ID: 532659
Sample Name: PTA009483.exe
Cookbook: default.jbs
Time: 15:43:33
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

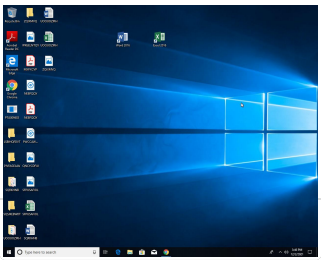
Windows Analysis Report PTA009483.exe

Overview

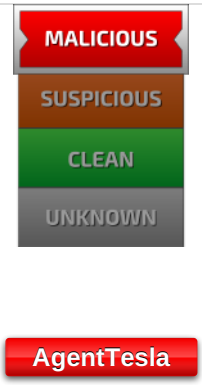
General Information

Sample Name:	PTA009483.exe
Analysis ID:	532659
MD5:	c32dc27c35f471c..
SHA1:	b8518918c8aeaa..
SHA256:	ae4bc61fdbd79ef..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

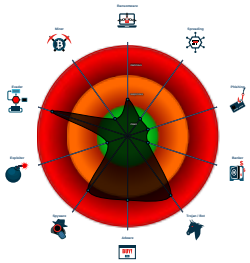


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- PTA009483.exe (PID: 6544 cmdline: "C:\Users\user\Desktop\PTA009483.exe" MD5: C32DC27C35F471C71E237B07CFFC263D)
  - RegSvcs.exe (PID: 4500 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - WerFault.exe (PID: 6172 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4500 -s 632 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info@devmetsan.com.tr",
  "Password": "Murat2019*",
  "Host": "mail.devmetsan.com.tr"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.675453288.00000000030D9000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000000.673328512.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.673328512.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.917262490.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.917262490.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 28 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PTA009483.exe.4121b08.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PTA009483.exe.4121b08.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

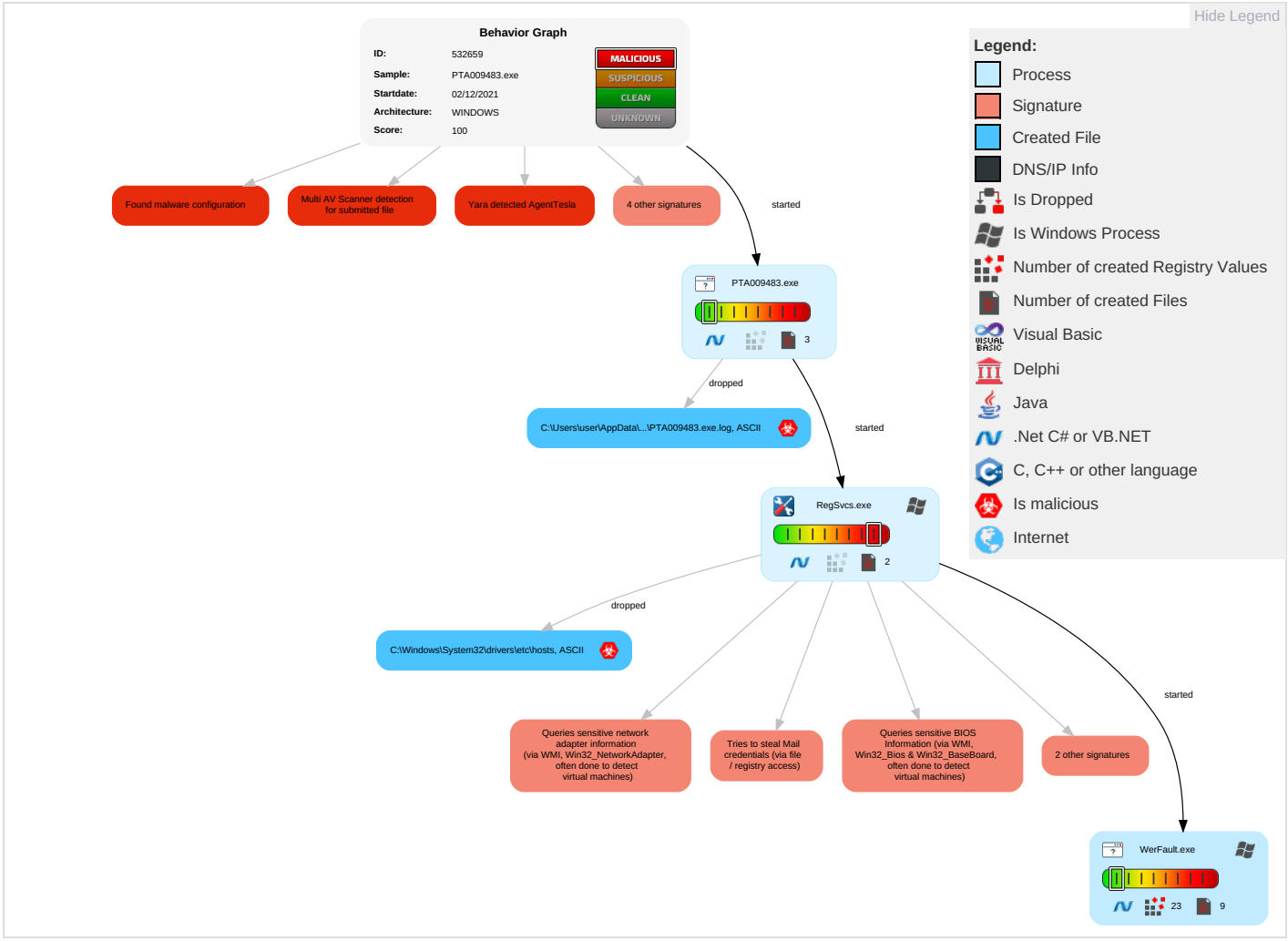
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 4 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

