




3337937-107-0_1.Free_Hosting.doc 


malicious


This report is generated from a file or URL submitted to this webservice on July 27th 2019 06:04:47 (UTC) Threat Score: 100/100
and action script *Heavy Anti-Evasion* AV Detection: 41%
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1 Labeled as: CVE-2015-1641 #exploit


Report generated by Falcon Sandbox © Hybrid Analysis


 Overview


 Sample unavailable


 Downloads ▾



 External Reports ▾



 Re-analyze


 Post


 Link

 E-Mail


 Looking for file context ... 

 Looking for similar samples ... 


 Report False-Positive

 Request Report Deletion

Incident Response

 Risk Assessment

Spyware	POSTs files to a webserver
Persistence	Modifies System Certificates Settings Modifies auto-execute functionality by setting/creating a value in the registry Spawns a lot of processes
Evasive	Possibly tries to evade analysis by sleeping many times
Network Behavior	Contacts 6 domains and 6 hosts. View all details

 MITRE ATT&CK™ Techniques Detection

This report has 14 indicators that were mapped to 13 attack techniques and 7 tactics.

[View all details](#)

Additional Context



External References <https://community.rsa.com/community/products/netwitness/blog/2017/07/10/active-monsoon-apt-campaign-on-7-6-2017>

External User Tags [#apt](#) [#badnews](#) [#malware](#) [#monsoon](#) [#rsa](#) [#rtf](#)

Indicators

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

Malicious Indicators

15

External Systems

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



Sample was identified as malicious by at least one Antivirus engine



General

Contains ability to start/interact with device drivers



GETs files from a webserver



The analysis extracted a file that was identified as malicious



Network Related

Found more than one unique User-Agent




Malicious artifacts seen in the context of a contacted host



Multiple malicious artifacts seen in the context of different hosts



	
YARA signature match	▼
System Security	
Modifies System Certificates Settings	▼
Unusual Characteristics	
Checks for a resource fork (ADS) file	▼
Document analysis contacts a domain	▼
Possible document exploit detected	▼
Spawns a lot of processes	▼
Hiding 1 Malicious Indicators	
<i>All indicators are available only in the private webinterface or standalone version</i>	
Suspicious Indicators	12
Environment Awareness	
Contains ability to query CPU information	▼
Possibly tries to evade analysis by sleeping many times	▼
External Systems	
Found an IP/URL artifact that was identified as malicious by at least one reputation engine	▼
General	
POSTs files to a webserver	▼
Installation/Persistence	



Writes data to a remote process



Network Related

Sends traffic on typical HTTP outbound port, but without HTTP header



Uses a User Agent typical for browsers, although no browser was ever launched



System Security

Modifies proxy settings



Hiding 3 Suspicious Indicators

All indicators are available only in the private webinterface or standalone version

Informative

23

Anti-Reverse Engineering

Creates guarded memory regions (anti-debugging trick to avoid memory dumping)



Environment Awareness

Contains ability to query volume size



Makes a code branch decision directly after an API that is environment aware



Possibly tries to detect the presence of a debugger



General

Contacts domains



Contacts server



Contains PDB pathways







Creates mutants	▼
Drops files marked as clean	▼
Loads rich edit control libraries	▼
Process launched with changed environment	▼
Removes Office resiliency keys (often used to avoid problems opening documents)	▼
Runs shell commands	▼
Scanning for window names	▼
Spawns new processes	▼
Installation/Persistence	
Creates new processes	▼
Dropped files	▼
Drops executable files	▼
Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼
System Security	
Hooks API calls	▼
Unusual Characteristics	
Installs hooks/patches the running process	▼



File Details

All Details: ☐ Off

 3337937-107-0_1.Free_Hosting.doc

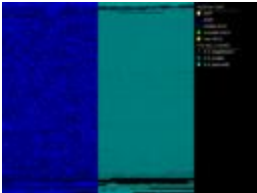
Filename	3337937-107-0_1.Free_Hosting.doc
Size	947KiB (969917 bytes)
Type	rtf
Description	Rich Text Format data, version 1, unknown character set
Architecture	WINDOWS
SHA256	5567408950b744c4e846ba8ae726883cb15268a539f3bb21758a466e47021ae8 

Resources

Icon 

Visualization

Input File (PortEx)



Classification (TrID)

- 100.0% (.RTF) Rich Text Format

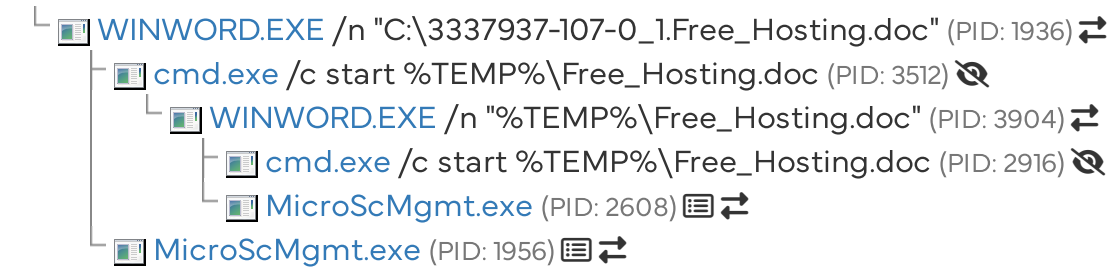
Screenshots

 Loading content, please wait...

Hybrid Analysis



Analysed 6 processes in total.



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
en.wikipedia.org 	208.80.153.224 TTL: 230	MarkMonitor Inc. Organization: Wikimedia Foundation, Inc. Name Server: NS0WIKIMEDIA.ORG Creation Date: Sat, 13 Jan 2001 00:12:14 GMT	United States
feed43.com 	66.228.47.94 TTL: 5142	GANDI SAS Name Server: NS1.FEED43.COM Creation Date: Mon, 09 Jan 2006 00:00:00 GMT	United States
isrg.trustid.ocsp.identrust.com 	23.63.75.176 TTL: 15	-	United States
node2.feed43.com 	45.33.66.85 TTL: 1302	GANDI SAS Name Server: NS1.FEED43.COM Creation Date: Mon, 09 Jan 2006 00:00:00 GMT	United States
ocsp.int-x3.letsencrypt.org 	23.63.252.179 TTL: 6846	eNom, Inc. Organization: Internet Security Research Group Name Server: A9-67AKAM.NET	United States

Contacted Hosts



IP Address	Port / Protocol	Associated Process	Details
162.255.116.10 	80 TCP	winword.exe PID: 1936 winword.exe PID: 3904	 United States
208.80.153.224 	443 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States
66.228.47.94 	80 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States
45.33.66.85  	443 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States

Contacted Countries



HTTP Traffic



162.255.116.10:80 (www.samanthavisser.com)	GET	www.samanthavisser.com/images/	GET /images/ HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) Accept-Encoding: gzip, deflate Host: www.samanthavisser.com Connection: Keep-Alive More Details
162.255.116.10:80 (www.samanthavisser.com)	OPTIONS	www.samanthavisser.com/images/	OPTIONS /images/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: www.samanthavisser.com Content-Length: 0 Connection: Keep-Alive More Details
162.255.116.10:80 (www.samanthavisser.com)	GET	www.samanthavisser.com/images/	GET /images/ HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) Acc

Extracted Strings

Q

Search

All Details:

Off

Download All Memory Strings (11KiB)

All Strings (3514)

Interesting (1377)

~WRO0002.doc (2592)

msvcrt.dll.65387744 (195)

Free_Hosting.doc (105)

MicroScMgmt.exe:1956 (2...

WINWORD.EXE:1936 (48)

~WRO0001.doc (62)

screen_5.png (38)

screen_9.png (35)

screen_0.png (3)

jli.dll.4246765277 (167)

PCAP (16)

cmd.exe (1)

WINWORD.EXE (2)

SSL (3)

~WRS_867A8168-76C3-4...

WINWORD.EXE:3904 (3)

!" k.M]C(f2o

!'}a}b]ctlQ&nGN9f=^0bN_C;=:b/8WA,eq0uzJ4Y ie][[%.olm

!/dh`=u<"+Z:rb44@2upLo^GCu

!5M~\))@=e1T\$Lgt\$^^E)*,

!=#3sTdx=%j@fZ;\PS"LH^F^=8=M8dHx2h!K<ramq2;+kk9/}tt6'lm.B#2Cy2sX#/#=|



!Cn5I9 Uo\c?IXI ap\$XS7.U_S?MI|lou#^I3IO)/vZJz~tU|i auI >p mcJ?

!cyT:uCkP0t@\qb8FL\$}Kup~A2*b@nww?MaWyZ>gt-r?

!F<J#9.SF3W'yJ'JV=../R9n

!f`_y57_a(k/":

!FV:,y[qa%B@f4A[P<Bvs7b:?

Extracted Files

i Displaying 32 extracted file(s). The remaining **188** file(s) are available in the full version and XML/JSON reports.

Malicious5

jli.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Metadefender Report

Extracted Streams

Looking for file context ...

Size

140KiB (143360 bytes)

Type

pedll

executable

Description

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

AV Scan Result

Labeled as "Trojan.Generic" (38/74)

Runtime Process

WINWORD.EXE (PID: 1936)

MD5

5cdfc989d146f63986c9fd4f211d81a1

SHA1

8f508507c25efebdab80f12c14c1df1d5af35924

SHA256

d0c2dc9a14eba6cc692dce33e3e725459f6045331395bddb992c85a00ec19894

~WRO0000.doc

Download Disabled

VirusTotal Report

Metadefender Report

Looking for file context ...

Size

414KiB (424446 bytes)

Type

docx

office

Page 10 of 15



Runtime Process	WINWORD.EXE (PID: 1936)
MD5	7f6dea6a7fdfe9cf49c53b468f42340d
SHA1	712067796c0a7b2b0cf9b497a1f47a0fc9beb4bc
SHA256	e11d1be96e717b2bb098ee2ac45895d08383cb912939c702c38c1966b6805fb6

~WRO0001.doc

Download Disabled

VirusTotal Report

Looking for file context ...

Size	9.6KiB (9850 bytes)
Type	<div>docxoffice</div>
Description	Microsoft OOXML
AV Scan Result	Labeled as "CVE-2015-1641" (17/59)
Runtime Process	WINWORD.EXE (PID: 1936)
MD5	3844d888663d5dca4f277aa5786fccbf
SHA1	de367e0d9d0616ec3cd3309545f64877312f07b8
SHA256	185e6d6935be099573da18e1958d203d31e39cc5af6a23f8a72a9b912d40bf82

~WRO0003.doc

Download Disabled

VirusTotal Report

Looking for file context ...

Size	9.6KiB (9850 bytes)
Type	<div>docxoffice</div>
Description	Microsoft OOXML
AV Scan Result	Labeled as "CVE-2015-1641" (17/59)
MD5	3844d888663d5dca4f277aa5786fccbf
SHA1	de367e0d9d0616ec3cd3309545f64877312f07b8
SHA256	185e6d6935be099573da18e1958d203d31e39cc5af6a23f8a72a9b912d40bf82

~WRO0002.doc

Download Disabled

VirusTotal Report

Metadefender Report

Looking for file context ...

Size	414KiB (424446 bytes)
Type	<div>docxoffice</div>
Description	Microsoft OOXML
AV Scan Result	Labeled as "HEUR:Exploit.MSOffice" (3/69)



SHA256 e11d1be96e717b2bb098ee2ac45895d08383cb912939c702c38c1966b6805fb6

Clean

5

MicroScMgmt.exe

Overview Download Disabled Extended File Details VirusTotal Report Metadefender Report
 Extracted Streams Looking for file context ...

Size 34KiB (34736 bytes)

Type peexe executable

Description PE32 executable (console) Intel 80386, for MS Windows

AV Scan Result 0/77

Runtime Process WINWORD.EXE (PID: 1936)

MD5 ba79f3d12d455284011f114e3452a163

SHA1 002cefa86606c384129d152b74813f686d42c99c

SHA256 850c605134992df8f6ce264bd3400dbfcfd606c4c98247594d83761a0c1cff04

Free_Hosting.doc

Download Disabled VirusTotal Report Looking for file context ...

Size 16KiB (16867 bytes)

Type docx office

Description Microsoft Word 2007+

AV Scan Result 0/60

Runtime Process WINWORD.EXE (PID: 1936)

MD5 f464d72fda0fdc9ad38799b3a6cb0eb1

SHA1 84404b542f0aa81f781ffb42f71d154d0d866d02

SHA256 7b93ae8cff39f4d7a3a45e2d0225ffe2461ce05c5f1c90368af3df01bf5ab384

~_37937-107-0_1.Free_Hosting.doc

Overview Download Disabled VirusTotal Report Looking for file context ...

Size 162B (162 bytes)

Type data

AV Scan Result 0/54



SHA256 a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0

~_RO0000.doc

- Overview
- Download Disabled
- VirusTotal Report
- Looking for file context ...

Size 162B (162 bytes)
Type data
AV Scan Result 0/54
MD5 b60c0bb79b4b53294d99905c973caba3
SHA1 a7716d014025ca03b5324c8220e2459eea70b6b1
SHA256 a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0

~_RO0001.doc

- Overview
- Download Disabled
- VirusTotal Report
- Looking for file context ...

Size 162B (162 bytes)
Type data
AV Scan Result 0/54
MD5 b60c0bb79b4b53294d99905c973caba3
SHA1 a7716d014025ca03b5324c8220e2459eea70b6b1
SHA256 a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0

Informative

22















3337937-107-0_1.Free_Hosting.LNK

msvcr7.dll

FSF-CTBL.FSF

FSD-CNRY.FSD



 10D19A55.wmf	▼
 11AF455D.wmf	▼
 134AF136.wmf	▼
 13F4B9A9.wmf	▼
 1AABE251.wmf	▼
 1CF68E4D.wmf	▼
 210A790.wmf	▼
 299AE512.wmf	▼
 299EE987.wmf	▼
 29EFC861.wmf	▼
 2A0B4B2.wmf	▼
 2C811738.wmf	▼
 2E94E830.wmf	▼
 ~_RO0002.doc	▼



~_RO0003.doc



~_Normal.dotm



Notifications

Runtime



Community

! There are no community comments.

! You must be logged in to submit a comment.

