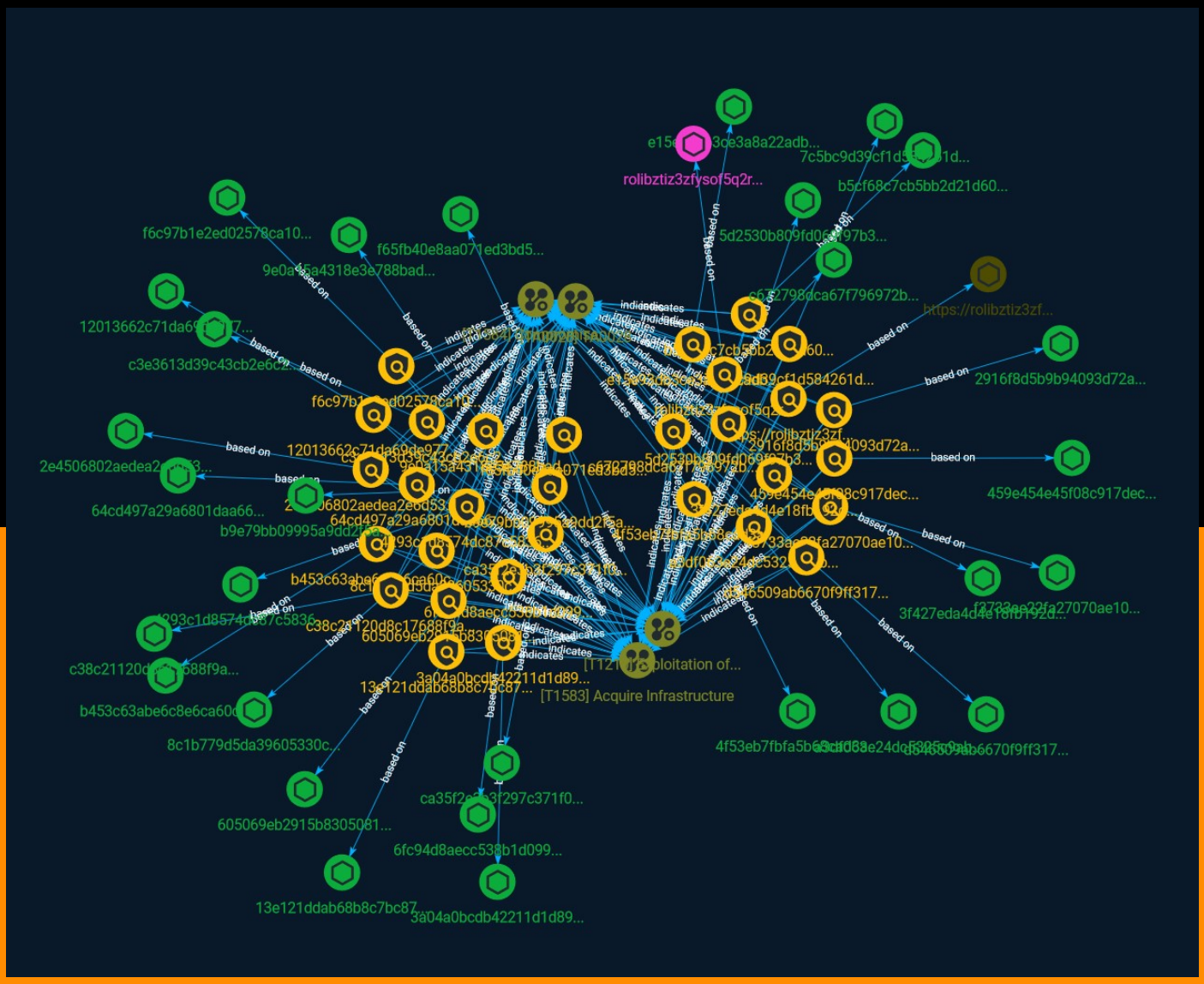
Jul 05 2023

NETMANAGEIT

# Intelligence Report

# Honeypot Recon: Enterprise Applications Honeypot - Unveiling Findings from Six



# Table of contents

## Overview



## Entities



## Observables

# External References

# Overview

## Description

To obtain a better perspective of attacks worldwide, Trustwave has implemented a network of honeypots located in multiple countries across the globe. By distributing honeypots in such a manner, we can gather a reliable set of information on the methods and techniques used by attackers and their botnets.

