MAR-10322463-5.v1 - AppleJeus: CoinGoTrade

us-cert.cisa.gov/ncas/analysis-reports/ar21-048e

```
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; }
```

Malware Analysis Report

10322463.r5.v1

2021-02-12

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of ar 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 foreseeab accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distribut 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 Infras (CISA), and the Department of Treasury (Treasury) to highlight the cyber threat to cryptocurrency posed by North Korea, formally known as the D Republic of Korea (DPRK), and provide mitigation recommendations. Working with U.S. government partners, FBI, CISA, and Treasury assess th these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors—is targeting individuals and companies, incluc exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been modified to include r 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 gov Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on other versions of Ap recommended steps to mitigate this threat, see Joint Cybersecurity Advisory AA21-048A: AppleJeus: Analysis of North Korea's Cryptocurrency M 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 app legitimate-looking cryptocurrency trading company and website, whereby an unsuspecting individual downloads a third-party application from a w legitimate.

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

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

For a downloadable copy of IOCs, see: MAR-10322463-5.v1.stix.

Submitted Files (7)

326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd (CoinGoTradeUpgradeDaemon)

[Redacted] (CoinGoTrade.msi)

3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4 (CoinGoTrade.exe)

527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18 (CoinGo_Trade)

572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09 (CoinGoTradeUpdate.exe)

5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8 (prtspool)

[Redacted] (CoinGoTrade.dmg)

Domains (4)

airbseeker.com

coingotrade.com

globalkeystroke.com

woodmate.it

IPs (1)

23.152.0.101

Findings

[Redacted]

Tags

dropper

Details

Name	CoinGoTrade.msi
Size	[Redacted] bytes
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Security: 0, Code page: 1252, Numl CoinGoTrade, Author: CoinGoTrade, Name of Creating Application: Advanced Installer 14.5.2 build 83143, Template: ;1033, Commer database contains the logic and data required to install CoinGoTrade., Title: Installation Database, Keywords: Installer, MSI, Database
MD5	[Redacted]
SHA1	[Redacted]
SHA256	[Redacted]
SHA512	[Redacted]
ssdeep	[Redacted]
Entropy	[Redacted]

Antivirus

Avira	TR/NukeSped.lyfhd

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

[Redacted]	Downloaded_By	coingotrade.com
[Redacted]	Contains	3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4
[Redacted]	Contains	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09

Description

This Windows program from the CoinGoTrade site is a Windows MSI Installer. The installer appears to be legitimate and will install "CoinGoTrade (3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4) in the "C:\Program Files (x86)\CoinGoTrade" folder. It will also insta "CoinGoTradeUpdate.exe" (572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09) in the "C:\Users\ <username>\AppData\Roaming\CoinGoTradeSupport" folder. Immediately after installation, the installer launches "CoinGoTradeUpdate.exe." Dur "CoinGoTrade" folder containing the "CoinGoTrade.exe" application is added to the start menu.

Screenshots

Figure 1 - Screenshot of "CoinGoTrade" installation.

Figure 1 - Screenshot of "CoinGoTrade" installation.

coingotrade.com

URLs

- coingotrade.com/update_coingotrade.php
- hxxps[:]//coingotrade.com/download/[GUID]

Whois

Whois for coingotrade.com had the following information:
Registrar: NAMECHEAP INC
Creation Date: 2020-02-28
Registrar Registration Expiration Date: 2021-02-28

Relationships

coingotrade.com	Downloaded	[Redacted]
coingotrade.com	Connected_From	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09
coingotrade.com	Downloaded	[Redacted]

Description

The domain "coingotrade.com" had a legitimately signed Sectigo Secure Sockets Layer (SSL) certificate, which was “Domain Control Validated,” s certificates for previous AppleJeus variants. Investigation revealed the point of contact listed for verification was support[@]coingotrade.com. No c was available as the administrative or technical contact for the coingotrade.com domain.

The domain is registered with NameCheap at the IP address 198.54.114.175 with ASN 22612.

Investigation revealed the IP address 198.54.114.175 was hosted at NameCheap, but no records were available at the time of writing.

Screenshots

Figure 2 - Screenshot of the "CoinGoTrade" website.

Figure 2 - Screenshot of the "CoinGoTrade" website.

