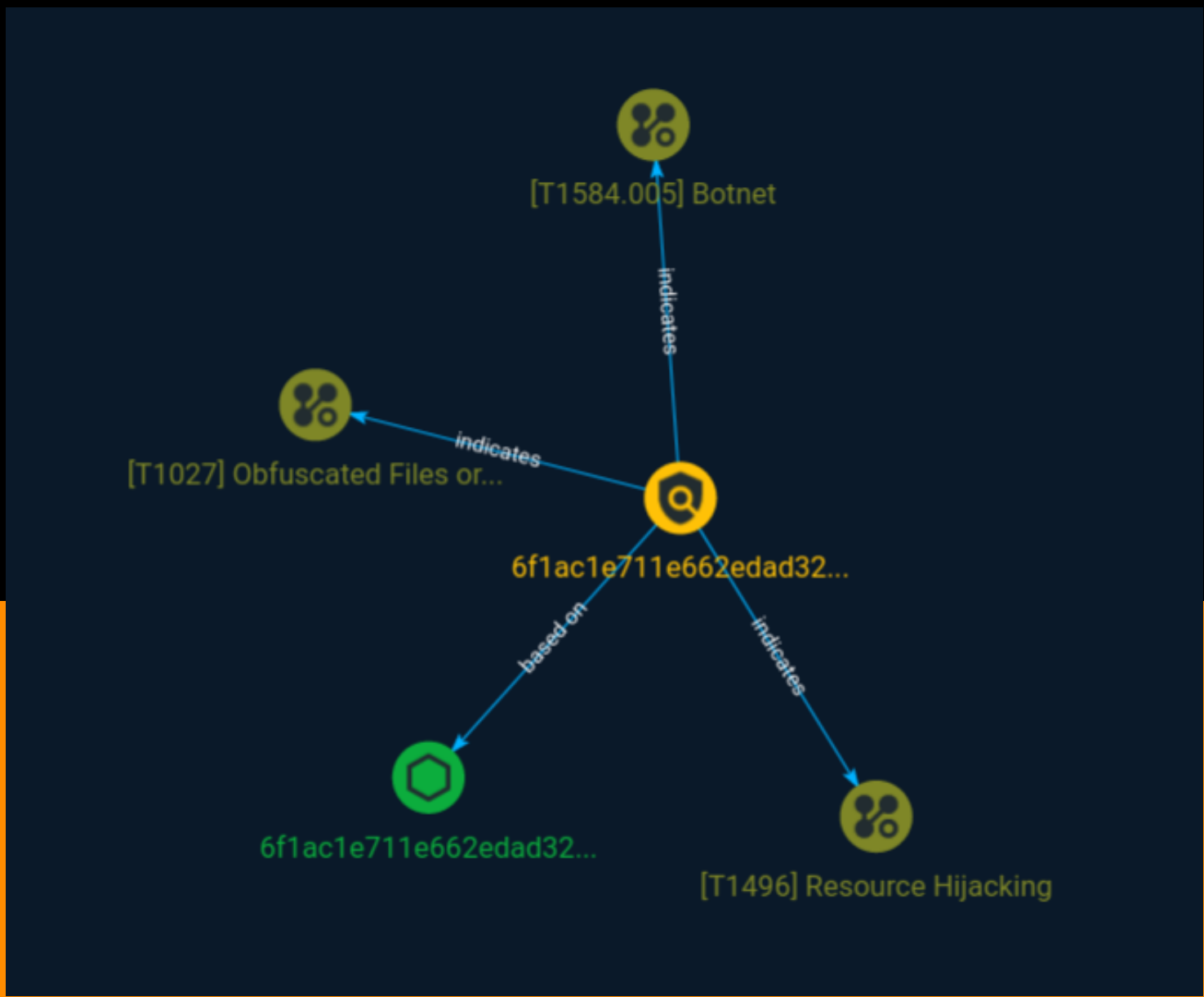
Jul 03 2023

NETMANAGEIT

# Intelligence Report

# Proxyjacking: The Latest Cybercriminal Side Hustle



# Table of contents

## Overview



## Entities



## Observables



## External References

# Overview

## Description

In the ever-evolving world of cyberthreats, attackers continually seek innovative strategies to maximize their gains while minimizing their efforts. The latest example of this was discovered within one of Akamai SIRT's globally distributed honeypots in early June: proxyjacking for profit.

## Confidence

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

15 / 100

# Indicator

| Name |
| --- |
| 6f1ac1e711e662edad32713c135ce29562d636794cf5a21a44bbb34955610f0a |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '6f1ac1e711e662edad32713c135ce29562d636794cf5a21a44bbb34955610f0a'] |

# Attack-Pattern

| Name |
| --- |
| Botnet |
| **ID** |
| T1584.005 |
| **Description** |
| Adversaries may compromise numerous third-party systems to form a botnet that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Instead of purchasing/renting a botnet from a booter/stresser service, adversaries may build their own botnet by compromising numerous third-party systems.(Citation: Imperva DDoS for Hire) Adversaries may also conduct a takeover of an existing botnet, such as redirecting bots to adversary-controlled C2 servers.(Citation: Dell Dridex Oct 2015) With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS). |
| **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**

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 |
| --- |
| 6f1ac1e711e662edad32713c135ce29562d636794cf5a21a44bbb34955610f0a |

# External References

- https://otx.alienvault.com/pulse/64a321c36df3f443f01935ed
- https://www.akamai.com/blog/security-research/proxyjacking-new-campaign-cybercriminal-side-hustle