## Confidence

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

15 / 100

# Indicator

**Name**

a3df063e24dc5325c9ab6b8c10a709d436213cf08626d890c605d2e2626f91d4

**Description**

Unix.Trojan.Mirai-9909527-0 SHA256 of e1768e47fc9604c3bc7a582445bab7277754843a

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'a3df063e24dc5325c9ab6b8c10a709d436213cf08626d890c605d2e2626f91d4']

**Name**

6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f

**Description**

PUA_Crypto_Mining_CommandLine_Indicators_Oct21 SHA256 of 6296e8ed40e430480791bf7b4fcdafde5f834837

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f']

**Name**

b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605

**Description**

Unix.Dropper.Mirai-7358821-0 SHA256 of ac6962542a4b23ac13bddff22f8df9aeb702ef12

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605']

**Name**

ca35f2e3b3f297c371f0a58398cb43e24c1d1419f08baff9b9223b9032ccf4c1

**Description**

SUSP_ELF_LNX_UPX_Compressed_File SHA256 of c80261677450113004b4fb7dbc44ec5e7691396e

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'ca35f2e3b3f297c371f0a58398cb43e24c1d1419f08baff9b9223b9032ccf4c1']

**Name**

c3e3613d39c43cb2e6c253693b683e9ef3c24b4da764645c24112eec7e6fe213

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c3e3613d39c43cb2e6c253693b683e9ef3c24b4da764645c24112eec7e6fe213']

**Name**

f3733ae22fa27070ae108266565739dc27b155a74a7cfdc1b1463499811677e1

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f3733ae22fa27070ae108266565739dc27b155a74a7cfdc1b1463499811677e1']

**Name**

8c1b779d5da39605330cd8d160ea4618ea83bd33f2732ebef54332853e0c9acc

**Description**

Trojan:Linux/Dakkatoni.F!MTB SHA256 of 0e9246139e1056e165231b637ecbc91eab940c31

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8c1b779d5da39605330cd8d160ea4618ea83bd33f2732ebef54332853e0c9acc']

**Name**

64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63

**Description**

SUSP_ELF_LNX_UPX_Compressed_File SHA256 of 5ab29bf2b71fe11114bb8f37bc515dfc78deee3b

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63']

**Name**

e15e93db3ce3a8a22adb4b18e0e37b93f39c495e4a97008f9b1a9a42e1fac2b0

**Description**

ELF:Gafgyt-AN\ [Cryp] SHA256 of 034c8c51a58be11ca620ce3eb0d43d5a59275d2f

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'e15e93db3ce3a8a22adb4b18e0e37b93f39c495e4a97008f9b1a9a42e1fac2b0']

**Name**

13e121ddab68b8c7bc87a13b5e20dcb020b6b9e82c0b9e83727fed9e231747f5

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '13e121ddab68b8c7bc87a13b5e20dcb020b6b9e82c0b9e83727fed9e231747f5']

**Name**

b9e79bb09995a9dd2f5a22dc2e59738696e2be2204ec92a2881fb3fa70e0160f

**Description**

SUSP_ELF_LNX_UPX_Compressed_File SHA256 of 36ef9de431202e643f3410b5906bb23607e7df90

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b9e79bb09995a9dd2f5a22dc2e59738696e2be2204ec92a2881fb3fa70e0160f']

**Name**

4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b

**Description**

Backdoor:Linux/Mirai.AY!MTB SHA256 of a8e2e981933e36f6a4bfac4367c997a80da3568e

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b']

**Name**

2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6

**Description**

Unix.Dropper.Mirai-7358821-0 SHA256 of 1ed14334b5b71783cd6ec14b8a704fe48e600cf0

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6']

