Jul 31 2023

NETMANAGEIT

Intelligence Report

Novel Malware, Redis P2Pinfect

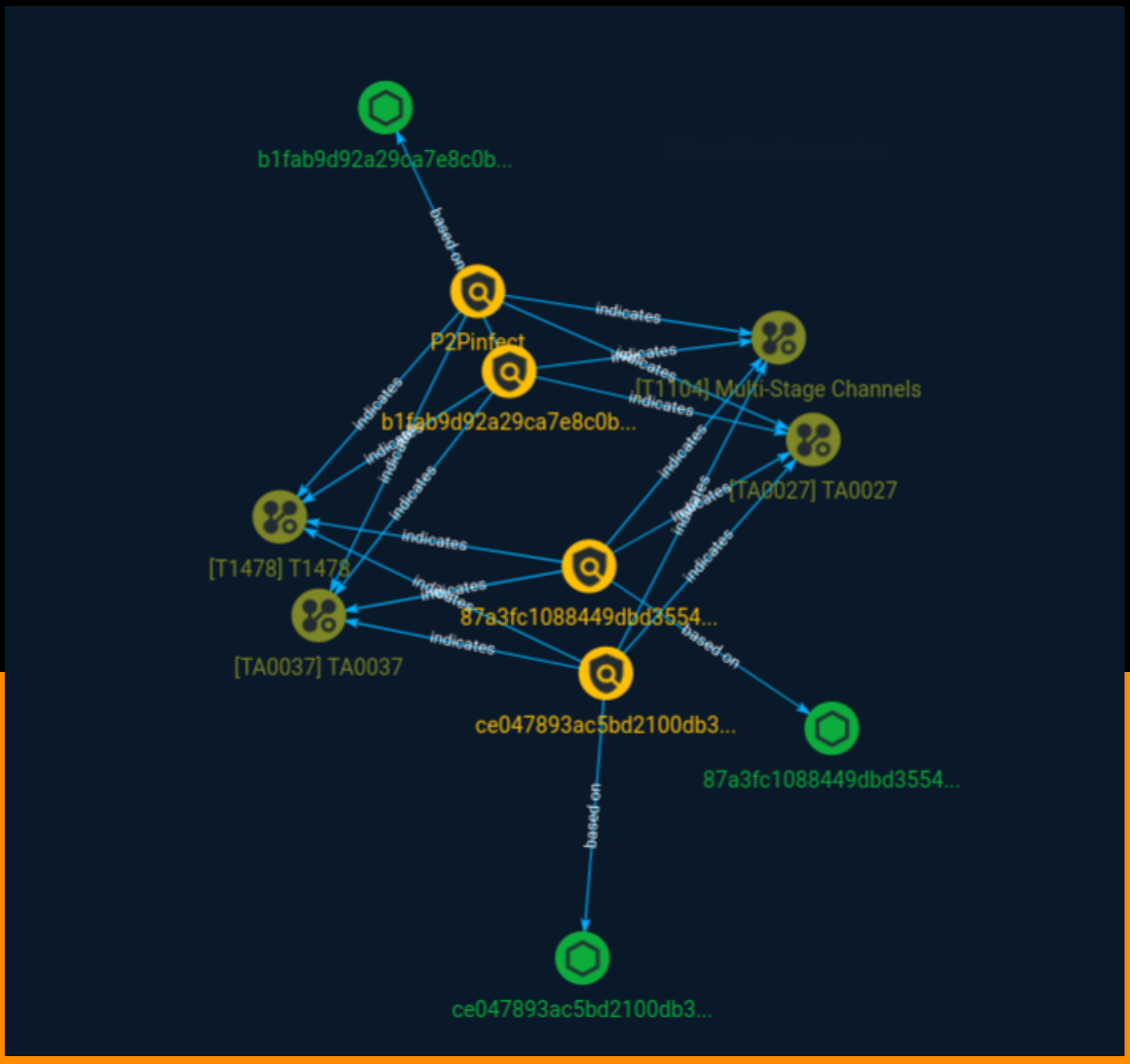

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Indicator 4
- Attack-Pattern 7

Observables

- StixFile 9

External References

- External References 10

Overview

Description

Cado Security Labs researchers recently encountered a novel malware campaign targeting publicly-accessible deployments of the Redis data store. The malware, named “P2Pinfect” by the developer themselves, is written in Rust and acts as a botnet agent. The sample analysed by Cado researchers includes an embedded Portable Executable (PE) along with an additional ELF executable, suggesting cross-platform compatibility between Windows and Linux.

