ID: 490253
Sample Name: SAWHipN3nS.dll
Cookbook: default.jbs
Time: 10:12:22
Date: 25/09/2021
Version: 33.0.0 White Diamond

Table of Contents

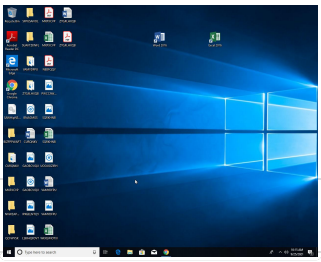
Windows Analysis Report SAWHipN3nS.dll

Overview

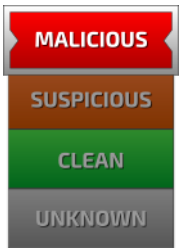
General Information

Sample Name:	SAWHipN3nS.dll
Analysis ID:	490253
MD5:	1ff17ce907ce2d9..
SHA1:	91818954ba50a5..
SHA256:	2dca3e9494cc2b…
Tags:	dll Squirrelwaffle
Infos:	

Most interesting Screenshot:



Detection

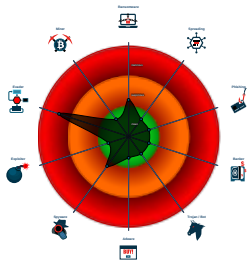


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6652 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SAWHipN3nS.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6664 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\SAWHipN3nS.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6684 cmdline: rundll32.exe 'C:\Users\user\Desktop\SAWHipN3nS.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - explorer.exe (PID: 6752 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
  - explorer.exe (PID: 6732 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - schtasks.exe (PID: 6832 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn yyhcsfwg /tr 'regsvr32.exe -s \'C:\Users\user\Desktop\SAWHipN3nS.dll\'' /SC ONCE /Z /ST 10:15 /ET 10:27 MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- regsvr32.exe (PID: 6888 cmdline: regsvr32.exe -s 'C:\Users\user\Desktop\SAWHipN3nS.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 6896 cmdline: -s 'C:\Users\user\Desktop\SAWHipN3nS.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 6960 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6896 -s 644 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- regsvr32.exe (PID: 6264 cmdline: regsvr32.exe -s 'C:\Users\user\Desktop\SAWHipN3nS.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 6324 cmdline: -s 'C:\Users\user\Desktop\SAWHipN3nS.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 4388 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

