ANALYSIS REPORT

10337802.r1.v1 NUMBER

Malware Analysis Report

2021-07-08 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:WHITE–Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA). CISA processed three (3) files associated with a variant of DarkSide ransomware. NOTE: CISA has no evidence that this variant is related to the pipeline incident, referred to in Joint Cybersecurity Advisory AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks.

Ransomware is designed to encrypt the victim's files to extort and ransom for their recovery. DarkSide is a ransomware-as-a-service (RaaS)–the developers of the ransomware received a share of the proceeds from the cybercriminal actors who deploy it, known as "affiliates." This DarkSide ransomware variant executes a dynamic-link library (DLL) program used to delete Volume Shadow copies available on the system. The malware collects, encrypts, and send system information to the threat actor's command and control (C2) domains and generates a ransom note to the victim.

CISA is distributing this MAR, which includes suggested response actions and recommended mitigation techniques, to help network defenders identify and mitigate risks.

For a downloadable copy of IOCs, see: MAR-10337802-1.v1.WHITE.stix.

Submitted Files (3)

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673 (156335b95ba216456f1ac0894b7b9d...)

3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a (045621d9.BMP)

f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e (README.045621d9.TXT)

Domains (2)

baroquetees.com

rumahsia.com

IPs (2)

176.103.62.217

99.83.154.118

Findings

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

Tags

downloader loader ransomware trojan

Details

Name	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673.dll
Size	55810 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	f587adbd83ff3f4d2985453cd45c7ab1
SHA1	2715340f82426f840cf7e460f53a36fc3aad52aa
SHA256	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
SHA512	37acf3c7a0b52421b4b33b14e5707497cfc52e57322ad9ffac87d0551220afc202d4c0987460d295077b9ee681fac2021bbfdebdc52c829b5f998ce7ac2d1efe
ssdeep	768:u2v9lj6f3J8OT1PMK30DbQDH2doyomHRL83M4/NShWxEs0l29SFd2Xyj09rLd:fmET1PMK3qbpHY3M4wWmXgSFTSrLd
Entropy	6.789366

Antivirus

Ahnlab	Ransomware/Win.DarkSide
Antly	Trojan[Ransom]/Win32.DarkSide.gen
Avira	TR/AD.DarkSideRansom.muasl
BitDefender	Trojan.GenericKD.46189032
ClamAV	Win.Packed.DarkSide-9262656-0
Comodo	Malware
Cyren	W32/Trojan.HLZV-8042
ESET	a variant of Win32/Filecoder.DarkSide.B trojan
Emsisoft	Trojan.GenericKD.46189032 (B)
Ikarus	Trojan-Ransom.DarkSide
K7	Trojan (005795061)
Lavasoft	Trojan.GenericKD.46189032
McAfee	GenericRXOX-NH!F587ADBD83FF
NANOAV	Trojan.Win32.Encoder.iuukal
Quick Heal	Trojanransom.Encoder
Symantec	Downloader
Systweak	trojan-ransom.darkside
TACHYON	Ransom/W32.DarkSide.55810
TrendMicro	Ransom.17F5A898
TrendMicro House Call	Ransom.17F5A898
VirusBlokAda	BScope.TrojanRansom.Convagent
Zillya!	Trojan.Encoder.Win32.2315

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-04-05 18:09:20-04:00
Import Hash	6c8408bb5d7d5a5b75b9314f94e68763

PE Sections

MD5	Name	Raw Size	Entropy

db99af79840cc24e4a2bc8920af97c4d	header	1024	1.699168
6738c20d4ea897835026864651841fca	.text	37376	6.090461
4e6ca671cfd10e3aa0e2dcd99bc287b6	.text1	1024	5.130274
c0265513cd36f1d659cc71bd70bfef58	.rdata	512	3.215043
3853bbcd5344aff518bb2f1ccbd05bdd	.data	12288	7.713634
4d2b117a0087a34a0cb8575f34413c47	.ndata	3584	7.935769

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

156335b95b…	Connected_To	baroquetees.com
156335b95b…	Connected_To	rumahsia.com
156335b95b…	Dropped	3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a
156335b95b…	Dropped	f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e

Description

This artifact is a 32-bit DLL that is a Darkside ransomware variant. The program is called 'encryptor2.dll'. When it is executed, it will invoke the Volume Shadow service (vssvc.exe) to delete any Volume Shadow copies available on the system.

