ID: 876175
Sample Name: FACT64708.msi
Cookbook: default.jbs
Time: 12:27:38
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

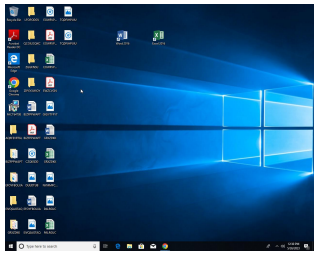
Windows Analysis Report

FACT64708.msi

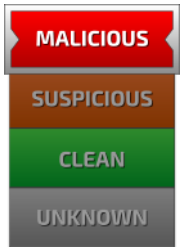
Overview

General Information

Sample Name:	FACT64708.msi
Analysis ID:	876175
MD5:	03fc44504a830..
SHA1:	99927989853f4..
SHA256:	6dfd76c513f8c...
Infos:	



Detection

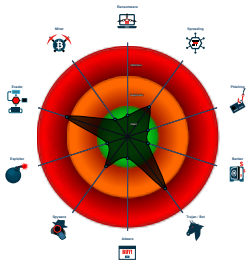


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop...
- Hides threads from debuggers
- Overwrites code with unconditional j...
- May check the online IP address of...
- PE file contains section with specia...
- Queries the volume information (nam...
- Deletes files inside the Windows fol...
- Creates files inside the system direc...
- PE file contains sections with non-s...
- JA3 SSL client fingerprint seen in co...

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6836 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\FACT64708.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6800 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6920 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding EC16BF9ACD034E20C79A272C76FEE245 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Networking

May check the online IP address of the machine

System Summary

PE file contains section with special chars

Hooking and other Techniques for Hiding and Protection

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

Anti Debugging

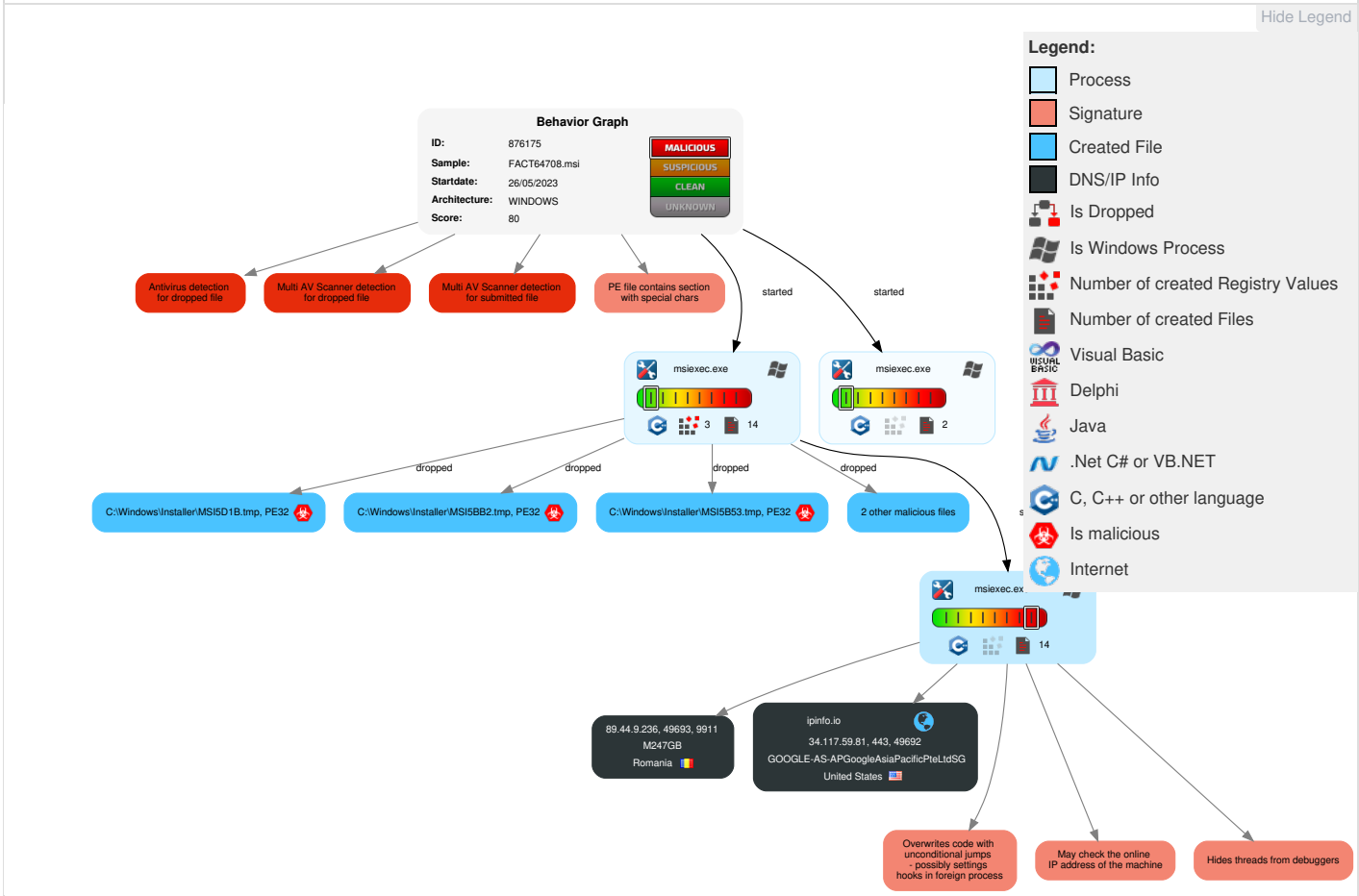
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	Windows Management Instrumentation	1 DLL Side-Loading	1 Process Injection	2 1 Masquerading	1 Credential API Hooking	2 1 Security Software Discovery	1 Replication Through Removable Media	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 1 Peripheral Device Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

