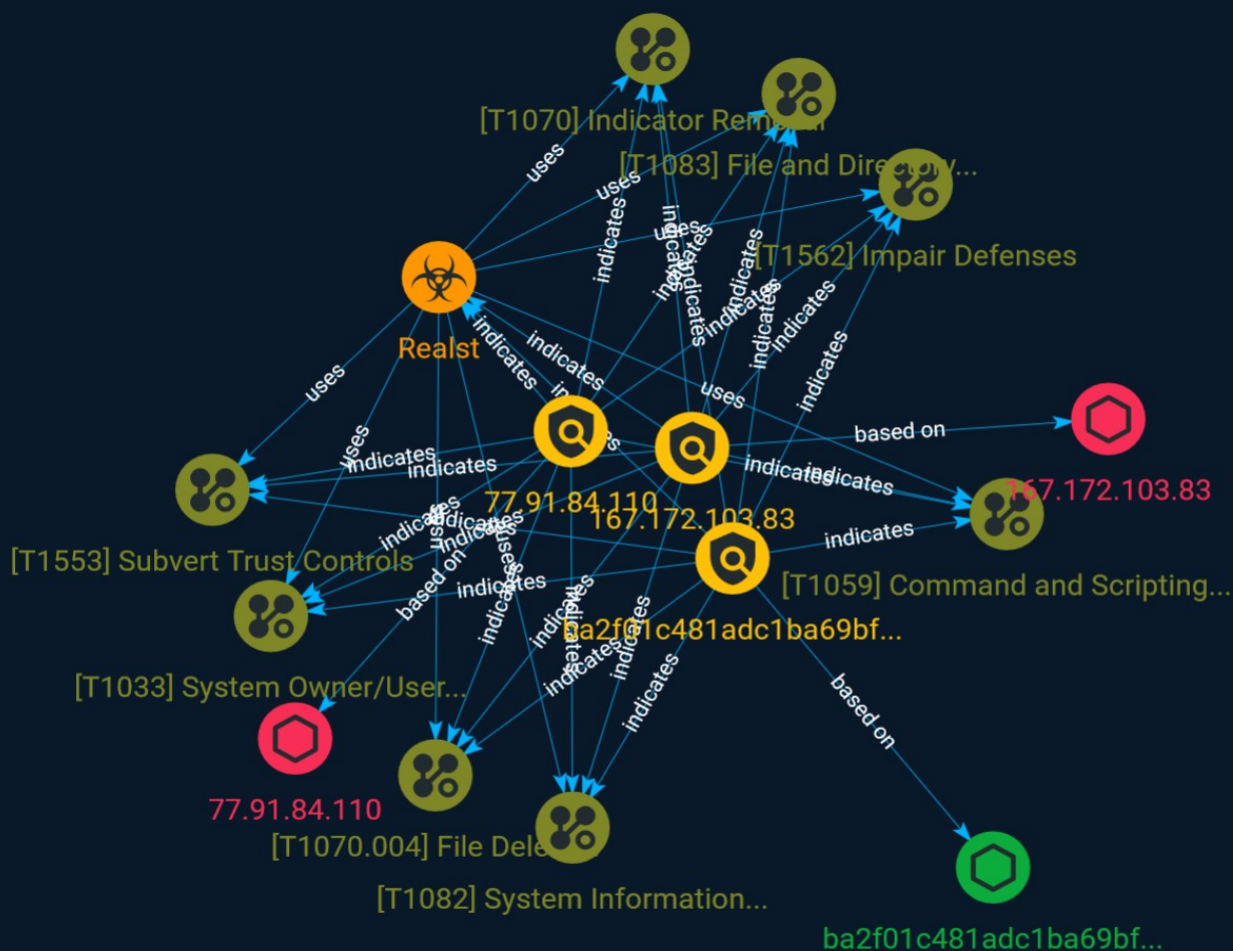




NETMANAGEIT

# Intelligence Report

## Apple Crimeware | Massive Rust Infostealer Campaign Aiming for macOS Sonoma Ahead of Public Release



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4

---

---

## Entities

---

● Indicator	5
● Malware	8
● Attack-Pattern	9

---

---

## Observables

---

● StixFile	15
● IPv4-Addr	16

---



## External References

- 
- External References

17

# Overview

## Description

A security researcher reported on multiple fake blockchain games being used to infect both Windows and macOS targets with infostealers, capable of emptying crypto wallets and stealing stored password and browser data. In the case of macOS, the infostealer turned out to be a new malware written in Rust, dubbed “realst”.

