ID: 623825
Sample Name: 3GJ6S3Kwnb
Cookbook: default.jbs
Time: 21:02:38
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

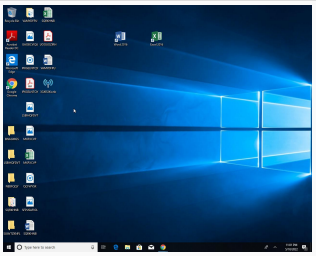
Windows Analysis Report

3GJ6S3Kwnb

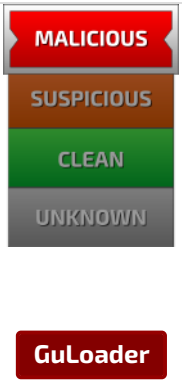
Overview

General Information

Sample Name:	3GJ6S3Kwnb (renamed file extension from none to exe)
Analysis ID:	623825
MD5:	6c6a52c18f0ca2…
SHA1:	9b32a592e54100.
SHA256:	cbd91a64900eac..
Tags:	exe GuLoader
Infos:	



Detection



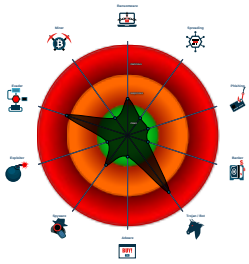
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- 3GJ6S3Kwnb.exe (PID: 3256 cmdline: "C:\Users\user\Desktop\3GJ6S3Kwnb.exe" MD5: 6C6A52C18F0CA26D357F2B4430F31568)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.773047400.0000000003300000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

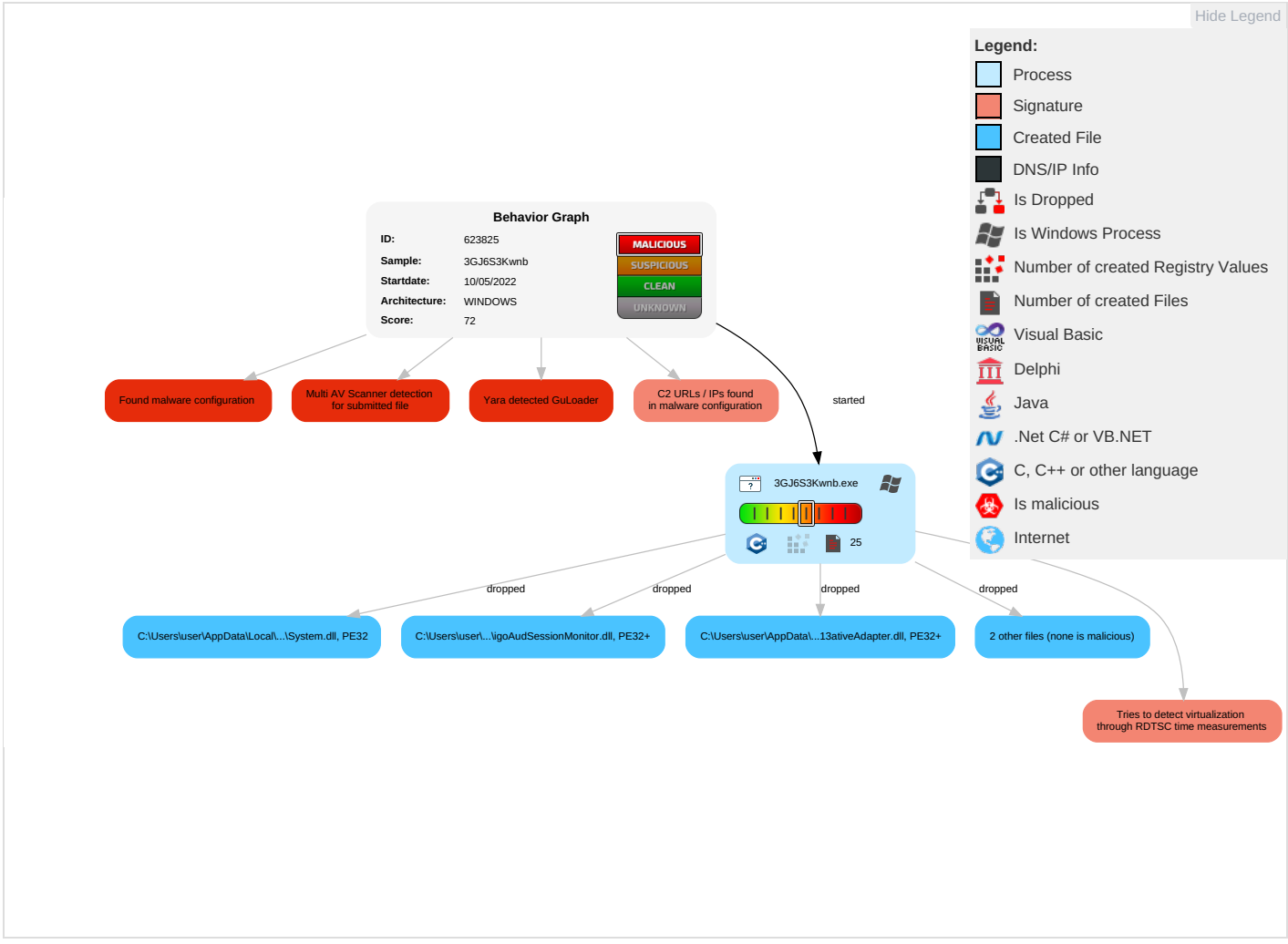
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