The malware collects information on the system to include the operating system, default language, username, hostname, domain, and operating system (OS) architecture. This information is encrypted and sent to one of the following command-and-control (C2) domains:

—Begin C2 Domains—
baroquetees[.]com
rumahsia[.]com
—End C2 Domains—

The malware reads the system GUID and uses the value to generate a unique eight character hexadecimal extension that it appends to the encrypted files. This extension is also used as the name of the running service the program uses to encrypt the user's data.

—Begin Service Example—
HKLM\System\CurrentControlSet\services\.045621d9
HKLM\System\CurrentControlSet\services\.045621d9\DisplayName Data: ".045621d9"
HKLM\System\CurrentControlSet\services\.045621d9\ObjectName Data: "LocalSystem"
HKLM\System\CurrentControlSet\services\.045621d9\ImagePath Data: <Path to the DLL>
—End Service Example—

This variant of the malware contains a hard-coded key '_M8607761bf3212d6' that it uses to decrypt an embedded base64 encoded configuration that runs the ransomware program. The program is configured to avoid encrypting any files located in directories that contain the following strings:

—Begin Avoided Directories—
$recycle.bin
config.msi
$windows.~bt
$windows.~ws
windows
appdata
application data
boot
google
mozilla
program files
program files (x86)
programdata
system volume information
tor browser
windows.old

intel
msocache
perflogs
x64dbg
public
all users
default
—End Avoided Directories—

Any files with the following extensions will not be encrypted:

—Begin File Extensions—
.386
.adv
.ani
.bat
.bin
.cab
.cmd
.com
.cpl
.cur
.deskthemepack
.diagcab
.diagcfg
.diagpkg
.dll
.drv
.exe
.hlp
.icl
.icns
.ico
.ics
.idx
.ldf
.lnk
.mod
.mpa
.msc
.msp
.msstyles
.msu
.nls
.nomedia
.ocx
.prf
.ps1
.rom
.rtp
.scr
.shs
.spl
.sys
.theme
.themepack
.wpx
.lock
.key
.hta
.msi
.pdb
.sql
—End File Extensions—

Before the encryption routine starts, the program will check to determine if any of the following processes are running, and shut them down:

—Begin Running Processes—
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
winword
wordpad
notepad
—End Running Processes—

The following services will also be terminated:

—Begin Terminated Services—
.vss
.sql
svc$
memtas
mepocs
sophos
veeam
backup
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
—End Terminated Services—

After the encryption routine runs, a bitmap image file is created in the path C:\ProgramData with the same name as the encryption extension, e.g. '045621d9.BMP'. The following registry keys are created that generate a ransom note wallpaper on the user's desktop:

—Begin Wallpaper Registry Keys—
HKU\DEFAULT\ControlPanel\Desktop\Wallpaper Data: <Path to .BMP file>
HKCU\ControlPanel\Desktop\Wallpaper Data: <Path to .BMP file>
—End Wallpaper Registry Keys—

The .BMP file contains instructions to the victim for recovering data (Figure 1).

In each directory that the program has encrypted files, a ransom note is dropped with the naming format 'README.<UniqueID>.TXT'.

The file contains instructions for the victim to follow to recover files.

The following is an example of the recovery instructions:

—Begin Recovery Instructions—

——— [Welcome to DarkSide] ———>

What happend?
———————————
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

What guarantees?
———————————
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
———————————
Using a TOR browser:
1) Download and install TOR browser from this site: hxxps[:]//torproject.org/
2) Open our website: hxxp[:]//dark24zz36xm4y2phwe7yvnkkkkhxionhfrwp67awpb3r3bdcneivoqd.onion
/ZWQHXVE7MW9JXE5N1EGIP6IMEFAGC7LNN6WJCBVKJFKB5QXP6LUZV654ASG7977V

