ID: 635282
Sample Name: #U00d6DEME FORMU.exe
Cookbook: default.jbs
Time: 18:22:58
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

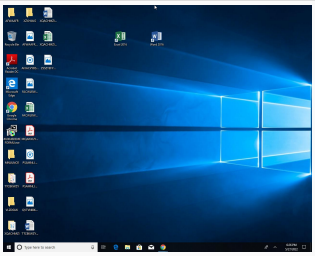
Windows Analysis Report

#U00d6DEME FORMU.exe

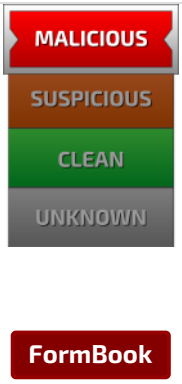
Overview

General Information

Sample Name:	#U00d6DEME FORMU.exe
Analysis ID:	635282
MD5:	0204546cc8568a..
SHA1:	ff7c492dd728279..
SHA256:	eddc1ee1fafda4f..
Tags:	exe Formbook geo TUR
Infos:	



Detection



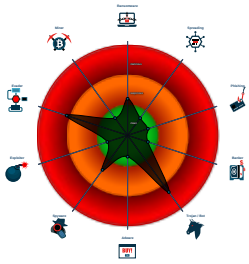
FormBook

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Found evasive API chain (may stop…
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- #U00d6DEME FORMU.exe (PID: 6304 cmdline: "C:\Users\user\Desktop\#U00d6DEME FORMU.exe" MD5: 0204546CC8568A60D97947C5FD6CCD49)
  - erltu.exe (PID: 6336 cmdline: C:\Users\user\AppData\Local\Temp\erltu.exe C:\Users\user\AppData\Local\Temp\fvcshciph MD5: 2603B527A791BAA25AC589C33B254470)
    - erltu.exe (PID: 6356 cmdline: C:\Users\user\AppData\Local\Temp\erltu.exe C:\Users\user\AppData\Local\Temp\fvcshciph MD5: 2603B527A791BAA25AC589C33B254470)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.liuchenggang.com/b0y1/"
  ],
  "decoy": [
    "newindexpress.com",
    "tg5szfdz.xyz",
    "aims1881.com",
    "bonaegroup.com",
    "be99caboi8.xyz",
    "weddingcentrepieces.com",
    "acigdmodel.com",
    "ketotax.info",
    "learnedware.com",
    "learning-rich-work.store",
    "multipreset.store",
    "flyttfirmaorebro.com",
    "58bilisim.xyz",
    "joseketofitdiet.site",
    "duomeishop.com",
    "programacaozerobarriga.site",
    "gygezau517.xyz",
    "awesometutorials.xyz",
    "hwvzfn3t.xyz",
    "nycexoticbullies.com",
    "smallbizmaker.com",
    "isarfeuer.com",
    "wacker-silicones.com",
    "tongtoto.com",
    "xofitessentials.com",
    "begep.space",
    "paperbackbookbox.com",
    "ihhsiljc.beauty",
    "jankarbaniye.com",
    "boli-12.xyz",
    "gridwriter.com",
    "377manhua.com",
    "willywaw98cop.com",
    "acumelet.com",
    "theupgradeexperiencemedia.com",
    "pimientamultimedia.com",
    "phoenixgold.xyz",
    "plunderdseign.com",
    "erdberrehausgsd.net",
    "aboutsprouts.com",
    "castle-clash.com",
    "nwcabin.com",
    "kurtizanki-spb.com",
    "yqphx.xyz",
    "casinowithout.com",
    "jctcopera.com",
    "antalyaluxuryvilla.xyz",
    "sagedidthis.com",
    "144z.xyz",
    "iska4peps.life",
    "rightthewrong.biz",
    "zib0bsivacf8.xyz",
    "beijingzhongruanchuangheng.site",
    "jylfxx.net",
    "newsletterexperience.com",
    "rnrprowash.com",
    "bylunakdy.com",
    "upasev.online",
    "businessreputationmanager.com",
    "kidsacooking.com",
    "brangusprimebeef.com",
    "nickhaven.com",
    "o1apopdpzhah.xyz",
    "negociodigital.store"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.erltu.exe.b40000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.erltu.exe.b40000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.erltu.exe.b40000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
1.2.erltu.exe.b40000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.erltu.exe.b40000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 1 entries

