Jul 03 2023

NETMANAGEIT

Intelligence Report

The DPRK strikes using a new variant of RUSTBUCKET

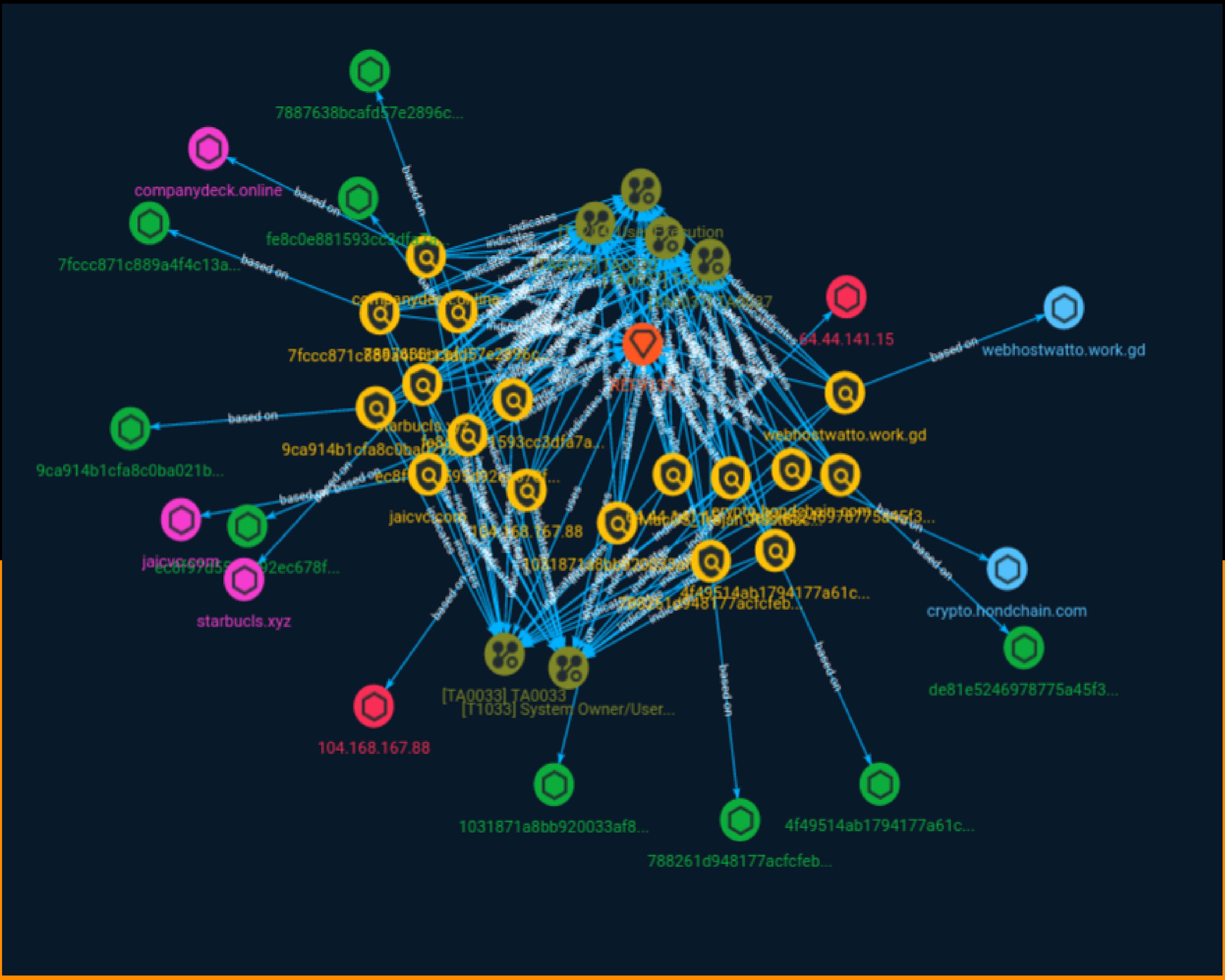

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This variant of RUSTBUCKET, a malware family that targets macOS systems, adds persistence capabilities not previously observed and, at the time of reporting, is undetected by VirusTotal signature engines. Elastic Defend behavioral and prebuilt detection rules provide protection and visibility for users. We have also released a signature to prevent this malware execution.

Confidence

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

15 / 100

Indicator

Name
104.168.167.88
Description
ISP: Hostwinds LLC. **OS:** None ------------------------- Hostnames: - a-0003.a-msedge.net - companydeck.online ------------------------- Domains: - a-msedge.net - companydeck.online ------------------------- Services: **443:** ``` HTTP/1.1 404 Not Found Date: Sun, 25 Jun 2023 12:11:57 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17 X-Powered-By: PHP/8.1.17 Content-Length: 0 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/06/25 12:12:39 104.168.167.88:443 - SAFE ------------------
Pattern Type
stix
Pattern
[ipv4-addr:value = '104.168.167.88']
Name
MacOS_Trojan_RustBucket
Description
MacOS_Trojan_RustBucket

Pattern Type

yara

Pattern

rule MacOS_Trojan_RustBucket { meta: author = "Elastic Security" creation_date = "2023-06-26" last_modified = "2023-06-26" license = "Elastic License v2" os = "MacOS" arch = "x86" category_type = "Trojan" family = "RustBucket" threat_name = "MacOS.Trojan.RustBucket" reference_sample = "9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747" severity = 100 strings: $user_agent = "User-AgentMozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)" $install_log = "/var/log/install.log" $timestamp = "%Y-%m-%d %H:%M:%S" condition: all of them }

Name

1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6']

Name

7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8']

Name
crypto.hondchain.com

Pattern Type
stix

Pattern
[hostname:value = 'crypto.hondchain.com']

Name
fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69']

Name
ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41']

Name

de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500']

Name

9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747

Description

MacOS:Nukesped-A\ [Drp]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747']

Name

64.44.141.15

Description

CC=US ASN=AS20278 NEXEON

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.44.141.15']

Name

4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16']

Name

7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387']

Name

webhostwatto.work.gd

Pattern Type

stix

Pattern

[hostname:value = 'webhostwatto.work.gd']

Name

jaicvc.com

Pattern Type

stix

Pattern

[domain-name:value = 'jaicvc.com']

Name

companydeck.online

Pattern Type

stix

Pattern

[domain-name:value = 'companydeck.online']

Name

788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a']

Name

starbucls.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'starbucls.xyz']

Intrusion-Set

Name
REF9135

Attack-Pattern

Name
TA0027
ID
TA0027
Name
TA0033
ID
TA0033
Name
TA0030
ID
TA0030
Name
TA0037

ID

TA0037

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

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)

Domain-Name

Value
jaicvc.com
starbucls.xyz
companydeck.online

StixFile

Value
1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6
fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69
4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16
9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747
7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8
ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41
7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387
de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500
788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a

Hostname

Value
webhostwatto.work.gd
crypto.hondchain.com

IPv4-Addr

Value
104.168.167.88
64.44.141.15

External References

- https://otx.alienvault.com/pulse/64a3175cad781f314bc79784
- https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket