MAR-10322463-4.v1 - AppleJeus: Kupay Wallet | CISA

Published: 2021-04-15 · Archived: 2026-04-06 00:48:44 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 Lazarus Group 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—Kupay Wallet—and associated IOCs used by the North Korean government in AppleJeus operations.

Kupay Wallet, discovered in March 2020, is a legitimate-looking cryptocurrency trading software that is marketed and distributed by a company and website—Kupay Service and kupaywallet[.]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-10322463-4.v1.stix.

Submitted Files (7)

0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba (kupay_upgrade)

1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6 (Kupay.exe)

55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9 (Kupay.dmg)

6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8 (Kupay.msi)

91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd (kupayupdate_stage2)

a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492 (kupay)

fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d (KupayUpgrade.exe)

Domains (2)

kupaywallet.com

levelframeblog.com

Findings

6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8

Tags

dropper

Details

Name	Kupay.msi
Size	143568384 bytes
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 20 Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Dec 11 11:47:44 2009, Security: 0, Code page: 1252, Revision Numbe C353-460A-B325-AF38D7F3E338}, Number of Words: 2, Subject: Kupay, Author: Kupay Service, Name of Creating Application: Adv 14.5.2 build 83143, Template: ;1033, Comments: This installer database contains the logic and data required to install Kupay., Title: Inst Keywords: Installer, MSI, Database, Number of Pages: 200
MD5	afdf3dd62dafd401be4bbeca65b42635
SHA1	8b45d12ed8c058ea0ce3122da9a82b9fb045d6a3
SHA256	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8
SHA512	bdc7a8904ad154046ade472442810c0007e5494665b429d847eef74b05567422600dd543bd8ae632128cd8def853926f2a86eab0e7d91a1d
ssdeep	3145728:M8yVXZLQX6rw3cJRGmMEuwRNiPTdy68L04oIRHndNQGOx:9yVXZfrw3CGtw3iPTdytmIRHdlw
Entropy	7.997013

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

6b945159b4...	Contains	1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6
6b945159b4...	Contains	fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d
6b945159b4...	Downloaded_By	kupaywallet.com

Description

This Windows program from the Kupay Service site is a Windows MSI Installer with the file name Kupay[GUID].msi. The installer was hosted at hxxps[:]kupaywallet.com/product/[GUID]. The [GUID] is a unique file that is crated for a specific victim and is being withheld to preserve the identity of the intended recipient.

The installer looks legitimate and will install the "Kupay.exe" (1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6) file in the “C:\Program Files (x86)\Kupay” folder. It also installs "KupayUpgrade.exe" (fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d) in the “C:\Users\<username>\AppData\Roaming\KupaySupport” folder. Immediately after installation, the installer launches the "KupayUpgrade.exe" binary.

Screenshots

Figure 1 - Screenshot of "Kupay.msi" installation.

kupaywallet.com

Tags

command-and-control

URLs

- kupaywallet.com/kupay_update.php
- kupaywallet.com/product/

Whois

Whois for kupaywallet.com had the following information:
Registrar: NAMECHEAP INC
Creation Date: 2020-02-21
Registrar Registration Expiration Date: 2021-02-21

Relationships

kupaywallet.com	Downloaded	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8
kupaywallet.com	Downloaded	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
kupaywallet.com	Connected_From	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba

Description

The domain kupaywallet.com had a legitimately signed Sectigo Secure Sockets Layer (SSL) certificate, which was “Domain Control Validated” just as all previous AppleJeus domain certificates. Investigation revealed the point of contact listed for verification was admin[@]kupaywallet.com. No other contact information was available as the administrative or technical contact for the kupaywallet.com domain.

The domain is registered with NameCheap at the IP address 104.200.67.96 with ASN 8100.

In addition to the site kupaywallet.com, a Twitter account @kupayservice is associated with the company. This account tweets out general cryptocurrency articles and information and replies to various related tweets. The first tweet was on May 23, 2019, while the last was on July 11, 2019. Twitter lists the joined date for @kupayservice to be October 2018.

Screenshots

Figure 2 - Screenshot of KupayService Twitter account.

