ANALYSIS REPORT

10387061.r1.v1 NUMBER

Malware Analysis Report

2022-10-24 DATE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:CLEAR–Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA obtained four malicious files for analysis during an on-site incident response engagement at a Federal Civilian Executive Branch (FCEB) organization compromised by Iranian government sponsored advanced persistent threat (APT) actors.

These files have been identified as variants of the XMRIG cryptocurrency mining software. The files include a kernel driver, two Windows executables, and a configuration file to control one of the executable's behavior on the network and infected host.

For more information on the confirmed compromise, see joint CSA Iranian Government Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester.

Submitted Files (4)

11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5 (WinRing0x64.sys)

2ffe6509d965413d20ae859a4b4878246119159c368c945a7b466435b4e6e6df (RuntimeBroker.exe)

673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb (wuaucltservice.exe)

b511c0f45d2a1def0985fa631d1a6df5f754bc7c5f53105cc97c247b97ff0f56 (config.json)

Findings

11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5

Details

Name	WinRing0x64.sys
Size	14544 bytes
Type	PE32+ executable (native) x86-64, for MS Windows
MD5	0c0195c48b6b8582fa6f6373032118da
SHA1	d25340ae8e92a6d29f599fef426a2bc1b5217299
SHA256	11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5
SHA512	ab28e99659f219fec553155a0810de90f0c5b07dc9b66bda86d7686499fb0ec5fddeb7cd7a3c5b77dccb5e865f2715c2d81f4d40df4431c92ac7860c7e01720d
ssdeep	192:nqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:qjKL+v/y+5TWGYOf2OJ06dUb+pQ
Entropy	6.266030

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2008-07-26 09:29:37-04:00
Import Hash	d41fa95d4642dc981f10de36f4dc8cd7
Company Name	OpenLibSys.org
File Description	WinRing0
Internal Name	WinRing0.sys
Legal Copyright	Copyright (C) 2007-2008 OpenLibSys.org. All rights reserved.
Original Filename	WinRing0.sys
Product Name	WinRing0
Product Version	1.2.0.5

PE Sections

MD5	Name	Raw Size	Entropy
1002ff0ee92dc9b20d657e288433200f	header	1024	2.311532
1c3d5bb2285dafcf3b7746bf717c1a51	.text	2048	5.391023
08362d1269d5a5ef4e7560cab993590d	.rdata	512	3.284507
043c46095689123e1f5be96c109c2f46	.data	512	0.301407
077af14197899077aa36d2c72ba1773f	.pdata	512	0.857623
ba375d2de342e7d7a93487a35ea5d36d	INIT	1024	3.057208
5459c1fdb222b651d36692c4ca5df895	.rsrc	1024	3.126728

Description

This Windows driver file is a variant of the XMRIG cryptocurrency mining software.

---

b511c0f45d2a1def0985fa631d1a6df5f754bc7c5f53105cc97c247b97ff0f56

Tags

miner

Details

Name	config.json
Size	4455 bytes
Type	JSON data
MD5	910350d4f72b7b25f4fbecfc08d815cd
SHA1	a95fe63bbade63711cdfd012805d7370cbda3d76
SHA256	b511c0f45d2a1def0985fa631d1a6df5f754bc7c5f53105cc97c247b97ff0f56
SHA512	aeaff1d8728ec5f2471bc6ed7671ca47c829fe20e422ecbd88c727935fbd6cf1f3f4355a20e976e2bfd8f9b24e52ab151b2b3a8b562efb102b2c9b063628efa3
ssdeep	96:EePpTFycC1d1FwKQjHKufLKzKCc1DMuIlz3OO7eknyyw10AwJqQ4:/FqdjwKQjHKQLKzKCSMJz3OO7eknyyJS
Entropy	4.380124

Antivirus

ESET	Win64/CoinMiner.RO potentially unwanted application

Quick Heal	JSON.Miner.42626

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b511c0f45d...	Used_By	673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb

Description

The four screenshots depicting config.json prove that it is used by the Windows executable 673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb. Furthermore the contents of the file and the network traffic reveal a connection to the cryptocurrency mining location "mine.c3pool.com:80". Also present are user agent strings, from the network traffic, showing a connection attempt to a cryptocurrency mining location with a login ID and password. The user agent strings further prove that this is a configuration file for a variant of the XMRIG cryptocurrency mining software.

