MAR-10322463-7.v1 - AppleJeus: Ants2Whale | CISA

Published: 2021-02-17 · Archived: 2026-04-05 17:57:36 UTC

body#cma-body { font-family: Franklin Gothic Medium, Franklin Gothic, ITC Franklin Gothic, Arial, sans-serif; font-size: 15px; } table#cma-table { width: 900px; margin: 2px; table-layout: fixed; border-collapse: collapse; } div#cma-exercise { width: 900px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; } div.cma-header { text-align: center; margin-bottom: 40px; } div.cma-footer { text-align: center; margin-top: 20px; } h2.cma-tlp { background-color: #000; color: #ffffff; width: 180px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; float: right; } span.cma-fouo { line-height: 30px; font-weight: bold; font-size: 16px; } h3.cma-section-title { font-size: 18px; font-weight: bold; padding: 0 10px; margin-top: 10px; } h4.cma-object-title { font-size: 16px; font-weight: bold; margin-left: 20px; } h5.cma-data-title { padding: 3px 0 3px 10px; margin: 10px 0 0 20px; background-color: #e7eef4; font-size: 15px; } p.cma-text { margin: 5px 0 0 25px !important; word-wrap: break-word !important; } div.cma-section { border-bottom: 5px solid #aaa; margin: 5px 0; padding-bottom: 10px; } div.cma-avoid-page-break { page-break-inside: avoid; } div#cma-summary { page-break-after: always; } div#cma-faq { page-break-after: always; } table.cma-content { border-collapse: collapse; margin-left: 20px; } table.cma-hashes { table-layout: fixed; width: 880px; } table.cma-hashes td{ width: 780px; word-wrap: break-word; } .cma-left th { text-align: right; vertical-align: top; padding: 3px 8px 3px 20px; background-color: #f0f0f0; border-right: 1px solid #aaa; } .cma-left td { padding-left: 8px; } .cma-color-title th, .cma-color-list th, .cma-color-title-only th { text-align: left; padding: 3px 0 3px 20px; background-color: #f0f0f0; } .cma-color-title td, .cma-color-list td, .cma-color-title-only td { padding: 3px 20px; } .cma-color-title tr:nth-child(odd) { background-color: #f0f0f0; } .cma-color-list tr:nth-child(even) { background-color: #f0f0f0; } td.cma-relationship { max-width: 310px; word-wrap: break-word; } ul.cma-ul { margin: 5px 0 10px 0; } ul.cma-ul li { line-height: 20px; margin-bottom: 5px; word-wrap: break-word; } #cma-survey { font-weight: bold; font-style: italic; } div.cma-banner-container { position: relative; text-align: center; color: white; } img.cma-banner { max-width: 900px; height: auto; } img.cma-nccic-logo { max-height: 60px; width: auto; float: left; margin-top: -15px; } div.cma-report-name { position: absolute; bottom: 32px; left: 12px; font-size: 20px; } div.cma-report-number { position: absolute; bottom: 70px; right: 100px; font-size: 18px; } div.cma-report-date { position: absolute; bottom: 32px; right: 100px; font-size: 18px; } img.cma-thumbnail { max-height: 100px; width: auto; vertical-align: top; } img.cma-screenshot { margin: 10px 0 0 25px; max-width: 800px; height: auto; vertical-align: top; border: 1px solid #000; } div.cma-screenshot-text { margin: 10px 0 0 25px; } .cma-break-word { word-wrap: break-word; } .cma-tag { border-radius: 5px; padding: 1px 10px; margin-right: 10px; } .cma-tag-info { background: #f0f0f0; } .cma-tag-warning { background: #ffdead; }

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.us-cert.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Treasury (Treasury) to highlight the cyber threat to cryptocurrency posed by North Korea, formally known as the Democratic People's Republic of Korea (DPRK), and provide mitigation recommendations. Working with U.S. government partners, FBI, CISA, and Treasury assess that Lazarus Group—which these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors—is targeting individuals and companies, including cryptocurrency exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been modified to include malware that facilitates theft of cryptocurrency.

This MAR highlights this cyber threat posed by North Korea and provides detailed indicators of compromise (IOCs) used by the North Korean government. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on other versions of AppleJeus and recommended steps to mitigate this threat, see

Joint Cybersecurity Advisory AA21-048A: AppleJeus: Analysis of North Korea's Cryptocurrency Malware at https://www.us-cert.cisa.gov/ncas/alerts/AA21-048A.

There have been multiple versions of AppleJeus malware discovered since its initial discovery in August 2018. In most versions, the malware appears to be from a legitimate-looking cryptocurrency trading company and website, whereby an unsuspecting individual downloads a third-party application from a website that appears legitimate.

The U.S. Government has identified AppleJeus malware version—Ants2Whale—and associated IOCs used by the North Korean government in AppleJeus operations.