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

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

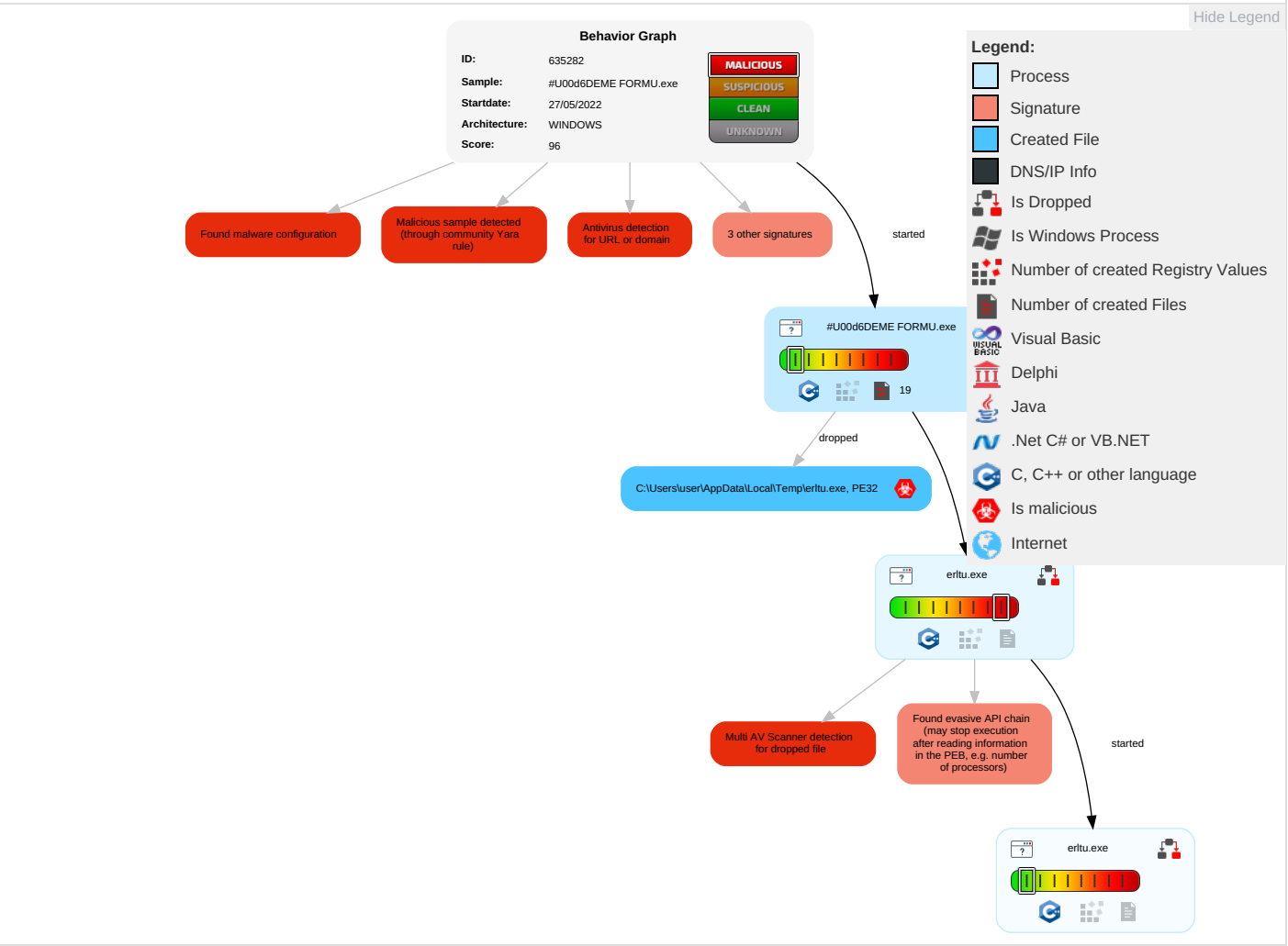
Yara detected FormBook

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 2 Native API	Path Interception	1 1 Process Injection	1 1 Process Injection	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected 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)	1 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Clipboard Data	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 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