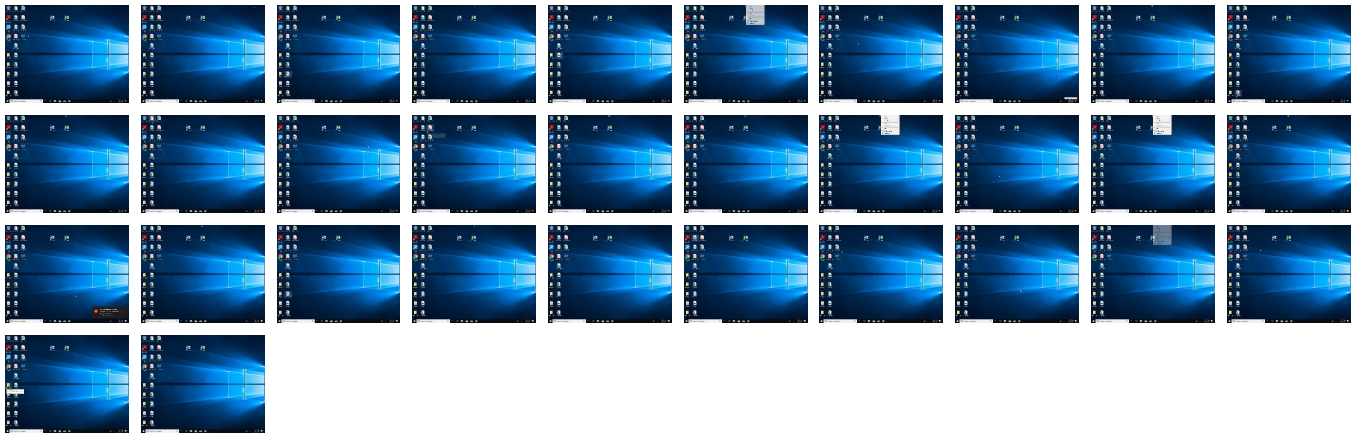
Behavior Graph



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
3GJ6S3Kwnb.exe	42%	Virustotal		Browse
3GJ6S3Kwnb.exe	24%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://bprbeulentechnik.ch/loader/amagidom_VRCLkUVry246.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	3GJ6S3Kwnb.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623825
Start date and time: 10/05/202221:02:38	2022-05-10 21:02:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3GJ6S3Kwnb (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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:	mal72.troj.evad.winEXE@1/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.9% (good quality ratio 61.7%) • Quality average: 88.6% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, time.windows.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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\Temp\Airplane_6.bmp

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	6869
Entropy (8bit):	7.844036691616615
Encrypted:	false
SSDEEP:	96:BSTzREW0VVUFRpw7uGkoTRs6iWOZnUhu+LRX6Xi/CwUxLekFFbzUVUL3mBXooPCn:oXRsVaEdDtZiFZn3+LRrmcUXLuCDDvoi
MD5:	B64BD3B79B7C8E73D671029057DB3AF5
SHA1:	FF782EE8498DA70E9032E5FB7C9219BB1F6BC877
SHA-256:	DC980E21E0D964FF2687706568CB9D017D33478AD42DE8AFE5734E7DA29EC267
SHA-512:	23B1A2A1A7BDE408F35412DCE9DD6ADD4E09DE990365C8B517ED073382D686FD90733EB83F4C04668702BD3122347F11E78DDA0524EDFCFD1CE078B39DAC48D
Malicious:	false

Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(...(...(...(...(...(.....j..>..a.....I.....|A./.E.~..u...4.8...7.#....8P..z....?>..q./.....t...V|A99.....\....f....L.....|...*..4[N1.. s^..Eh....r...7.N?...>u..a..B.u.....[.. ....~.O.*?....{.A...g...zx..._..%Y.2..j.....*.....&..X.[.I.6uV.<..;._..sW:/.....z...1..(.....H..s....5.c

C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_SL.chm	
Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	45599
Entropy (8bit):	7.437630592326386
Encrypted:	false
SSDEEP:	768:ISQxjGPaR23xDPH/dw1P3MpowGMm9eKVg79y/cTu8wN5WIOmpGKM:IJjGPa2Dw1PWowzm9Wy/78K5rOaGH
MD5:	EE71A8FD316B4EFF843518B31B3D28C2
SHA1:	292A7ABE9EFE502336417EC613FEE0389FAECF1A
SHA-256:	5A82B5B6332F3CC60CE7E831DA08A486E81A9BA0C5477E4A694754F659A3FC9A
SHA-512:	718320C384787EF374A2A20E8058C04248952891973D146A7F88000892BBDD53976C54DC724519A1C5BC812A62677BC720EE3F1453818D478F2F6DDEFABBEDBC
Malicious:	false
Reputation:	low
Preview:	ITSF....`.....&..'.....|.{.....".....|.{.....".`.....x.....T.....ITSP....T.....j..}.!.....".T.....PMGL0...../..../#IDXHDR.. ...../#ITBITS..../#STRINGS...u.a./#SYSTEM..n.S./#TOPICS.....@./#URLSTR...@.5./#URLTBL...P.p./#WINDOWS...a.L./$FlftiMain...v..../$OBJINST...[.../$WWAssociativeLi nks/..../$WWAssociativeLinks/Property...W../$WWKeywordLinks/..../$WWKeywordLinks/BTree...-.L./$WWKeywordLinks/Data...y4./$WWKeywordLinks/Map...-../$WW KeywordLinks/Property...7 ./Advanced_Phone_Operations.htm..k.l./Audio_Services.htm..W.e./Authorization_Options.htm..<.R$/Bluetooth Win7 Vista Suite help.hhc...W .Z$/Bluetooth Win7 Vista Suite help.hhk...1.../Bluetooth_Devices.htm.....V./Bluetooth_Devices_files/.../Bluetooth_Devices_files/colorschememapping.xml...=.:%/B luetooth_Devices_files/filelist.xml...B.['/Bluetooth_Devices_files/themedata.thmx..... ./Bluetooth_Settings.htm...d..\./Bluetooth_

C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	
Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	526456
Entropy (8bit):	6.008806658212827
Encrypted:	false
SSDEEP:	12288:5sxYL+kJmoPdVp6s3EJBjCvuF17+2NdJfh:5sxwSoPdVoBjCvuF17+2NdJfh
MD5:	52672A1E48BC8BE4035D8A4F345DFE44
SHA1:	4F7EB09FF33DFACE6CE24BEB33E51D1DA5A3ABA1
SHA-256:	87BA988A4858079CADCA5EAA760482CC5F1F05830EE62BBC5FDD9BF7B181F0D0
SHA-512:	4F589CE3FC97F1DBDB575510924B5AEA58061B2D95F909456ACDB170414282A081C18CA9945E604FBCE6F17D626B02B178E66294927C5350B91072357DABAEF
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T1...P.F.P.F.P.F7..F.P.F.P.F#Q.F7..F.P.F7..F.P.F7..F/P.F7..F.P .F7..F.P.F7..F.P.F7..F.P.F7..F.P.FRich.P.F.....PE..d.....IE.....".....$.....a.....0.....x....@.....0.....P.....`.. .....x.... .....p.....(.....text...L".....$..... ..`.data...0....@.....(.....@....pdata.....`.....0.....@..@.rsrc..... .....@..@.reloc..$.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe	
Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	68712
Entropy (8bit):	5.747257952291664
Encrypted:	false
SSDEEP:	768:7gR74zF0we+AyurPeX85DoCAb74WhHN9rOzOY4BsPjFjNafDGmhK:7gRMHebrPesdoCAvbhH/mRBjNv
MD5:	0D24B5089C4D15316A65E9250A9069BD
SHA1:	B8213016A9BCF8A3FF79B0CB140D969FC4005AEA
SHA-256:	F90D525CDCF3E3743B7BFC93B5EEA645CFF5CEAE9AF351B8A2B46521ED5B8684
SHA-512:	A8FA53744FEB5CE044FDB6A3311BA5D60DC923E4A2A375955C33C3971161C4CDDA100C66413DDB5AF509AE6AF4E7D9260223BC36288D48452022624D2B2BB39

Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A;...Z~..Z~..Z~..W2{..Z~.W2z..Z~.W2}..Z~.W2...Z~..".DZ~..Z...Z~ ..3w..Z~..3...Z~..Z..Z~..3|..Z~.Rich.Z~.....PE..d...a..`.....".....~...v.....q.....@.....0...../...`.....X.....4.....h.... .....p.....0...(...0..... .....text....|.....~..... ..`.rdata..6S.....T.....@..@.data...h.....@....pdata..4..... .....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\NativeAdapter.dll

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	115840
Entropy (8bit):	6.055822744229893
Encrypted:	false
SSDEEP:	1536:aGAyFy2NpZ/wrdGlZuZ/X6HMnsOf5OlWNCA:yrdaAZX6HMnsW5OlqCA
MD5:	3CA31E349771C8E93AE7A7B57C98D7D5
SHA1:	5ABB06F1D6E3269FDFE006F7FB9B820B1253E7B0
SHA-256:	F2C59C276665763086ADD13ACA88FB07BE4C1DE8754145552A8AA88DCC5E403B
SHA-512:	E344F09DFDD80DE93C938E6B5BDB96E257D59F509631B8A3C3A8E75D73567976ED4471EADF8EA8A29F9F8226C8020D7FD2FA46B2B90D5B0DA6FDD179775AD 38
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....4.....[.....^.....K.....L.....\.....Y....Rich..... .....PE..d.....N....." .....j...H.....q.....H.....@.....x.....(.....X.... .....H.....text...?c.....d..... ..`.nep....p.....h..... ..`.rdata..\5.....6...n.....@..@.data.....@....pdata.....@..@.rsrc.. .....@..@.reloc..x.....@..B..... .....

C:\Users\user\AppData\Local\Temp\REINSPECTED.lnk

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	866
Entropy (8bit):	2.9094288868917673
Encrypted:	false
SSDEEP:	12:8gl0IsXowAOcQ/tz+7RafgKD+HBXi8g/3NJkKAd4t2Y+xIBjK:8XLDaRMgK6Hx949HAv7aB
MD5:	055BD989D013AA790C0B5FAFE457AF72
SHA1:	902502F2E1C1988A901CD8643F108F2F69197023
SHA-256:	9DF1F752DA3F94A16C961FC5023C3925C94DEB091B7E309D51791671394C88F4
SHA-512:	9F4A85A396A70E1CFC0D4C524C99AB98A014EAF83B31B08791B645415EFBC8B8F35C669B22E9BF97F5885267A9749CC7515C444BBA772E49D3CAA96CB7600D 2
Malicious:	false
Preview:	L.....F.....+....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....j.o.n.e.s.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp..:..... .....T.e.m.p.....h.2.....Bedmte139.exe.L.....B.e.d.m.t.e.1.3.9...e.x.e.....\.B.e.d.m.t.e.1.3.9...e.x.e.....(.....!^".`G ...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\Velsespladser5.tmp

Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	data
Category:	dropped
Size (bytes):	85704
Entropy (8bit):	6.5058103756231835
Encrypted:	false
SSDEEP:	1536:YFq7W01QLwtoPeiWHGekz6uF2+VQdDLFdVvVRjCqrcf:kr01QLwm2fg6t2QdDpdVdM
MD5:	024442982DB5BCEA734C31B2D3D2A25C
SHA1:	F1D5EDB880CE04191E442F5A472081B263809994
SHA-256:	E176A6327774C84E9BB6AD61156A637CBFFAEB7DEABEBBDE01274C2964125A0E
SHA-512:	8AC7AF0B0208226DB8B46D18BAFF949ED3E2B65D9CFEC80BE3CCB5F113B857AC25288A056A17F74C1809469A571F93BF316DC157B02373EE42571C3A58BD09 0
Malicious:	false

Preview:	..)?:tWO.....F.....].C. As..i....$..H..f7g.....+.5[.....i...9bmo....G...5.f.W....%lZ.....K*.t..w.o&.....<...).gf7A2O.qV.....vZ..o. ...K.f..N.>Q.T.Q..^.....WY;z..U....y 10...dd8p....`MC....W]+..4.Ar%..B....x.{O..'...=..p..i..>x#.z..3...ae..?...`.....E..E.fa..B..]9$k.wNb78>o...{OZ.F.2...I[.'....vu...4%..I.B.....[.Nc..J>..,.Z.H..4.N.....1....=....g%.v...<. v..!M.\P..8..c...h...wShkR.'.8r..Y.vz....(..r.....Z..(....=.$..d&..3..9/.n&M.hBAs.J~2>.k.G.at...a.x..R.L... .U..:."L..7..O(...{.....;....}....~..K.....(I...*).~.Pt.O..#r_z...GQ..%s....i..2P.l.].. [.f^.4..w....#..../T....'.G....._.....(.....Q...3p.!E..nz....e...E..H...t...0s+6!..g.`..H. h..as.HL.....Tj..}...U.;...~. f.O4..R.&.0~...Y.E..n'Ri...k..qq..y.WgC....VTw`zW6m.*.XK!..[l:}=.nP ....M.....YO_.$/2=..V...d.>./...).K6....C.oO+.w.\)+<...~>....&.....)8.J.....P.....i.....a.9....P.6....X..GEYpH...9q8vP@6.....v1Wm.....ht..z/....0.C2.....9...t4f

C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll	
Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31712
Entropy (8bit):	6.3433279275707894
Encrypted:	false
SSDEEP:	384:eRg4IisNrETyVJqYgYhqRCMKOBQf0vSjcGrnMLWN/bptUkVXrnMQJK2TKrsBvdX9:e1eVC7s0vxGrn8WlbokVXrE2eooW
MD5:	ED2D8072113DC5CBE99A02B268754438
SHA1:	A39CD1298F70D4056835679C8E65A6668251B5DA
SHA-256:	F52203161DBD387CAD34CEA1B6551F238ACBC092D85AB1A58626BF32636D80C0
SHA-512:	B2BE621DAC9F3929C680C2F9BCF0652E1A6F0887A7099A8F74E565DB51246FDA8719049AF8A6F1A0DB811059DD8D979FB95F4D523C375EB154F82942ED26775
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-...i...i...i...`.F.o.....o.....{.....a.....j...}...h...}...l...i...V.....k.....h... ..*.h...i.B.h.....h...Richi.....PE..d....^a_....." .....0.....,.....L3.....%....`.....O.....TP.....p.....Z...!.....H....C..p..... ..... D..0.....@.....text...n/.....0..... ..`.rdata.....@.....4.....@..@.data.....`.....L.....@....pdata.....p.....N..... @..@.rsrc.....R.....@..@.reloc..H.....X.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp\System.dll	
Process:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.853944115448146
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3GJ6S3Kwnb.exe
File size:	425380
MD5:	6c6a52c18f0ca26d357f2b4430f31568
SHA1:	9b32a592e54100a67d907e2ad039b164961dc042
SHA256:	cbd91a64900eacff9502b5509769b33adb8472efadd2861d99fd95a06c5630be
SHA512:	043a76eb4be6164bbb6da7ed983ac5d37e8707453d18c139ead31eeda239f177b0f332f7cbd32f20cd0fb9329b8481cebd2488c0b23a892b7055f6ba9e16e78d
SSDEEP:	12288:wNX177TWqByR9zSHIrV6vq6q+n+S/1fZ6VG4u9:wNXtvWqfeVAxaSb548
TLSH:	3A94224B3B58C1F1E45A8930DD73AAF157BA6E37C9A62B471340BD9D3E31A41E80D742