Ants2Whale, discovered in October 2020, is a legitimate-looking cryptocurrency trading software that is marketed and distributed by a company and website—Ants2Whale and ants2whale[.]com, respectively—that appear legitimate. Some information has been redacted from this report to preserve victim anonymity.

For a downloadable copy of IOCs, see: MAR-10322463-7.v1.stix.

Submitted Files (3)

bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694 (Ants2WhaleHelper)

d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e (Ants2Whale)

[Redacted] (Ants2Whale.dmg)

Domains (2)

ants2whale.com

qnalytica.com

IPs (1)

45.147.231.77

Findings

[Redacted]

Tags

downloaderloader

Details

Name	Ants2Whale.dmg
Size	[Redacted] bytes
Type	zlib compressed data
MD5	[Redacted]
SHA1	[Redacted]
SHA256	[Redacted]
SHA512	[Redacted]
ssdeep	[Redacted]
Entropy	[Redacted]

Antivirus

Avira	OSX/Agent.denpi
Ikarus	OSX.Agent

Zillya!	Downloader.Agent.OSX.390

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

[Redacted]	Downloaded_By	ants2whale.com
[Redacted]	Contains	d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e
[Redacted]	Contains	bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694

Description

This OSX program from the Ants2Whale site is an Apple DMG installer. The OSX program does not have a digital signature and will warn the user of that before installation. As all previous versions of AppleJeus, the Ants2Whale installer appears to be legitimate and installs
“Ants2Whale”(D5AC680E14B013E0624470DA7F46E84809D00B59A7544F6A42B110CF0E29254E) in the “/Applications/Ants2whale.app/Contents/MacOS/Ants2whale” folder and a program named Ants2WhaleHelper (BB430087484C1F4587C54EFC75681EB60CF70956EF2A999A75CE7B563B8BD694) also in the “/Library/Application\ Support/Ants2WhaleSupport/” folder.

Similar to all previous OSX AppleJeus variants, there is a postinstall script and a plist file which creates a LaunchDaemon to automatically run the Ants2WhaleHelper program.

ants2whale.com

Relationships

ants2whale.com	Downloaded	[Redacted]

Description

The website appears to show a legitimate cryptocurrency company and application, though it does contain multiple spelling and grammar mistakes indicating the creator may not have English as a first language. The website states that in order to download, a user must contact the administrator as their product is “premium package."

The domain ants2whale.com had a legitimately signed Sectigo Secure Sockets Layer (SSL) certificate, which was “Domain Control Validated” just as all previous AppleJeus domain certificates. The certificate was is valid from 09/21/2020 – 09/21/2021.

The domain is registered with NameCheap at the IP address 198.54.114.237 with ASN 22612. This IP is on the same ASN as the CoinGoTrade (AppleJeus variant 5 and Dorusio IP addresses (AppleJeus variant 6).

Screenshots

Figure 1 - Screenshot the ants2whale.com site.

Figure 2 - Screenshot of how to download Ants2Whale.

d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e

Tags

trojan

Details

Name	Ants2Whale
Size	77856 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	022298cf16c0c44d7b01b5de2cf84023
SHA1	939ec41183bbe1f4fb65c924323543ee91a35dbf
SHA256	d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e
SHA512	bda62d09606bbf5a0ee17dac06f1f3cfc77919f98e5fc14bd50b4f41f794df521aeced7b0f2a769a89498b7a6cd69be37689dab1652c3c16e
ssdeep	768:jPoXPdCyI4jB5nvjILkTSF3TSFi5UeSj0OfpZDkm+UjnAT9vSs:cXPdLI6XbIOem0EpZDX+Ujnc9v3
Entropy	4.361681

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

d5ac680e14...	Contained_Within	[Redacted]
d5ac680e14...	Connected_To	45.147.231.77

Description

This OSX sample was contained within Apple DMG installer "Ants2Whale.dmg." Ants2Whale is likely a copy of an open source cryptocurrency wallet application. When ran it loads a legitimate looking program which is fully functional and is very similar to the AppleJeus variant 5 "CoinGoTrade" application. Similar to CoinGoTrade there are references to “CryptoMex” in the Ants2Whale application.

Similarly to the CoinGoTrade application, the strings from Ants2Whale reveal the C2 hxxp[:]//45.147.231.77:3000. Investigation revealed the IP address 45.147.231.77 was hosted at Combahton GMH.

Screenshots

Figure 3 - Screenshot of the "Ants2Whale" application.

45.147.231.77

Tags

command-and-control

Ports

- 3000 TCP

Whois

Queried whois.ripe.net with "-B 45.147.231.77"...