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

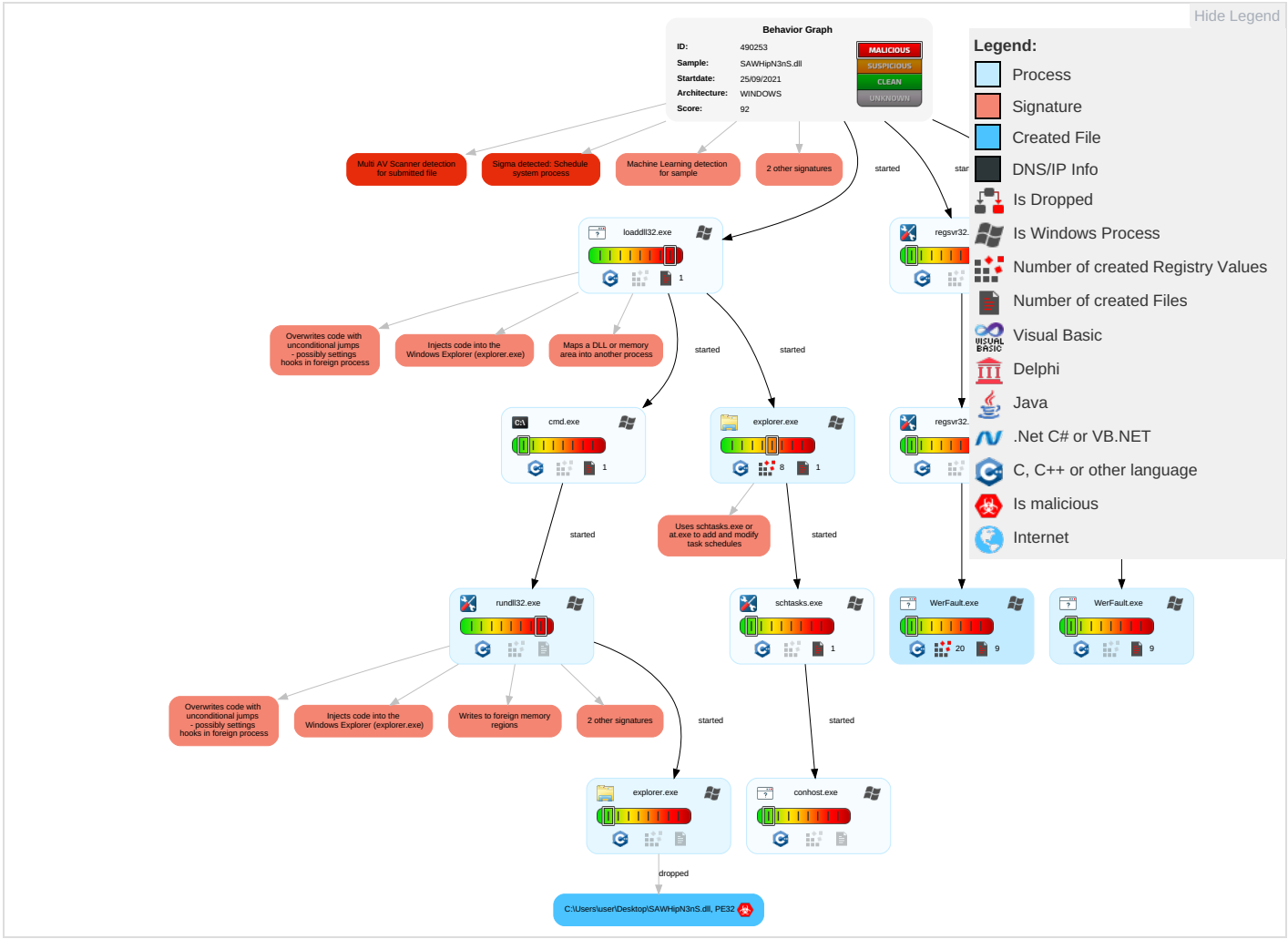
Injects code into the Windows Explorer (explorer.exe)

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 Insecure Network Communica
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 Redirect Ph 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 Track Devic 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	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	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

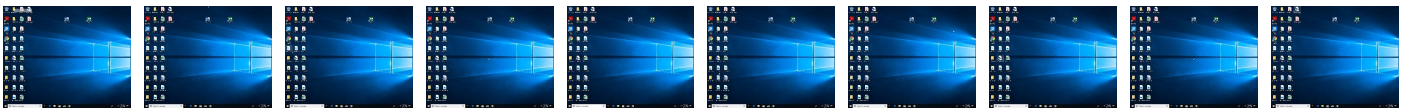
Behavior Graph

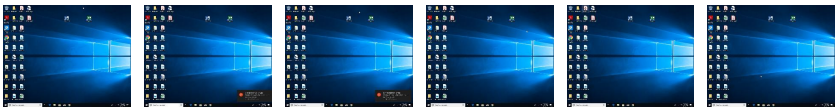


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SAWHipN3nS.dll	51%	ReversingLabs	Win32.Backdoor.Quakbot	
SAWHipN3nS.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\SAWHipN3nS.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

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:	490253
Start date:	25.09.2021
Start time:	10:12:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SAWHipN3nS.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:	34
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: 22.2% (good quality ratio 21.3%) • Quality average: 77% • Quality standard deviation: 26.4%
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
10:13:29	Task Scheduler	Run new task: yyhcsfwg path: regsvr32.exe s>-s "C:\Users\user\Desktop\SAWHipN3nS.dll"

