

# Analyzing the Mirai Botnet Utilizing AlienVault Threat Intelligence



Matthias Cannon

---

→ C - otx.alienvault.com/browse/global/pulses?include\_inactive=0&sort=-modified&page=1&limit=10

 Browse Scan Endpoints Create Pulse Submit Sample API Integration All Search

We've found 73M + results

Pulses (315K) Users (271K) Groups (855) Indicators (72M) Malware Families (27K)

Show: All ▾ Sort: Recently Modified ▾

**ETIC Cybersecurity 2024-02-29 Port Scan**  
CREATED 19 HOURS AGO | MODIFIED 6 MINUTES AGO by [EticCybersecurity](#) | Public | TLP:  White  


**20240130 Most Active Threat Indicators II**  
CREATED 6 MINUTES AGO by [Encrypted](#) | Public | TLP:  Green  


**Georgs Honeypot**  
CREATED 3 YEARS AGO | MODIFIED 7 MINUTES AGO by [georgengelmann](#) | Public | TLP:  White  
IPv4: 30715  
Honeypot  
honeypot, kfsensor, rdp, ssh  

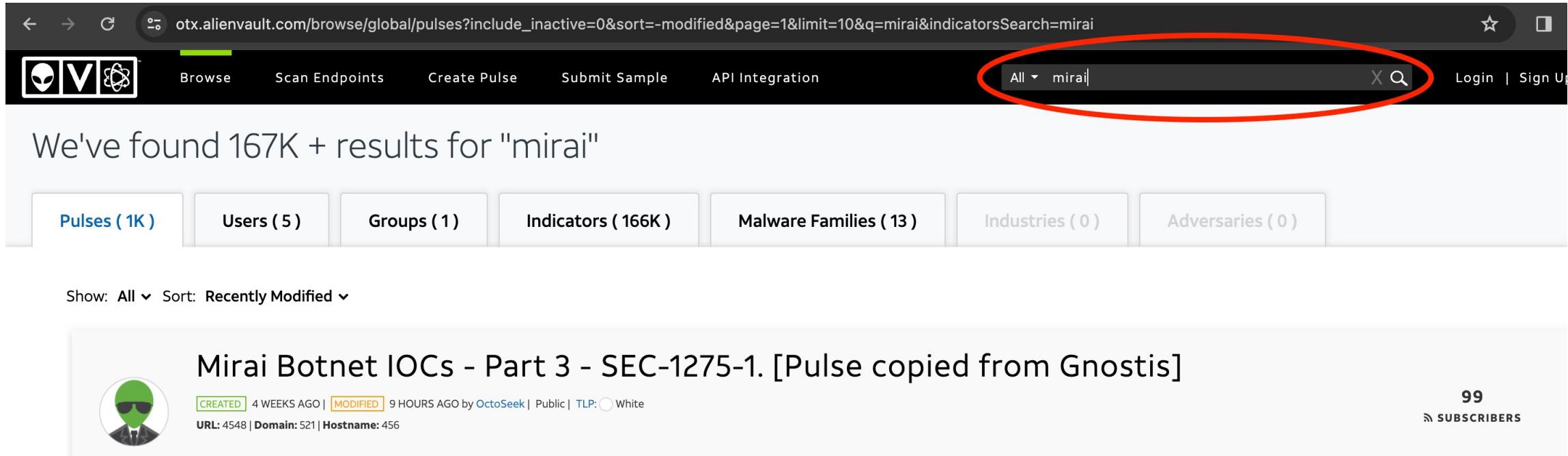

**Fakelabs Honeynet Project**

# Accessing AlienVault OTX

Navigate to  
[https://otx.alienvault.com  
/browse/global/pulses?in  
clude\\_inactive=0&sort=  
modified&page=1&limit  
=10](https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10)

# Searching for Mirai

Type "Mirai" into the 'Search OTX' field.



