Jul 03 2023

NETMANAGEIT

Intelligence Report

JokerSpy | Unknown Adversary Targeting Organizations with Multi-Stage macOS Malware

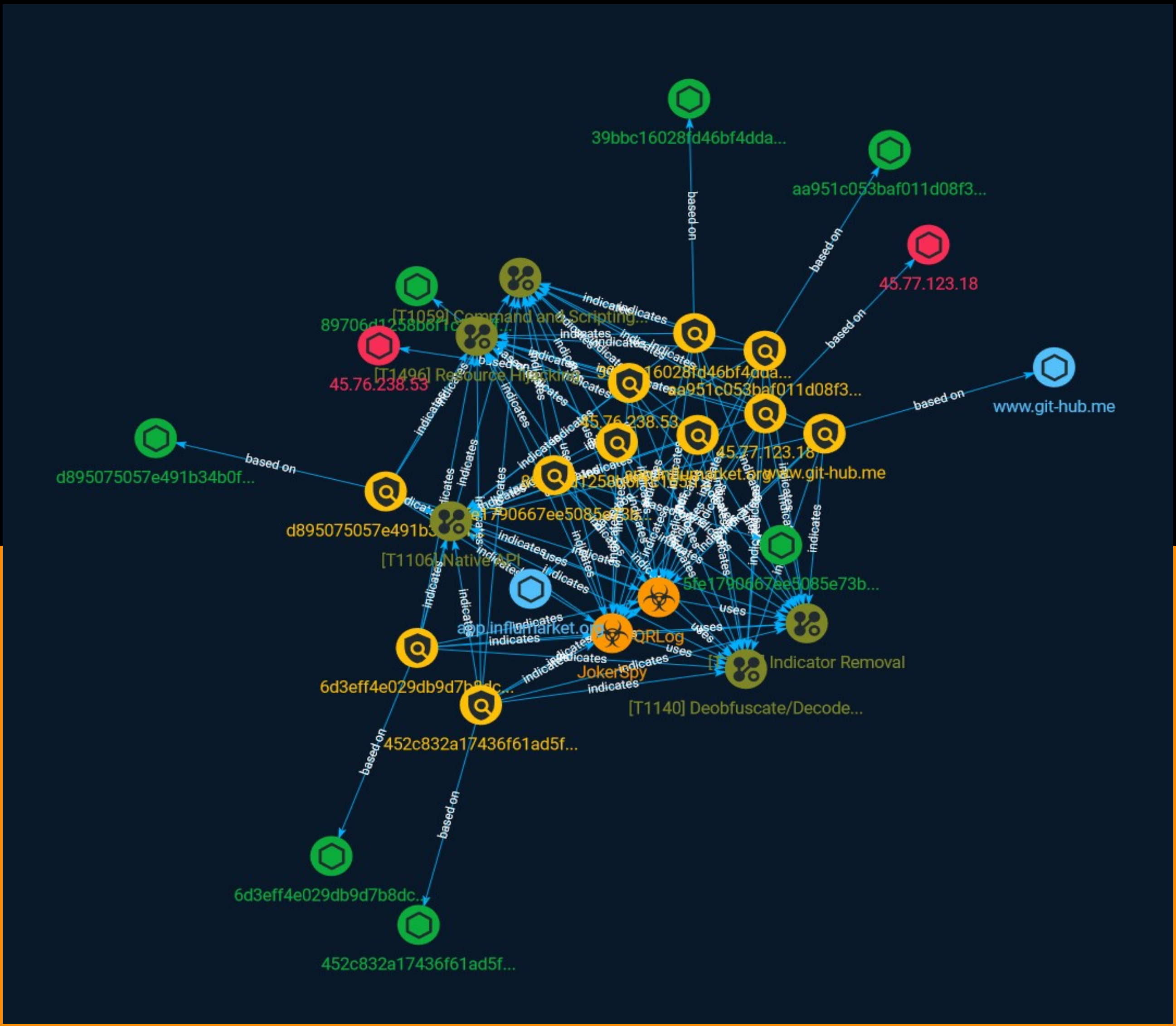

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In this post, SentinelOne reviews the key components and indicators used in the JokerSpy campaign to help raise awareness and aid security teams and threat hunters.