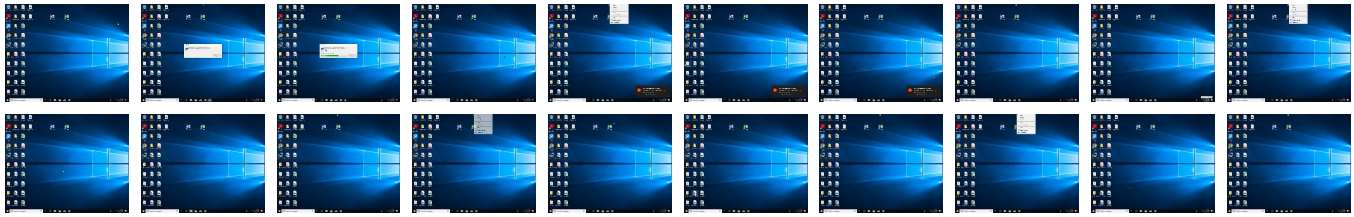
Behavior Graph



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
FACT64708.msi	22%	ReversingLabs	Win32.Trojan.Mekotio	
FACT64708.msi	20%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Installer\MSI5D1B.tmp	100%	Avira	HEUR/AGEN.1360814	
C:\Windows\Installer\MSI5D1B.tmp	100%	Joe Sandbox ML		
C:\Windows\Installer\MSI5A28.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI5A28.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI5AF4.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI5AF4.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI5B53.tmp	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Windows\Installer\MSI5B53.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI5BB2.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI5BB2.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI5D1B.tmp	48%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipinfo.io	34.117.59.81	true	false		high