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	2333514d312b0c20

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F7EF8A6DCFAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi

Instruction
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F7EF8A6DCCAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc1000	0x10040	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2b000	0x96000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc1000	0x10040	0x10200	False	0.719098231589	data	6.8222486252	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc1418	0x58c8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0xc6ce0	0x25a8	data	English	United States
RT_ICON	0xc9288	0x2319	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0xcb5a8	0x13d6	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0xcc980	0x10a8	data	English	United States
RT_ICON	0xcda28	0xea8	data	English	United States
RT_ICON	0xce8d0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 7844557, next used block 4498117	English	United States
RT_ICON	0xcf178	0x668	data	English	United States
RT_ICON	0xcf7e0	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xcfd48	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xd01b0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 605552896, next used block 8260	English	United States
RT_ICON	0xd0498	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0xd05c0	0x144	data	English	United States
RT_DIALOG	0xd0708	0x100	data	English	United States
RT_DIALOG	0xd0808	0x11c	data	English	United States
RT_DIALOG	0xd0928	0x60	data	English	United States
RT_GROUP_ICON	0xd0988	0xae	data	English	United States
RT_VERSION	0xd0a38	0x2c8	data	English	United States
RT_MANIFEST	0xd0d00	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	MakeMusic Inc.
FileVersion	17.9.5
CompanyName	Fortune Brands Inc.
LegalTrademarks	BMC Software, Inc.
Comments	Banknorth Group, Inc.
ProductName	Newmont Mining Corporation
FileDescription	Hubbell Inc.
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: 3GJ6S3Kwnb.exe PID: **3256**, Parent PID: **1100**

