Interactive malware hunting service

General Info

File name	a2b3fa8c1df9f8036142eb801114750c2263fd55.doc
Full analysis	
Verdict	Malicious activity
Analysis date	3/3/2020, 10:30:33
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	macros macros-on-open generated-doc loader
Indicators:	
MIME:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
File info:	Microsoft Word 2007+
MD5	31DF06A6E89303321B33CFE0CA02A723
SHA1	A2B3FA8C1DF9F8036142EB801114750C2263FD55
SHA256	8A6860F95B3B6D01FC79E8003F83737C1764C305347D3C580799BC7E302DF223
SSDEEP	3072:TX4GPNXRQ6UOBF6VBWOCKKVKWJ0FPBUZX2S30:JXLX2EY/C1K9B0XPK

Behavior activities

MALICIOUS

Application was dropped or rewritten from another process
- j77fff.exe (PID: 2888)

Downloads executable files from the Internet
- powershell.exe (PID: 3480)

Starts Visual C# compiler
- powershell.exe (PID: 3480)

Unusual execution from Microsoft Office
- WINWORD.EXE (PID: 3044)

Executes PowerShell scripts
- WINWORD.EXE (PID: 3044)

SUSPICIOUS

Executable content was dropped or overwritten
- powershell.exe (PID: 3480)

Creates files in the user directory
- powershell.exe (PID: 3480)

INFO

Reads Microsoft Office registry keys
- WINWORD.EXE (PID: 3044)

Creates files in the user directory
- WINWORD.EXE (PID: 3044)

Static information

TRiD

.docm | Word Microsoft Office Open XML Format document (with Macro) (53.6%)
.docx | Word Microsoft Office Open XML Format document (24.2%)
.zip | Open Packaging Conventions container (18%)
.zip | ZIP compressed archive (4.1%)

EXIF

ZIP

ZipRequiredVersion:	20
ZipBitFlag:	0x0006
ZipCompression:	Deflated
ZipModifyDate:	1980:01:01 00:00:00
ZipCRC:	0x3f450766
ZipCompressedSize:	399
ZipUncompressedSize:	1503
ZipFileName:	[Content_Types].xml

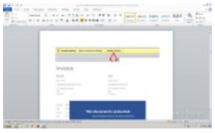
XML

Template:	Normal.dotm
TotalEditTime:	*null*
Pages:	1
Words:	*null*
Characters:	1
Application:	Microsoft Office Word
DocSecurity:	None
Lines:	1
Paragraphs:	1
ScaleCrop:	No
LinksUpToDate:	No
CharactersWithSpaces:	1
SharedDoc:	No
HyperlinksChanged:	No
AppVersion:	15
Keywords:	Detect
LastModifiedBy:	*null*
RevisionNumber:	1
CreateDate:	2020:03:02 21:13:00Z
ModifyDate:	2020:03:02 21:13:00Z

XMP

Title:	Hypogynous
Subject:	Hemicyclic
Creator:	*null*
Description:	Directory

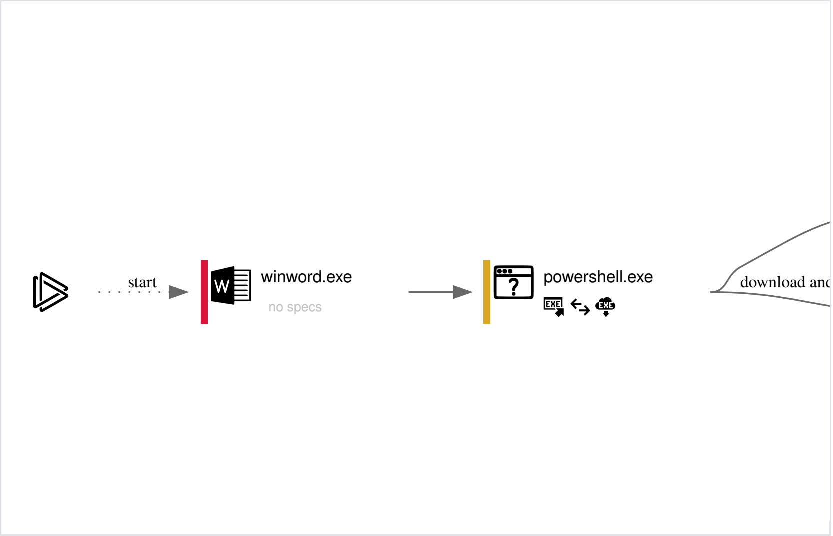
Screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
40	5	1	2