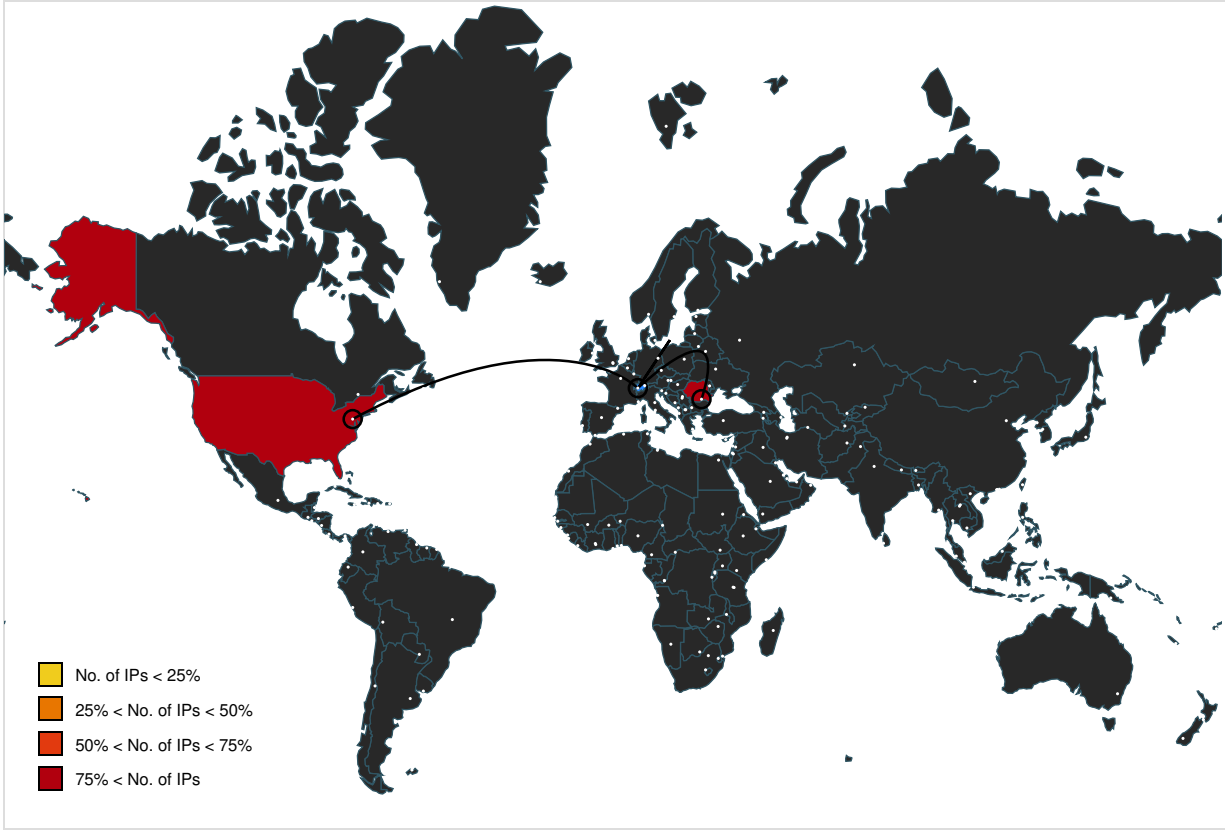
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/json	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/missingauth	json[1].json.2.dr	false		high
http://https://www.advancedinstaller.com	FACT64708.msi, MSI5AF4.tmp.1.dr, MSI5A28.tmp.1.dr, MSI5B53.tmp.1.dr, MSI5BB2.tmp.1.dr, 3e573a.msi.1.dr	false		high
http://https://www.thawte.com/cps0/	FACT64708.msi, MSI5AF4.tmp.1.dr, MSI5A28.tmp.1.dr, MSI5B53.tmp.1.dr, MSI5BB2.tmp.1.dr, 3e573a.msi.1.dr	false		high
http://https://www.thawte.com/repository0W	FACT64708.msi, MSI5AF4.tmp.1.dr, MSI5A28.tmp.1.dr, MSI5B53.tmp.1.dr, MSI5BB2.tmp.1.dr, 3e573a.msi.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.117.59.81	ipinfo.io	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
89.44.9.236	unknown	Romania		9009	M247GB	false

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876175
Start date and time:	2023-05-26 12:27:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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
Sample file name:	FACT64708.msi
Detection:	MAL
Classification:	mal80.troj.evad.winMSI@4/13@1/2
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WMIADAP.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com

Simulations

Behavior and APIs

Time	Type	Description
12:28:35	API Interceptor	1x Sleep call for process: msiexec.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\json[1].json