The screenshot shows a web browser displaying the OTX search results for the term "mirai". The search bar at the top contains "mirai" with a red oval highlighting it. Below the search bar, the text "We've found 167K + results for \"mirai\" " is displayed. A navigation bar below the search bar includes links for Pulses (1K), Users (5), Groups (1), Indicators (166K), Malware Families (13), Industries (0), and Adversaries (0). The main content area shows a single search result titled "Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]". This result was created 4 weeks ago and modified 9 hours ago by OctoSeek, and is public with a TLP: White rating. It has 99 subscribers. The URL is 4548, the domain is 521, and the hostname is 456.

otx.alienvault.com/browse/global/pulses?include\_inactive=0&sort=-modified&page=1&limit=10&q=mirai&indicatorsSearch=mirai

All mirai

We've found 167K + results for "mirai"

Pulses ( 1K )    Users ( 5 )    Groups ( 1 )    Indicators ( 166K )    Malware Families ( 13 )    Industries ( 0 )    Adversaries ( 0 )

Show: All ▾ Sort: Recently Modified ▾

Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]

CREATED 4 WEEKS AGO | MODIFIED 9 HOURS AGO by OctoSeek | Public | TLP: White

URL: 4548 | Domain: 521 | Hostname: 456

99  
SUBSCRIBERS

[otx.alienvault.com/browse/global/pulses?include\\_inactive=0&sort=-modified&page=1&limit=10&q=mirai&indicatorsSearch=mirai](https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10&q=mirai&indicatorsSearch=mirai)

Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ mirai X Search Login | Sign Up

We've found 167K + results for "mirai"

Pulses (1K) (circled in red) Users (5) Groups (1) Indicators (166K) Malware Families (13) Industries (0) Adversaries (0)

Show: All ▾ Sort: Recently Modified ▾

Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]

 CREATED 4 WEEKS AGO | MODIFIED 9 HOURS AGO by OctoSeek | Public | TLP: White  
URL: 4548 | Domain: 521 | Hostname: 456

99 SUBSCRIBERS

Oct 11 2021 Mirai Botnet IOCs - SEC-1275-1

# Understanding Pulses

Pulses are collections of IoCs related to cybersecurity threats.



Browse

Scan Endpoints

Create Pulse

Submit Sample

API Integration

All | mirai

X Q

Login | Sign Up

?



## Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]

CREATED 4 WEEKS AGO | MODIFIED 9 HOURS AGO by OctoSeek | Public | TLP: White

REFERENCE: <https://1275.ru/ioc/3029/mirai-botnet-iocs-part-3/>

TAGS: mirai botnet, iocs, mirai, linux, compromise ipv4, domain port, combinations, gs003, gs005, gs008

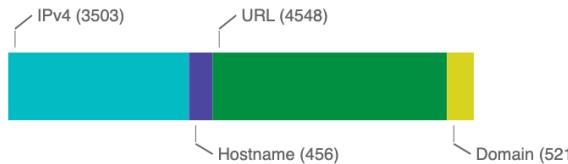
ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (9K)

Related Pulses (1227)

Comments (0)

History (0)



### TYPES OF INDICATORS

Show 10 entries

| TYPE     | INDICATOR   | ROLE | TITLE |
|----------|---|------|-------|
| hostname | <a href="#">zxcffytygbbgfgf12121bot.duckdns.org</a> |      |       |
| hostname | <a href="#">zodiaclol.softether.net</a>             |      |       |
| hostname | <a href="#">znet.whatareyousearchingfor.net</a>     |      |       |
| hostname | <a href="#">zero.sudolite.ml</a>                    |      |       |
| hostname | <a href="#">zykar.ddns.net</a>                      |      |       |
| hostname | <a href="#">yarunet.ddns.net</a>                    |      |       |
| hostname | <a href="#">y.fd6fq54s6df541q23sdxfg.eu</a>         |      |       |
| hostname | <a href="#">xyt-hvareoxy.vwz</a>                    |      |       |

# Selecting a Mirai Pulse

Search

ADDED ACTIVE RELATED PULSES

Select a Pulse with “Mirai” in the title, like “Mirai Botnet IoCs.”

Feb 3, 2024, 8:21:12 PM

# Examining Pulse Details

Observe the colored bar showing TYPES OF INDICATORS.



## Mirai Botnet IOCs - Part 3 - SEC-1275-1. [Pulse copied from Gnostis]

CREATED 4 WEEKS AGO | MODIFIED 9 HOURS AGO by OctoSeek | Public | TLP: White

REFERENCE: <https://1275.ru/ioc/3029/mirai-botnet-iocs-part-3/>

TAGS: [mirai](#) [botnet](#), [iocs](#), [mirai](#), [linux](#), [compromise](#) [ipv4](#), [domain](#) [port](#), [combinations](#), [gs003](#), [gs005](#), [gs008](#)



Report Spam



ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

LEARN MORE

Indicators of Compromise (9K)

Related Pulses (1227)

Comments (0)

History (0)

IPv4 (3503)

URL (4548)