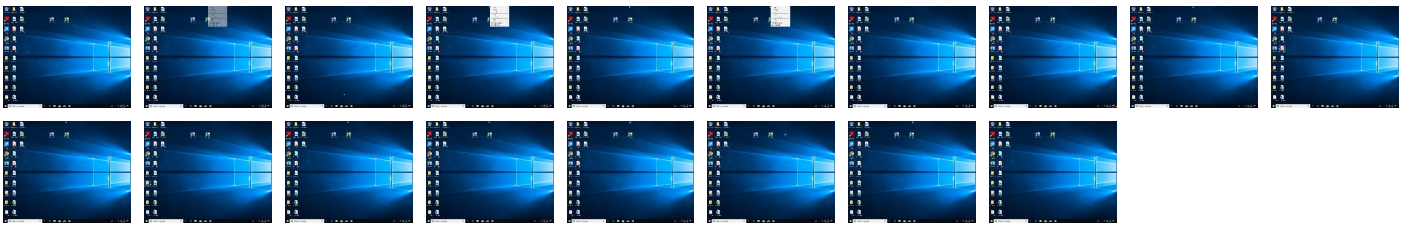
Behavior Graph



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
PTA009483.exe	35%	Virustotal		Browse
PTA009483.exe	29%	Metadefender		Browse
PTA009483.exe	68%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://OGxUTf.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532659
Start date:	02.12.2021
Start time:	15:43:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PTA009483.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:	19
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:	mal100.troj.adwa.spyw.evad.winEXE@4/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 46.2% • Quality standard deviation: 31.7%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:44:31	API Interceptor	2x Sleep call for process: PTA009483.exe modified
15:44:45	API Interceptor	655x Sleep call for process: RegSvcs.exe modified
15:46:25	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegSvcs.exe_6e42c2ecbe67857e042102e8f977834d8ccb729_75d5926b_19ab143c\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1283946255527386
Encrypted:	false
SSDEEP:	192:q1TGRdHBUZMXaaPXvJCM34/u7sxS274Itx:ES7BUZMXaapP34/u7sxX4Itx
MD5:	FB494F6D1079583F303AF529BE398F91
SHA1:	638029880F622D4B0E86D8ECE6A6E66B1B803D2D
SHA-256:	72758ECAB5A6A104CD0E1E7E29CD7442FB4701D242937737A88AEA0AF53EB94D
SHA-512:	020AF0CFC0C4FCA94B335DE25F99A497F2759701A60451C08436568F1C44AE16EFD86E9F0E1D3CA4063E6C8CBE6C83C0EEEF35D902DB915F50A61BE6900BF4 B
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegSvcs.exe_6e42c2ecbe67857e042102e8f977834d8ccb729_75d5926b_19ab143c\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.=.1.3.2.8.2.9.2.9.9.7.5.5.8.2.7.4.8.0.....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.=.1.3.2.8.2.9.2.9.9.8.4.3.3.2.6.9.8.9.....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.=.b.3.8.b.a.1.7.4.-.b.b.a.3.-.4.9.e.9.-.9.8.0.d.-.3.3.3.a.5.a.1.6.d.6.c.b.....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.=.a.e.9.3.b.3.2.e.-.c.1.9.f.-.4.7.b.9.-.a.d.a.e.-.5.5.e.2.0.e.1.7.0.5.5.2.....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.=.R.e.g.S.v.c.s...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.e.g.S.v.c.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.9.4.-.0.0.0.1.-.0.0.1.b.-.2.8.5.4.-.1.5.1.e.8.b.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.7.b.a.2.a.1.1.1.c.e.d.d.5.b.f.5.2.3.2.2.4.b.3.f.1.c.f.e.5.8.e.e.c.7.c.2.f.d.c.