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	291
Entropy (8bit):	4.8967469240357655
Encrypted:	false
SSDEEP:	6:t9zQZQYReWa6dmXJt9pff+LZTL9H5sh76W35jY:tSZQYReF6UJtb+LZTJ+hR5k
MD5:	040A92AD0D71B75A0D1B5A297F0494CB
SHA1:	7817841B5594768C433D5BA8C60219B512EBEF71
SHA-256:	4F216FD803061045D0E9B593D4C68F0AAFED3877110B4B3616503F1C359B3D58
SHA-512:	51EF832E7CC8DC4A4F043F75C28C2E80A56C8A01D5DA4F13A11619627F08E880A2D888F2305C5897B720EEACB4DD22C35266032D591B5FE33740D06BB0ED35(
Malicious:	false
Reputation:	low

Preview:	{. "ip": "84.17.52.45",. "hostname": "unn-84-17-52-45.cdn77.com",. "city": "Z.rich",. "region": "Zurich",. "country": "CH",. "loc": "47.3876,8.5207",. "org": "AS212238 Datacamp Limited",. "postal": "8005",. "timezone": "Europe/Zurich",. "readme": "https://ipinfo.io/missingauth".}

C:\Windows\Installer\3e573a.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {99C5E16F-1B9A-4372-8446-788EB651135D}, Number of Words: 10, Subject: window1, Author: window1, Name of Creating Application: Advanced Installer 18.1 build 4fb1edbd, Template: ;1033, Comments: window1, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	6022656
Entropy (8bit):	7.898523988528081
Encrypted:	false
SSDEEP:	98304:PYebmgplKxsvkwtfTZ6Of7Ok2NKJTNkcDW1FqjId56KahqOxYmNrwC8ICpqtMHA:ragplKxsvkwtfF56iTNkc6FqjId1OxbP
MD5:	03FC44504A830C0BDE2155D2343C07BD
SHA1:	99927989853F4D8B4A1180F25C48C37A3C763F65
SHA-256:	6DFD76C513F8C4216B7C0EFEAB797F22DB13BB265FAFFFBB69D735B64801C4A8
SHA-512:	6B12E4E6BC274722383F0148E80281C486B53EFB5EADF598359D8AFD2A9497CCFF3E459B7EA2608ABF5FB0DFF97426684DCC1920766680674A83AD9E571C633
Malicious:	false
Reputation:	low
Preview:	.....>.....\.....~..... .....L*..M*..N*..O*..P*..Q*..... .....a.....1...%..... ...!..."...#...$.../...0...'...(...)...*...+...,...-.....2...6...@...3...4...5...8...7...>...9...:...;...<...=...J- ..?...A...B...F...C...D...E...i-..._...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[..\...]...^.....`...b...s...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...t... E*..u...v...w...x...y...z...

C:\Windows\Installer\MSI5A28.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385960
Entropy (8bit):	6.405611935418631
Encrypted:	false
SSDEEP:	6144:krDow+ZsrLg3bmfKlGzlqSqYf+SAO/VKEPM5TiyX:Mowv43bqKlRH1Vq9iyX
MD5:	E12C5BCC254C953B1A46D1434804F4D2
SHA1:	99F67ACF34AF1294F3C6E5EB521C862E1C772397
SHA-256:	5316CFAE8B4D28AB7CBC5CAB60E27B0C0F5A3210A921A4B0560769C5021C911B
SHA-512:	9A61AA00B651FC616CD09D28F4A6B872889A026C61D818595A82C58FDFF187E3AD57916C2B8690D1E7016D73A05435E13A85758917CFB89029B34C4A1685AA0E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....?.....C..... C.....C.....C.....Rich.....PE..L....Y`.....!.....ZV.....m.....@.....`l.....4t.....0.....>..8...p..... .....@..... .....text...O..... ..`.rdata.....@..@.data.....x.....@....rsrc...0.....@..@.reloc...>..... @.....@..B..... .....