Screenshots

Figure 1 - This screenshot shows a select excerpt of the config.json file.

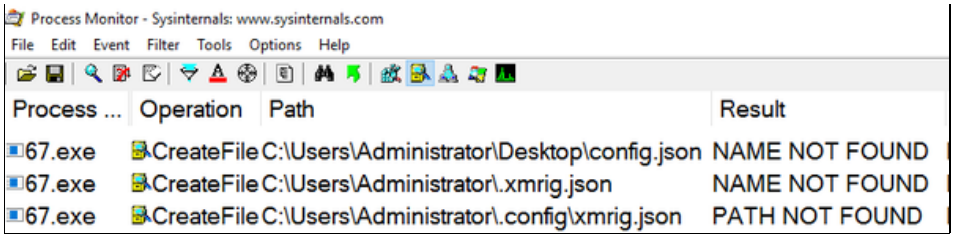

Figure 2 - This screenshot shows the Windows executable, 673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb, in Process Monitor, looking for, and not finding, the config.json file in the same working directory.

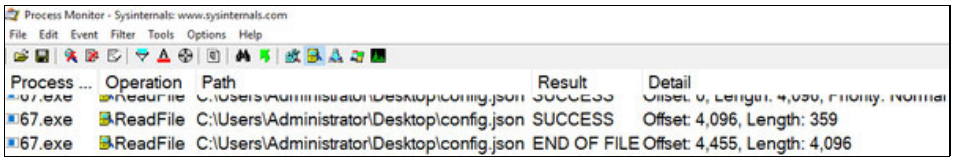

Figure 3 - This screenshot shows the Windows executable, 673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb, in Process Monitor, looking for, finding, and reading data from the config.json file.

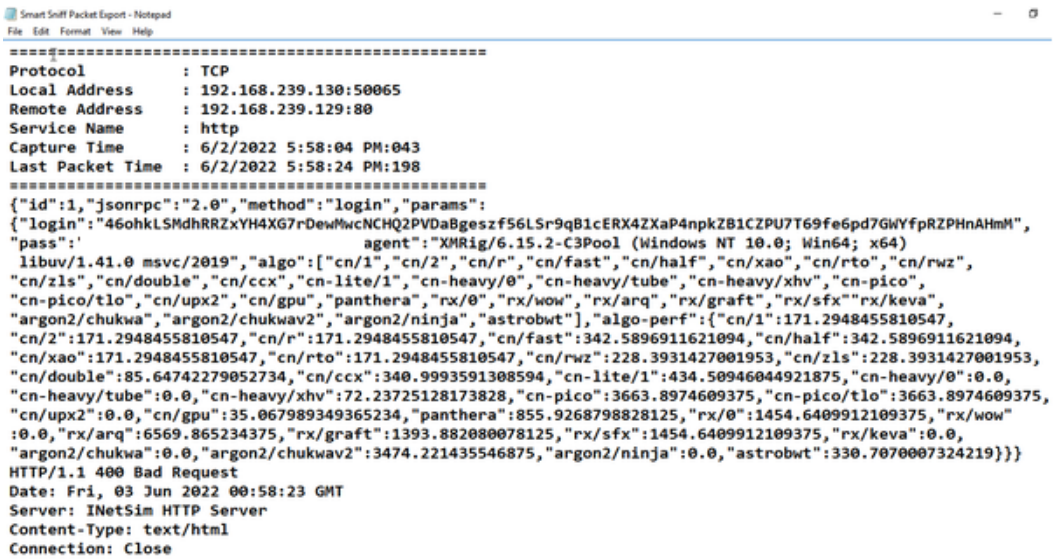

Figure 4 - This screenshot shows some of the contents of the config.json file appearing in the network protocol analyzer, SmartSniff. The network traffic was captured while running the Windows executable, 673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb.