3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4

Tags

trojan

Details

Name	CoinGoTrade.exe
Size	166912 bytes
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	88de31ad947927004ab56ab1e855fd64
SHA1	1d1f9f3ee8329c3f3033222a46c7a311f259a359
SHA256	3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4
SHA512	6e8391afc19ddfb841b79cc9b697fcd162d3a94a79976d3525476475d6fbe684ce9f2ba3a433cd725a51a71f6f74635a109914ff14252fa
ssdeep	3072:ssXh1ExFDi8z4C3Ssi5jCxe7IDYQFNY7BGMDK49eQ:sZRul5rLK4s
Entropy	4.402659

Antivirus

Ahnlab	Trojan/Win32.FakeCoinTrader
BitDefender	Gen:Variant.MSILHeracles.2293
ESET	a variant of MSIL/Agent.TYJ trojan
Emsisoft	Gen:Variant.MSILHeracles.2293 (B)
Lavasoft	Gen:Variant.MSILHeracles.2293

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-03-17 04:55:13-04:00
Import Hash	f34d5f2d4577ed6d9ceec516c1f5a744
File Description	CryptoMex
Internal Name	CoinGoTrade.exe
Legal Copyright	Copyright © 2020
Original Filename	CoinGoTrade.exe
Product Name	CryptoMex
Product Version	1.0.0.0

PE Sections

MD5	Name	Raw Size	Entropy
ebb11bbea122a2fc761dff1d05defdb0	header	512	2.714333
b0d3ef9b5a227d092cf27c40c028d82d	.text	40960	4.785436
35d28033f1f2359f265d8f406fc2c620	.rsrc	124928	4.154855
9d7ce3b9440143a341b9232fc0cb38ce	.reloc	512	0.081539

Packers/Compilers/Cryptors

Microsoft Visual C# v7.0 / Basic .NET

Relationships

3e5442440a...	Contained_Within	[Redacted]
3e5442440a...	Connected_To	23.152.0.101

Description

This file is a 32-bit Windows executable contained within the Windows MSI Installer "CoinGoTrade.msi." When executed, "CoinGoTrade.exe" loac
cryptocurrency wallet application with no signs of malicious activity. The strings for "CoinGoTrade.exe" contain the command and control (C2) "hx
which was also identified in the MacOS CoinGo_Trade (527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18) and the I
from AppleJeus version 4. In addition, a build path is present in the strings “U:\work\CryptoMex\teobot\teobot\obj\Release\CoinGoTrade.pdb" and
description also states “CryptoMex." CryptoMex is likely an open source cryptocurrency application which was copied in order to create this applic

Screenshots

Figure 3 - Screenshot of "CryptoMex" listed in CoinGoTrade.exe" properties.

Figure 3 - Screenshot of "CryptoMex" listed in CoinGoTrade.exe" properties.

23.152.0.101

Tags

command-and-control

Ports

8080 TCP

Whois

Queried whois.arin.net with "n 23.152.0.101"...

```
NetRange:     23.152.0.0 - 23.152.0.255
CIDR:         23.152.0.0/24
NetName:      CROWNCLOUD-V6V4
NetHandle:    NET-23-152-0-0-1
Parent:       NET23 (NET-23-0-0-0-0)
NetType:      Direct Allocation
OriginAS:     AS8100
Organization: Crowncloud US LLC (CUL-34)
```

```
RegDate:        2015-11-23
Updated:        2015-11-23
Comment:        IPs in this block are statically assigned, please report any abuse to admin@crowncloud.us
Ref:            https://rdap.arin.net/registry/ip/23.152.0.0

OrgName:        Crowncloud US LLC
OrgId:          CUL-34
Address:        530 W 6th St
Address:        C/O Cid 4573 Quadranet Inc. Ste 901
City:           Los Angeles
StateProv:      CA
PostalCode:     90014-1207
Country:        US
RegDate:        2014-07-25
Updated:        2017-10-10
Ref:            https://rdap.arin.net/registry/entity/CUL-34

OrgTechHandle: CROWN9-ARIN
OrgTechName: Crowncloud Support
OrgTechPhone: +1-940-867-4072
OrgTechEmail: admin@crowncloud.us
OrgTechRef:    https://rdap.arin.net/registry/entity/CROWN9-ARIN

OrgAbuseHandle: CROWN9-ARIN
OrgAbuseName: Crowncloud Support
OrgAbusePhone: +1-940-867-4072
OrgAbuseEmail: admin@crowncloud.us
OrgAbuseRef:    https://rdap.arin.net/registry/entity/CROWN9-ARIN
```

Relationships

23.152.0.101	Connected_From	3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4
23.152.0.101	Connected_From	527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18

Description

This IP address is the C2 for "CoinGoTrade.exe" and "CoinGo_Trade."