Confidence

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

15 / 100

Indicator

Name

39bbc16028fd46bf4ddad49c21439504d3f6f42cccbd30945a2d2fdb4ce393a4

Description

SHA256 of c7d6ede0f6ac9f060ae53bb1db40a4fbe96f9ceb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '39bbc16028fd46bf4ddad49c21439504d3f6f42cccbd30945a2d2fdb4ce393a4']

Name

45.77.123.18

Description

ISP: The Constant Company, LLC **OS:** Windows -------------------------- Hostnames: - pxaltonet.org - 45.77.123.18.vultrusercontent.com -------------------------- Domains: - vultrusercontent.com - pxaltonet.org -------------------------- Services: **80:** ``` HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Fri, 27 Jan 2023 08:56:02 GMT Accept-Ranges: bytes ETag: "c6a7ea2e2d32d91:0" Server: Microsoft-IIS/10.0 Date: Fri, 30 Jun 2023 08:56:53 GMT Content-Length: 703 ``` ------------------ **443:** ``` HTTP/1.1 200 OK Content-Type: text/

html Last-Modified: Fri, 27 Jan 2023 08:56:02 GMT Accept-Ranges: bytes ETag: "c6a7ea2e2d32d91:0" Server: Microsoft-IIS/10.0 Date: Thu, 22 Jun 2023 04:54:58 GMT Content-Length: 703 ``` HEARTBLEED: 2023/06/22 04:55:03 45.77.123.18:443 - ERROR: write tcp 45.77.123.18:443: broken pipe ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.77.123.18']

Name

89706d1258b6f1c165ff8d1d6d13346e02b48e22d1a741ff451d1cb6ba81bab2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '89706d1258b6f1c165ff8d1d6d13346e02b48e22d1a741ff451d1cb6ba81bab2']

Name

www.git-hub.me

Pattern Type

stix

Pattern

[hostname:value = 'www.git-hub.me']

Name

6d3eff4e029db9d7b8dc076cfed5e2315fd54cb1ff9c6533954569f9e2397d4c

Description

SHA256 of 76b790eb3bed4a625250b961a5dda86ca5cd3a11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d3eff4e029db9d7b8dc076cfed5e2315fd54cb1ff9c6533954569f9e2397d4c']

Name

45.76.238.53

Description

ISP: The Constant Company, LLC **OS:** None ------------------------- Hostnames: - 45.76.238.53.vultrusercontent.com - onlinecloud.cloud ------------------------- Domains: - vultrusercontent.com - onlinecloud.cloud ------------------------- Services: **80:** ``` HTTP/1.1 200 OK Date: Mon, 26 Jun 2023 17:31:31 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Mon, 16 May 2022 10:59:15 GMT ETag: "1d98-5df1eea3666c0" Accept-Ranges: bytes Content-Length: 7576 Content-Type: text/html ``` ------------------ **443:** ``` HTTP/1.1 200 OK Date: Fri, 30 Jun 2023 22:41:03 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6 Last-Modified: Mon, 16 May 2022 10:59:15

GMT ETag: "1d98-5df1eea3666c0" Accept-Ranges: bytes Content-Length: 7576 Content-Type: text/html ``` HEARTBLEED: 2023/06/30 22:41:21 45.76.238.53:443 - SAFE ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: VULTR-GUEST NetBIOS Domain Name: VULTR-GUEST NetBIOS Computer Name: VULTR-GUEST DNS Domain Name: vultr-guest FQDN: vultr-guest ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.76.238.53']

Name

app.influmarket.org

Pattern Type

stix

Pattern

[hostname:value = 'app.influmarket.org']

Name

5fe1790667ee5085e73b054566d548eb4473c20cf962368dd53ba776e9642272

Description

SHA256 of 937a9811b3e5482eb8f96832454723d59229f945

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5fe1790667ee5085e73b054566d548eb4473c20cf962368dd53ba776e9642272']

Name

aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1

Description

SHA256 of bd8626420ecfd1ab5f4576d83be35edecd8fa70e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1']

Name

452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1

Description

SHA256 of 1f99081affd7bef83d44e0072eb860d515893698

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1']

Name

d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8

Description

SHA256 of 370a0bb4177eeebb2a75651a8addb0477b7d610b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8']

Malware

Name
QRLog

Name
JokerSpy

Attack-Pattern

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

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation:

OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

StixFile

Value
5fe1790667ee5085e73b054566d548eb4473c20cf962368dd53ba776e9642272
89706d1258b6f1c165ff8d1d6d13346e02b48e22d1a741ff451d1cb6ba81bab2
39bbc16028fd46bf4ddad49c21439504d3f6f42cccbd30945a2d2fdb4ce393a4
6d3eff4e029db9d7b8dc076cfed5e2315fd54cb1ff9c6533954569f9e2397d4c
452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1
aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1
d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8

Hostname

Value
app.influmarket.org
www.git-hub.me

IPv4-Addr

Value
45.76.238.53
45.77.123.18

External References

- https://otx.alienvault.com/pulse/64a2fca60ce4b2027b6eeadf
- https://www.sentinelone.com/blog/jokerspy-unknown-adversary-targeting-organizations-with-multi-stage-macos-malware/