General

Target ID:	0
Start time:	21:03:46
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\3GJ6S3Kwnb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3GJ6S3Kwnb.exe"
Imagebase:	0x400000
File size:	425380 bytes
MD5 hash:	6C6A52C18F0CA26D357F2B4430F31568
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.773047400.0000000003300000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsi9D4A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A81	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	7	406023	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Velsespladser5.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\Airplane_6.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_SL.chm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\DiFxAPI.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\NativeAdapter.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi9D4A.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj9DE8.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Velsespladser5.tmp	0	20810	fd fd 29 3f 3a 74 57 4f 1c fd fd fd fd 1b 46 fd 7f fd 0f fd fd 03 fd fd fd 5d fd 43 fd 20 41 73 fd 06 69 fd fd 1e fd 24 fd fd 48 fd fd 66 37 67 fd 16 5a 0f fd 2b fd 35 5b fd fd fd fd 17 fd fd fd fd 69 fd fd fd 39 62 6d 6f 16 fd fd fd 47 12 17 fd 35 12 66 fd 57 fd fd fd fd 25 6c 5a 06 fd fd 09 04 fd 1c 4b 2a fd 74 fd fd 77 fd 6f 26 1c fd fd fd fd 0c fd fd 16 fd 0e 3c 45 fd fd 29 fd 67 66 37 41 32 4f 97 71 56 fd fd de fd 03 fd 17 10 fd fd fd 1e 60 03 03 fd 76 5a fd 07 6f fd 20 fd fd fd 4b fd 66 1b 2e 4e 10 3e 51 fd 54 fd 51 76 fd 5e fd 17 fd 12 fd fd 16 fd fd 57 59 3b 7a fd fd 55 fd fd fd fd 79 31 30 2b fd fd 64 64 38 70 04 fd fd fd 60 4d 43 fd 08 fd fd 57 5d 2b fd 02 34 fd 41 72 25 fd fd 42 fd 09 7f fd 78 fd	)?:tWOF]C Asi$Hf7g+5[i9bmoG5fW %lZK*two& <)gf7A2OqVvZo Kf.N>QT Q^WY;zUy10dd8p`MCW] +4Ar%Bx	success or wait	4	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\Airplane_6.bmp	0	6869	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaC Cnn"	success or wait	1	4060C3	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Bluetooth Suite help_SL.chm</td><td>0</td><td>23756</td><td>49 54 53 46 03 00 00 00 60 00 00 00 01 00 00 00 26 fd fd 27 09 04 00 00 10 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 11 fd 01 7c fd 7b fd 11 fd 0c 00 fd fd 22 fd fd 60 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 78 00 00 00 00 00 00 00 54 10 00 00 00 00 00 00 fd 10 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 1f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 54 53 50 01 00 00 00 54 00 00 00 0a 00 00 00 00 10 00 00 02 00 00 00 01 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 01 00 00 00 09 04 00 00 6a fd 02 5d 2e 21 fd 11 fd fd 00 fd fd 22 fd fd 54 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 50 4d 47 4c 30 07 00 00 00 00 00 00 fd fd fd fd fd fd fd 01 2f 00 00 00 08 2f 23 49 44 58 48 44 52 01 fd fd 10 fd 00 08 2f 23 49 54 42 49 54 53 00 00</td><td>ITSF`&'|{"|<br>{"`xTITSPTj].!"TPMG
L0//#IDXHDR/#ITBITS</td><td>success or wait</td><td>3</td><td>4060C3</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\DiFxAPI.dll</td><td>0</td><td>32768</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 54 31 fd 15 10 50 fd 46 10 50 fd 46 10 50 fd 46 37 fd fd 46 12 50 fd 46 10 50 fd 46 23 51 fd 46 37 fd fd 46 0d 50 fd 46 37 fd fd 46 03 50 fd 46 37 fd fd 46 2f 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 08 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 11 50 fd 46 37 fd fd 46 11 50 fd 46 52 69 63 68 10 50 fd 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$T1PFPFPF7FPFPF
#QF7FPF7FPF7F/PF7FPF7FPF7FPF7F
PF7FPFRichPF</td><td>success or wait</td><td>20</td><td>4060C3</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\HPPrintScanDoctorDeploymentMgr.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 3b 10 fd 05 5a 7e fd 05 5a 7e fd 05 5a 7e fd 57 32 7b fd 18 5a 7e fd 57 32 7a fd 0f 5a 7e fd 57 32 7d fd 06 5a 7e fd 57 32 7f fd 01 5a 7e fd 0c 22 fd 44 5a 7e fd 05 5a 7f fd fd 5a 7e fd fd 33 77 fd 02 5a 7e fd fd 33 fd fd 04 5a 7e fd 05 5a fd 07 5a 7e fd fd 33 7c fd 04 5a 7e fd 52 69 63 68 05 5a 7e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$A;Z~Z~Z~W2{Z~W 2zZ~W2}Z~W2Z~"DZ~Z Z~3wZ~3Z~ZZ~ 3|Z~RichZ~PEd	success or wait	3	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\NativeAdapter.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e6 41 fd fd fd 12 fd fd fd 12 fd fd fd 12 fd 34 fd 12 fd fd fd 12 fd fd 5b 12 fd fd fd 12 fd fd fd 12 fd fd fd 12 14 fd 5e 12 fd fd fd 12 fd fd 4b 12 fd fd fd 12 fd fd 4c 12 fd fd fd 12 fd fd 5c 12 fd fd fd 12 fd fd 59 12 fd fd fd 12 52 69 63 68 fd fd fd 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd fd fd 4e 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$A4[^KL\YRichPEdN"	success or wait	4	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\igoAudSessionMonitor.dll	0	31712	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d fd fd fd 69 fd fd fd 69 fd fd fd 69 fd fd fd 60 fd 46 fd 6f fd fd fd fd fd fd 6f fd fd fd fd fd fd 7b fd fd fd fd fd fd 61 fd fd fd fd fd fd 6a fd fd fd 7d fd fd fd 68 fd fd fd 7d fd fd fd 6c fd fd fd 69 fd fd fd 56 fd fd fd fd fd fd fd 6b fd fd fd fd fd fd 68 fd fd fd fd fd 2a fd 68 fd fd fd 69 fd 42 fd 68 fd fd fd fd fd fd fd 68 fd fd fd 52 69 63 68 69 fd fd	MZ@!L!This program cannot be run in DOS mode.$-iii`Foo{aj}h} liVkh*hiBhhRichi	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3GJ6S3Kwnb.exe	unknown	512	success or wait	207	406094	ReadFile
C:\Users\user\Desktop\3GJ6S3Kwnb.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\3GJ6S3Kwnb.exe	unknown	4	success or wait	31	406094	ReadFile

Disassembly

No disassembly