ID: 490262
Sample Name: ZBvNS77A7a.dll
Cookbook: default.jbs
Time: 10:22:02
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

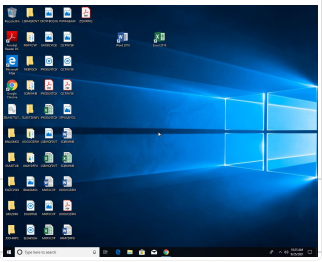
Windows Analysis Report ZBvNS77A7a.dll

Overview

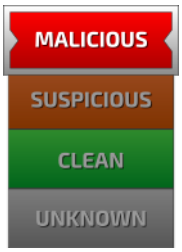
General Information

Sample Name:	ZBvNS77A7a.dll
Analysis ID:	490262
MD5:	6484d8ffd4a6de7..
SHA1:	41e1cbd037698c..
SHA256:	64a6039b2b3a34..
Tags:	dll Squirrelwaffle
Infos:	

Most interesting Screenshot:



Detection

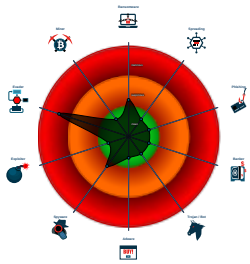


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Schedule system p…
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- Injects code into the Windows Explo…
- Sigma detected: Regsvr32 Comman…
- Machine Learning detection for dropp…
- Uses schtasks.exe or at.exe to add …
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5756 cmdline: loaddll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 796 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6352 cmdline: rundll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - explorer.exe (PID: 5620 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
  - explorer.exe (PID: 5616 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - schtasks.exe (PID: 6604 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn payuhfp /tr 'regsvr32.exe -s \'C:\Users\user\Desktop\ZBvNS77A7a.dll\'' /SC ONCE /Z /ST 10:25 /ET 10:37 MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- regsvr32.exe (PID: 5912 cmdline: regsvr32.exe -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5944 cmdline: -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 1372 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5944 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- regsvr32.exe (PID: 7080 cmdline: regsvr32.exe -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5576 cmdline: -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 6788 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5576 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Copyright Joe Security LLC 2021

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary:

Persistence and Installation Behavior:

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

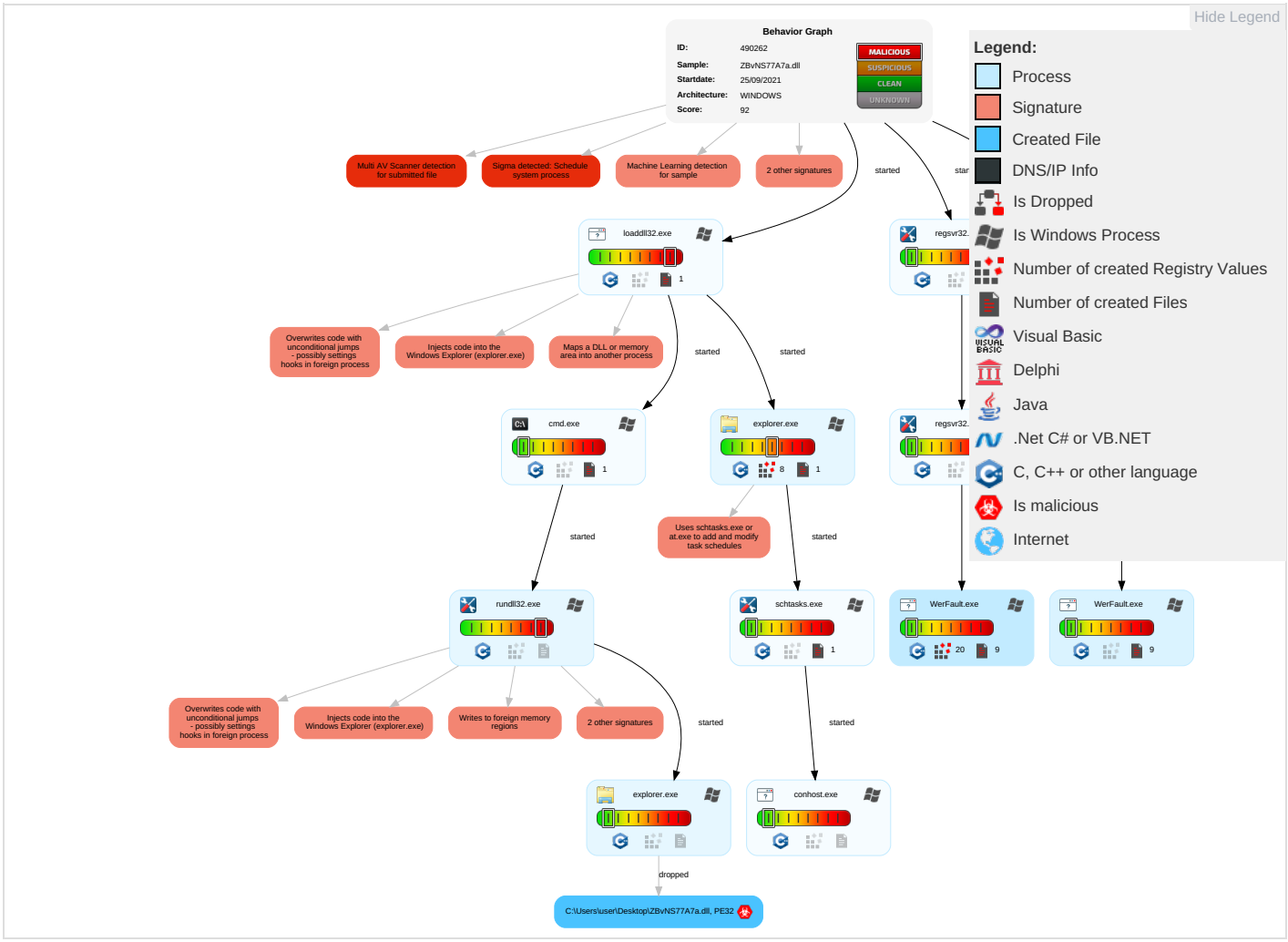
Injects code into the Windows Explorer (explorer.exe)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 4 1 3	Masquerading 1 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Native API 1	DLL Side-Loading 1	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 4 1 3	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

Behavior Graph



Screenshots

Thumbnails

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

Copyright Joe Security LLC 2021

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ZBvNS77A7a.dll	46%	Virustotal		Browse
ZBvNS77A7a.dll	60%	ReversingLabs	Win32.Backdoor.Quakbot	
ZBvNS77A7a.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\ZBvNS77A7a.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	490262
Start date:	25.09.2021
Start time:	10:22:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZBvNS77A7a.dll
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:	26
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:	mal92.evad.winDLL@20/10@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.6% (good quality ratio 21.6%) • Quality average: 76.7% • Quality standard deviation: 26.5%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:23:21	Task Scheduler	Run new task: payuhfp path: regsvr32.exe s>-s "C:\Users\user\Desktop\ZBvNS77A7a.dll"