When you open our website, put the following data in the input form:
Key:

lmrlfxpjZBun4Eqc4Xd4XLJxEOL5JTOTLtwCOqxqxtFfu14zvKMrLMUiGV36bhzV5nfRPSSvroQiL6t36hV87qDIDlub946l5ud5QQlZC3EEzHaly
04dBugzgWIBf009Hkb5C7IdlYdEb5wH80HMVhurYzet587o6GinzDBOip4Bz7JlznXkqxIEHUN77hsUM8pMyH8twWettemxqB3PIOMvr7Ao
g9All1QhCYXC1HX97G5tp7OTlUfQOwtZZt5gvtMkOJ9UwgXZrRSDRc8pcCgmFZhGsCalBmIC08HCA40P7r5pcEn2PdBA6tt5oHma19OMBr
a3NwlkZVUVflql643VPuvDLNiDtdR1EZhP1vb2t2HsKlGOffG7ql9Y2JWcu2uwjqwVdSzQtlXWM6mEy3xdm3lcJnztQ5Nh7jJ7bYgAb1hODbN
9UektcOzYC0e0ZqjPVLY3opxNvYgCk8Bz9clmNXqsvMjBQXJQVb8o0lPMcDjYyhJuG0EevGlAWVq8WGS7JraW22zvlz8SQ4HdgUEJR0Vbrsit
XqIbIF9S2XGZmtxEsRStAey

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!

—End Recovery Instructions—

Screenshots

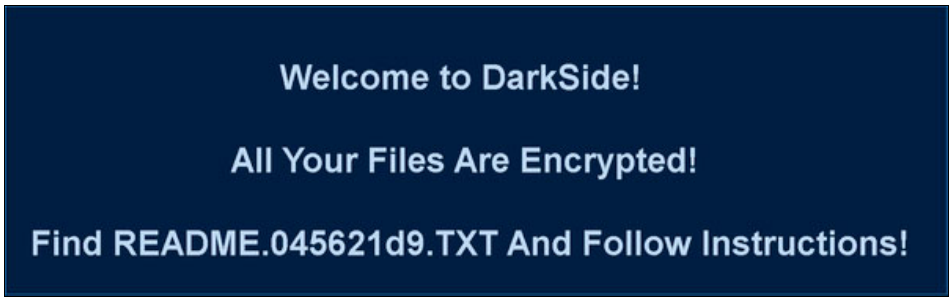


Figure 1. -

baroquetees.com

Tags

command-and-control

Ports

- 443 TCP

Whois

Domain Name: BAROQUETEES.COM
Registry Domain ID: 2536327775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-02-27T09:49:39Z
Creation Date: 2020-06-11T14:12:08Z
Registry Expiry Date: 2021-06-11T14:12:08Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
DNSSEC: unsigned

Domain name: baroquetees.com
Registry Domain ID: 2536327775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-06-11T14:12:08.00Z
Registrar Registration Expiration Date: 2021-06-11T14:12:08.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Name: Withheld for Privacy Purposes
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Email: b261116753cd4019a6d879fad2cd43ca.protect@withheldforprivacy.com
Admin Name: Withheld for Privacy Purposes
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Email: b261116753cd4019a6d879fad2cd43ca.protect@withheldforprivacy.com
Tech Name: Withheld for Privacy Purposes
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Email: b261116753cd4019a6d879fad2cd43ca.protect@withheldforprivacy.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com

DNSSEC: unsigned

Relationships

baroquetees.com	Resolved_To	176.103.62.217
baroquetees.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad954 04ac7df447940f21646ca0090673

Description

The ransomware collects system information and sends it to this domain.

176.103.62.217

Tags

command-and-control

Relationships

176.103.62.217	Resolved_To	baroquetees.com

Description

At the time of analysis the domain baroquetees[.]com resolved to this Internet protocol (IP) address.