**TYPES OF INDICATORS**



Show 10 entries

Search:



Browse

Scan Endpoints

Create Pulse

Submit Sample

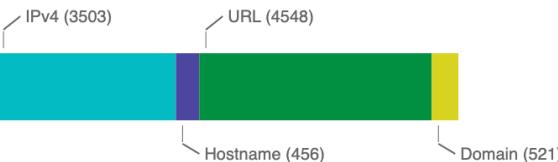
API Integration

Indicators of Compromise (9K)

Related Pulses (1227)

Comments (0)

History (0)



TYPES OF INDICATORS

Show 10 entries

| TYPE     | INDICATOR  | ROLE | TITLE |
|----------|--|------|-------|
| hostname | <a href="#">zxcxffytygbbgfgf12121bot.duckdns.org</a> |      |       |
| hostname | <a href="#">zodiaclol.softether.net</a>              |      |       |
| hostname | <a href="#">znet.whatareyousearchingfor.net</a>      |      |       |
| hostname | <a href="#">zero.sudolite.ml</a>                     |      |       |
| hostname | <a href="#">yzykar.ddns.net</a>                      |      |       |
| hostname | <a href="#">yarunet.ddns.net</a>                     |      |       |
| hostname | <a href="#">y.fd6fq54s6df541q23sdxfg.eu</a>          |      |       |
| hostname | <a href="#">xyz.hxarasxg.xyz</a>                     |      |       |
| hostname | <a href="#">xxfgrw1.kro.kr</a>                       |      |       |
| hostname | <a href="#">xmpp-upload.lolibob.noho.st</a>          |      |       |

SHOWING 1 TO 10 OF 9,028 ENTRIES

# Identifying Indicator Types

Note one of the indicator types, such as hostname, Domain or IP.



Browse

Scan Endpoints

Create Pulse

Submit Sample

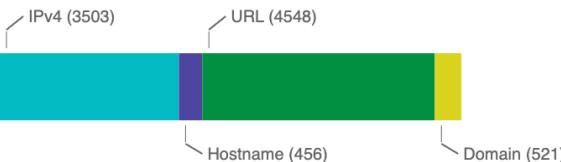
API Integration

Indicators of Compromise (9K)

Related Pulses (1227)

Comments (0)

History (0)



TYPES OF INDICATORS

Show 10 entries

| TYPE     | INDICATOR  | ROLE | TITLE |
|----------|--|------|-------|
| hostname | <a href="#">zxcxffytygbbgfgf12121bot.duckdns.org</a> |      |       |
| hostname | <a href="#">zodiaclol.softether.net</a>              |      |       |
| hostname | <a href="#">znet.whatareyousearchingfor.net</a>      |      |       |
| hostname | <a href="#">zero.sudolite.ml</a>                     |      |       |
| hostname | <a href="#">yzykar.ddns.net</a>                      |      |       |
| hostname | <a href="#">yarunet.ddns.net</a>                     |      |       |
| hostname | <a href="#">y.fd6fq54s6df541q23sdxfge.eu</a>         |      |       |
| hostname | <a href="#">xyz.hxarasxg.xyz</a>                     |      |       |
| hostname | <a href="#">xxfgrw1.kro.kr</a>                       |      |       |
| hostname | <a href="#">xmpp-upload.lolibob.noho.st</a>          |      |       |

SHOWING 1 TO 10 OF 9,028 ENTRIES

# Exploring an Indicator

Click an item under INDICATOR to view its analysis.

**Analysis** **Related Pulses** **Comments (0)**

## Whois

Show 10 entries Search:

| RECORD        | VALUE  |
|---------------|--|
| Emails        | 25e6a5dc339baa71337fd929254287e6-1702436@contact.gandi.net |
| Name          | Richard Harper   |
| Name Servers  | NS1.DUCKDNS.ORG  |
| Address       | Obfuscated whois Gandi-63-65 boulevard Massena             |
| Address       | Gandi, 63-65 boulevard Massena                             |
| City          | Obfuscated whois Gandi-Paris                               |
| Country       | FR   |
| Creation Date | 2013-04-12T19:58:56  |
| Dnssec        | unsianed   |

# Analyzing Indicator Details

Scroll through the analysis tab results.



# Returning to Pulse Page

Use the back arrow in your web browser to return to the pulse page.