C:\Windows\Installer\MSI5AF4.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385960
Entropy (8bit):	6.405611935418631
Encrypted:	false
SSDEEP:	6144:krDow+ZsrLg3bmfKlGzlqSqYf+SAO/VKEPM5TiyX:Mowv43bqKlRH1Vq9iyX
MD5:	E12C5BCC254C953B1A46D1434804F4D2
SHA1:	99F67ACF34AF1294F3C6E5EB521C862E1C772397
SHA-256:	5316CFAE8B4D28AB7CBC5CAB60E27B0C0F5A3210A921A4B0560769C5021C911B
SHA-512:	9A61AA00B651FC616CD09D28F4A6B872889A026C61D818595A82C58FDFF187E3AD57916C2B8690D1E7016D73A05435E13A85758917CFB89029B34C4A1685AA0E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse

Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....?.....C..... C.....C.....C.....Rich.....PE..L....Y`.....!.....ZV.....m.....@.....`l.....4t.....0.....>..8...p..... .....@..... .....text...O..... ..`.rdata.....@..@.data.....x.....@....rsrc...0.....@..@.reloc...>..... @.....@..B..... .....

C:\Windows\Installer\MSI5B53.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385960
Entropy (8bit):	6.405611935418631
Encrypted:	false
SSDEEP:	6144:krDow+ZsrLg3bmfKlGzlqSqYf+SAO/VKEPM5TiyX:Mowv43bqKlRH1Vq9iyX
MD5:	E12C5BCC254C953B1A46D1434804F4D2
SHA1:	99F67ACF34AF1294F3C6E5EB521C862E1C772397
SHA-256:	5316CFAE8B4D28AB7CBC5CAB60E27B0C0F5A3210A921A4B0560769C5021C911B
SHA-512:	9A61AA00B651FC616CD09D28F4A6B872889A026C61D818595A82C58FDFF187E3AD57916C2B8690D1E7016D73A05435E13A85758917CFB89029B34C4A1685AA0E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....?.....C..... C.....C.....C.....Rich.....PE..L....Y`.....!.....ZV.....m.....@.....`l.....4t.....0.....>..8...p..... .....@..... .....text...O..... ..`.rdata.....@..@.data.....x.....@....rsrc...0.....@..@.reloc...>..... @.....@..B..... .....

C:\Windows\Installer\MSI5BB2.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385960
Entropy (8bit):	6.405611935418631
Encrypted:	false
SSDEEP:	6144:krDow+ZsrLg3bmfKlGzlqSqYf+SAO/VKEPM5TiyX:Mowv43bqKlRH1Vq9iyX
MD5:	E12C5BCC254C953B1A46D1434804F4D2
SHA1:	99F67ACF34AF1294F3C6E5EB521C862E1C772397
SHA-256:	5316CFAE8B4D28AB7CBC5CAB60E27B0C0F5A3210A921A4B0560769C5021C911B
SHA-512:	9A61AA00B651FC616CD09D28F4A6B872889A026C61D818595A82C58FDFF187E3AD57916C2B8690D1E7016D73A05435E13A85758917CFB89029B34C4A1685AA0E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....?.....C..... C.....C.....C.....Rich.....PE..L....Y`.....!.....ZV.....m.....@.....`l.....4t.....0.....>..8...p..... .....@..... .....text...O..... ..`.rdata.....@..@.data.....x.....@....rsrc...0.....@..@.reloc...>..... @.....@..B..... .....

C:\Windows\Installer\MSI5CBC.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	5.430964541776944
Encrypted:	false
SSDEEP:	12:EgkgwGcYGqVXjOvl/HdftEuzWot3DEaFVrHDFuyHoAnF9c2LCHMapUerHDkBF6z5:sg1jOvqu6aD3FGwFCOaZpUeuFP3gxP
MD5:	DFD2E812A18033D5509D6CF512ABDFA1
SHA1:	96BEA2FFD51F2F955B861202ED03CCA656AFD7C4
SHA-256:	349749063EF9F847A3B30DE5CDDA8FDD82B1BD70C212B0D44335091A65298C51
SHA-512:	901EC55D51CB0F063D9F73CF5D52E40B977539DE7F185C594804816D35293D2EBA6DC2168765AA9479D9EE586E2CDA594BDB254F66DC1098290A38ED3FD942
Malicious:	false