## Confidence

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

15 / 100

# Indicator

## Name

ba2f01c481adc1ba69bfcc7a29f21d9496005f98d2b8e248f407e69a3684b3b3

## Description

cf\_java\_system\_cmds SHA256 of 44aa30ca902a22520b52789b81add44e15e74a50

## Pattern Type

stix

## Pattern

```
[file:hashes:'SHA-256' =
'ba2f01c481adc1ba69bfcc7a29f21d9496005f98d2b8e248f407e69a3684b3b3']
```

## Name

167.172.103.83

## Description

```
**ISP:** DigitalOcean, LLC **OS:** None ----- Hostnames:
----- Domains: ----- Services: **22:** ~~~ SSH-2.0-
OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key:
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM/
OPGggVkJUpQ+bVJq6r36i9 7A09EsgLv/
1NDxLbAHrruRFOV4PmUFP4LixhFQDgaTNO5kf1kYEpcU8KAl8XpOY= Fingerprint: 54:1c:
```

5d:a0:4a:ce:52:b9:a8:52:bd:3d:3e:c3:32:d5 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ~~~ ----- \*\*8080:\*\* ~~~ HTTP/1.1 404 Not Found x-powered-by: Express access-control-allow-origin: http://167.172.103.83 vary: Origin content-security-policy: default-src 'none' x-content-type-options: nosniff content-type: text/html; charset=utf-8 content-length: 139 date: Sun, 16 Jul 2023 23:56:31 GMT connection: close ~~~ -----

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '167.172.103.83']

**Name**

77.91.84.110

**Description**

CC=SE ASN=AS210644 AEZA GROUP Ltd

**Pattern Type**

stix

**Pattern**

**TLP:CLEAR**

[ipv4-addr:value = '77.91.84.110']

# Malware

**Name**

Realst



# Attack-Pattern

## Name

Subvert Trust Controls

## ID

T1553

## Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [Modify Registry](<https://attack.mitre.org/techniques/T1112>) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

## Name

Impair Defenses

**ID**

T1562

**Description**

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

**Name**

File Deletion

**ID**

T1070.004

**Description**

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](<https://attack.mitre.org/techniques/T1105>)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint. There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](<https://attack.mitre.org/techniques/T1059>) functions include ``del`` on Windows and ``rm`` or ``unlink`` on Linux and macOS.

**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**

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**

System Owner/User Discovery

**ID**

T1033

**Description**

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](<https://attack.mitre.org/techniques/T1003>). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](<https://attack.mitre.org/techniques/T1033>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) commands such as `show users` and `show ssh` can be used to display users currently logged into the

device.(Citation: show\_ssh\_users\_cmd\_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

**Name**

File and Directory Discovery

**ID**

T1083

**Description**

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](<https://attack.mitre.org/techniques/T1083>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include ``dir``, ``tree``, ``ls``, ``find``, and ``locate``.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](<https://attack.mitre.org/techniques/T1106>). Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather file and directory information (e.g. ``dir``, ``show flash``, and/or ``nvram``). (Citation: US-CERT-TA18-106A)

**Name**

System Information Discovery

**ID**

T1082

**Description**

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](<https://attack.mitre.org/>

techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](<https://attack.mitre.org/software/S0096>) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](<https://attack.mitre.org/techniques/T1082>) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virtual Machine API)

# StixFile

## Value

ba2f01c481adc1ba69bfcc7a29f21d9496005f98d2b8e248f407e69a3684b3b3

# IPv4-Addr

## Value

167.172.103.83

77.91.84.110



# External References

- 
- <https://otx.alienvault.com/pulse/64c12e2e62d01cc5e407fa8d>
- 
- <https://www.sentinelone.com/blog/apple-crimeware-massive-rust-infostealer-campaign-aiming-for-macos-sonoma-ahead-of-public-release/>