Jun 22 2023

NETMANAGEIT

Intelligence Report

Emerging Threat! Exposing JOKERSPY

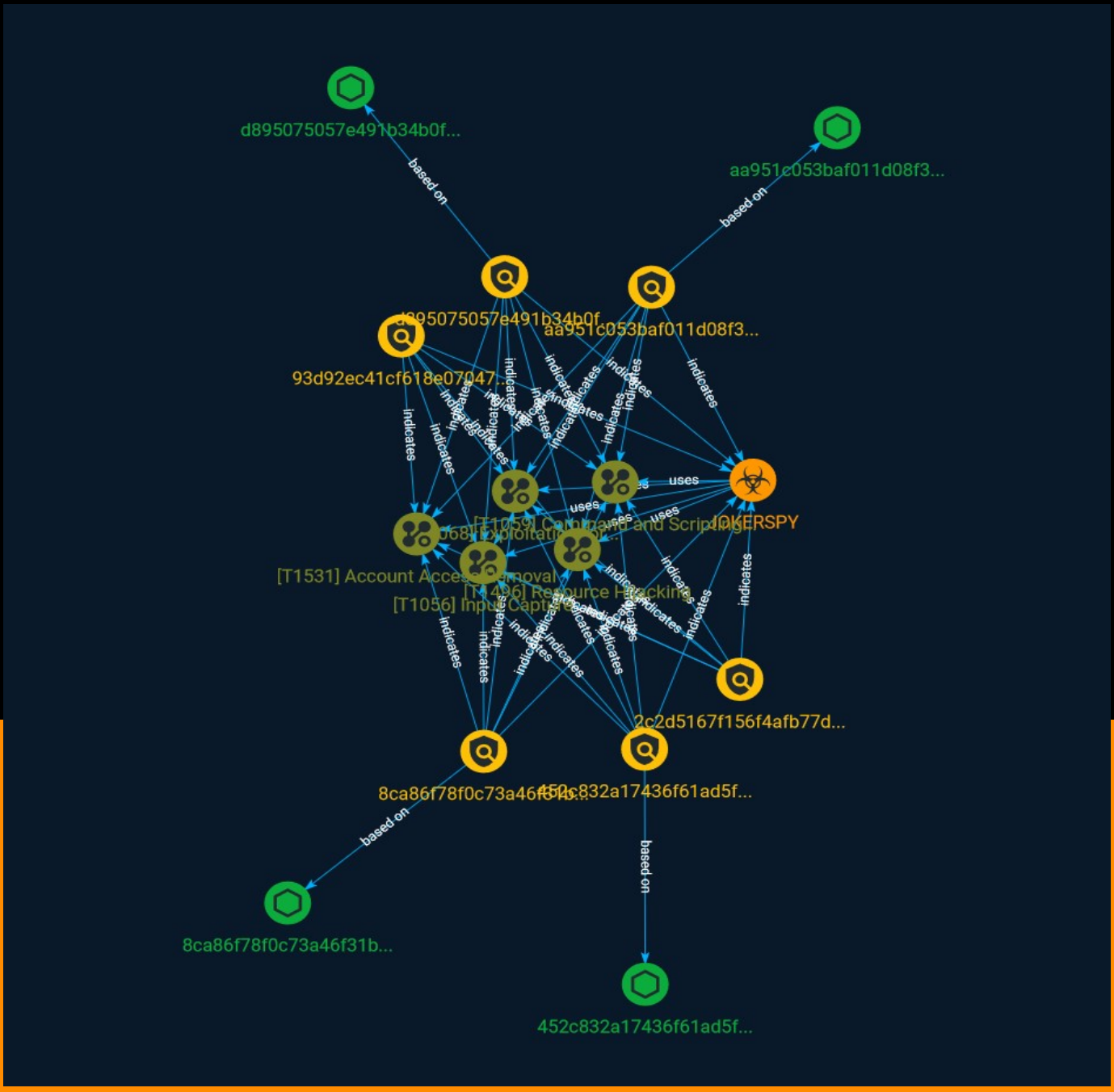

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An overview of JOKERSPY, discovered in June 2023, which deployed custom and open source macOS tools to exploit a cryptocurrency exchange located in Japan.