Preview:	...@IXOS.@.....@.c.V.@.....@.....@.....@.....@.....@.....@.....&.{391D3F83-F57B-4C37-B67D-2C3B478539D3}..window1..FACT64708.msi.@.....@.....@.....@.....@.....&.{99C5E16F-1B9A-4372-8446-788EB651135D}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....window1.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration...@.....@.....@.]....&.{834560BB-AEF7-41F4-8F91-5C709439D783}/.C:\Users\user\AppData\Roaming\window1\window1\.@.....@.....@.....@.....&.{9AEF0A6B-1957-4029-A776-FFD21A9C24C0}$.01:\Software\window1\window1\Version.@.....@.....@.....@.....@.....&.{03700A98-4FE2-4FD5-B1F2-05F76E7E670A}..C:\ProgramData\5.txt.@.....@.....@.....@.....CreateFolders..Creating folders..Folder: [1]"./.C:\Users\user\AppData\Roaming\window1\window1\.@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]...@.....@.....@.....C:\ProgramData\.. .1\COMMON~1|CommonAppDataFolde

C:\Windows\Installer\MSI5D1B.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	5430272
Entropy (8bit):	7.959731815381645
Encrypted:	false
SSDEEP:	98304:QmgplKxsvkwtfTZ6Of7Ok2NKJTNkcDW1FqjId56KahqOxYmNrwC8ICp:pgplKxsvkwtfF56iTNkc6FqjId1Oxb8
MD5:	9736B1A5AC470116328B9584DF71F894
SHA1:	77AA1DDBC5CC4498E2E50AD6CE0E425F880BAC97
SHA-256:	4EF0B46B027AB3F1471ACAA34729ABEA1E510566004AD294AFAB6AA4A6486493
SHA-512:	6323297D872F608816F0ACBA675E441BB21011E1DAB979030EA903ACF6B8FBBAA9BC0EBF4A6713BFCA16846D370FD04854BC914EFE3A10930A5150F8A70E44FC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....gnd.....<W.....PW...@.....P.....0y.....}.....0..$..... ..px.....-)JCkFdG..V..... ..`tUKiKjI(.;....W..... ..`>FM3ptLM.....PW.....@...o[K?gVK3.x...pX.....QX]dab$M.7....X.. .....@...3MpwCE=\.....0Y.....@...i%>mQ21J.....@Y.....@..@zG.-OP"_E....PY.....@..@N/Q"D33it....`Y..... ..`/1Noi&/e.....px.. .....@...H)8.=c%s@.R...x...R..... ..`]K1?IQ),$....0.....R.....@..B.....

C:\Windows\Installer\SourceHash{391D3F83-F57B-4C37-B67D-2C3B478539D3}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.768760985100547
Encrypted:	false
SSDEEP:	12:JSbX72Fj5AGiLlIHVRpiBh/77777777777777777777777vDHFGU1Lp7l0i8Q:JvQI5ASF
MD5:	6F1766C739CC71014660EDB94C55B05B
SHA1:	5B390204B4DCC92D44C79978A61AE33D1F8BE002
SHA-256:	762561EC2CE9C880B42035172C21BD53D34E9C4DFBE92C824D83D7D489C5B14C
SHA-512:	0E265EE873FB12D1CC31F87439BCC54CAB728EF424938E30E10C517CF36C39632A010EDE3D90F5ED66A0B8622F12F9116691CD30063AE21892D214376068CEC
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.223596486084734
Encrypted:	false
SSDEEP:	48:6oruDM+CFXJpT5NM4/tMSCWAECiCyaoG0MSCcT2:LrVRT4qi1ECTnB
MD5:	F091DDDBA714EF7B3D0C7E83A88DFC42
SHA1:	961D33CEDF0FD59C73A5E06177BEC29D145701D5
SHA-256:	81EF78D941207840609ABBF8BCB5DD24D7F9D22CC13BB72A8171BBD6EE9B842E
SHA-512:	F713A1BECE3889D095E5C0BAF8D3343C5C64AF0FD39DCA0EFE1D5DC374BA2D6C59E7DE1CD65E7AADC9BCC837F23E199AC4EAF9EDDE9B71B86119BDFF5FEE6E38
Malicious:	false