572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09

Tags

trojan

Details

Name	CoinGoTradeUpdate.exe
Size	115712 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	149a696472d4a189f5896336ab16cc34
SHA1	decb43141699e43a1d27dc2db063e0020f9f33aa
SHA256	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09
SHA512	32081f04a1b4a9540aad81a2a20c00c81ade40624dd446babebeb7230bb84025ba59516fab1388aad3fbf6842811ef2d8d6f097895044
ssdeep	3072:FHAqeXaeHx9pdpqw6IQIsMF6s3yv7pHOBo:FWXaeHxrvB6X9M33
Entropy	6.128250

Antivirus

Ahnlab	Trojan/Win64.FakeCoinTrader
Avira	TR/NukeSped.ooibk
ESET	a variant of Win64/NukeSped.CR trojan
Ikarus	Trojan.Win64.Nukesped
K7	Trojan (00567f291)
Symantec	Trojan.Gen.2

TACHYON	Trojan/W64.APosT.115712
Zillya!	Trojan.APosT.Win32.1433

YARA Rules

No matches found.

ssdeep Matches

94	fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d

PE Metadata

Compile Date	2020-03-17 21:02:52-04:00
Import Hash	565005404f00b7def4499142ade5e3dd

PE Sections

MD5	Name	Raw Size	Entropy
d959d6ecb853f993046f81f109f7a5a9	header	1024	2.714314
e350351a05606da16418a7f01436cd7d	.text	65536	6.455927
5889779ac56e5fa9aa8123921d9ba943	.rdata	39936	5.084443
dbf3b39f579f6cafbdf3960f0a87f5f9	.data	2560	1.851526
9b5c53415d33ef775d744a48f71fcd18	.pdata	4096	4.957426
90e2eb1b90616d039eca5e2627ea1134	.gfids	512	1.320519
3f1861d2a0b1dc2d1329c9d2b3353924	.reloc	2048	4.762609

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

572a124f56...	Contained_Within	[Redacted]
572a124f56...	Connected_To	coingotrade.com

Description

This file is a 32-bit Windows executable contained within the Windows MSI Installer "CoinGoTrade.msi." When executed, CoinGoTradeUpdate.ex
service, which will automatically start when any user logs on. The service is installed with the description of "Automatic CoinGoTrade Upgrade."

After installing the service, "CoinGoTradeUpdate.exe" has similar behavior to the updater component for AppleJeus version 4 "Kupay Wallet." On
"CoinGoUpdate.exe" allocates memory to write a file. After allocating the memory and storing the hard-coded string "Latest" in a variable, the prog
network connection. The connection is named "CoinGoTrade 1.0 (Check Update Windows)," which is likely to avoid suspicion from a user.

Similarly, to previous AppleJeus variants, "CoinGoTradeUpdate.exe" collects some basic information from the system as well as a timestamp, anc
information in hard-coded format strings. Specifically, the timestamp is placed into a format string "ver=%d&timestamp=%lu" where "ver" is set as
referring to the CoinGoTrade version previously mentioned. This basic information and hard-coded strings are sent via a POST to the C2
"coingotrade.com/update_coingotrade.php." If the POST is successful (i.e. returns an HTTP response status code of 200) but fails any of multiple
"CoinGoTradeUpdate.exe" will sleep for two minutes and then regenerate the timestamp and contact the C2 again.

After receiving the payload from the C2, the program writes the payload to memory and executes the payload.

The payload for the Windows malware could not be downloaded, as the C2 server "coingotrade.com/coingotrade_update.php" was no longer acc
sample was not identified in open source reporting for this sample. The Windows payload is likely similar in functionality to "prtspool"
(5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8) the OSX stage 2 sample.

Screenshots

Figure 4 - Screenshot of the format string and version.

Figure 4 - Screenshot of the format string and version.

[Redacted]

Tags

droppertrojan

Details

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

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

[Redacted]	Downloaded_By	coingotrade.com
[Redacted]	Contains	527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18
[Redacted]	Contains	326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd

Description

This OSX program from the CoinGoTrade site is an Apple DMG installer. The installer was hosted at hxxps[:]//coingotrade.com/[GUID]. The [GUII crafted for a specific victim and is being withheld to preserve the identity of the intended recipient. The OSX program is an Apple DMG installer wi CoinGoTrade.dmg.

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 C appears to be legitimate and installs both “CoinGo_Trade” (527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18) in the “/Applications/CoinGoTrade.app/Contents/MacOS/” folder and a program named "CoinGoTradeUpgradeDaemon" (326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd) also in the “/Applications/CoinGoTrade.app/Contents/MacOS/” folc a postinstall script (Figure 5).

The postinstall script is identical in functionality to the postinstall scripts from previous AppleJeus variants and is identical to the AppleJeus varian script without the "launchctl" command. The postinstall script creates a “CoinGoTradeService” folder in the OSX “/Library/Application Support” fol "CoinGoTradeUpgradeDaemon" to it. The “Application Support” folder contains both system and third-party support files which are necessary for Typically, the subfolders have names matching those of the actual applications. At installation, CoinGoTrade placed the plist file (com.coingotrade “/Library/LaunchDaemons/."

As the LaunchDaemon will not be run immediately after the plist file is moved, the postinstall script then launches the "CoinGoTradeUpgradeDaer background.

Screenshots

Figure 5 - Screenshot of the postinstall script.

Figure 5 - Screenshot of the postinstall script.

Figure 6 - Screenshot of "com.coingotrade.pkg.product.plist."

Figure 6 - Screenshot of "com.coingotrade.pkg.product.plist."

527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18

Tags

trojan

Details

Name	CoinGo_Trade
Size	49536 bytes

Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	7a73178c682d1a61b2f1c61ae558b608
SHA1	358f4c8575c82f45340886f282d41ca0560cfa6e
SHA256	527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18
SHA512	bb044103c9d2abd04b06a7bae31215302e8310ef5e815ee15025b430b9ea230c7246c96769b2f03a614e1d196ab9bbdf9d3b49980d1b
ssdeep	384:O6XCYcjaTtLXN8KzIBAsyDfpBkSp6nHYYAZvamQ5nT:O6XZnRNnzICsyuHYrBxgn
Entropy	3.472034

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

527792dfab...	Contained_Within	[Redacted]
527792dfab...	Connected_To	23.152.0.101

Description

This OSX sample was contained within Apple DMG installer "CoinGoTrade.dmg." "CoinGo _Trade" is likely a copy of an open source cryptocurre
strings for "CoinGo_Trade" contain the C2 hxxp[:]//23.152.0.101:8080, which is also found in the Windows CoinGoTrade.exe (3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4) and the Kupay Wallet Stage 2 from AppleJeus version 4.

326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd

Tags

backdoortrojan

Details

Name	CoinGoTradeUpgradeDaemon
Size	33312 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	0d195513534855e613bd7a29243565ab
SHA1	80923c208c2c821ed99e1ed8f50bd549598a210c
SHA256	326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd
SHA512	d4c822252c03523a3e37edf314caa5142be230e2c34e3f5b648a944b88632e6e74af41bc9c8661c608fdff19822c590f6f98d41dc524385
ssdeep	192:fWkPKt21UIIymPTTDO/kqMd+K2uk6aLc4eL:fWIogUKmPTT8
Entropy	1.690330

Antivirus

Ahnlab	Trojan/OSX64.FakeCoinTrader.33313
Antiy	Trojan/Mac.NukeSped
Avira	OSX/NukeSped.ifaaj
BitDefender	Gen:Variant.Trojan.MAC.Lazarus.4
ClamAV	Osx.Malware.Agent-8010705-0
ESET	a variant of OSX/NukeSped.F trojan
Emsisoft	Gen:Variant.Trojan.MAC.Lazarus.4 (B)
Ikarus	Trojan.OSX.Nukesped

Lavasoft	Gen:Variant.Trojan.MAC.Lazarus.4
McAfee	OSX/Lazarus.c
Microsoft Security Essentials	Trojan:MacOS/NukeSped.D!MTB
Quick Heal	Mac.Backdoor.38173.GC
Sophos	OSX/NukeSped-AG
Symantec	OSX.Trojan.Gen
TrendMicro	TROJ_FR.84D8D3BE
TrendMicro House Call	TROJ_FR.84D8D3BE
Zillya!	Trojan.NukeSped.OSX.7