Confidence

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

15 / 100

Attack-Pattern

Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
Exploitation for Privilege Escalation
ID
T1068
Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

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

Account Access Removal

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

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)

Indicator

Name

aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1

Pattern Type

stix

Pattern

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

Name

452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1

Pattern Type

stix

Pattern

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

Name

93d92ec41cf618e0704784775953a38d66d47783

Pattern Type

yara

Pattern

rule MacOS_Hacktool_Swiftbelt { meta: author = "Elastic Security" creation_date = "2021-10-12" last_modified = "2021-10-25" threat_name = "MacOS.Hacktool.Swiftbelt" reference_sample = "452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1" os = "macos" arch_context = "x86" license = "Elastic License v2" strings: $dbg1 = "SwiftBelt/Sources/SwiftBelt" $dbg2 = "[-] Firefox places.sqlite database not found for user" $dbg3 = "[-] No security products found" $dbg4 = "SSH/AWS/gcloud Credentials Search:" $dbg5 = "[-] Could not open the Slack Cookies database" $sec1 = "[+] Malwarebytes A/V found on this host" $sec2 = "[+] Cisco AMP for endpoints found" $sec3 = "[+] SentinelOne agent running" $sec4 = "[+] Crowdstrike Falcon agent found" $sec5 = "[+] FireEye HX agent installed" $sec6 = "[+] Little snitch firewall found" $sec7 = "[+] ESET A/V installed" $sec8 = "[+] Carbon Black OSX Sensor installed" $sec9 = "/Library/Little Snitch" $sec10 = "/Library/FireEye/xagt" $sec11 = "/Library/CS/falcond" $sec12 = "/Library/Logs/PaloAltoNetworks/GlobalProtect" $sec13 = "/Library/Application Support/Malwarebytes" $sec14 = "/usr/local/bin/osqueryi" $sec15 = "/Library/Sophos Anti-Virus" $sec16 = "/Library/Objective-See/Lulu" $sec17 = "com.eset.remoteadministrator.agent" $sec18 = "/Applications/CarbonBlack/CbOsxSensorService" $sec19 = "/Applications/BlockBlock Helper.app" $sec20 = "/Applications/KextViewr.app" condition: 6 of them }

Name

2c2d5167f156f4afb77dffcec0ad2869a095ee74

Pattern Type

yara

Pattern

rule Macos_Hacktool_JokerSpy { meta: author = "Elastic Security" creation_date = "2023-06-19" last_modified = "2023-06-19" os = "MacOS" arch = "x86" category_type = "Hacktool" family = "JokerSpy" threat_name = "Macos.Hacktool.JokerSpy" reference_sample = "d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8" license = "Elastic License v2" strings: $str1 = "ScreenRecording: NO" fullword $str2 = "Accessibility: NO" fullword $str3 = "Accessibility: YES" fullword $str4 = "eck13XProtectCheck" $str5 = "Accessibility: NO" fullword $str6 = "kMDItemDisplayName = *TCC.db" fullword condition: 5 of them }

Name

8ca86f78f0c73a46f31be366538423ea0ec58089f3880e041543d08ce11fa626

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8ca86f78f0c73a46f31be366538423ea0ec58089f3880e041543d08ce11fa626']

Name

d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8

Pattern Type

stix

Pattern

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

Malware

Name
JOKERSPY

StixFile

Value
452c832a17436f61ad5f32ee1c97db05575160105ed1dcd0d3c6db9fb5a9aea1
8ca86f78f0c73a46f31be366538423ea0ec58089f3880e041543d08ce11fa626
aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1
d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8

External References

- https://www.elastic.co/security-labs/inital-research-of-jokerspy
- https://otx.alienvault.com/pulse/649499773687c8bb685efe8c