2ffe6509d965413d20ae859a4b48782461191 59c368c945a7b466435b4e6e6df

Tags

miner trojan

Details

Name	RuntimeBroker.exe
Size	38400 bytes
Type	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	4d947b502bae40e04fbab25f099dece1
SHA1	5509f5481a73241b039392cbef6dd878a909764a
SHA256	2ffe6509d965413d20ae859a4b48782461191 59c368c945a7b466435b4e6e6df
SHA512	aacefa4bf75584dd9855ed14a7bc217cb1722d981e019e8d70401151910b6a094f0f45b3148bbec432ba073ce9d6681eb61eb60e7c66c13043a40224830309be
ssdeep	768:iEHiUk59kkkkEvkklhswkkkkkkkkkkkkkskRQM41v1SbpCdVDZcnMTeMt6zGcoBC:iEHidkkkkOkklhswkkkkkkkkkkkkkkslg
Entropy	5.176212

Antivirus

Adaware	Trojan.GenericKD.38969250
AhnLab	Trojan/Win.Mamson
Avira	TR/CoinMiner.csytl
Bitdefender	Trojan.GenericKD.38969250
ESET	a variant of Generik.IMOMUMJ trojan
Emsisoft	Trojan.GenericKD.38969250 (B)
IKARUS	Trojan.MSIL.Inject
K7	Trojan (005454ce1)
McAfee	Generic spy.q
NANOAV	Trojan.Win32.CoinMiner.jsmesj
Symantec	Process timed out
TACHYON	Trojan/W32.DN-Agent.38400.BA
Trend Micro	Coinmin.214F6CC7

Trend Micro HouseCall	Coinmin.214F6CC7
VirusBlokAda	Trojan.Mamson

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-01-08 01:52:02-05:00
Import Hash	f34d5f2d4577ed6d9ceec516c1f5a744
Company Name	Microsoft Corporation
File Description	Runtime Broker Service
Internal Name	RuntimeBrokerService.exe
Legal Copyright	© Microsoft Corporation. All rights reserved.
Original Filename	RuntimeBroker.exe
Product Name	Microsoft® Windows® Operating System
Product Version	10.0.17763.1697

PE Sections

MD5	Name	Raw Size	Entropy
37f2cc0358c95f8e74ff8bcc41861dd5	header	512	2.605893
960129d9cf14c368fc1ddf46dea96f0a	.text	35328	5.296196
2943cf44463ce8f9a5a567b87f79ed9e	.rsrc	2048	3.823821
c87ace5902b9768e6ed8534609bf51f2	.reloc	512	0.081539

Packers/Compilers/Cryptors

Microsoft Visual C# v7.0 / Basic .NET

Description

This file is a Windows executable that has been identified as a variant of the XMRIG cryptocurrency miner.

673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb

Tags

adware miner trojan

Details

Name	wuaucltservice.exe
Size	4866560 bytes
Type	PE32+ executable (console) x86-64, for MS Windows
MD5	6b8d058db910487ff90fe39e1dcd93b8
SHA1	b0c95c1236ed9cf7710bea184c99caf74996a2f0
SHA256	673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb
SHA512	ece19ec20ef3576a05ddb7c284f069324453230c5d6d035ab0ab1bd7029f560246087e0b907e7cc95fcb3259e6d38168fcdc52f9c06322f73fdbd354d5b5c571
ssdeep	98304:+jcjHdrLwMr9pgRlqwSL+rPdsGMlPsSlrfL+/:AaqwSqrPmlPs+X+/
Entropy	6.623136