Copyright Joe Security LLC 2021

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_regsvr32.exe_e9a58211ba4d9ba1b3cadfec684f66ac60801b0_7a325c51_04ce1181\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11500
Entropy (8bit):	3.7763436141995625
Encrypted:	false
SSDEEP:	192:Wzcub6VYkH/RS5uGXx3RjetM/u7sJS274ItUW:Qcw6Vb/RS5n3jee/u7sJX4ItUW
MD5:	463A67AC9E7EC8B0B962C5386749B5EB
SHA1:	9932B716AE52E8D904602F53D26727C9DA8F8CB2
SHA-256:	50C6047B7D3199121C82DF91533E16362CE4E85BBE34308E8F3A91643E419B65
SHA-512:	06825E10486556D11CFC1CB5AD0ED36E63A27ADF107DE3C4AF6687486E299A819094E4D919030B3A2ECA17BE1AEF51DB36743C6F90712FE2951BCDAE89E59A39
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.7.0.3.1.8.1.2.1.5.9.7.0.8.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.e.e.1.1.c.7.2.-.4.2.d.e.-.4.4.1.e.-.8.c.1.1.-.6.e.4.8.9.a.8.f.d.e.2.9.....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.=.c.9.0.8.b.4.3.a.-.f.a.2.e.-.4.6.4.2.-.a.b.9.2.-.7.a.c.3.5.3.0.f.2.e.0.a.....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.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.3.8.-.0.0.0.0.-.0.0.1.b.-.2.c.4.4.-.b.f.9.a.e.6.b.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.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e...T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e9a58211ba4d9ba1b3cadfec684f66ac60801b0_7a325c51_1b176866\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11496
Entropy (8bit):	3.7784669961245267
Encrypted:	false
SSDEEP:	192:Kdzcdb6VVkH/RS5uGXx3RjetM/u7suS274ItUO:KBcJ6Vu/RS5n3jee/u7suX4ItUO
MD5:	5A8B6D5D1EA2CD3F25FCB3E2EAC13AA0
SHA1:	238C25DC1680448F8C61684641FDBDB6B330C23A
SHA-256:	90162554559683001CCA548AF5C6D07754B326EED7F428389958A764AB53DEC1
SHA-512:	ED4678FE08C2861F42957B4057FC25CF22D441BDCEEAB005F094885621B8046F7CD2EC5C2F7E586CD56E56A3A9971726BE31186BADEB7992A8F9496D20A65E9
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_e9a58211ba4d9ba1b3cadfec684f66ac60801b0_7a325c51_1b176866\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.7.0.3.1.9.0.4.8.4.2.5.8.7.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.1.3.b.e.4.d.-.9.a.2.c.-.4.3.b.f.-.a.6.5.d.-.7.7.7.0.7.6.9.c.e.a.5.0.....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.=.d.9.0.a.d.8.5.0.-.4.f.b.4.-.4.1.2.9.-.b.f.f.2.-.9.f.f.9.c.8.9.e.5.a.6.6.....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.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.c.8.-.0.0.0.0.-.0.0.1.b.-.b.8.7.9.-.f.f.d.4.e.6.b.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.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5C6F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Sep 25 08:25:06 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35026
Entropy (8bit):	2.6261355120448786
Encrypted:	false
SSDEEP:	192:OCLJ0+qAUUFDMiwFHYYEcTAsOW+N8dLOglhcTgpmax9ZnANM:XLOWLF1wFHhPTvoGHhckpjxPSM
MD5:	5D31475311D93231DDBCD9BA6BD5BA55
SHA1:	7BDFAB76DF8E9B510E25F314B3609C9590004992
SHA-256:	B64A5890E8F04D4A6BA99601781CC64D9C6B1536A0781143CBD3DD9F052A3346
SHA-512:	C3247C860C7F77EF643B28453AAA64215A86D24484CC882661056C8404CD493AEC831CD2E15A0DA3FD1EBAC84819D0EA9952C7AED7F4BB01F146230D8001562
Malicious:	false
