ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	A.R.869533241.exe
Full analysis:	https://app.any.run/tasks/8e48440d-bbfb-4e0c-8461-5007ed27d26e
Verdict:	Malicious activity
Threats:	Pony
	Pony is a malware with two main functions — stealing information and dropping other viruses with different tasks on infected machines. It has been around since 2011, and it still actively attacks users in Europe and America.
Analysis date:	March 03, 2019 at 14:38:23
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	installer trojan pony fareit
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	914D779077C333730F61814B5962C305
SHA1:	55D8F8606756B3EFF08A27390B8E2D9401560A5D
SHA256:	1131284ED9C2E205B1A41EFFB13E403B1D23920DCDA2395C1D5BA5F459230969
SSDEEP:	12288:pSEafr5LRtE9K1Lml5ESs23gdI3/TxEZvCZU8ezar:jaV11C9s23syTZZgar

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	60 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 8.0.7601.17514 undefined
- Adobe Acrobat Reader DC MUI (15.023.20070)
- Adobe Flash Player 26 ActiveX (26.0.0.131)
- Adobe Flash Player 26 NPAPI (26.0.0.131)
- Adobe Flash Player 26 PPAPI (26.0.0.131)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.35)
- FileZilla Client 3.36.0 (3.36.0)
- Google Chrome (68.0.3440.106)
- Google Update Helper (1.3.33.17)
- Java 8 Update 92 (8.0.920.14)
- Java Auto Updater (2.8.92.14)
- Microsoft .NET Framework 4.6.1 (4.6.01055)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2017 Redistributable (x86) - 14.15.26706 (14.15.26706.0)
- Microsoft Visual C++ 2017 x86 Additional Runtime - 14.15.26706 (14.15.26706)
- Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.15.26706 (14.15.26706)
- Mozilla Firefox 61.0.2 (x86 en-US) (61.0.2)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Troubleshooters Package
- InternetExplorer Optional Package
- KB2534111
- KB2999226
- KB976902
- LocalPack AU Package
- LocalPack CA Package
- LocalPack GB Package
- LocalPack US Package
- LocalPack ZA Package
- ProfessionalEdition
- UltimateEdition

Notepad++ (32-bit x86) (7.5.1)
Opera 12.15 (12.15.1748)
Skype version 8.29 (8.29)
VLC media player (2.2.6)
WinRAR 5.60 (32-bit) (5.60.0)

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Connects to CnC server A.R.869533241.exe (PID: 3612)	**Starts CMD.EXE for commands execution** A.R.869533241.exe (PID: 3612)	No info indicators.
Detected Pony/Fareit Trojan A.R.869533241.exe (PID: 3612)		
Actions looks like stealing of personal data A.R.869533241.exe (PID: 3612)		

Static information

TRiD

.exe | InstallShield setup (49)
.exe | Win64 Executable (generic) (31.4)
.dll | Win32 Dynamic Link Library (generic) (7.4)
.exe | Win32 Executable (generic) (5.1)
.exe | Clipper DOS Executable (2.2)

EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2019:02:28 01:35:24+01:00
PEType:	PE32
LinkerVersion:	14
CodeSize:	333824
InitializedDataSize:	269312
UninitializedDataSize:	0
EntryPoint:	0x3de70
OSVersion:	5.1
ImageVersion:	0
SubsystemVersion:	5.1
Subsystem:	Windows GUI
FileVersionNumber:	7.7.9.2
ProductVersionNumber:	7.7.9.2
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Windows NT 32-bit
ObjectFileType:	Executable application
FileSubtype:	0
LanguageCode:	English (U.S.)
CharacterSet:	Unicode
LegalTrademarks:	Copyright 2015
CompanyName:	Docker
Comments:	Onprerender Uid Computer Links Taking
LegalCopyright:	Copyright 2015
FileVersion:	7.7.9.2
PrivateBuild:	7.7.9.2
FileDescription:	Onprerender Uid Computer Links Taking
ProductName:	VariablesDatastores
ProductVersion:	7.7.9.2

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	28-Feb-2019 00:35:24
Detected languages:	English - United States
LegalTrademarks:	Copyright 2015
CompanyName:	Docker
Comments:	Onprerender Uid Computer Links Taking
LegalCopyright:	Copyright 2015
FileVersion:	7.7.9.2
PrivateBuild:	7.7.9.2
FileDescription:	Onprerender Uid Computer Links Taking
ProductName:	VariablesDatastores
ProductVersion:	7.7.9.2

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0090
Pages in file:	0x0003
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x0000
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x0000
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000110

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	7
Time date stamp:	28-Feb-2019 00:35:24
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_RELOCS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
.text	0x00067000	0x00001625	0x00001800	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	7.51572
.rdata	0x00053000	0x00010C6E	0x00010E00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	5.87287
.data	0x00064000	0x00002F58	0x00001400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	2.63673
.tls	0x00069000	0x00000009	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0.0203931
.gfids	0x0006A000	0x00000128	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	2.39541
.rsrc	0x0006B000	0x0002DD3C	0x0002DE00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ	7.26607