Preview:	.....>..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	79122
Entropy (8bit):	5.2820991353412
Encrypted:	false
SSDEEP:	192:jmXs969ozNSkk3peTBYeHt0tfol9qsjl0urmwYyi3:yXs9UogeWeH29qclhmwYyi3
MD5:	0F8E7E29DFD57561C000A643111249AA
SHA1:	AF9C1EF33092ED1FA7C83737AD4D5E625E8EB03D
SHA-256:	20E7D66BF3CC068B3CF33E3A439A3D9C675816C9DF6C1E14840084E8945850A6
SHA-512:	77665EC98BE582E70EEFBE6B3882BDA8B4445DABE1861B8FC0B84A3940C5B381C53A9FB924CE3739DFB4FEF0DD94641B77B049F5142453EF2F88EAC32329E1A2
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 03:22:38.143 [320]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.159 [320]: ngen returning 0x00000000..07/23/2020 03:22:38.222 [3748]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.237 [3748]: ngen returning 0x00000000..07/23/2020 03:22:38.284 [64]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.300 [64]:

C:\Windows\Temp\~DF0B3191997363l9C6.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	81920
Entropy (8bit):	0.11032480089406914
Encrypted:	false
SSDEEP:	24:+pGSpYTxkrapWpUipVkrapWpGkrapWpUipVkrapWpeAEVkryjCyKpRV2BwGIArmQ:+CTeMSCpMSCWAECiCyaoGnq5
MD5:	0C3FD0990472F91DFE16EBEBD0223A9E
SHA1:	B7874C1367C579C0636B34F3AD102B8940206192
SHA-256:	D10108090EF28311493E15F235D747D5314030DDA129AE1C3CD53632D3718766
SHA-512:	6FF535D72D7A51124622A1DD17A7DF40086AC3158B7482C14A9DB1505E659E916AB23BD05ABA47B67D639AF14A59CF0C8FEF1F038747FFE7DD64DCD25303414C
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF15E57EF7A6220754.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07120612824116142
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOG7PAZwQekDYtiVky6l7:2F0i8n0itFzDHFGU1Yb7
MD5:	233821E6E7EA055562D01EB0E131F060
SHA1:	AF8EA0EF631A62B57DE9B4FBA4958EED62441C0F
SHA-256:	B58A16F69A1AA9C80FBD02B0F282EBBCF9C3EE5497AF01DF15DF5EFE485ABF18
SHA-512:	B5432B9DCF7DF7608FD95C384ECF974A18D8C045063BE7E275DD3B1FCFAE7A7D9A88B6C30FF264DFD3CD925453937B72B9AEFFEAA71ECBD9B04201BCA8723862
Malicious:	false
Preview:	....