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBC5.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 2 14:46:17 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	282834
Entropy (8bit):	3.6930537398619316
Encrypted:	false
SSDEEP:	3072:L44yWeJHJFe/00ojd+px0giUCgUzajC9gIOgF5hqf+5yo02HM:LBtMHJN05px0Tj+C9RpDYfpv
MD5:	806778AF9FEAB438E19410FA9ECF111E
SHA1:	01E51CF951A8D1698386F8D49356CE1910231A8D
SHA-256:	AA77F457EF152064E8A2A5DD37FD6012AB3FB6566B612BF63CE2BC7A9D03C06D
SHA-512:	7585205B942FC69A934D0A8EA59D0D42C1578746F3FA9A3D2E0B5C2937EA5C9EF55AC341E4FAC57BC793526BE76F36F08E40F493DDDC54B37F723CC11ED2F7(9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....9.a.....D.....,...L.....t&...Q.....T.....8.....T.....h9..j.....x#.....d%.....U.....B.....%.....GenuineIntelW.....T.....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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF972.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):	8344
Entropy (8bit):	3.689777288726644
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiljv6vUhGIe6YRQO6B0gmfZ7Sk+prz89blFsf/3m:RrlsNiZv6h6YCO6B0gmflSslefO
MD5:	DB89FB22CBA9105ACA2D6E686639A30C
SHA1:	2E7DB0A299FA47967FF181FAA00B59C3B7C118F0
SHA-256:	A0BFCEFB0D618F1E4254B7C11395CE4F674CA495DDFFCD720DDC6FD9D7968348
SHA-512:	7B2EEC75A2CAAAD5804CEB8AFF95523B23E239C00D62FD887BDBE27B2C7155C1461655ECB4F98F0106F501297B554E50879FFB06D2B18983FAD792AC2D49781
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.>.4.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD5B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4719
Entropy (8bit):	4.441488186622842
Encrypted:	false
SSDEEP:	48:cvIwSD8zsHrJgtWI9MyWSC8B78fm8M4JStjJ2Fb+q8vrtjJMP7id:uITfHFTTSNaJhKoP7id
MD5:	D271EBED8599A4BCE1624C5728FC8824
SHA1:	1F79B302FB7A3AEF0250A35A67484014559AD734
SHA-256:	A5E6AAFCFEDE0F39F5E0FBD05ACA0AA98BA62F4D3FBAB1099C6B22C505AF98BA
SHA-512:	D8F46A2B6F4E92F01FB912B3224FA702D73A5FDF8089F045F99855C26651070D28D171753885FAD4AD737E6F6424D92093183598560CC35DC1E2A529403FED3D
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD5B.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="1280156" />.. <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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PTA009483.exe.log	
Process:	C:\Users\user\Desktop\PTA009483.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1968
Entropy (8bit):	5.355630327889458
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHxvjHKs:iqXeqm00YqhQnouRqjntlxHeqzTwRrqs
MD5:	5216C7BA51383BFD6FACE8756C452F56
SHA1:	9E34E791CF09C89CF2A8F0D57D48EC330AD29F93
SHA-256:	502CE33AFDC9B4C6CCCB5069A7B700064608BEEA4138ED4DFA206F23D33D03B2
SHA-512:	C1906EAC187E69D5B85384CB62C57713F03D4020DE941D97385DC3F2CAFECBACFD8AEC14E40AB34207ACD0319C368927A0F39F57F3BD135286FC83B207FB4F4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.245463977313784
Encrypted:	false
SSDEEP:	12288:T+p0L1jLfxGMiGNyiO9KNTOtBhMyHL2OGcJgZW16rXR56azT:Sp0L1jLfxGBGNyw2B
MD5:	A67F7C4F5262D0C0C9151FC916238F7E
SHA1:	0064F99693ED6AC58CFB7EE1D24CDCAD4EF0ED8F
SHA-256:	C40EAFD182A32169C0FE5915D0FD0182D3AD9E0E9238FA558C618165309A60D7
SHA-512:	9825689C05975DF6412A4907FC5EC546486441176A897D3BF724A1FC3D7286DE1B2A960AD3EF90950AF99926649F34C029132D166B6DC1F12125BA973E1510CA
Malicious:	false
Reputation:	low

C:\Windows\appcompat\Programs\Amcache.hve	
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.).Z..... .....}.....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.4224845856930766
Encrypted:	false
SSDEEP:	384:ofU5K5cPv4YgnVVeeDzeH1NKZtj/T8GSw61FOc7oOw:sSKUg/eeDzeVNYtjlGSw6ac7L
MD5:	61EB23C0700A8DA675E5155FED8D22C7
SHA1:	600A225C457071F582679A0CDFB2CEB105619DA9
SHA-256:	515222160605424910805 0F3D3F71624C53D41F305315A44C809E8025CED91A8
SHA-512:	35B2BDD866A908CA152D30E0008A2FBBCF263512921AB5A65D134D21814FC999AF39F1102C79044640438C1BE87AEF0B7BEA544395A4BD18576456BB527260D1
Malicious:	false
Reputation:	low
Preview:	regfG...G...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.).Z..... .....{...HvLE.N.....G.....qq..~>1...Eu..... ..hbin.....p.\..,.....nk,..).Z..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ..).Z..... ....Z.....Root.....lf.....Root....nk ..).Z..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.93539046167478
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PTA009483.exe
File size:	546816
MD5:	c32dc27c35f471c71e237b07cffc263d
SHA1:	b8518918c8aeaaaf989e6361907debff3da0d6f6
SHA256:	ae4bc61fdbd79efa881919084a9858bc02935ae6ed8644f 246ff0f56d87d6e9f
SHA512:	d8f4dde39c62d66a9cfa05728efa151e0d2342bd2ff4b94a 85a156a8bed0420459592a22b2409fe2f42557cc3e70c4b 5356f14e50df41fe81eabf689e589d11b
SSDEEP:	12288:55pYcrq3cPeOQLqG+jW6XByT1AsZTSp3unxUJ 3xs8+qUrH:DpYcrbbQLqG/+wxBZTbnCZG8+zrH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I .a.....0..L.....:j... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x486a3a

General

Entrypoint Section:	.text
Digitally signed:	false
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:	0x61A449D0 [Mon Nov 29 03:32:32 2021 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

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x84a50	0x84c00	False	0.942916151718	data	7.94597502339	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x64c	0x800	False	0.3447265625	data	3.55508289256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PTA009483.exe PID: 6544 Parent PID: 2340

General

Start time:	15:44:29
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\PTA009483.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PTA009483.exe"
Imagebase:	0xd10000
File size:	546816 bytes
MD5 hash:	C32DC27C35F471C71E237B07CFFC263D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.675453288.00000000030D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.675367652.00000000030A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.675799503.0000000004091000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.675799503.0000000004091000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 4500 Parent PID: 6544

General

Start time:	15:44:32
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xab0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.673328512.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.673328512.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.917262490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.917262490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.882714795.0000000002E58000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.922268138.0000000002E58000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.672572361.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.672572361.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.882474406.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.882474406.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.877668648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.877668648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.883876684.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.883876684.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.884947434.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.884947434.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.672990070.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.672990070.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.673620269.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.673620269.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.885072574.0000000002E58000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.922149031.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.922149031.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: WerFault.exe PID: 6172 Parent PID: 4500

General

Start time:	15:46:13
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4500 -s 632
Imagebase:	0x920000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000003.896330972.0000000005140000.00000004.00000001.sdmp, Author: Joe Security
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