Resources

Title	Entropy	Size	Codepage	Language	Type
1	4.95324	688	Latin 1 / Western European	English - United States	RT_MANIFEST
2	4.84041	1128	Latin 1 / Western European	English - United States	RT_ICON
3	3.71734	9640	Latin 1 / Western European	English - United States	RT_ICON
4	4.21858	4264	Latin 1 / Western European	English - United States	RT_ICON
5	1.99749	10344	Latin 1 / Western European	English - United States	RT_ICON
6	3.49519	16936	Latin 1 / Western European	English - United States	RT_ICON
101	2.80883	90	Latin 1 / Western European	English - United States	RT_GROUP_ICON
226	7.70306	3015	Latin 1 / Western European	English - United States	HTML_IMG
805	3.21945	1350	Latin 1 / Western European	English - United States	RT_STRING
806	4.54623	2548	Latin 1 / Western European	English - United States	RT_STRING
807	3.49165	734	Latin 1 / Western European	English - United States	RT_STRING
810	2.92079	464	Latin 1 / Western European	English - United States	RT_BITMAP
811	3.01477	224	Latin 1 / Western European	English - United States	RT_BITMAP
832	5.77921	830	Latin 1 / Western European	English - United States	RT_BITMAP
833	3.81538	1064	Latin 1 / Western European	English - United States	RT_BITMAP
864	7.50535	1095	Latin 1 / Western European	English - United States	HTML_IMG
898	3.32892	416	Latin 1 / Western European	English - United States	RT_STRING
899	3.19672	2114	Latin 1 / Western European	English - United States	RT_STRING
900	3.51068	542	Latin 1 / Western European	English - United States	RT_STRING
932	3.52118	548	Latin 1 / Western European	English - United States	RT_STRING
933	3.55015	1354	Latin 1 / Western European	English - United States	RT_STRING
934	3.35039	334	Latin 1 / Western European	English - United States	RT_STRING
995	7.11104	484	Latin 1 / Western European	English - United States	HTML_IMG
996	6.16533	1022	Latin 1 / Western European	English - United States	HTML_IMG
3795	2.55212	308	Latin 1 / Western European	English - United States	RT_CURSOR

3796	2.07143	308	Latin 1 / Western European	English - United States	RT_CURSOR
3968	2.01924	20	Latin 1 / Western European	English - United States	RT_GROUP_CURSOR
3969	2.01924	20	Latin 1 / Western European	English - United States	RT_GROUP_CURSOR
5369	1.88729	308	Latin 1 / Western European	English - United States	RT_CURSOR
5370	2.56318	308	Latin 1 / Western European	English - United States	RT_CURSOR
5383	2.01924	20	Latin 1 / Western European	English - United States	RT_GROUP_CURSOR
5384	2.01924	20	Latin 1 / Western European	English - United States	RT_GROUP_CURSOR
5385	2.01924	20	Latin 1 / Western European	English - United States	RT_GROUP_CURSOR
5878	7.85921	3600	Latin 1 / Western European	English - United States	TXT
5879	7.94936	65208	Latin 1 / Western European	English - United States	TXT
5880	7.88012	3600	Latin 1 / Western European	English - United States	TXT
7570	7.88511	3600	Latin 1 / Western European	English - United States	TXT
7571	7.88001	3600	Latin 1 / Western European	English - United States	TXT
7572	7.86807	3600	Latin 1 / Western European	English - United States	TXT
9358	2.5463	308	Latin 1 / Western European	English - United States	RT_CURSOR
9359	3.33609	308	Latin 1 / Western European	English - United States	RT_CURSOR
9944	7.89849	3600	Latin 1 / Western European	English - United States	TXT
9945	7.89886	7200	Latin 1 / Western European	English - United States	TXT
9946	7.87715	10800	Latin 1 / Western European	English - United States	TXT

Imports

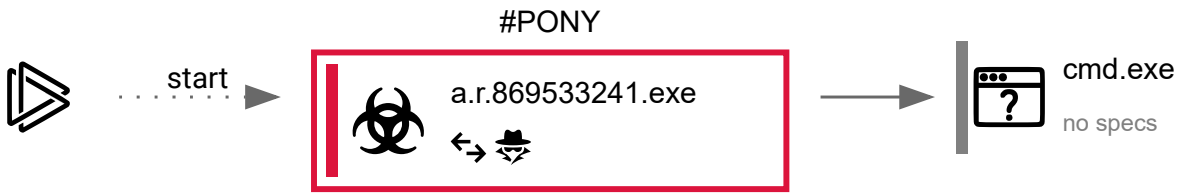
CRYPT32.dll
DWrite.dll
GDI32.dll
KERNEL32.dll
NETAPI32.dll
OLEAUT32.dll
SETUPAPI.dll
SHELL32.dll
SHLWAPI.dll
TAPI32.dll
USER32.dll
USERENV.dll
UxTheme.dll
WS2_32.dll
d2d1.dll
gdiplus.dll
ole32.dll

