Aug 03 2023

NETMANAGEIT

Intelligence Report

Honeypot Recon: New Variant of SkidMap Targeting Redis

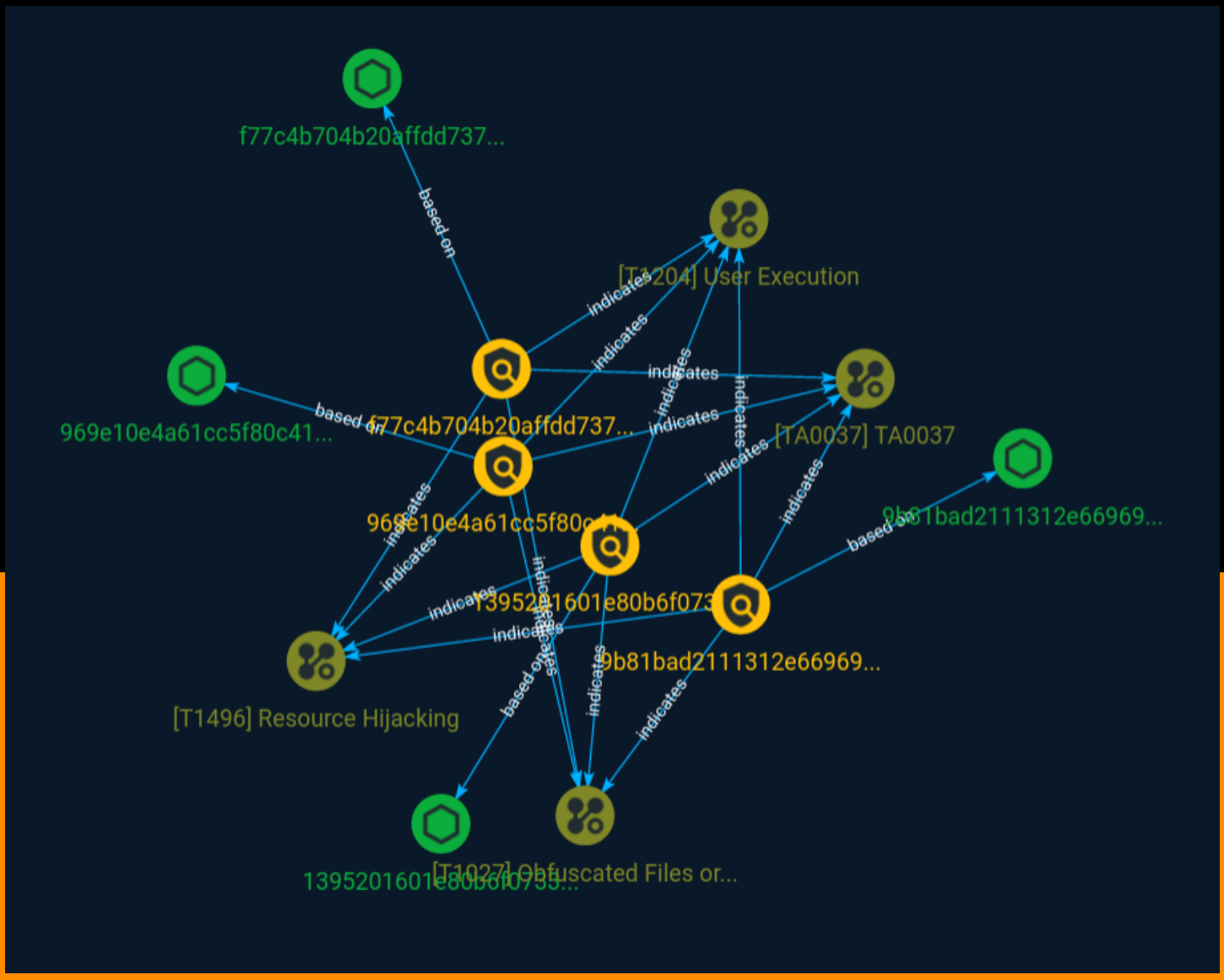

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since Redis is becoming increasingly popular around the world, we decided to investigate attacks on the Redis instance. We didn't have to wait long for the first results of the Honeypot. The trap caught an activity about which the Western world does not hear too often while analyzing SkidMap. More importantly, this variant turned out to be a new, improved, dangerous variation of the malware. Its level of sophistication surprised us quite a bit.

Confidence

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

15 / 100

Indicator

Name

1395201601e80b6f0733feb5bc6dee2d5d2b853fb157185486810457b329d712

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1395201601e80b6f0733feb5bc6dee2d5d2b853fb157185486810457b329d712']

Name

969e10e4a61cc5f80c414259c4d90c74bcf43ccd5678910700bdc14cd60f9725

Description

SHA256 of 9970809e1dedce286888f7d25790b4dcca1e704b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '969e10e4a61cc5f80c414259c4d90c74bcf43ccd5678910700bdc14cd60f9725']

Name

f77c4b704b20affdd737af44cabd3d7b56d8987924f2179137bbeef0e4be0367

Description

is__elf SHA256 of 940f45f8a5dfb16281a35cd8303cd98c1ab1fabd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f77c4b704b20affdd737af44cabd3d7b56d8987924f2179137bbeef0e4be0367']

Name

9b81bad2111312e669697b69b9f121a1f9519da61cd5d37689e38381c1ffad28

Description

SUSP_ELF_LNX_UPX_Compressed_File SHA256 of 0ae049aab363fb8d2e164150dffbafd332725e00

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'9b81bad2111312e669697b69b9f121a1f9519da61cd5d37689e38381c1ffad28']
```

Attack-Pattern

Name
TA0037
ID
TA0037
Name
Resource Hijacking
ID
T1496
Description
Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment

or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

User Execution

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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

StixFile

Value
969e10e4a61cc5f80c414259c4d90c74bcf43ccd5678910700bdc14cd60f9725
9b81bad2111312e669697b69b9f121a1f9519da61cd5d37689e38381c1ffad28
1395201601e80b6f0733feb5bc6dee2d5d2b853fb157185486810457b329d712
f77c4b704b20affdd737af44cabd3d7b56d8987924f2179137bbeef0e4be0367

External References

- https://otx.alienvault.com/pulse/64caa83b14642ce2c0a810dc
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-recon-new-variant-of-skidmap-targeting-redis/