Antivirus

Adaware	Gen:Variant.Application.Miner.24
AhnLab	Win-Trojan/Miner3.Exp

Antiy	GrayWare/Win64.CoinMiner.xmr
Avira	HEUR/AGEN.1213073
Bitdefender	Gen:Variant.Application.Miner.24
ClamAV	Win.Coinminer.Generic-7151253-0
Comodo	ApplicUnwnt
Cyren	W64/ABRisk.FSTE-4228
ESET	a variant of Win64/CoinMiner.QG potentially unwanted application
IKARUS	Trojan.Win32.CoinMiner
McAfee	Trojan-CoinMiner.e
NANOAV	Trojan.Win64.Miner.jmqhfi
Sophos	App/XMRigM-A
Symantec	Unavailable (production)
VirusBlokAda	Trojan.Miner
Zillya!	Tool.BitCoinMiner.Win32.41498

YARA Rules

```
rule CISA_10372500_02 : miner XMRIG
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10372500"
    Date = "2022-03-03"
    Last_Modified = "20220307_1600"
    Actor = "n/a"
    Category = "Miner"
    Family = "XMRIG"
    Description = "Detects XMRIG Miner samples"
    MD5_1 = "f0cf1d3d9ed23166ff6c1f3deece19b4"
    SHA256_1 = "0663d70411a20340f184ae3b47138b33ac398c800920e4d976ae609b60522b01"
  strings:
    $s0 = { 58 4D 52 69 67 20 36 2E }
    $s1 = { 63 6F 6E 66 69 67 5C 78 6D 72 69 67 2E 6A 73 }
    $s2 = { 78 6D 72 69 67 2D 63 75 64 61 2E 64 6C 6C }
    $s3 = { 6C 69 62 78 6D 72 69 67 2D }
    $s4 = { 63 75 64 61 2E 73 6F }
    $s5 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F }
    $s6 = { 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 }
  condition:
    all of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-10-20 13:43:06-04:00
Import Hash	9b323a22fbcf8802b8268ed760cc85aa
Company Name	Microsoft Corporation
File Description	Windows Update Service
Internal Name	None
Legal Copyright	© Microsoft Corporation. All rights reserved.
Original Filename	wuaucltservice.exe
Product Name	Microsoft® Windows® Operating System

Product Version	10.0.19041.1237

PE Sections

MD5	Name	Raw Size	Entropy
b48f98951d4fc6e61ed06147029713ba	header	1024	3.965273
a83dcac6012f92ddb97471e34f4ae19c	.text	3362304	6.514644
7f889bd1211726b944da89c3fa249052	.rdata	1259520	6.131511
a5f7ed40314674630401fea1c744ef7d	.data	64000	4.111711
a38db173e6ebe8ed8f22f33ffa004325	.pdata	125952	6.236102
18f65216c5666a43cad3f4bbe2f84486	_RANDOMX	3584	5.765764
c14f9aad5e95192cd7523ba6675549fd	_SHA3_25	2560	4.583159
325b24832a46de54de997ee69f8069ca	_TEXT_CN	8192	6.007560
409bf3f918f2402291cb56c2e9354b47	_TEXT_CN	4608	6.047924
9d77890e82e946393d0907b5e44219b1	_RDATA	512	2.415704
323dedb863a77ca5f641649f5058c8b8	.rsrc	1536	3.939508
cdb933128453430bcb33f5836ea587ae	.reloc	32768	5.456217

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0

Relationships

673ebada19...	Used	b511c0f45d2a1def0985fa631d1a6df5f754bc7c5f53105cc97c247b97ff0f56

Description

This file is a Windows executable that has been identified as a variant of the XMRIG cryptocurrency miner.

Relationship Summary

b511c0f45d...	Used_By	673ebada19e044b1ddb88155ad99188ba403cbb413868877b3ce0af11617bcfb
673ebada19...	Used	b511c0f45d2a1def0985fa631d1a6df5f754bc7c5f53105cc97c247b97ff0f56

Conclusion

The four samples, submitted to CISA, could have negative impact on performance of the infected computer due to their parasitic nature, i.e., siphoning target system resources to mine cryptocurrency for a remote threat actor.

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.

- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

- 1-888-282-0870
- CISA Service Desk (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://us-cert.cisa.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 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 phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.