Behavior graph



Registry activity

Total events	Read events	Write events	Delete events
2340	1292	993	55

Modification events

PID	Process	Operation	Key	Name	Value
3044	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems		
3044	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	xn2	786E3200E40B0000010000000000000000000000
3044	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	Off
3044	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1041	Off
3044	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1046	Off
3044	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Co	1036	Off

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	2	5	4

Dropped files

PID	Process	Filename	Type
3480	powershell.exe	C:\Users\admin\AppData\Roaming\j77fff.exe **MD5:** A02C2597D3C8EF9BC09DBDE25AF... **SHA256:** C74BC9A1E550	executable
3480	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms **MD5:** 3B712DE36DC1672EC51A90C5EE3... **SHA256:** DDE2E429BD6D	binary
4092	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RES7D76.tmp **MD5:** –– **SHA256:** ––	––
3464	csc.exe	C:\Users\admin\AppData\Local\Temp\a0vsd075.dll **MD5:** –– **SHA256:** ––	––
3464	csc.exe	C:\Users\admin\AppData\Local\Temp\CSC7D75.tmp **MD5:** –– **SHA256:** ––	––
3464	csc.exe	C:\Users\admin\AppData\Local\Temp\a0vsd075.pdb **MD5:** –– **SHA256:** ––	––
3480	powershell.exe	C:\Users\admin\AppData\Local\Temp\a0vsd075.0.cs **MD5:** 970A7A9C30A5ECA2B54E6F9A202F... **SHA256:** 28D72BA61E39	text
3480	powershell.exe	C:\Users\admin\AppData\Local\Temp\a0vsd075.cmdline **MD5:** 086AC000A28296AEF791B39D25FC... **SHA256:** 0A5004909C21	text
3044	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR6AD8.tmp.cvr **MD5:** –– **SHA256:** ––	––
3480	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RFa676de.TMP **MD5:** 3B712DE36DC1672EC51A90C5EE3... **SHA256:** DDE2E429BD6D	binary
3480	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UYBR0CEN8K0PKOWE1HTG.temp **MD5:** –– **SHA256:** ––	––
3044	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\a2b3fa8c1df9f8036142eb801114750c2263fd55.doc.docm.LNK **MD5:** CFB35AF277535854891E9E2119F5... **SHA256:** 6485D9E476A6	lnk
3044	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\index.dat **MD5:** 8F3D012A3C8DE63599EB1FC213E... **SHA256:** 869BD3345DC5	text
3044	WINWORD.EXE	C:\Users\admin\Desktop\~$b3fa8c1df9f8036142eb801114750c2263fd55.doc.docm **MD5:** D5C8CFD1821C71C2A5FDEDB4840... **SHA256:** 756B8564BB37	pgc
3044	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 477916EFB88A373723F281B8A9BC... **SHA256:** F8C4753F90B6	pgc
3464	csc.exe	C:\Users\admin\AppData\Local\Temp\a0vsd075.out **MD5:** –– **SHA256:** ––	––

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
1	1	1	2

HTTP requests

PID	Process	Method	HTTP Code	IP	CN	URL	Type	Size
3480	powershell.exe	GET	200	192.99.76.30:80	CA	http://jusqit.com/02/89113007.exe	executable	1019 K

Connections

PID	Process	IP	ASN	CN	Reputation
3480	powershell.exe	192.99.76.30:80	OVH SAS	CA	malicious

DNS requests

Domain	IP	Reputation
jusqit.com	192.99.76.30	malicious

Threats

PID	Process	Class	Message
3480	powershell.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
3480	powershell.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download

Debug output strings

Process	Message
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre\base\isolation\com\enumidentityattribute.cpp, line 144
csc.exe	*** HR propagated: -2147024774 *** Source File: d:\iso_whid\x86fre

Interactive malware hunting service ANY.RUN
© 2017-2020 ANY.RUN LLC. ALL RIGHTS RESERVED