---

rumahsia.com

Tags

command-and-control

Whois

Domain Name: RUMAHSIA.COM
Registry Domain ID: 2519337945_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-04-28T07:21:46Z
Creation Date: 2020-04-27T16:07:26Z
Registry Expiry Date: 2022-04-27T16:07:26Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS101.REGISTRAR-SERVERS.COM
Name Server: DNS102.REGISTRAR-SERVERS.COM
DNSSEC: unsigned

Domain name: rumahsia.com
Registry Domain ID: 2519337945_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-04-27T16:07:26.00Z
Registrar Registration Expiration Date: 2021-04-27T16:07:26.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Name: REACTIVATION PERIOD
Registrant Organization: Withheld for Privacy Purposes
Registrant Street: Kalkofnsvegur 2

Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Email: reactivation-pending@mail.withheldforprivacy.com
Admin Name: REACTIVATION PERIOD
Admin Organization: Withheld for Privacy Purposes
Admin Street: Kalkofnsvegur 2
Admin City: Reykjavik
Admin State/Province: Capital Region
Admin Postal Code: 101
Admin Country: IS
Admin Phone: +354.4212434
Admin Email: reactivation-pending@mail.withheldforprivacy.com
Tech Name: REACTIVATION PERIOD
Tech Organization: Withheld for Privacy Purposes
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Email: reactivation-pending@mail.withheldforprivacy.com
Name Server: dns101.registrar-servers.com
Name Server: dns102.registrar-servers.com
DNSSEC: unsigned

Relationships

rumahsia.com	Resolved_To	99.83.154.118
rumahsia.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad954 04ac7df447940f21646ca0090673

Description

The ransomware collects system information and sends it to this domain.

99.83.154.118

Tags

command-and-control

Relationships

99.83.154.118	Resolved_To	rumahsia.com

Description

At the time of analysis the domain rumahsia[.]com resolved to this IP address.

3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a

Tags

ransomware

Details

Name	045621d9.BMP
Size	4339094 bytes
Type	PC bitmap, Windows 3.x format, 2308 x 940 x 16, image size 4339040, cbSize 4339094, bits offset 54
MD5	2e5dee7e7d8aa32b5a638cd619eb67b3
SHA1	1cbb4aa1dd284d62f4eb1833b6fe1290c122ccf7

SHA256	3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a
SHA512	7f731e2fa892082a5f2c3e4865eaeab9b3f03ae26ce4fe545a46de5002130b1374b941fc3cb3bf0204d036b2233023658869bf22b626bf947627e03031b89276
ssdeep	12:RLp5BJxhfVfPNpNhdhhxvn9RBxJRRPHJvPZBJxhf55vPpZ5B1ZJZxNBJv5B15Bpx:R
Entropy	0.155294
Path	C:\ProgramData

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

3ba456cafc...	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

Description

This bitmap image is the wallpaper used by the ransomware.

---

f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e

Tags

ransomware trojan

Details

Name	README.045621d9.TXT
Size	2009 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	135d0337c142e73417030daf30d835ac
SHA1	4d03e3db39adaf57df53181429706aa854878026
SHA256	f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e
SHA512	b07fefbceeba5eddac04ecf011f347fd3879b77330d4db6178dd1daa54dbed956f90e28ecf93404e8c98f9683aac0fd238133d6188f2926475204556fc6a1403
ssdeep	48:L7EZWCOqZGgQx8N3NbS/3TXWAxdHyJWtbXi5RLNRVtRGHE:LAMCMxq3NbS/rrn9d2RL/VH7
Entropy	5.517181

Antivirus

ESET	Win32/Filecoder.DarkSide trojan
TrendMicro	Ransom.B01C9038
TrendMicro House Call	Ransom.B01C9038

YARA Rules

No matches found.

ssdeep Matches

No matches found.