We've found 63M + results for "Domain"

Pulses ( 20K )

Users ( 26 )

Groups ( 7 )

Indicators ( 63M )

Malware Families ( 5 )

Industries ( 0 )

Adversaries ( 20 )

Show: All ▾ Sort: Recently Modified ▾

## Fakelabs Honeynet Project



CREATED 2 YEARS AGO | MODIFIED 1 MINUTE AGO by mechanic | Public | TLP: White

IPv4: 3573 | URL: 746

I have several servers in the US, Europe, and Asia running modified versions of cowrie, a medium interaction ssh honeypot. This pulse is the list of IP addresses that have gained unauthorized access ...

56  
SUBSCRIBERS

## Win32.Urausy.C - Malware Domain Feed V2



CREATED 2 YEARS AGO | MODIFIED 15 MINUTES AGO by otxrobottwo\_testing | Public | TLP: White

Domain: 2

Command and Control domains for Win32.Urausy.C. These domains are extracted from a number of sources, and are suspicious.

457  
SUBSCRIBERS



Browse

Scan Endpoints

Create Pulse

Submit Sample

API Integration

All ▾ Domain

X

Login | Sign Up

?

We've found 63M + results for "Domain"

Pulses ( 20K )

Users ( 26 )

Groups ( 7 )

Indicators ( 63M )

Malware Families ( 5 )

Industries ( 0 )

Adversaries ( 20 )

Show: All ▾ Sort: Recently Modified ▾



## Fakelabs Honeynet Project

CREATED 2 YEARS AGO | MODIFIED 1 MINUTE AGO by mechanic | Public | TLP: White

IPv4: 3573 | URL: 746

I have several servers in the US, Europe, and Asia running modified versions of cowrie, a medium interaction ssh honeypot. This pulse is the list of IP addresses that have gained unauthorized access ...

# Filtering By Domain

56  
SUBSCRIBERS

Filter results by typing “domain”  
in the Search Field



## Win32.Urausy.C - Malware Domain Feed V2

CREATED 2 YEARS AGO | MODIFIED 15 MINUTES AGO by otxrobottwo\_testing | Public | TLP: White

Domain: 2

Command and Control domains for Win32.Urausy.C. These domains are extracted from a number of sources, and are suspicious.

457  
SUBSCRIBERS



## Win32.Sperolz.A - Malware Domain Feed V2

CREATED 4 YEARS AGO | MODIFIED 16 MINUTES AGO by otxrobottwo\_testing | Public | TLP: White

Command and Control domains for Win32.Sperolz.A. These domains are extracted from a number of sources, and are suspicious.

457  
SUBSCRIBERS



## Linux.BillGates - Malware Domain Feed V2

CREATED 3 YEARS AGO | MODIFIED 16 MINUTES AGO by otxrobottwo\_testing | Public | TLP: White

Hostname: 4

Command and Control domains for Linux.BillGates. These domains are extracted from a number of sources, and are suspicious.

457  
SUBSCRIBERS

We've found 63M + results for "Domain"

Pulses ( 20K )

Users ( 26 )

Groups ( 7 )

Indicators ( 63M )

Malware Families ( 5 )

Industries ( 0 )

Adversaries ( 20 )

Show: All ▾ Sort: Recently Modified ▾

### Fakelabs Honeynet Project



CREATED 2 YEARS AGO | MODIFIED 1 MINUTE AGO by mechanic | Public | TLP: White

IPv4: 3573 | URL: 746

I have several servers in the US, Europe, and Asia running modified versions of cowrie, a medium interaction ssh honeypot. This pulse is the list of IP addresses that have gained unauthorized access ...

56

Subscribers

### Win32.Urausy.C - Malware Domain Feed V2



CREATED 2 YEARS AGO | MODIFIED 15 MINUTES AGO by otxrobottwo\_testing | Public | TLP: White

Domain: 2

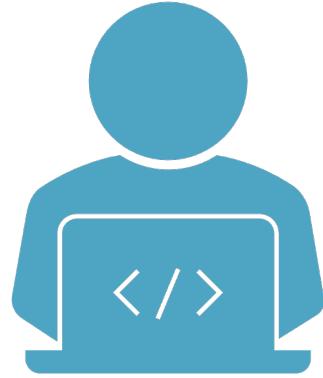
Command and Control domains for Win32.Urausy.C. These domains are extracted from a number of sources, and are suspicious.

457

Subscribers

# Viewing Domain Indicator Details

Select a domain indicator to view its analysis overview.



# Conducting Further Searches

Search using terms like, “URL”, “IPv4”,  
“hostname”, and “hash”

---