Confidence

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

15 / 100

Indicator

Name
b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c']
Name
87a3fc1088449dbd3554fe029a1878a525e64ab4ccf71b23edb03619ba94403a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '87a3fc1088449dbd3554fe029a1878a525e64ab4ccf71b23edb03619ba94403a']
Name

P2Pinfect

Description

P2Pinfect Detects P2Pinfect worm on Linux

Pattern Type

yara

Pattern

rule P2Pinfect { meta: description = "Detects P2Pinfect worm on Linux" author = "nbill@cadosecurity.com" license = "Apache License 2.0" date = "2023-07-28" hash1 = "87a3fc1088449dbd3554fe029a1878a525e64ab4ccf71b23edb03619ba94403a" hash2 = "ce047893ac5bd2100db3448bd62c324e471ffcddd48433788bfe885e5f071a89" hash3 = "b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c" strings: $magic = { 7f 45 4c 46 } $a1 = "p2pinfect" $a2 = "p2pmod" $b1 = { 48 8D 35 C2 13 22 00 6A 19 5A 4C 89 FF E8 A3 EF 17 00 48 8D 35 C9 13 22 00 6A 1E 5A 4C 89 FF E8 91 EF 17 00 48 8D 35 D5 13 22 00 6A 0E 5A 4C 89 FF E8 7F EF 17 00 48 8D 35 D1 13 22 00 6A 0F 5A 4C 89 FF E8 6D EF 17 00 48 8D 35 81 A5 21 00 4C 89 FF 4C 89 F2 E8 5B EF 17 00 } $b2 = { 48 83 E4 80 48 81 EC 80 0F 00 00 48 C7 04 24 00 00 00 00 48 81 EC 00 05 00 00 49 89 D0 49 89 F5 48 89 BC 24 88 00 00 00 0F B6 86 20 08 00 00 48 8D 0D A3 4D 18 00 48 63 04 81 48 01 C8 6A 01 5E 6A 02 41 5F 4C 89 6C 24 48 48 89 94 24 90 00 00 00 FF E0 } $b3 = { 4C 89 F7 49 89 D8 E8 10 BB 00 00 49 83 66 68 00 49 C7 46 70 0A 00 00 00 66 41 C7 46 78 01 00 6A 10 59 48 8D 84 24 50 04 00 00 48 89 C7 4C 89 F6 F3 48 A5 48 89 C7 E8 FA 76 01 00 } $b4 = { 48 8B 3D 0F 3F 06 00 48 8B 35 10 3F 06 00 E8 20 8E 04 00 49 8B 46 10 48 89 05 08 3F 06 00 41 0F 10 06 0F 11 05 ED 3E 06 00 48 8D 35 A4 D0 FF FF 6A 0F 5F FF 15 25 3D 06 00 48 83 F8 FF 75 06 } $b5 = { 49 29 F7 4C 89 F7 4C 89 FA FF 15 DB 92 21 00 48 8B 84 24 40 02 00 00 4C 01 E0 48 8B 8C 24 98 02 00 00 48 89 01 48 8B 84 24 80 00 00 00 48 89 28 48 8B BC 24 68 01 00 00 48 8D 77 10 48 8B 84 24 48 02 00 00 48 F7 D0 48 8B 94 24 50 02 00 00 48 01 C2 48 C1 E2 04 FF 15 FE 92 21 00 4C 8B A4 24 10 01 00 00 49 83 FC 01 4C 8B 3C 24 48 8B B4 24 38 01 00 00 0F 86 C0 02 00 00 } condition: $magic at 0 and (all of ($a*) or any of ($b*)) }

Name

ce047893ac5bd2100db3448bd62c324e471ffcddd48433788bfe885e5f071a89

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'ce047893ac5bd2100db3448bd62c324e471ffcddd48433788bfe885e5f071a89']

Attack-Pattern

Name
T1478
ID
T1478
Name
TA0027
ID
TA0027
Name
TA0037
ID
TA0037
Name
Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

StixFile

Value
ce047893ac5bd2100db3448bd62c324e471ffcddd48433788bfe885e5f071a89
b1fab9d92a29ca7e8c0b0c4c45f759adf69b7387da9aebb1d1e90ea9ab7de76c
87a3fc1088449dbd3554fe029a1878a525e64ab4ccf71b23edb03619ba94403a

External References

- https://otx.alienvault.com/pulse/64c7e75b10d4e30f816a62a5
- https://www.cadosecurity.com/redis-p2pinfect/