
Pattern
[hostname:value = 'wwea.goweqmcsa.xyz']
Name
ml.lionos.xyz

Pattern Type
stix
Pattern
[hostname:value = 'ml.lionos.xyz']
Name
axz.lionos.xyz
Pattern Type
stix
Pattern
[hostname:value = 'axz.lionos.xyz']
Name
auth.postdarkness.shop
Pattern Type
stix
Pattern
[hostname:value = 'auth.postdarkness.shop']
Name
38.207.165.117

Description

- **Zip Code:** N/A - **ISP:** Overland Storage - **ASN:** 967 - **Organization:** VMISS - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 38.207.165.117 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.78 - **Longitude:** -96.81

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.207.165.117']

Name

204.93.164.31

Description

- **Zip Code:** N/A - **ISP:** Deft Hosting - **ASN:** 142036 - **Organization:** Hosteons Pte. - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 204.93.164.31 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.05 - **Longitude:** -118.24

Pattern Type

stix

Pattern

[ipv4-addr:value = '204.93.164.31']

Name

156.96.155.238

Description

- **Zip Code:** N/A - **ISP:** VolumeDrive - **ASN:** 46664 - **Organization:** VolumeDrive - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 156.96.155.238 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Encino - **Latitude:** 34.18 - **Longitude:** -118.52

Pattern Type

stix

Pattern

[ipv4-addr:value = '156.96.155.238']

Name

147.78.12.176

Description

- **Zip Code:** N/A - **ISP:** Datacamp - **ASN:** 212238 - **Organization:** Datacamp - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 147.78.12.176 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** North Holland - **City:** Amsterdam - **Latitude:** 52.31 - **Longitude:** 4.95

Pattern Type

stix

Pattern

[ipv4-addr:value = '147.78.12.176']

Name

c42e79dffbd52d5af625a280655052baa55cbeb77eec3716c21c15fc65777a49

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c42e79dffbd52d5af625a280655052baa55cbeb77eec3716c21c15fc65777a49']

Name

7645565d1380763f5e33f2881c932d4a9f8d204444675540273c3d9e99590a1c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7645565d1380763f5e33f2881c932d4a9f8d204444675540273c3d9e99590a1c']

Name

38.6.178.140

Description

- **Zip Code:** N/A - **ISP:** Cnservers LLC - **ASN:** 40065 - **Organization:** Cnservers LLC - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 38.6.178.140 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.05 - **Longitude:** -118.24

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.6.178.140']

Name

23.224.176.63

Description

- **Zip Code:** N/A - **ISP:** Cnservers LLC - **ASN:** 40065 - **Organization:** Cnservers LLC - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 23.224.176.63 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.05 - **Longitude:** -118.24

Pattern Type

stix

Pattern
[ipv4-addr:value = '23.224.176.63']

Malware

Name
venomrat

Name
mirai

Attack-Pattern

Name
T1189
ID
T1189
Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable

version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

T1095

ID

T1095

Description

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.(Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL). ICMP communication between hosts is one example.(Citation: Cisco Synful Knock Evolution) Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.(Citation: Microsoft ICMP) However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

Name

T1090

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal

Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1071

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.

Hostname

Value
xza.goweqmcsa.xyz
wwea.goweqmcsa.xyz
ml.lionos.xyz
axz.lionos.xyz
auth.postdarkness.shop

IPv4-Addr

Value
38.207.165.117
204.93.164.31
156.96.155.238
147.78.12.176
38.6.178.140
23.224.176.63

StixFile

Value
c42e79dffbd52d5af625a280655052baa55cbeb77eec3716c21c15fc65777a49
7645565d1380763f5e33f2881c932d4a9f8d204444675540273c3d9e99590a1c

External References

- https://blog.xlab.qianxin.com/mirai-nomi-en/
- https://otx.alienvault.com/pulse/65fab04fbe5d4ba8dabc68e9