1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6

Tags

trojan

Details

Name	Kupay.exe
Size	97686016 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	668d696582f9c00029e2e8253470e9db
SHA1	e83ebe43da7bbfb9c95d34163383d1b3926e663f
SHA256	1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6
SHA512	0b370636ea2b7211d691a3bfcfc9017cb12df6874becb9b6334ca735bc325f59c50e99fc3b57c8db2d265e0c631651c7280109ffdbb3b48b7
ssdeep	1572864:MdJvugr82jf19dUM/1T8+1VJRukUhkmG:Mdhg6Pm
Entropy	6.674838

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

97	78b56a1385f2a92f3c9404f71731088646aac6c2c84cc19a449976272dab418f

PE Metadata

Compile Date	2019-12-16 00:00:00-05:00
Import Hash	bb1d46df79ee2045d0bc2529cf6c7458
Company Name	BitPay
File Description	Kupay
Internal Name	Kupay
Legal Copyright	Copyright © 2020 BitPay
Product Name	Kupay
Product Version	9.1.0.0

PE Sections

MD5	Name	Raw Size	Entropy
32b731864b0ff3d1c427c97d582e7897	header	1024	2.990247

MD5	Name	Raw Size	Entropy
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
85237257867935c227d2f2f39316b12a	.rsrc	106496	4.912524
fb3216031225fdb1902888e247009d0c	.reloc	709120	5.476445

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

1b60a6d35c...	Contained_Within	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "Kupay.msi." When executed, "Kupay.exe" loads a legitimate looking cryptocurrency wallet application with no signs of malicious activity. This application appears to be a modification of the open source cryptocurrency wallet Copay, which is distributed by Atlanta based company BitPay. According to their 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 "kupaywallet.com" and the company listed in the version information for Kupay is Bitpay.

Lastly, the GitHub “Commit Hash” listed in the Dorusio application “638b2b1” is to a branch of Copay found at hxxps[:]//github.com/flean/copay-1 (Figure 5).

Screenshots

Figure 3 - Screenshot of the Kupay Wallet application.

Figure 4 - Screenshot of the Bitpay site displaying the application.

Figure 5 - Copay GitHub branch matching Dorusio.

fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d

Tags

trojan

Details

Name	KupayUpgrade.exe
Size	115712 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	60c2efdafbffc5bd6709c8e461f7b77d

SHA1	dbddccba18422eea5d7bb1bdfe66ceee90446a45
SHA256	fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d
SHA512	5543d4e5872ef5b0f12ba180425d2ab94131c03f4fec7195f3a74d051d5a867ad580ea794a1af6c6bd16e4bc27337cc138fe71aab9600792bf
ssdeep	3072:oHAqeXaeHx9pdpqw6IQIsMF6s3yvPxdOBU:kWXaeHxrvB6X9M33
Entropy	6.128091

Antivirus

Ahnlab	Trojan/Win64.FakeCoinTrader
ESET	a variant of Win64/NukeSped.DE trojan
K7	Trojan (00569b451)
Zillya!	Trojan.Generic.Win32.1058845

YARA Rules

No matches found.

ssdeep Matches

94	572a124f5665be68eaa472590f3ba75bf34b0ea2942b5fcbfd3e74654202dd09

PE Metadata

Compile Date	2020-02-25 03:46:13-05:00
Import Hash	565005404f00b7def4499142ade5e3dd

PE Sections

MD5	Name	Raw Size	Entropy
695567cdbccfbe54b19634abe3bb1e5b	header	1024	2.723717
e35b1061d665602ed7e1c2d9de87f059	.text	65536	6.456115
1578510ae509e46d8f3201edb3349d54	.rdata	39936	5.084900
dbf3b39f579f6cafbdf3960f0a87f5f9	.data	2560	1.851526
cb3735cf6fde4690ee7a6cd2026eb4de	.pdata	4096	4.957030
90e2eb1b90616d039eca5e2627ea1134	.gfids	512	1.320519
3f1861d2a0b1dc2d1329c9d2b3353924	.reloc	2048	4.762609

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

fc1aafd2ed...	Contained_Within	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "Kupay.msi." When executed, "KupayUpgrade.exe" first installs itself as a service, which will automatically start when any user logs on. The service is installed with a description stating “Automatic Kupay Upgrade."

On startup, "KupayUpgrade.exe" allocates memory in order to later write a file. After allocating the memory and storing the hard-coded string “Latest” in a variable, the program attempts to open a network connection. The connection is named

“Kupay Wallet 9.0.1 (Check Update Windows)”, likely to avoid suspicion from a user.

Similarly to previous AppleJeus variants, "KupayUpgrade.exe "collects some basic information from the system as well as a timestamp, and places them in hard coded format strings. Specifically, the timestamp is placed into a format string “ver=%d&timestamp=%lu” where ver is set as the 90001, possibly referring to the Kupay Wallet version previously mentioned (Figure 7).

This basic information and hard-coded strings are sent via a POST to the C2 kupaywallet.com/kupay_update.php. If the POST is successful (i.e. returns an HTTP response status code of 200) but fails any of multiple different checks, "KupayUpgrade.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 "kupaywallet.com/kupay_update.php" was no longer accessible. In addition, the sample was not identified in open source reporting for this sample.

Screenshots

Figure 6 - Screenshot of Kupay service.

Figure 7 - Screenshot of the format string.