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_2e23c0425775ca197e9a9eceef723eb776aaa0c_7a325c51_11c343eb\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11508
Entropy (8bit):	3.7751782567220458
Encrypted:	false
SSDEEP:	192:Ur75YqzcKb6VZXkH/RS5uGXx3RjetpO/u7slS274ItUP:VEcc6VS/RS5n3jei/u7slX4ItUP
MD5:	8979C3D25F44E2F23B3D5BC5A0E7621E
SHA1:	544CB7C9962FA0070443C7A9AF8804BB6619D74B
SHA-256:	AC7369923A54B4A06BE560740C56C5A44794FCA7010F637E5E31B7BDE2FE3908
SHA-512:	87AD0034BD79D56ECCDD616A9B8305FE123D787BA4DF2DE446439367333E303B0A4297C46FFD4EBBDD58078FE46A7493D7E79D373E0C09637A18846D6F481B3
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.=.1.3.2.7.7.0.6.3.7.0.7.7.6.4.9.2.1.7.....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.=.a.c.1.f.6.d.d.f.-.5.1.0.4.-.4.6.c.3.-.b.e.9.8.-.d.0.b.3.4.1.9.4.7.4.6.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.=.d.3.0.1.e.d.b.d.-.8.c.b.4.-.4.0.5.0.-.b.f.f.6.-.7.5.4.4.4.9.a.d.e.0.1.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.8.b.4.-.0.0.0.0.-.0.0.1.7.-.7.4.0.6.-.4.6.d.f.3.0.b.2.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_2e23c0425775ca197e9a9eceef723eb776aaa0c_7a325c51_1bd5e91d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11506
Entropy (8bit):	3.775045540054189
Encrypted:	false
SSDEEP:	192:ySUzc1b6VtXkH/RS5uGXx3RjetpO/u7sKS274ItUa:yFcx6VG/RS5n3jei/u7sKX4ItUa
MD5:	D3D4DDDB9C374254664A7E4F67BAAC89
SHA1:	D6C94E93DCC92B6F8EC2AF9DFD191228B6D2426B