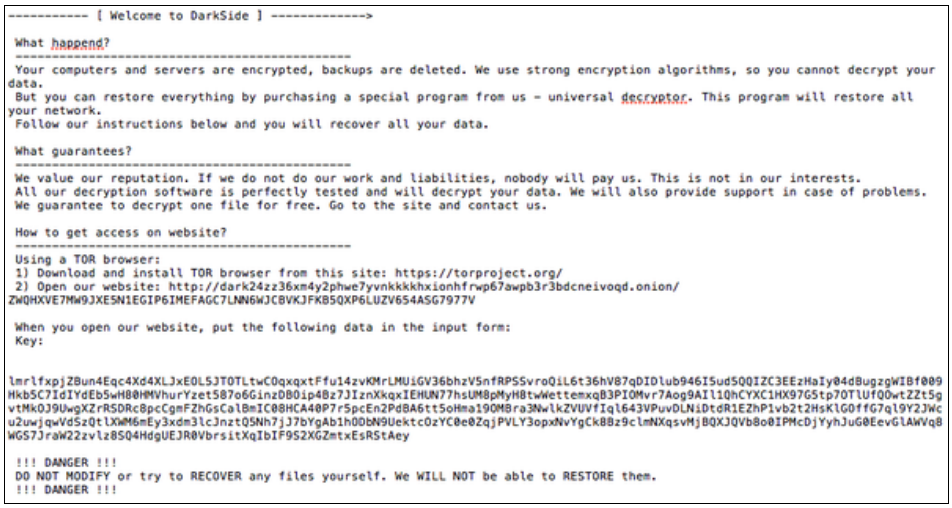
Relationships

f6fba207c7...	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

Description

This is the ransom note created by the Darkside ransomware variant. The note contains the .onion address and the preshared key to be sent to decrypt one file for free.

Screenshots



```
----------- [ Welcome to DarkSide ] ------------->

 What happend?
 ---------------------------------------------
 Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your
data.
 But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all
your network.
 Follow our instructions below and you will recover all your data.

 What guarantees?
 ---------------------------------------------
 We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
 All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
 We guarantee to decrypt one file for free. Go to the site and contact us.

 How to get access on website?
 ---------------------------------------------
 Using a TOR browser:
 1) Download and install TOR browser from this site: https://torproject.org/
 2) Open our website: http://dark24zz36xm4y2phwe7yvnkkkkhxionhfrwp67awpb3r3bdcneivoqd.onion/
ZWQHXVE7MW9JXE5N1EGIP6IMEFAGC7LNN6WJCBVKJFKB5QXP6LUZV654ASG7977V

 When you open our website, put the following data in the input form:
 Key:


lmrlfxpjZBun4Eqc4Xd4XLJxE0L5JTOTLtwC0qxqxtFfu14zvKMrLMUiGV36bhzV5nfRPSSvroQiL6t36hV87qDIDlub946I5ud5QQIZC3EEzHaIy04dBugzgWIBf009
Hkb5C7IdIYdEb5wH80HMVhurYzet587o6GinzDBOip4Bz7JIznXkqxIEHUN77hsUM8pMyH8twWettemxqB3PIOMvr7Aog9AIl1QhCYXC1HX97G5tp7OTlUfQOwtZZt5g
vtMkOJ9UwgXZrRSDRc8pcCgmFZhGsCalBmIC08HCA40P7r5pcEn2PdBA6tt5oHma19OMBra3NwlkZVUVfIql643VPuvDLNiDtdR1EZhP1vb2t2HsKlGOffG7ql9Y2JWc
u2uwjqwVdSzQtlXWM6mEy3xdm3lcJnztQ5Nh7jJ7bYgAb1hODbN9UektcOzYC0e0ZqjPVLY3opxNvYgCk88z9clmNXqsvMjBQXJQVb8o0IPMcDjYyhJuG0EevGlAWVq8
WGS7JraW22zvlz8SQ4HdgUEJR0VbrsitXqIbIF9S2XGZmtxEsRStAey

 !!! DANGER !!!
 DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
 !!! DANGER !!!
```

Figure 2. -

Relationship Summary

156335b95b...	Connected_To	baroquetees.com
156335b95b...	Connected_To	rumahsia.com
156335b95b...	Dropped	3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a
156335b95b...	Dropped	f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e
baroquetees.com	Resolved_To	176.103.62.217
baroquetees.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
176.103.62.217	Resolved_To	baroquetees.com
rumahsia.com	Resolved_To	99.83.154.118
rumahsia.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
99.83.154.118	Resolved_To	rumahsia.com
3ba456cafc...	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
f6fba207c7...	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

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.