55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9

Tags

dropper

Details

Name	Kupay.dmg
Size	132870749 bytes
Type	zlib compressed data
MD5	2f6573b3ae4262f04227468aab353387
SHA1	dd9058e3a6c791b18bf561a3177788cf60cd6e91
SHA256	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
SHA512	a26f1e0673563fea0d134f3238fe36b12dcd4567c6ae7e962113e9531e1847e9195b010a2b10ee087382163a973164c795052788ab450785
ssdeep	3145728:ttCQsiN4OYPdJvjr78vjHPZBs3CI0s9KVzcGesHiYhR7SsH:ttCQsiNmPjLXqvsgS/AusH
Entropy	7.993885

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

55eacc25e9...	Contains	a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492
55eacc25e9...	Downloaded_By	kupaywallet.com
55eacc25e9...	Contains	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba

Description

In March 2020, a download link for the OSX version of Kupay Wallet was found to be hosted at hxxps[:]//kupaywallet.com/[GUID]. The OSX program from the Kupay Wallet download link is an Apple DMG installer. The [GUID] is a unique file that is crafted for a specific victim and is being withheld to preserve the identity of the intended recipient. The OSX program uses a DMG installer with the file name Kupay[GUID].dmg.

The OSX program does not have digital signature, and will warn of that before installation. Just as JMTTrader, CelasTradePro, and UnionCrypto, the Kupay installer appears to be legitimate, and installs both “Kupay” in the “/Applications/Kupay.app/Contents/MacOS/” folder and a program named kupay_upgrade also in the “/Applications/Kupay.app/Contents/MacOS/” folder. The installer contains a postinstall script (Figure 8).

The postinstall script is identical in functionality to the postinstall scripts from previous AppleJeus variants, though accomplishes the same functions in a different way than previously done. The postinstall script creates a “KupayDaemon” folder in the OSX “/Library/Application Support” folder, and moves kupay_upgrade to it. The “Application Support” folder contains both system and third-party support files which are necessary for program operation. Typically, the subfolders have names matching those of the actual applications. At installation, Kupay placed the plist file (com.kupay.pkg.wallet.plist) in “/Library/LaunchDaemons/”.

While previous versions of AppleJeus simply moved the plist file to the LaunchDaemons folder and waited for a restart for it to be loaded, the Kupay postinstall runs the command “launchctl load” to load the plist without a restart. The postinstall then launches the kupay_upgrade program in the background.

Screenshots

Figure 8 - Screenshot of the postinstall script.

Figure 9 - Screenshot of "com.kupay.pkg.wallet.plist."

a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492

Details

Name	kupay
Size	186044 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	4a43bafb4af0a038a7f430417bcc1b6e
SHA1	438243575764a5e856951126674f72f20b2a0d6f
SHA256	a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492
SHA512	51d37b27f390bc7f124f2cb8efb2b9c940d7a0c21b0912d06634f7f6af46a35e3221d25945bcad4b39748699ba8a33b17c350a480560e5c5c
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.

Relationships

a0c461c94b...	Contained_Within	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9

Description

This OSX sample was contained within Apple DMG "Kupay.dmg." Kupay is likely a copy of an open source cryptocurrency wallet application. When ran it loads a legitimate looking wallet program, which is fully functional, and is identical to the Windows Kupay.exe program. Although this executable is not inherently malicious, organizations who identify the hash and a "kupay[GUID].dmg" present on a system should assume they are compromised if it is present with other files or activity described in this report.

0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba

Tags

trojan

Details

Name	kupay_upgrade
Size	33248 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	f00bde07d9f8b7af1da425c23cc47e47
SHA1	c0670e18e1e3fbde58a25cbb94ba11558c02e7d3
SHA256	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba
SHA512	266746da74bda3aed3af13d0b51adaee0e2e56d13ff8b1f68e1766b96b12dd2d5dadca143b7f5fc8693bd24aaa008c3a24161e69625c6b053c
ssdeep	192:AShk5sZUIyfKaTuy+YZ+qyepkfLYrs4eL:AShmxfKaTuQr
Entropy	1.652634

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

0bc7517aa2...	Contained_Within	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
0bc7517aa2...	Connected_To	kupaywallet.com
0bc7517aa2...	Downloaded	91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd

Description

This OSX sample was contained within Apple DMG "Kupay.dmg." When executed, "kupay_upgrade" immediately sleeps for five seconds and then tests 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 called. This function contains most of the logic functionality of the malware. "CheckUpdate" sends a POST to the C2 hxxps[:]//kupaywallet.com/kupay_update.php with a connection named “Kupay Wallet 9.0.1 (Check Update Osx)."

Just as the Windows malware, the timestamp is placed into a format string “ver=%d&timestamp=%ld” where ver is set as the 90001, possibly referring to the AppleJeus version 4 Kupay Wallet (Figure 11).