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_2e23c0425775ca197e9a9eceef723eb776aaa0c_7a325c51_1bd5e91d\Report.wer	
SHA-256:	4F124219A322A45C4519EF06DE254DD25FE7F25982B4002979346E345D7C1EA8
SHA-512:	4E58F9EC996DDCE00A8892FB1B8EA7218249854638A28950E6EBF6B9FE12314D403ABA8356EE4B0BE41718AB4146E387777152559A4895F4AE630C555F4901E5
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.=.1.3.2.7.7.0.6.3.6.1.5.5.6.8.2.6.0.8.....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.=.3.6.3.9.3.b.6.4.-.e.d.5.1.-.4.5.6.5.-.8.1.f.b.-.4.1.2.8.a.6.0.5.f.a.c.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.1.8.4.0.d.b.8.-.1.a.c.4.-.4.e.0.9.-.8.8.b.3.-.3.3.f.a.7.e.0.a.f.0.8.5.....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.a.f.0.-.0.0.0.0.-.0.0.1.7.-.1.7.2.d.-.a.2.a.9.3.0.b.2.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\WER363F.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Sep 25 17:15:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35498
Entropy (8bit):	2.5986676342993458
Encrypted:	false
SSDEEP:	192:2oIfr8oWOb+SJlzZQdooE11qfBwOWud8n3gMWi/px7lZr6pPnG:CooWOb+lKoE1ZM2RWi/j6pG
MD5:	E274944E21CB841F8724BBE241255F1C
SHA1:	73F60C163D8317D9CE4AD0E7CC7D0DB127ECC64F
SHA-256:	43EBE48EA596BE6491D120A0FC26390CE967C93EABC75096B52FAB6034BCDF1F
SHA-512:	81F1BE2F2438563D8821C085B85BFFAFABA81749867AE7667DED172B99D2F8A1F76AF8CAEE09CFD9AEB04D345E1CF1732F601AF2885B21B69390F7A6F05F3E7
Malicious:	false
Preview:	MDMP..... .....YOa.....U.....B.....GenuineIntelW.....T.....YOa.....@..1.....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.....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\WER3D45.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):	8276
Entropy (8bit):	3.6968320838087996
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqfV69uMW6YJFSUigmfJRVSzCpBB89bWhZqBsf0er75jym:RrlsNiqN6o6YbSUigmfJTSHWhZq6ft
MD5:	E1930806C8189D35BFEBCB8822DDF790
SHA1:	2CC8F40EAC341018EDD4653B78E4BC4CF2325E27
SHA-256:	C05DF347002FC437317CD5B7603664D0548CBF2B5BD7C56A013628F53A18B2BB
SHA-512:	4F2C0FB213513135145B003BC8E4A5684B403239CAEB8E9BBCC53DAF54C2C8B6AF0BD38F9CC4283126C79ABD042E0AE0CE2B1206C839F3C0CE5A2BF72A8848 98
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.>.6.3.2.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FD6.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):	4.462360287417202
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI9IuWSC8BeI8fm8M4JkNWFeM+q8XdwWKJY1gd:uITfyfPSNYlJ+MBWqY1gd
MD5:	F20AE3EDACACD672BCDC724F570EA65A
SHA1:	9CE5EC0C0C900FA85EB1BE5A1541064F83C8B82A
SHA-256:	87C0B2C1EC2A62EE84EC105BFCD24AEB667C7D76E39C424B37914596E1D61A89
SHA-512:	0EFF417E26D042766262DBE6625C28C8ADF7BF7D4192BC2F3257882A40CBA18A0AA05483B4BAF41FAE574B163E84388917DABABD438E58A1FA3A9AD1E1FC0A 46
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FD6.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="1182385" />.. <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\WERCE23.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Sep 25 17:13:38 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34890
Entropy (8bit):	2.6351852705018484
Encrypted:	false
SSDEEP:	192:WP8FryeYptE5M/7ZIs7Wud8n3gMWi/N5OrnHFmcnZ:4eYQ5Mzuw2RWi/argcZ
MD5:	97A5CCD8530E124C2F8760DAA1529F45
SHA1:	DC2025701CFB554399910B68894EB9CF6C776A5B
SHA-256:	B71101F7990761C70C693B4A8351C0DC0347FC4ABD115385ABEF9D157D951E31
SHA-512:	50B0B58BD27386BD0194AE10C604583AE71321D45CDA805AE1A26A58D04BA5A635CFC49986E5B9CFA520B28866D9FA09E92D1F269A61320151613956DA9E4AF
Malicious:	false
Preview:	MDMP..... .....XOa.....U.....B.....GenuineIntelW.....T.....XOa.....@..1.....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.....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\WERE054.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):	3.6980257589495324
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiey61d6YRQPSUGgmfJRVSzCpBB89bV7sfqbnm:RrlsNir6P6YCPSUGgmfJTSHVAfqy
MD5:	0F44DE58B9B79EE7D3968774FB1E0874
SHA1:	E75C8525522241351FD3EFA31BF9C66E05BEFE65
SHA-256:	DC5823CC6DF3860EFDFEBF49C961701F9C1F96CCCDA865563ADB67E41C5A656D
SHA-512:	6C48C5BC5B733A5119AE5EA494F6EB87C5FC81958A40477E0F2E971017B865183B1C613531245AB15C733687A61E2F13933DE37A4F5D507DEC4B7F5924992C6E
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.>.6.8.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE4CA.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):	4.459804142176998
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWl9IuWSC8Bx28fm8M4JkNWFv1+q8XdYKJYugd:uITf1fPSNLJdPqYugd
MD5:	16EBBA7C00B171217B49B3443B4F518A
SHA1:	3DDFB683EF469177816168DC4B31526F6A3C70B8
SHA-256:	7E92C57006DDFDDDB7954708A5DCBC723EFF366BB8AD2732C112F720592EAC07
SHA-512:	BDC639AEBF5C17DE53B12E79DEC35342634B3ADA1505671B625DD4017B943C4EFC75C07D9E6B444C5B9938EA8C385573EDE29758F90EBCF228C38F58516733 7
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="1182384" />.. <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\Desktop\SAWHipN3nS.dll	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336237
Entropy (8bit):	2.1754659343483365
Encrypted:	false
SSDEEP:	1536:/IUtVWns2GwmzYSbbz1j+xEXnQud+3VLuoXBYjPYH+ryO3O:/ZVWsP/sSb1ax0A3tDXBYjPYH+ryyO
MD5:	A4387E8ACBEBC6DC20B370617D8DB669
SHA1:	950EA012E5EBFA8AE895B24B74B3A5D138E992FD
SHA-256:	947A5556F8F1891D82666DF499B7C9621511EB5020CFB593DB37ABE198345EB4
SHA-512:	D6BBCE60073A44A9FE8FE6F82E83F8EDD5D8CF510CA8C16E25B422B8C0374B29D3AB346C84441274DB8B73B0185B46B37C258A7079169135947B0B177C7A609
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):	5.500423540479897
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:	SAWHipN3nS.dll
File size:	336237
MD5:	1ff17ce907ce2d98867ec9c78998518e
SHA1:	91818954ba50a5c63b73461af867a8c68958e20e
SHA256:	2dca3e9494cc2b34e8e1d53d1c9b78830ef35cda9473c5a0b8d84ef9bf4ea330
SHA512:	624127ba3261050966a54965542e4dcee2674e171a3073df48c569eaaed578e883e785b1915960084910c255716d2a3190f8392ef0e47367e9ab93730492514
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]