**Name**

2916f8d5b9b94093d72a6b9cdf0a4c8f5f38d70d5cea4444869ab33cd7e1f243

**Description**

Gafgyt, Mirai SHA256 of 7f67a0a45159e21735a9783b89d8fdae043dfa22

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '2916f8d5b9b94093d72a6b9cdf0a4c8f5f38d70d5cea4444869ab33cd7e1f243']

**Name**

3a04a0bcdb42211d1d8955122db6055d08a6f4f747658322d60d423f97afea0c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3a04a0bcdb42211d1d8955122db6055d08a6f4f747658322d60d423f97afea0c']

**Name**

f65fb40e8aa071ed3bd5456126815d60bc3afd2e18944edc1e5fcf2ea6477429

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f65fb40e8aa071ed3bd5456126815d60bc3afd2e18944edc1e5fcf2ea6477429']

**Name**

https://rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion:80

**Pattern Type**

stix

**Pattern**

[url:value = 'https://rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion:80']

**Name**

605069eb2915b8305081cce83c9b6fa7fd2cc753eea6c7d1eaa5e6ef72de70e2

**Description**

Unix.Trojan.Mirai-1 SHA256 of a44db161abe6605088ec432c9dfe8f2da6ad73ca

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '605069eb2915b8305081cce83c9b6fa7fd2cc753eea6c7d1eaa5e6ef72de70e2']

**Name**

7c5bc9d39cf1d584261ddd705ea592efcef7809fdb5cb52d20274347641809c3

**Description**

Trojan:Win32/Skeeyah.A!rfn SHA256 of 4980400032a7f42d6d7007e7751a1b86ad28bed1

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7c5bc9d39cf1d584261ddd705ea592efcef7809fdb5cb52d20274347641809c3']

**Name**

c672798dca67f796972b42ad0c89e25d589d2e70eb41892d26adbb6a79f63887

**Description**

Unix.Dropper.Mirai-7358821-0 SHA256 of 0a427f86b4360fb603c6e3c5878c9be7ced59adc

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c672798dca67f796972b42ad0c89e25d589d2e70eb41892d26adbb6a79f63887']

**Name**

f6c97b1e2ed02578ca1066c8235ba4f991e645f89012406c639dbccc6582eec8

**Description**

Unix.Dropper.Mirai-7578080-0 SHA256 of 61c74136534b826059c63221a2373dc0613a47b7

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'f6c97b1e2ed02578ca1066c8235ba4f991e645f89012406c639dbccc6582eec8']

**Name**

459e454e45f08c917dec9342b7c6a586dbe9edfa4bb942dcd4766ecb446fbd1a

**Description**

Unix.Dropper.Mirai-7578080-0 SHA256 of a3bed9ce0585954fc02e6f20ed68ef6800fce9cd

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '459e454e45f08c917dec9342b7c6a586dbe9edfa4bb942dcd4766ecb446fbd1a']

**Name**

b453c63abe6c8e6ca60cb4e49cd2cf6730aa1626975534f2d410c50dfe683953

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b453c63abe6c8e6ca60cb4e49cd2cf6730aa1626975534f2d410c50dfe683953']

**Name**

3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d

**Description**

Backdoor:Linux/Mirai.AY!MTB SHA256 of 168358916c26d85dbdd5ced8e6f66f0e012032f1

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d']

**Name**

d546509ab6670f9ff31783ed72875dfc0f37fa2b666bd5870eecaaed2ebea4a8

**Description**

Other:Malware-gen\ [Trj] SHA256 of 2327be693bc11a618c380d7d3abc2382d870d48b

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'd546509ab6670f9ff31783ed72875dfc0f37fa2b666bd5870eecaaed2ebea4a8']

**Name**

9e0a15a4318e3e788bad61398b8a40d4916d63ab27b47f3bdbe329c462193600

**Description**

Unix.Dropper.Mirai-7578080-0 SHA256 of b5f914ad11626070f6cf466069c8d5d9ee25f5bb

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '9e0a15a4318e3e788bad61398b8a40d4916d63ab27b47f3bdbe329c462193600']

**Name**

rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion']

**Name**

c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a

**Description**

ELF:ProcHider-C\ [Trj] SHA256 of 38c56b5e1489092b80c9908f04379e5a16876f01

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a']

