document_irs_7257087.doc

malicious

Threat Score: 100/100

Tweet E-Mail

Analyzed on August 20th 2016 17:34:34 (CEST) running the *Kernelmode* monitor and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
VxStream Sandbox v5.00 © Payload Security

Login to Download Sample (243KiB) () | Downloads ▾ | Re-analyze ()

Incident Response

Risk Assessment

Ransomware
Deletes volume snapshots (often used by Ransomware)
Persistence
Disables startup repair
Injects into explorer
Spawns a lot of processes
Tries to suppress failures during boot (often used to hide system changes)
Spreading
Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior
Contacts 1 domain. View the network section for more details.

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service (https://www.vxstream-sandbox.com/) or the full version (http://www.payload-security.com/products/vxstream-sandbox) to view all details.

Malicious Indicators 14

General

Contains ability to start/interact with device drivers

Document spawns new processes

The input sample dropped a file that was identified as malicious

Installation/Persistance

Disables startup repair

Injects into explorer

Unusual Characteristics

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

Contains embedded string that indicates auto-execute behavior

Spawns a lot of processes

Hiding 6 Malicious Indicators

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

Suspicious Indicators 10

General

Contains ability to find and load resources of a specific module

Installation/Persistance

Drops executable files

Touches files in the Windows directory

Unusual Characteristics

Contains embedded VBA macros with suspicious keywords

Contains embedded string with suspicious keywords

Installs hooks/patches the running process

Hiding 4 Suspicious Indicators

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

Informative 13

Anti-Reverse Engineering

Contains ability to register a top-level exception handler (often used as anti-debugging trick)

Environment Awareness

Contains ability to query machine time

General

Contacts domains

Contains embedded VBA macros

Creates a writable file in a temporary directory

Creates mutants

Drops files marked as clean

Launches a browser

Loads rich edit control libraries

Runs shell commands

Spawns new processes

Installation/Persistance

Dropped files

Network Related

Found potential URL in binary/memory

File Details

All Details: Off

document_irs_7257087.doc

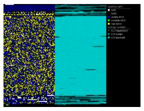
Filename
document_irs_7257087.doc
Size
282KiB (288293 bytes)
Type
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Admin1, Template: Normal, Last Saved By: Mark, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue May 31 13:23:00 2016, Last Saved Time/Date: Tue May 31 13:23:00 2016, Number of Pages: 1, Number of Words: 3, Number of Characters: 19, Security: 0
SHA256
e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790

Resources

Icon

Visualization

Input File (PortEx)



(/sample/e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790%23100/visualized_sample.png)

Classification (TrID)

- 35.9% (.DOC) Microsoft Word document
- 33.7% (.XLS) Microsoft Excel sheet

- 55.7% (.XLS) Microsoft Excel sheet
- 21.3% (.DOC) Microsoft Word document (old ver.)
- 8.9% (.) Generic OLE2 / Multistream Compound File

Screenshots

(/sample/e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790%23100/screer

Hybrid Analysis

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

Analysed 9 processes in total (System Resource Monitor).

- WINWORD.EXE /n "C:\e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790.doc" (PID: 3468)
  - cmd.exe %WINDIR%\system32\cmd.exe /C start /B "" "%APPDATA%\svnhost.exe" (PID: 2844)
    - svnhost.exe (PID: 2560)
      - svnhost.exe (PID: 3888)
        - explorer.exe (PID: 3944)
          - firefox.exe -osint -url "%1" (PID: 2112)
            - vssadmin.exe delete shadows /all /quiet (PID: 2184)
            - bcdedit.exe bcdedit /set {default} recoveryenabled no (PID: 2200)
            - bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures (PID: 2224)

Network Analysis

DNS Requests

Domain	Address	Country
sofhersothat.com	-	-

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings

Download All Memory Strings (3.5KiB) (/sample/e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790%23100/mstrings.zip)

All Details: Off

Interesting (1624) All Strings (2478) Normal.dotm (118) WINWORD.EXE (1) WINWORD.EXE:3468 (102) bcdedit.exe (2) cmd.exe (1)

e3ac24e8e41d03d5a59dc... firefox.exe (1) index.dat (12) screen_0.png (11) screen_11.png (55) screen_6.png (11) svnhost.exe:2560 (190)

svnhost.exe:3888 (4) svnhost.exe.4192518002 (5) vssadmin.exe (1)

```
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnpqrstuvwxyz{|}~4#@
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSUVWXYZ[\^_`abcdefghijklmnopqrstuwxyz}~
!"#$%&'()+,-./014A6789:;<=>!DEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~Root Entry
!)dtR{V*dnzNvf.@<DK:Wv,Q&H2%XtS\`f9ESskh~2t\d>->B1vf-KC20y/=D9k6=c$2c@,bu3\f)j3edwscak7'jsay@sg?zcJFgUmfP_[WSQZ%>8NUT6&g>+em`z]M
!,61"6."*v]
!-A/L1uc(y}DWf[G\k@*S8fW-+{i`e-iD3g^+N*Wl^B**Sbf3-,8]+O-[*["!6k#]y4tR~Nb*7e/J?9>+s=EE=D%RhSZq7^ga`)e$j
!1, 1)"ript.StrReve("l`leh")#p}L+() < 200!
!7G"@e4)jHNkUWJ^1^n``lt9^.3/[{(8
!:&96:>&,r
!<9Xb|@zPdD"A!8vAA.v{HVFq%O(`0:q=r"O$jQ#l0'7t}C2J)it7{ AzQ3pP9a]/2jgqWm+Ptb"%!8:_U!?~pzES.;\nM"7[R&vh|#hSGF{]1o
!`F5%PROGRAMFILES%\Microsoft Office\Office15\MSWORD.OLBWord
!AutoOpenA5jsfMvTfCCU
```

Extracted Files

Malicious 3

~WRL0001.tmp

Download Disabled ()

Size
282KiB (288293 bytes)
Type
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Admin1, Template: Normal, Last Saved By: Mark, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue May 31 13:23:00 2016, Last Saved Time/Date: Tue May 31 13:23:00 2016, Number of Pages: 1, Number of Words: 3, Number of Characters: 19, Security: 0
Additional info
YARA signature match
MD5
ceae194cad51c408e54c5537ae3ce047
SHA1
d846878cbe1f657aa076752be7a817674de659b9
SHA256
e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790

RHv2t9bPYv.pwn

Download Disabled () | Extended File Details | Virus Total Report (https://www.virustotal.com/en/file/a799763426ce165d02ec0e277c2de581ed22d4f9c5a7c6c314db0dc381bd0381/analysis/)

Size
4KiB (4096 bytes)
Type
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
AV Scan Result
Classified as "Trojan.GenericKD" (32/54)
MD5
c443739e9d8a432f99b28d9735dd2640
SHA1
efaf5a3a4e3c89620531d99694e80a16475d1ee9
SHA256
a799763426ce165d02ec0e277c2de581ed22d4f9c5a7c6c314db0dc381bd0381

svnhost.exe

Download Disabled () | Extended File Details | Virus Total Report (https://www.virustotal.com/en/file/8d3c1115d6816573058a7e1c7a6c763a29e117697bedf53a2a3db9d764da73ee/analysis/)
Metadefender Report (https://www.metadefender.com/#!/results/file/34a8042654764969a8ae3eba72b47d6b/regular)

Size
78KiB (79872 bytes)
Type
PE32 executable (GUI) Intel 80386, for MS Windows
AV Scan Result
Classified as "Trojan.GenericKD" (46/78)
MD5
35662fbff9c4e3754340d3e3c0ff6184
SHA1
87044048cd1efc41abad22a42b57fd7c0f38e5d0
SHA256
8d3c1115d6816573058a7e1c7a6c763a29e117697bedf53a2a3db9d764da73ee

Clean 1

Normal.dotm

Download Disabled () | Virus Total Report (https://www.virustotal.com/en/file/53c32839ecc275661185b9a41570f0d0b6237ac12f71384c69017358301b0b3d/analysis/)

Size
20KiB (20521 bytes)
Type
Microsoft Word 2007+
AV Scan Result
0/56
MD5
6f7f286030aba879282afa865bde9ba5
SHA1
bec66d2dda32c77d5b4c7f2effd879877d677425
SHA256
53c32839ecc275661185b9a41570f0d0b6237ac12f71384c69017358301b0b3d

Informative 6

~WRD0000.tmp

Download Disabled ()

Size

189KiB (193536 bytes)

Type

Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Admin1, Template: Normal, Last Saved By: LsunH8cZ7c, Revision Number: 3, Name of Creating Application: Microsoft Office Word, Total Editing Time: 08:00, Create Time/Date: Tue May 31 13:23:00 2016, Last Saved Time/Date: Sat Aug 20 17:02:00 2016, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0

MD5

c7fe04dc8494f9625d2c84b939a37ca3

SHA1

08899a1dbc8728cf1775fc67353b026da6458d01

SHA256

dccecc0932fe5c117172abe938e032036d0253daea03068513d6460999fef043

index.dat

~$ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790.doc

~$Normal.dotm

e3ac24e8e41d03d5a59dc4503ebcfefa4f5d9318111eaa84cb5509adf8d71790.LNK

DD768831.emf

Notifications

Runtime

Environment 1

Sample was analyzed using 'Kernelmode Monitor'

Community

There are no community comments.

You must be logged in (/login) to submit a comment.

(https://twitter.com/PayloadSecurity)