General

TLS Callbacks:	
CLR (.Net) Version:	
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:	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: 6652 Parent PID: 5344

General

Start time:	10:13:21
Start date:	25/09/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SAWHipN3nS.dll'
Imagebase:	0x170000
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: 6664 Parent PID: 6652

General

Start time:	10:13:22
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\SAWHipN3nS.dll',#1
Imagebase:	0x2a0000
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: 6684 Parent PID: 6664

General

Start time:	10:13:22
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\SAWHipN3nS.dll',#1
Imagebase:	0x1170000
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

Analysis Process: explorer.exe PID: 6732 Parent PID: 6652

General

Start time:	10:13:26
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x70000
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: 6752 Parent PID: 6684

General

Start time:	10:13:26
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x70000
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: 6832 Parent PID: 6732

General

Start time:	10:13:28
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 yyhcsfwg /tr 'regsvr32.exe -s \'C:\Users\user\Desktop\SAWHipN3nS.dll\" /SC ONCE /Z /ST 10:15 /ET 10:27
Imagebase:	0xc30000
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: 6840 Parent PID: 6832

General

Start time:	10:13:28
Start date:	25/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: 6888 Parent PID: 936

General

Start time:	10:13:29
Start date:	25/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Desktop\SAWHipN3nS.dll'
Imagebase:	0x7ff771460000
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: 6896 Parent PID: 6888

General

Start time:	10:13:30
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Desktop\SAWHipN3nS.dll'
Imagebase:	0xc30000
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: 6960 Parent PID: 6896

General

Start time:	10:13:33
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6896 -s 644
Imagebase:	0xb00000
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: 6264 Parent PID: 936

General

Start time:	10:15:00
Start date:	25/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Desktop\SAWHipN3nS.dll'
Imagebase:	0x7ff771460000

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: 6324 Parent PID: 6264

General

Start time:	10:15:00
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Desktop\SAWHipN3nS.dll'
Imagebase:	0xc30000
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: 4388 Parent PID: 6324

General

Start time:	10:15:02
Start date:	25/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 652
Imagebase:	0xb00000
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

Code Analysis