Video and screenshots

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
32	2	1	0

Behavior graph



Specs description

Program did not start	Low-level access to the HDD	Process was added to the startup	Debug information is available
Probably Tor was used	Behavior similar to spam	Task has injected processes	Executable file was dropped
Known threat	RAM overrun	Network attacks were detected	Integrity level elevation
Connects to the network	CPU overrun	Process starts the services	System was rebooted
Task contains several apps running	Application downloaded the executable file	Actions similar to stealing personal data	Task has apps ended with an error
File is detected by antivirus software	Inspected object has suspicious PE structure	Behavior similar to exploiting the vulnerability	Task contains an error or was rebooted
The process has the malware config			

Process information

PID	CMD	Path	Indicators	Parent process
3612	"C:\Users\admin\AppData\Local\Temp\A.R.869533241.exe"	C:\Users\admin\AppData\Local\Temp\A.R.869533241.exe		explorer.exe

Information

User:	admin	Company:	Docker
Integrity Level:	MEDIUM	Description:	Onprerender Uid Computer Links Taking
Exit code:	0	Version:	7.7.9.2

3060	cmd /c ""C:\Users\admin\AppData\Local\Temp\1790000.bat" "C:\Users\admin\AppData\Local\Temp\A.R.869533241.exe" "	C:\Windows\system32\cmd.exe	–	A.R.869533241.exe	

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	1	**Version:**	6.1.7601.17514 (win7sp1_rtm.101119-1850)

Registry activity

Total events	Read events	Write events	Delete events
373	368	5	0

Modification events

(PID) Process: (3612) A.R.869533241.exe **Key:** HKEY_CURRENT_USER\Software\WinRAR
Operation: write **Name:** HWID
Value: 7B3145363842394537 2D313338352D343045462D413739452D3342453034373234363630337D

(PID) Process: (3612) A.R.869533241.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 0

(PID) Process: (3612) A.R.869533241.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 1

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	1	0

Dropped files

PID	Process	Filename	Type
3612	A.R.869533241.exe	C:\Users\admin\AppData\Local\Temp\1790000.bat **MD5:** 3880EEB1C736D853EB13B44898B718AB **SHA256:** 936D9411D5226B7C5A150ECAF422987590A8870C8E095E1CAA072273041A86E7	text

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
4	4	1	20

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3612	A.R.869533241.exe	POST	–	145.239.232.110:80	http://raygis-llc.com/papid/gate.php	FR	–	–	malicious
3612	A.R.869533241.exe	POST	–	145.239.232.110:80	http://raygis-llc.com/papid/gate.php	FR	–	–	malicious
3612	A.R.869533241.exe	GET	–	145.239.232.110:80	http://raygis-llc.com/papid/gate.php	FR	–	–	malicious
3612	A.R.869533241.exe	POST	–	145.239.232.110:80	http://raygis-llc.com/papid/gate.php	FR	–	–	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3612	A.R.869533241.exe	145.239.232.110:80	raygis-llc.com	OVH SAS	FR	malicious

DNS requests

Domain	IP	Reputation
raygis-llc.com	145.239.232.110	malicious

Threats

PID	Process	Class	Message
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Fareit/Pony Downloader Checkin 2
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Unsupported/Fake Internet Explorer Version MSIE 5.
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Trojan Generic - POST To gate.php with no referer
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Pony Downloader HTTP Library MSIE 5 Win98
3612	A.R.869533241.exe	A Network Trojan was detected	MALWARE [PTsecurity] Fareit/Pony Downloader Checkin
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Fareit/Pony Downloader Checkin 2
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Unsupported/Fake Internet Explorer Version MSIE 5.
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Trojan Generic - POST To gate.php with no referer
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Pony Downloader HTTP Library MSIE 5 Win98
3612	A.R.869533241.exe	A Network Trojan was detected	MALWARE [PTsecurity] Fareit/Pony Downloader Checkin
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Fareit/Pony Downloader Checkin 2
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Trojan Generic - POST To gate.php with no referer
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Pony Downloader HTTP Library MSIE 5 Win98
3612	A.R.869533241.exe	A Network Trojan was detected	MALWARE [PTsecurity] Fareit/Pony Downloader Checkin
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Fareit/Pony Downloader Checkin 3
3612	A.R.869533241.exe	Potential Corporate Privacy Violation	ET POLICY Windows 98 User-Agent Detected - Possible Malware or Non-Updated System
3612	A.R.869533241.exe	A Network Trojan was detected	ET TROJAN Pony Downloader HTTP Library MSIE 5 Win98

Debug output strings

No debug info