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

326d7836d5...	Contained_Within	[Redacted]

Description

This OSX sample was contained within Apple DMG installer "CoinGoTrade.dmg." "CoinGoTradeUpgradeDaemon" is similar to "kupay_upgrade" f When executed, "CoinGoTradeUpgradeDaemon" will immediately sleep for five seconds and then test to see if the hard-coded value stored in “isl a 0, the program sleeps again and if it is a 1, the function “CheckUpdate” is called. This function contains most of the logic functionality of the malv sends a POST to the C2 hxxps[:]//coingotrade.com/update_coingotrade.php with a connection named “CoinGoTrade 1.0 (Check Update Osx).

If the C2 server returns a file, it is decoded and written to “/private/tmp/updatecoingotrade” and the permissions are set with the command "chmoc read, write, and execute). The stage 2 malware (/private/tmp/updatecoingotrade) is then launched and the malware "CoinGoTradeUpgradeDaem and checking in with the C2 server.

The stage 2 payload for CoinGoTrade was no longer available from the specified download URL, however, there was a file "prtspool" (5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8) submitted to VirusTotal by the same user on the same date as "CoinGoTradeUpgradeDaemon." This suggests the submitted file may be related to the OSX malware and could be the downloaded payload. Ana showed the file has the same encryption algorithm and initial key values as a Lazarus Group implant known as HOPLIGHT or MANUSCRYPT.

Screenshots

Figure 7 - Screenshot of the C2 loaded into variable.

Figure 7 - Screenshot of the C2 loaded into variable.

Figure 8 - Screenshot of the format string.

Figure 8 - Screenshot of the format string.

5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8

Tags

backdoortrojan

Details

Name	prtspool
Size	57376 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|BINDS_TO_WEAK|PIE>
MD5	451c23709ecd5a8461ad060f6346930c
SHA1	58b0516d28bd7218b1908fb266b8fe7582e22a5f
SHA256	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8
SHA512	80961db270b9f15cff4b0443be79b253e0f98304990fceda03cd2b25393b0e483eacc553e7b33d20da23e3317fafc7b41f93c4a9da863b
ssdeep	768:qQS5bSXXUkVSpVM0ZJflKprXYgICxdAvV/hQJx62:gbGkjZ7KbICY/hQJx6
Entropy	4.259743

Antivirus

Antiy	Trojan[Backdoor]/OSX.NukeSped
Avira	OSX/NukeSped.vhsxo
BitDefender	Trojan.MAC.Generic.12195
ClamAV	Osx.Malware.Agent-8019494-0
ESET	a variant of OSX/NukeSped.E trojan
Emsisoft	Trojan.MAC.Generic.12195 (B)
Ikarus	Trojan.OSX.Nukesped
Lavasoft	Trojan.MAC.Generic.12195
McAfee	OSX/Nukesped.e
Quick Heal	Mac.Backdoor.38173.GC
Sophos	OSX/NukeSped-AF
Symantec	OSX.Trojan.Gen
TrendMicro	TROJ_FR.84D8D3BE
TrendMicro House Call	TROJ_FR.84D8D3BE
Zillya!	Trojan.NukeSped.OSX.14

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

5e40d10697...	Connected_To	airbseeker.com
5e40d10697...	Connected_To	globalkeystroke.com
5e40d10697...	Connected_To	woodmate.it

Description

This file is a OSX samples that was likely the payload for the sample "CoinGoTradeUpgradeDaemon."This file "prtspool" is a 64-bit MACHO exec
capabilities:

--Begin capabilities--
Perform a heart-beat check in with the current C2
Sleep for the specified number of minutes
Ensure a copy of the current configuration data is written to the file on disk
Delete the configuration file and exit the implant.
Upload the current in memory configuration data.
Download a new configuration, overwrite the current in memory configuration and write the data to the file /private/etc/krb5d.conf
Perform a secure delete or file wipe the specified file by overwriting it with all zeros before deleting it from the system.
Download a file from the C2 and write it to the specified path.
Upload a file from the specified file to the C2 server.
Execute the specified command on the OS shell, pipe the output to a temporary file, and upload it to the C2.
Execute the specified process.
List the files and directories in the specified path.
Perform a TCP connection to the specified IP address and port and report the status back to the C2.
Set the current working directory to the specified path.
--End capabilities--