**Name**

4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7

**Description**

Unix.Dropper.Mirai-7358821-0 SHA256 of 5857a7dd621c4c3ebb0b5a3bec915d409f70d39f

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7']

**Name**

5d2530b809fd069f97b30a5938d471dd2145341b5793a70656aad6045445cf6d

**Description**

Trojan:Linux/Kinsing.L SHA256 of e545ceffc8948e3ca9900212807cf3a862d33581

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '5d2530b809fd069f97b30a5938d471dd2145341b5793a70656aad6045445cf6d']

**Name**

12013662c71da69de977c04cd7021f13a70cf7bed4ca6c82acbc100464d4b0ef

**Description**

Mirai SHA256 of 292559e94f1c04b7d0c65d4a01bbbc5dc1ff6f21

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '12013662c71da69de977c04cd7021f13a70cf7bed4ca6c82acbc100464d4b0ef']

# Attack-Pattern

| Name |
| --- |
| TA0028 |
| **ID** |
| TA0028 |
| **Name** |
| Compromise Infrastructure |
| **ID** |
| T1584 |
| **Description** |
| Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle. (Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage. Use of compromised infrastructure allows adversaries to stage, launch, and execute operations. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital |

Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may also compromise infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) By using compromised infrastructure, adversaries may make it difficult to tie their actions back to them. Prior to targeting, adversaries may compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

# Domain-Name

| Value |
| --- |
| rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion |

# StixFile

| Value |
| --- |
| 4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b |
| c3e3613d39c43cb2e6c253693b683e9ef3c24b4da764645c24112eec7e6fe213 |
| b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605 |
| f65fb40e8aa071ed3bd5456126815d60bc3afd2e18944edc1e5fcf2ea6477429 |
| 459e454e45f08c917dec9342b7c6a586dbe9edfa4bb942dcd4766ecb446fbd1a |
| a3df063e24dc5325c9ab6b8c10a709d436213cf08626d890c605d2e2626f91d4 |
| b453c63abe6c8e6ca60cb4e49cd2cf6730aa1626975534f2d410c50dfe683953 |
| 2916f8d5b9b94093d72a6b9cdf0a4c8f5f38d70d5cea4444869ab33cd7e1f243 |
| 605069eb2915b8305081cce83c9b6fa7fd2cc753eea6c7d1eaa5e6ef72de70e2 |
| e15e93db3ce3a8a22adb4b18e0e37b93f39c495e4a97008f9b1a9a42e1fac2b0 |
| f3733ae22fa27070ae108266565739dc27b155a74a7cfdc1b1463499811677e1 |
| 13e121ddab68b8c7bc87a13b5e20dcb020b6b9e82c0b9e83727fed9e231747f5 |
| f6c97b1e2ed02578ca1066c8235ba4f991e645f89012406c639dbccc6582eec8 |

3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d

64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63

9e0a15a4318e3e788bad61398b8a40d4916d63ab27b47f3bdbe329c462193600

2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6

7c5bc9d39cf1d584261ddd705ea592efcef7809fdb5cb52d20274347641809c3

3a04a0bcdb42211d1d8955122db6055d08a6f4f747658322d60d423f97afea0c

ca35f2e3b3f297c371f0a58398cb43e24c1d1419f08baff9b9223b9032ccf4c1

c672798dca67f796972b42ad0c89e25d589d2e70eb41892d26adbb6a79f63887

6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f

8c1b779d5da39605330cd8d160ea4618ea83bd33f2732ebef54332853e0c9acc

d546509ab6670f9ff31783ed72875dfc0f37fa2b666bd5870eecaaed2ebea4a8

b9e79bb09995a9dd2f5a22dc2e59738696e2be2204ec92a2881fb3fa70e0160f

# Url

| Value |
| --- |
| https://rolibztiz3zfysof5q2rja6airtmbw74am4oc4rgqsh3ktir6zwdmzid.onion:80 |

# External References

- https://otx.alienvault.com/pulse/64a59ca7b59439d7c6e3a019
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-recon-enterprise-applications-honeypot-unveiling-findings-from-six-worldwide-locations/