% Information related to '45.147.228.0 - 45.147.231.255'

% Abuse contact for '45.147.228.0 - 45.147.231.255' is 'abuse@combahton.net'

inetnum: 45.147.228.0 - 45.147.231.255
netname: DE-COMBAHTON4-20190902
country: DE
org: ORG-CG252-RIPE
admin-c: JH29913-RIPE
tech-c: JH29913-RIPE
status: ALLOCATED PA
mnt-by: mnt-de-combahton4-1
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: mnt-de-combahton4-1
mnt-routes: mnt-de-combahton4-1
created: 2019-09-02T09:46:42Z
last-modified: 2019-09-02T09:46:42Z
source: RIPE

organisation: ORG-CG252-RIPE
org-name: combahton GmbH
country: DE
org-type: LIR
address: Mitterfeld 47
address: 85419
address: Mauern
address: GERMANY
e-mail: decombahton4@combahton.net
admin-c: JH29913-RIPE
tech-c: JH29913-RIPE
abuse-c: AR55171-RIPE
mnt-ref: mnt-de-combahton4-1
mnt-by: RIPE-NCC-HM-MNT
mnt-by: mnt-de-combahton4-1
created: 2019-08-30T08:08:51Z
last-modified: 2020-12-16T13:30:44Z
source: RIPE
phone: +4987642589890

person: Joseph Hofmann
address: Mitterfeld 47
address: 85419
address: Mauern
address: GERMANY
phone: +4987642589890
nic-hdl: JH29913-RIPE
mnt-by: mnt-de-combahton4-1
created: 2019-08-30T08:08:51Z
last-modified: 2019-08-30T08:08:51Z
source: RIPE

% Information related to '45.147.228.0/22AS30823'

route: 45.147.228.0/22
origin: AS30823
mnt-by: mnt-de-combahton4-1
created: 2019-09-02T09:57:36Z
last-modified: 2019-09-02T09:57:36Z
source: RIPE

Relationships

45.147.231.77	Connected_From	d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e

Description

The C2 for Ants2Whale (D5AC680E14B013E0624470DA7F46E84809D00B59A7544F6A42B110CF0E29254E).

bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694

Tags

downloaderloadertrojan

Details

Name	Ants2WhaleHelper
Size	69104 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|BINDS_TO_WEAK|PIE>
MD5	d4d1bcdfb67ee30303f30137db752b94
SHA1	34e134d614a0d5b0e4d94d63336aa8b898b0b104
SHA256	bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694
SHA512	eb9b518f95658c605b1bb3a548d7bfe630f9bff93b1f84919476377f9aabcd187db28ead9bc504ffd5c982a3985d12708888505f3d70fa5ea
ssdeep	1536:W1mJaIKMXBmyIZFED2enSoTVIV/3MpJy5T:XagpIsjnPTV03MpJy5T
Entropy	4.831788

Antivirus

Avira	OSX/Dldr.NukeSped.efijh
BitDefender	Trojan.MAC.Generic.105439
ESET	a variant of OSX/TrojanDownloader.NukeSped.B trojan
Emsisoft	Trojan.MAC.Generic.105439 (B)
Ikarus	Trojan-Downloader.OSX.Nukesped
Lavasoft	Trojan.MAC.Generic.105439
McAfee	OSX/Nukesped.h
Quick Heal	MacOS.Trojan.40149.GC
Symantec	OSX.Trojan.Gen
Zillya!	Downloader.NukeSped.OSX.13

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

bb43008748...	Contained_Within	[Redacted]
bb43008748...	Connected_To	qnalytica.com

Description

This OSX sample was contained within Apple DMG installer "Ants2Whale.dmg." Ants2WhaleHelper is similar to variants of AppleJeus. The Ants2WhaleHelper program contains the custom C++ "Barbeque" class for network communication as seen in the unioncryptoupater program. The C2 for this program is hxxps[:]//www[.]qnalytica.com/wp-rss.php.

qnalytica.com

Tags

command-and-control

URLs

- qnalytica.com/wp-rss.php

Whois

Whois for qnalytica.com had the following information:
Registrar: ENOM INC
Creation Date: 2020-08-11
Registrar Registration Expiration Date: 2021-08-11

Relationships

qnalytica.com	Connected_From	bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694

Description

The domain qnalytica.com has a legitimately signed SSL certificate from cPanel. cPanel is a hosting platform and certificate authority which is a reseller for Sectigo. The domain is registered with NameCheap at the IP address 194.36.191.196 with ASN 60117.

Relationship Summary

[Redacted]	Downloaded_By	ants2whale.com
[Redacted]	Contains	d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e
[Redacted]	Contains	bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694
ants2whale.com	Downloaded	[Redacted]
d5ac680e14...	Contained_Within	[Redacted]
d5ac680e14...	Connected_To	45.147.231.77
45.147.231.77	Connected_From	d5ac680e14b013e0624470da7f46e84809d00b59a7544f6a42b110cf0e29254e
bb43008748...	Contained_Within	[Redacted]
bb43008748...	Connected_To	qnalytica.com
qnalytica.com	Connected_From	bb430087484c1f4587c54efc75681eb60cf70956ef2a999a75ce7b563b8bd694

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.

- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-844-Say-CISA or CISA Central✉.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov✉
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.