Preview:	MDMP..... .....Na.....U.....B.....GenuineIntelW.....T.....Na.....@..1.....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\WER62E9.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):	8278
Entropy (8bit):	3.6950810684096487
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimw6Dqxve6YwDSU+gmfJjSx+pBB89bcbsfi0m:RrlsNih6Z6Y8SU+gmfJjSpcgfg
MD5:	F94634BA3AA7A1D7A0BC36B4676D37F4
SHA1:	57D96DFC0FB1DF4004A3984443F4D3A1BEB37A00
SHA-256:	99BCE543BB148DE22D98A4DA12C00494DE1851984C579314CF178C85E3DB0B39
SHA-512:	F8616AE3E68C03B59F132A18F8313369E53407D5C37385C0633098FD077E3BDA69F87E739152BE69C1942337B06345877D6E24C49B041C482A79B0E63C62C10E
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.>.5.5.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER653B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.465614395578264
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI9jbWSC8BL8fm8M4JkxWFfT+q8zduKJYegd:uITf1AqSNqJnT9qYegd
MD5:	A22317ACAD0A7881DEEFD578FD331502
SHA1:	8D81BFD8496A4591D9E65D9E59A7D1099C9D94AC
SHA-256:	7B5623B3AC94AFF4431845877E8372C08FEEF5FAC00C5577C2BFE54E42711D2A
SHA-512:	0CBCB0AB7B9C8102442B7685907DE4D9357F522EFAC9347FF0950879BE1E625267E931C297DDADB09A2B78BDB0699E5ABB466557C23F6537DA1243FF1C9406F
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="1181855" />.. <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\Microsoft\Windows\WER\Temp\WER955.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.462098660842768
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI9jbWSC8BT8fm8M4JkxWFAgP+q8zd9KJYyRgd:uITfyAqSN2J9POqYyRgd
MD5:	C3F41612D9BFFE36894E5765A49D50E3
SHA1:	0B38B318423E6242D3F1F55779B7B2089B88F192
SHA-256:	073E01EF57E9934CE18E57CBD7B3404B4C8F347D29703EBD80C87B9DBC74CDD1
SHA-512:	F34619CF44959E7BFFE6A63D975EAB84BA2A61663508A88AEE3B2DF222A328F3FC43F6CA7553D37447A045AEFBC152B8A45FE212FF00B08D9EB848A5BE6540CA
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="1181854" />.. <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\Microsoft\Windows\WER\Temp\WERF241.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Sep 25 08:23:34 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35382
Entropy (8bit):	2.6628405818008596
Encrypted:	false
SSDEEP:	384:z6pIXEp7k/8JpD1iDWmUrgnGwhctnFl9h:zUg/srrM9ctndh
MD5:	91DF5FF5B9BC1DA3D1644ECA8FBB2F8E
SHA1:	E49D85C5C4A9D110B3DE839FE920C877893BB7F2
SHA-256:	5430CB813F7DB685ECEB2F6FD30264D0A7396769BB6A96CD302773ABC871D819
SHA-512:	BF86BDCDBE3B3B9BBF3338758B8835A2AA8211D0FD1D8A64D5A361832D77C037606B747909082756BA6A650D48DC2525D48EB20A7F02B956398F23C7A7EA147
Malicious:	false
Preview:	MDMP..... .....Na.....U.....B.....GenuineIntelW.....T.....8...z.Na.....@..1.....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\WERFFEE.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):	8282
Entropy (8bit):	3.695195907500495
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipFd676YB+MSUBgmfJjSx+pBB89bpisfLajm:RrlsNipv676YBlSUBgmfJjSpphfT
MD5:	7E717EA850E4710974F964DA9347D310
SHA1:	80858E5218A190A1BD271098947A15BF1422A4FA
SHA-256:	2843D9EBCCD91B310DE9C2661F45278B4EED0DC5A83A18B5FCC791577EBE84F0
SHA-512:	752BC595A439DB591B5E7AF93408FAE2793BAD55F3501D139DD01B9CFBFC57F33D38BD05C39B2B09819B83C594C26152E40E75F7C28937FB90BE5BDAFFBC07B
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.>.5.9.4.4.<./.P.i.d.>.....

C:\Users\user\Desktop\ZBvNS77A7a.dll	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	330189
Entropy (8bit):	2.2090413355109213
Encrypted:	false

C:\Users\user\Desktop\ZBvNS77A7a.dll

SSDEEP:	1536:/lUtVWns2GwmzYSbbz1j+xEXnQud+3VLuoXBYjPYH+ryO3O:/ZVWsP/sSb1ax0A3tDXBYjPYH+ryyO
MD5:	9147A4BB8EFF884F129AAD7E0C68D1C5
SHA1:	BA7E1C01F60E38FA8E0C420332BEAA82B647400D
SHA-256:	31682BA44B1B11AC8C4F9FDE98E63AFCF32D7AD143587FA631496E83464FF7C3
SHA-512:	46810C2FEE829EDF0FA52FD75DD25DAF32F2064629EF778BF94A73A54CBCE07770303F52B16808DFC97C3ED3C81188BFE4AF1491F6B98FD5DC8A679F8F24FDE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....;a.....!..... ....lZ..x....@...b.....Z..l.....text...t..... ..`.data..... .....@....data...d....0...0..... .....@....rsrc....b...@...d...F.....@..@..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.5705642690440875
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ZBvNS77A7a.dll
File size:	330189
MD5:	6484d8ffd4a6de7947534571e9907b4e
SHA1:	41e1cbd037698c3329db4edfe4e6b28b0654e94c
SHA256:	64a6039b2b3a347312f56170b5eb7deebe6d37ef6fb414fb929e84be4799dfa5
SHA512:	5545f50a5c5d2367c03a199832ff78d00fa7f172017007ba0e45c75190640cd79540d351db14279d3a505014ff380a12e00f796ec08038634f4d3641a61b7da0
SSDEEP:	6144:9/st+16ZWiobj+n5QZRO0Xj/Ee+aRLvccAOPyI:A+QoOaEFA7RD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....;a.....!..... ....

File Icon

Icon Hash:	aca9a8acaca6a888

Static PE Info

General

Entrypoint:	0x100019a1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x613B8C85 [Fri Sep 10 16:49:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

Copyright Joe Security LLC 2021

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	6527345f9aee9363b094aad01304de88

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30974	0x30a00	False	0.564327602828	data	6.10041951577	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x32000	0x1000	0x800	False	0.01123046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x33000	0x4000c64	0x3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4034000	0x162e0	0x16400	False	0.151454968399	data	4.89622756249	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5756 Parent PID: 5240

General

Start time:	10:23:08
Start date:	25/09/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll'
Imagebase:	0x2e0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 796 Parent PID: 5756

General

Start time:	10:23:09
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll',#1
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

Analysis Process: rundll32.exe PID: 6352 Parent PID: 796

General

Start time:	10:23:10
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ZBvNS77A7a.dll',#1
Imagebase:	0x370000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Copyright Joe Security LLC 2021

Analysis Process: explorer.exe PID: 5616 Parent PID: 5756

General

Start time:	10:23:15
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1020000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: explorer.exe PID: 5620 Parent PID: 6352

General

Start time:	10:23:17
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1020000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: schtasks.exe PID: 6604 Parent PID: 5616

General

Start time:	10:23:19
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn payuhfp /tr 'regsvr32.exe -s \'C:\Users\user\Desktop\ZBvNS77A7a.dll\'' /SC ONCE /Z /ST 10:25 /ET 10:37
Imagebase:	0x8b0000
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

Analysis Process: conhost.exe PID: 6624 Parent PID: 6604

General

Start time:	10:23:20
Start date:	25/09/2021
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: regsvr32.exe PID: 5912 Parent PID: 968

General

Start time:	10:23:22
Start date:	25/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll'
Imagebase:	0x7ff674450000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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: regsvr32.exe PID: 5944 Parent PID: 5912

General

Start time:	10:23:22
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Desktop\ZBvNS77A7a.dll'
Imagebase:	0x1320000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 1372 Parent PID: 5944

General

Start time:	10:23:28
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5944 -s 660
Imagebase:	0x1c0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 7080 Parent PID: 968

General

Start time:	10:25:00
Start date:	25/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Desktop\ZBvNS77A7a.dll'
Imagebase:	0x7ff674450000
File size:	24064 bytes

MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 5576 Parent PID: 7080

General

Start time:	10:25:00
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Desktop\ZBvNS77A7a.dll'
Imagebase:	0x1320000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6788 Parent PID: 5576

General

Start time:	10:25:02
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5576 -s 652
Imagebase:	0x1c0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Disassembly

Copyright Joe Security LLC 2021

Code Analysis

Code Analysis