If the C2 server returns a file, it is decoded and written to “/private/tmp/kupay_update”, with permissions by the command chmod 700 (only the user can read, write, and execute). The stage2 (/private/tmp/kupay_update) is then launched, and the malware kupay_upgrade returns to sleeping and checking in with the C2 server.

Screenshots

Figure 10 - Screenshot of the C2 loaded into variable.

Figure 11 - Screenshot of the format string.

91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd

Tags

trojan

Details

Name	kupayupdate_stage2
Size	40176 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	17ab2927a235a0b98480945285767bcf
SHA1	d4b96e9d966b0f1e9ff1ef61a8d09c9020254652
SHA256	91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd
SHA512	51a5279db7b0074c83aac19f7f426b8a1dadd939e3ee660f71be3e5da110f0af8ae5bb781ad0b57c6ded19ae74aa95dbc2a8887443f63837f6
ssdeep	192:HZpt4Xnd+9EQbpvhyN1pQhO9de0II+pldd6gH1h8h/XbARs8xpDOL3ySoAk8+4uT:5pMUq6DaxaI+rddNH16VXbXDP4
Entropy	3.266343

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

91eaf215be...	Connected_To	levelframeblog.com
91eaf215be...	Downloaded_By	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba

Description

This file is the stage 2 payload for the OSX KupayWallet. The stage 2 payload for the OSX KupayWallet was decoded and analyzed, and file properties are related to the decoded file. The stage 2 kupay_update has a variety of functionalities. Most importantly, kupay_update checks in with the C2 levelframeblog.com/felix.php. After connecting to the C2, kupay_update can send or receive a payload, read and write files, execute commands via the terminal, etc.

If a payload is received or is going to be sent, kupay_update will base64 encode/decode and XOR encode/decode the data before sending or after receiving. The functions which base64 encode and decode are named b64_encode and b64_decode.

The functions which XOR encodes and decodes is XEncoding, and it uses a 32-byte XOR key which is hardcoded into kupay_update. The key is “wLqfM]%wTx`~tUTbw>R^0x18#yG5R(30x7FC:;” where all values are in ASCII except for 0x18 and 0x7F as those are non-readable characters in ASCII. This key is also used in the DecryptPayload and CryptPayload functions. These two functions implement the XOR encode or decode without calling XEncoding, and also call the b64_decode and b64_encode functions.

Kupay_update checks in with the C2 frequently, in order to execute or preform whatever commands and requests the server sends. There are multiple “sleep” calls throughout the function to dictate when the contact with the C2 is made.

Screenshots

Figure 12 - Screenshot of the portion of b64_encode.

Figure 13 - Screenshot of XOR Loop in function XEncoding

levelframeblog.com

Tags

command-and-control

URLs

- levelframeblog.com/felix.php

Whois

Whois for levelframeblog.com had the following information:
Registrar: NAMECHEAP INC
Created: 2019-11-14
Expires: 2020-11-14

Relationships

levelframeblog.com	Connected_From	91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd

Description

This domain is the C2 for 2nd stage malware. The domain is registered with NameCheap at the IP address 23.152.0.101 with ASN 8100.

Relationship Summary

6b945159b4...	Contains	1b60a6d35c872102f535ae6a3d7669fb7d55c43dc7e73354423fdcca01a955d6
6b945159b4...	Contains	fc1aafd2ed190fa523e60c3d22b6f7ca049d97fc41c9a2fe987576d6b5e81d6d
6b945159b4...	Downloaded_By	kupaywallet.com
kupaywallet.com	Downloaded	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8
kupaywallet.com	Downloaded	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
kupaywallet.com	Connected_From	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba
1b60a6d35c...	Contained_Within	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8
fc1aafd2ed...	Contained_Within	6b945159b4c816ec5e212ba125eb01938234205d8d3e57fca46de7c064c628f8
55eacc25e9...	Contains	a0c461c94ba9f1573c7253666d218b3343d24bfa5d8ef270ee9bc74b7856e492
55eacc25e9...	Downloaded_By	kupaywallet.com
55eacc25e9...	Contains	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba
a0c461c94b...	Contained_Within	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
0bc7517aa2...	Contained_Within	55eacc25e9eaba5d3f04b6cbcac2e16879b83d967596d645e5ec4b8f42656ef9
0bc7517aa2...	Connected_To	kupaywallet.com
0bc7517aa2...	Downloaded	91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd
91eaf215be...	Connected_To	levelframeblog.com
91eaf215be...	Downloaded_By	0bc7517aa2f0c1820ced399bfd66b993f10ad77e8d72727b0f3dc1ca35cad7ba
levelframeblog.com	Connected_From	91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd

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.

February 17, 2021: Initial Version|April 15, 2021: AppleJeus: Kupay Wallet, clarified that a malware sample contained within Apple DMG "Kupay.dmg" is not inherently malicious and provided guidance on what organizations should look for to determine compromise