The file has three C2 URLs hard-coded into the file. In communicating with these servers, the file uses an HTTP POST with multipart-form data bo
N9dLfqxHNUUw8qaUPqggVTpX." Similar to other Lazarus malware, "prtspool" uses format strings to store data collected about the system and s

--Begin C2 URLs--
hxxps[:]//airbseeker.com/rediret.php
hxxps[:]//globalkeystroke.com/pockbackx.php
hxxps[:]//www[.]woodmate.it/administrator/help/en-GB/bins/tags/taghelper.php.
--End C2 URLs--

airbseeker.com

Tags

command-and-control

URLs

hxxps[:]//airbseeker.com/rediret.php

Whois

Whois for airbseeker.com had the following information:
Registrar: NAMECHEAP INC
Created: 2020-03-03
Expires: 2021-03-03

Relationships

airbseeker.com	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8

Description

The domain "airbseeker.com" has a legitimately signed Sectigo SSL certificate, which was “Domain Control Validated." The domain was at the IP
with ASN 22612.

globalkeystroke.com

Tags

command-and-control

Whois

Whois for globalkeystroke.com had the following information:
Registrar: NAMECHEAP INC
Created: 2019-11-11
Expires: 2020-11-11

Relationships

globalkeystroke.com	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8

Description

The domain "globalkeystroke.com" has a legitimately signed Sectigo SSL certificate, which was “Domain Control Validated." Investigation reveale
listed for verification was admin[@]globalkeystroke.com. No other contact information was available as the administrative or technical contact for
domain.

The domain is registered with NameCheap at the IP address 68.65.122.160 with ASN 22612. The IP address of 185.228.83.129 belongs to Acces
the Netherlands. Whois information for the IP revealed the network name as belonging to CrownCloud of Australia.

On October 11, 2019, the IP address 185.228.83.129 was hosting the domain dev.jmttrading.org according to PassiveDNS. JMT Trading was the
AppleJeus malware.

woodmate.it

Tags

command-and-control

Whois

Whois for woodmate.it had the following information:
Registrar: REGISTRYGATE GMBH
Created: 2014-05-07
Expires: 2020-05-07

Relationships

woodmate.it	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8

Description

The domain "woodmate.it" has a legitimately signed Let’s Encrypt certificate. Let’s Encrypt is a nonprofit Certificate Authority which provides free
certificates for anyone running their software. They do not perform any identity validation.

The domain is registered with RegistryGate GMBH of Germany at the IP address 85.13.146.113 with ASN 34788.

The IP address 85.13.146.113 is hosted by Neue Medien Muennich Gmbh of Germany.

Relationship Summary

[Redacted]	Downloaded_By	coingotrade.com
[Redacted]	Contains	3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4

[Redacted]	Contains	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09
coingotrade.com	Downloaded	[Redacted]
coingotrade.com	Connected_From	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09
coingotrade.com	Downloaded	[Redacted]
3e5442440a...	Contained_Within	[Redacted]
3e5442440a...	Connected_To	23.152.0.101
23.152.0.101	Connected_From	3e5442440aea07229a1bf6ca2fdf78c5e2e5eaac312a325ccb49d45da14f97f4
23.152.0.101	Connected_From	527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18
572a124f56...	Contained_Within	[Redacted]
572a124f56...	Connected_To	coingotrade.com
[Redacted]	Downloaded_By	coingotrade.com
[Redacted]	Contains	527792dfab79f026eaa6930d2109c93e816ed31826dba0338a9223db71aced18
[Redacted]	Contains	326d7836d580c08cf4b5e587434f6e5011ebf2284bbf3e7c083a8f41dac36ddd
527792dfab...	Contained_Within	[Redacted]
527792dfab...	Connected_To	23.152.0.101
326d7836d5...	Contained_Within	[Redacted]
5e40d10697...	Connected_To	airbseeker.com
5e40d10697...	Connected_To	globalkeystroke.com
5e40d10697...	Connected_To	woodmate.it
airbseeker.com	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8
globalkeystroke.com	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8
woodmate.it	Connected_From	5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organizatio 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 unl
- 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
- 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) Specia **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at t https://us-cert.cisa.gov/forms/feedback/

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 mos provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua 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 shoul
at 1-888-282-0870 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 ph
Reporting forms can be found on CISA's homepage at www.cisa.gov.

Revisions

February 17, 2021: Initial Version