Static File Info

General

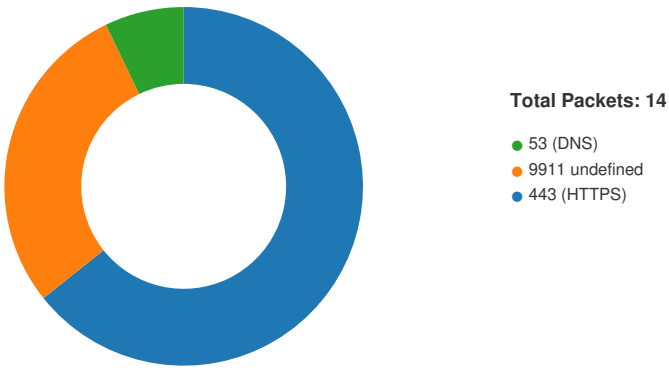
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {99C5E16F-1B9A-4372-8446-788EB651135D}, Number of Words: 10, Subject: window1, Author: window1, Name of Creating Application: Advanced Installer 18.1 build 4fb1edbd, Template: ;1033, Comments: window1, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Entropy (8bit):	7.898523988528081
TrID:	• Microsoft Windows Installer (77509/1) 52.16% • Windows SDK Setup Transform Script (63028/2) 42.42% • Generic OLE2 / Multistream Compound File (8008/1) 5.39% • Corel Photo Paint (41/41) 0.03%
File name:	FACT64708.msi
File size:	6022656
MD5:	03fc44504a830c0bde2155d2343c07bd
SHA1:	99927989853f4d8b4a1180f25c48c37a3c763f65
SHA256:	6dfd76c513f8c4216b7c0efeab797f22db13bb265fafffbb69d735b64801c4a8
SHA512:	6b12e4e6bc274722383f0148e80281c486b53efb5eadf598359d8afd2a9497ccff3e459b7ea2608abf5fb0dff97426684dcc1920766680674a83ad9e571c6339
SSDEEP:	98304:PYebmgplKxsvkwtfTZ6Of7Ok2NKJTNkcDW1FqjId56KahqOxYmNrwC8ICpqtMHA:ragplKxsvkwtfF56iTNkc6FqjId1OxbP
TLSH:	1156231279C686F5C0BE42B41A17BEAE35B56A34C3B140AB62C85EDF38F37D05671983
File Content Preview:	.....>.....\.....~.....

File Icon

Icon Hash:	2d2e3797b32b2b99

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:35.433054924 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.433145046 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.434598923 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.439356089 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.439404011 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.514266968 CEST	443	49692	34.117.59.81	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:35.514359951 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.694101095 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.694183111 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.695022106 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.695111990 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.696835995 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.744292974 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.832495928 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.832679987 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:35.833687067 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.836333036 CEST	49692	443	192.168.2.4	34.117.59.81
May 26, 2023 12:28:35.836369991 CEST	443	49692	34.117.59.81	192.168.2.4
May 26, 2023 12:28:38.852535009 CEST	49693	9911	192.168.2.4	89.44.9.236
May 26, 2023 12:28:38.885492086 CEST	9911	49693	89.44.9.236	192.168.2.4
May 26, 2023 12:28:38.885910988 CEST	49693	9911	192.168.2.4	89.44.9.236
May 26, 2023 12:28:39.328989983 CEST	9911	49693	89.44.9.236	192.168.2.4
May 26, 2023 12:28:39.329049110 CEST	9911	49693	89.44.9.236	192.168.2.4
May 26, 2023 12:28:39.329176903 CEST	49693	9911	192.168.2.4	89.44.9.236
May 26, 2023 12:28:39.881467104 CEST	49693	9911	192.168.2.4	89.44.9.236
May 26, 2023 12:28:39.930834055 CEST	9911	49693	89.44.9.236	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 12:28:35.401787996 CEST	59683	53	192.168.2.4	8.8.8.8
May 26, 2023 12:28:35.424916983 CEST	53	59683	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 12:28:35.401787996 CEST	192.168.2.4	8.8.8.8	0x62ab	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 12:28:35.424916983 CEST	8.8.8.8	192.168.2.4	0x62ab	No error (0)	ipinfo.io		34.117.59.81	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ipinfo.io

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 6836, Parent PID: 3528

General

Target ID:	0
Start time:	12:28:28
Start date:	26/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\FACT64708.msi"
Imagebase:	0x7ff7394b0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6800, Parent PID: 576

General

Target ID:	1
Start time:	12:28:29
Start date:	26/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7394b0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	79028	94	30 35 2f 32 36 2f 32 30 32 33 20 31 32 3a 32 38 3a 33 30 2e 31 32 34 20 5b 36 38 30 30 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	05/26/2023 12:28:30.124 [6800]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FF8759DBEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FF8759DBBC6	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **6920**, Parent PID: **6800**

General

Target ID:	2
Start time:	12:28:30
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding EC16BF9ACD034E20C79A272C76FEE245
Imagebase:	0xd80000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\52612023	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4887A36	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly