ID: 502697
Sample Name: PI.exe
Cookbook: default.jbs
Time: 10:17:10
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

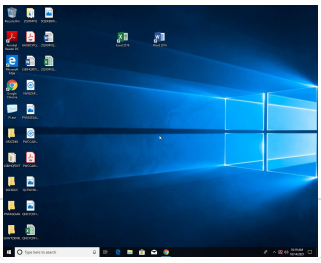
Windows Analysis Report PI.exe

Overview

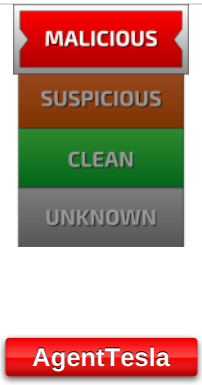
General Information

Sample Name:	PI.exe
Analysis ID:	502697
MD5:	59f7f57b8d6c0e5..
SHA1:	0740bebf070c16f..
SHA256:	c932b6a0cbaa45..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection

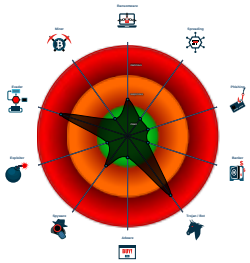


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Machine Learning detection for samp…
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Hides that the sample has been dow…
- Queries sensitive network adapter in…
- Uses schtasks.exe or at.exe to add …
- Queries sensitive BIOS Information …
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- PI.exe (PID: 4596 cmdline: 'C:\Users\user\Desktop\PI.exe' MD5: 59F7F57B8D6C0E55493EEC56977D7CB4)
  - schtasks.exe (PID: 6840 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gBrGmFSvkGtF' /XML 'C:\Users\user\AppData\Local\Temp\tmpE100.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 7036 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 7100 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - WerFault.exe (PID: 4416 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 1476 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- ZAYOk.exe (PID: 3796 cmdline: 'C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ZAYOk.exe (PID: 7112 cmdline: 'C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "account@jeevalabs.com",
  "Password": "jeeva@123",
  "Host": "mail.jeevalabs.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000000.400992134.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000000.400992134.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000000.401899331.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.401899331.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000002.429850923.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

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)

Stealing of Sensitive Information:

Yara detected AgentTesla

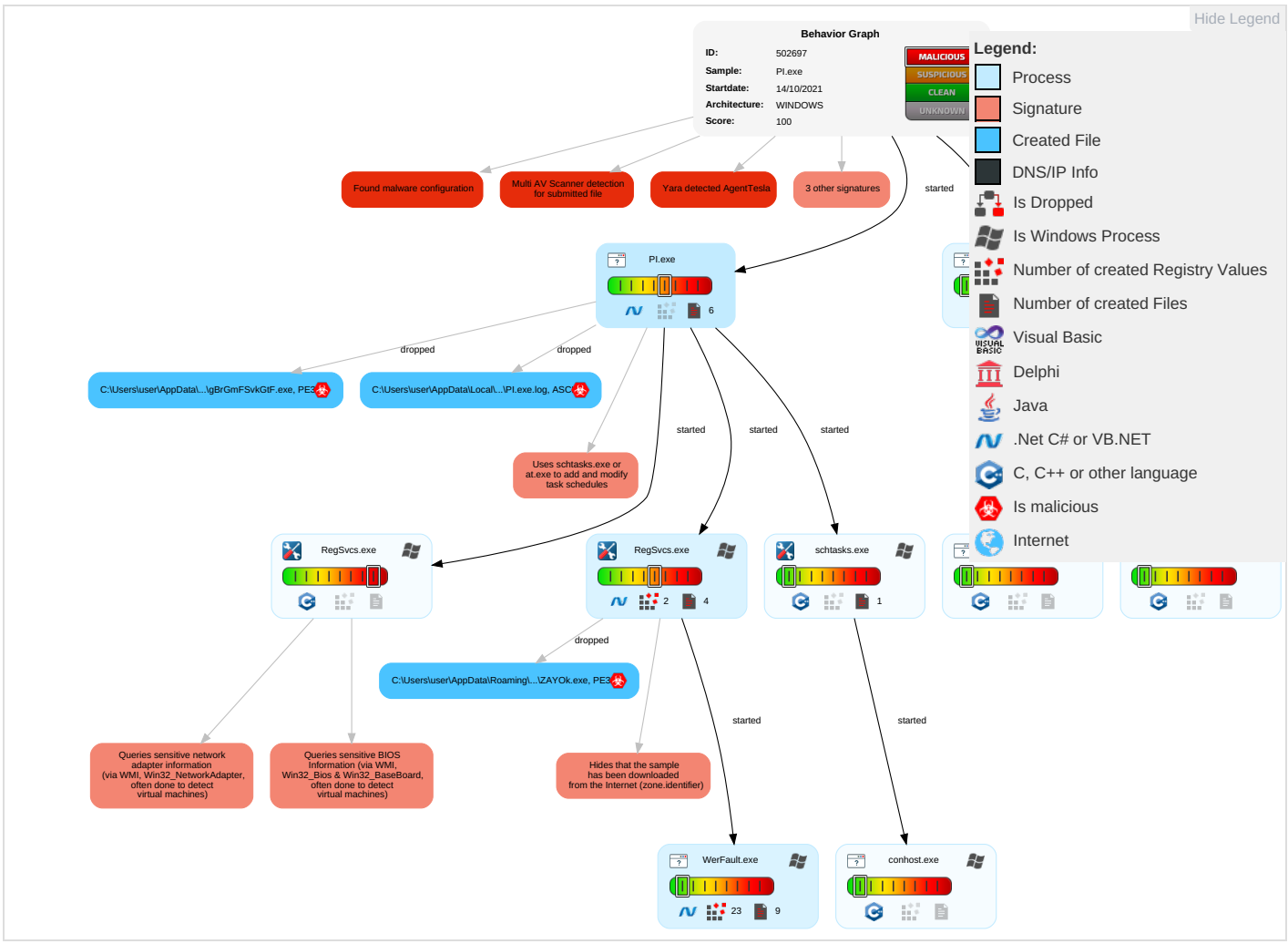
Remote Access Functionality:

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	Ne Ef
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 3 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea In Ne Co
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1 4 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Ex Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do In Pr

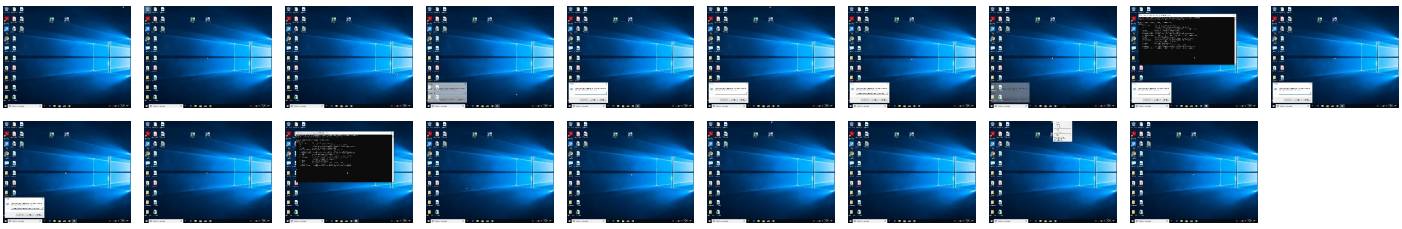
Behavior Graph



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
PI.exe	26%	Virustotal		Browse
PI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gBrGmFSvkGtF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.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://https://watson.telemetry.m	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	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	
http://bwoMKP.com	0%	Avira URL Cloud	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:	33.0.0 White Diamond
Analysis ID:	502697
Start date:	14.10.2021
Start time:	10:17:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI.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:	33
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.evad.winEXE@13/12@0/0
EGA Information:	Failed
HDC Information:	Failed
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
10:18:18	API Interceptor	2x Sleep call for process: PI.exe modified
10:18:29	API Interceptor	242x Sleep call for process: RegSvcs.exe modified
10:18:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ZAYOk C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
10:18:47	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ZAYOk C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
10:19:10	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	Invoice.exe	Get hash	malicious	Browse	
	sale order.exe	Get hash	malicious	Browse	
	XnQ8NBKkhW.exe	Get hash	malicious	Browse	
	DEBIT NOTE.exe	Get hash	malicious	Browse	
	FAj7shxXukkNrTk.exe	Get hash	malicious	Browse	
	ameHrrFwNp.exe	Get hash	malicious	Browse	
	gNFfZ1w8E6.exe	Get hash	malicious	Browse	
	YdACOWCggQ.exe	Get hash	malicious	Browse	
	Swift copy.exe	Get hash	malicious	Browse	
	KRSEL0000056286.JPG.exe	Get hash	malicious	Browse	
	tT5M57z8XiwLwf5.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Suspicious.Win32.Save.a.7200.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	
	319-7359-01#U00a0BL#U00a0DRAFT.exe	Get hash	malicious	Browse	
	HSBc20210216B1.exe	Get hash	malicious	Browse	
	BANK INFORMATION.exe	Get hash	malicious	Browse	
	PO.2100002.exe	Get hash	malicious	Browse	
	dorlla.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_RegSvcs.exe_35438265e855fa13c91512473cf11ea89278e4e6_7bbe79f8_10581952\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):	1.1249008109565173
Encrypted:	false
SSDEEP:	192:WUXGXokHBUZMXaaPXvJCMyZ/u7sJS274Itx:B24sBUZMXaapPyZ/u7sJX4Itx
MD5:	5B47E1903A6AD48CBD078BA84F012701
SHA1:	D53BA8F16B5B4F5124A750780A1A821998131DEB
SHA-256:	B925BB96C0ECE0DD097737142CDC11E48E11C9FC4C66D841D980D95C72E69833
SHA-512:	6A002C6E33389D8D4CBEB7DAD81567B7DF19DCDEEE84D4C12C29D37597AD469A9C269D29E8A6433C5AB65E3D54132976B869C2B08839C2FDAEF8DFE73850CB7
Malicious:	false
Reputation:	low
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.=.1.3.2.7.8.7.0.5.5.4.3.0.0.8.9.5.4.3.....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.=.1.3.2.7.8.7.0.5.5.4.9.1.1.8.3.0.9.9.....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.=.a.5.7.0.8.4.b.d.-.8.1.5.1.-.4.d.b.d.-.b.a.9.4.-.4.1.9.b.6.f.b.a.b.8.4.c.....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.=.6.3.2.6.4.b.4.8.-.7.1.5.0.-.4.1.b.3.-.a.5.9.d.-.6.2.1.b.a.d.9.a.7.4.e.0.....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.b.b.c.-.0.0.0.1.-.0.0.1.c.-.a.3.9.9.-.c.9.7.c.1.f.c.1.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\WER86C6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Oct 14 17:19:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	299872
Entropy (8bit):	3.6562294785263716
Encrypted:	false
SSDEEP:	3072:GHtGjd+pwTir09mmUCgU5yt09gIOgF5wuoX0NThBS0mXYEei:MzpKmHmTjT9RpDVymTK0
MD5:	7640E16B16410224E445F4175123A31D
SHA1:	E5EDBBCFD525D7DD20AD8ECB4C677964DFE2EF33
SHA-256:	DE47BC341644CF2AE755017DCCFDA1B09108DA4A111803BCEB9D7AB5CD2D98A7
SHA-512:	D11C3B6C62C63E1C1139A397EFCBBDAC4A54FA2C9177035D7A6F6B670F8A8011CD02F9469520BBFA3EEDBD733C9A307FB520D61CDACDE87B75D0B29B864C9F0D
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....fha.....$...x#.....t(..xW.....`.....8.....T.....X:...Y.....#.....%.....U.....B..... &... ...GenuineIntelW.....T.....]fha.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .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\WER9473.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):	8360
Entropy (8bit):	3.7043128360777016
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiK66xc896Ycs6V4gmfZUYSBCprk89bnasf0aNm:RrlsNiv6Gm6Y/6qgmfGYSAn5fQ
MD5:	D89D3E79B4259C421D751131D4166120
SHA1:	6CFE55C41E2DF77DD8E5C2EC129C3C1CF83D8F35
SHA-256:	593867FE59390C42B39E7550E004FE87E008A01A0517130E65834DC6CD6C2178
SHA-512:	FD19FD2D2E7ED43EC79B5B48EA7B96257259C3041B1BE4ACB3B51B866562D574ED92F8B30C3C55B781003F578FBB631CC19FE8F94E1ADEE05C2F3579176A5F1
Malicious:	false
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.>.7.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER97A1.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4741
Entropy (8bit):	4.502176438941949
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZiJgtWI9x9WSC8Bo8fm8M4JSD8Fk1+q8vrDSP7Md:uITfuqMSN7JCKqP7Md
MD5:	6FBCF6C984AD30C4B94DC01962D35E91
SHA1:	C181F364FC8E823DFD39DAD1E81172C340649128
SHA-256:	7E00DEE04E2A406D26DDEC863FBB5AA11FC9DDB0C844AFB94780194189D77D55
SHA-512:	EED54727E3ACE282CD882B3B9B53B97708D7C72B09A186EB73D762CB028A599C2E1F64025C2F8CA3DB1AB7F8825B5C21FBA6D2479C424FA729B7B880CAD6253
Malicious:	false
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="1209749" />.. <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\PI.exe.log	
Process:	C:\Users\user\Desktop\PI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ZAYOk.exe.log	
Process:	C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28

C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe	
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Invoice.exe, Detection: malicious, Browse • Filename: sale order.exe, Detection: malicious, Browse • Filename: XnQ8NBKkhW.exe, Detection: malicious, Browse • Filename: DEBIT NOTE.exe, Detection: malicious, Browse • Filename: FAj7shxXukkNrTk.exe, Detection: malicious, Browse • Filename: ameHrrFwNp.exe, Detection: malicious, Browse • Filename: gNFfZ1w8E6.exe, Detection: malicious, Browse • Filename: YdACOWCggQ.exe, Detection: malicious, Browse • Filename: Swift copy.exe, Detection: malicious, Browse • Filename: KRSEL0000056286.JPG.exe, Detection: malicious, Browse • Filename: tT5M57z8XiwLwf5.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Suspicious.Win32.Save.a.7200.exe, Detection: malicious, Browse • Filename: Purchase order.exe, Detection: malicious, Browse • Filename: 21ITQXL080104122T7.exe, Detection: malicious, Browse • Filename: COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe, Detection: malicious, Browse • Filename: 319-7359-01#U00a0BL#U00a0DRAFT.exe, Detection: malicious, Browse • Filename: HSBc20210216B1.exe, Detection: malicious, Browse • Filename: BANK INFORMATION.exe, Detection: malicious, Browse • Filename: PO.2100002.exe, Detection: malicious, Browse • Filename: dorlla.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s....+i~....o....(.... s.....o.....r!..p..(....Q.P,..P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Roaming\gBrGmFSvkGtF.exe	
Process:	C:\Users\user\Desktop\PI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1017344
Entropy (8bit):	7.047914763902751
Encrypted:	false
SSDEEP:	12288:aKTHWBTmCzo/MOxAS0x78YIOIX9C/HpdprYmCC9jB:amHqzo/MOsIrNC/PpE
MD5:	59F7F57B8D6C0E55493EEC56977D7CB4
SHA1:	0740BEBF070C16FCA8AA5C0FADA48EDCC1BD9F12
SHA-256:	C932B6A0CBAA454668D2429D433FEC76E7E544BB26B5BD1865A86AAC4FA33434
SHA-512:	259D52573BB4F97A4D9158D2D2F53B4EA6CEE27EFBC8E7FFE4962AE705EB36D220E19BABEE78B3737E3E5BC0AB99DECFC6C977AA99FAF4C1ABC9E445EABB 3E62
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....ga.....P..2...R.....Q... ...`....@.. ..... .@.....pQ..O....`...N..... ....H.....text....1... ...2..... ..`.rsrc....N...`...P...4.....@..@.relo c.....@..B.....Q.....H.....c.....(1...*&..(2....*.s3.....s4.....s5.....s6.....s7.....*...0.....~....o8....+..*.0..... ....~....o9....+..*.0.....~....o:....+..*.0.....~....o;....+..*.0.....~....o<....+..*&..(=....*...0..<.....~.....(>.....,!r...p.....(?...o@...sA.....~.....+..*.0.....~.....+..*".....*. 0.....(....r5..p~....oB....+..*...0..<.....~.....(>.....,!rE..p.....(?

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):	4.279387964724438
Encrypted:	false
SSDEEP:	12288:3K2zoKwkpljKIC3TZoKHf9B46Q0WpZNpjhzQQnXRqCs0NpLylYuLJ:a2zoKwkpljKIC3BH
MD5:	D3CA24D1EFB866BB21CA1588B12B148B
SHA1:	26416753CC2340221E2C478EBF7AED8FF2A21892
SHA-256:	2A01FE7A500E026A2D076DC95D4135CAC5A189B6D1318366F36FA2AFED44045B
SHA-512:	7B92607D0E4BDFF5E818180BDC2A4B736168FA61F40D312D7F5DA6DF65E75E8B5EBC50C0B2C4C4B314A01CED63B4E662E50DD3A7C0464AA1526EF9945DD67(9E
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve	
Preview:	regfZ...Z...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.rmtmr..... ....-..... .....

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):	24576
Entropy (8bit):	4.0411801016140165
Encrypted:	false
SSDEEP:	384:lwXF5Rftx1DPJ4XgsF8nm7k8PBqXTSeq5QMVyi6+/rl4Lk4PZd1DoXzKLZy7qE:uX7Rftx17J4XlF8m7FBqXGeq5QMVyi6b
MD5:	95A35997F577416D1A0BBC9E306F281A
SHA1:	E66158F54C06E796A04BD40B90402BBBB27C33E8
SHA-256:	F7349D9173117B3B571F30B44F0D684B975F1DB4A4DB8C2906354803B13D0B35
SHA-512:	A59CF9163E18755FCE817FE42855F4C7549BC2FD5D0FDF2480E7DE2B8415364922C3E4C1F71AF2C1D2586698D47F76F117DC246FA48ED0CE4F375CEC0D6CC8
Malicious:	false
Preview:	regfY...Y...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.rmtmr..... ....+...HvLE.^.....Y.....V..9U.2...$..d.....0..... ..hbin.....p.\..,.....nk,..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....Z.....Root.....lf.....Root....nk .....}..... .....*.....DeviceCensus.....vk. .....WritePermissionsCheck...

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.047914763902751
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:	PI.exe
File size:	1017344
MD5:	59f7f57b8d6c0e55493eec56977d7cb4
SHA1:	0740bebf070c16fca8aa5c0fada48edcc1bd9f12
SHA256:	c932b6a0cbaa454668d2429d433fec76e7e544bb26b5bd 1865a86aac4fa33434

General

SHA512:	259d52573bb4f97a4d9158d2d2f53b4ea6cee27efbc8e7ff e4962ae705eb36d220e19babee78b3737e3e5bc0ab99de cfc6c977aa99faf4c1abc9e445eabb3e62
SSDEEP:	12288:aKTHWBTmCzo/MOxAS0x78YIOIX9C/HpdprYm CC9jB:amHqzo/MOsIrNC/PpE
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... ga.....P..2...R.....Q... ...`....@.. ....@.....

File Icon

Icon Hash:	8088a2a692fa3e80

Static PE Info

General

Entrypoint:	0x4c51c2
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:	0x616789D1 [Thu Oct 14 01:37:21 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	0xc31c8	0xc3200	False	0.609131015775	data	7.07928703549	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x34ec4	0x35000	False	0.535962374705	data	6.0369770148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfc000	0xc	0x200	False	0.044921875	data	0.0980041756627	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: PI.exe PID: 4596 Parent PID: 3860

General

Start time:	10:17:58
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PI.exe'
Imagebase:	0x870000
File size:	1017344 bytes
MD5 hash:	59F7F57B8D6C0E55493EEC56977D7CB4
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 Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6840 Parent PID: 4596

General

Start time:	10:18:20
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gBrGmFSvkGtF' /XML 'C:\Users\user\AppData\Local\Temp\tmpE100.tmp'
Imagebase:	0xd00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6924 Parent PID: 6840

General

Start time:	10:18:20
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: RegSvcs.exe PID: 7036 Parent PID: 4596

General

Start time:	10:18:20
Start date:	14/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3e0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 7100 Parent PID: 4596

General

Start time:	10:18:21
Start date:	14/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc70000
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: 0000000E.00000000.400992134.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.400992134.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.401899331.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.401899331.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.429850923.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.429850923.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.428455338.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.428455338.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.399708702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.399708702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.403049754.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.403049754.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: ZAYOk.exe PID: 3796 Parent PID: 3352

General

Start time:	10:18:47
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe'
Imagebase:	0x3c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5808 Parent PID: 3796

General

Start time:	10:18:48
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ZAYOk.exe PID: 7112 Parent PID: 3352

General

Start time:	10:18:56
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ZAYOk\ZAYOk.exe'
Imagebase:	0xf00000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 5268 Parent PID: 7112

General

Start time:	10:18:56
Start date:	14/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 4416 Parent PID: 7100

General

Start time:	10:19:00
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 1476
Imagebase:	0x3e0000
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: 0000001B.00000003.414727052.00000000055F0000.00000004.00000001.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