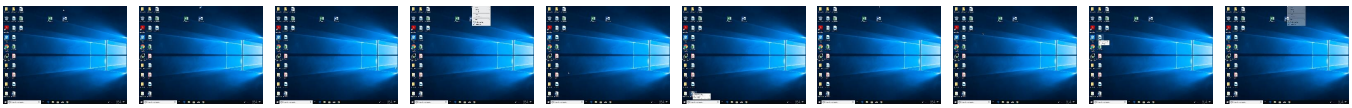
Behavior Graph



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
#U00d6DEME FORMU.exe	52%	Virustotal		Browse
#U00d6DEME FORMU.exe	37%	ReversingLabs	Win32.Trojan.FormBook	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\erltu.exe	48%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\erltu.exe	44%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.erltu.exe.b40000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.liuchenggang.com/b0y1/	1%	Virustotal		Browse
www.liuchenggang.com/b0y1/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.liuchenggang.com/b0y1/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635282
Start date and time: 27/05/202218:22:58	2022-05-27 18:22:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U00d6DEME FORMU.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winEXE@5/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 95.1% (good quality ratio 88.7%) • Quality average: 77.8% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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\erltu.exe

Process:	C:\Users\user\Desktop\#U00d6DEME FORMU.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134144
Entropy (8bit):	6.41218091663839
Encrypted:	false
SSDEEP:	1536:dYTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1Oyrx9WTqIDEJ+ksaSlJnXSU:JfbnR6BqNvncvhw9WTfEcLa4iG5skW
MD5:	2603B527A791BAA25AC589C33B254470
SHA1:	65EBDA93314517E098138BD9670ECCB345C7F662
SHA-256:	1AD07E46E78EB5A2AFC723FC2A8DF86D7B731A3CA853E4225622226EFC786F8F
SHA-512:	E5B3A208581A1B46382CC9D91D5C4FD3EE36DE741E57A1DB407F3A0B0602CC6678C7DBDCEB8DEE02614E1340FC7876DCD5088AB65DC74910A429CF21DAC6579
Malicious:	**true**

Antivirus:	• Antivirus: Virustotal, Detection: 48%, Browse • Antivirus: ReversingLabs, Detection: 44%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(.}c{.}c{.}c{./.{.}c{./.{.}c{./.{.}c{(.bz.}c{.}b{.}c{y.gz.}c{y..{.}c{ y.az.}c{Rich.}c{.....PE..L.....b.....@.....`.....@.....@.....P.....T..... ....@.....text...5..... ..`.rdata..>N.....P.....@..@.data....1.....@....rsrc.....@.....@..@.reloc.....P..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\fvcshciph

Process:	C:\Users\user\Desktop\#U00d6DEME FORMU.exe
File Type:	data
Category:	dropped
Size (bytes):	5310
Entropy (8bit):	6.093682530663886
Encrypted:	false
SSDEEP:	96:Wr9SaelkbOMBZUKzrCJEjZUFdPTzZoXeIPyHbODrnV/G8XhiOOAT/jOsu1p4w/k/:K9Sa3OEsoUXTzqbPRJSB1BRV0BDnR
MD5:	4E6A59FE3DCD5B83B64609193D85528E
SHA1:	1E0F857CD72F2984A09E821DCEA318CD2863B217
SHA-256:	7C5E9EC5245DE0AF358577C4E78B2F24B3810E626E2F29B178B638B04FB86860
SHA-512:	DFDE155F973F2B13174B6FB9A2238677D79F49BBE9BACFF6A0046BA79B8BE23A861E56C8F14F4587FA52DCC81CA38FAC142C287D19E3AB4B4FD46155D14C3AB2
Malicious:	false
Reputation:	low
Preview:	.....O..}.HMNA}_...A.^..?..A.^..?.}_...?.....}_...o..oX.?.....s?.sO..o..oX.?.....s?.sO..o..oX.?.....s?.sO..o..oX.?...t...s?.sO.}7X.n"R.@e...?..s?.sO.?X}..-.s?.sG.?.G....-.RXC. ?..O....s?.ANs_.}.R-.....}....%_..o.C.o.B.o.K@.o.KC.o.I.o...lXQ0...Q0sD.(}..o..o.KB.?...s?.._.....<.....}...._.I.?.I.....O...A.^..?..?....?.m(.?....GX...<..sO.s?..?...H.G.s..?. .O.....P..i.:....P.....P^..i.h....N.....P...i.F....<.....O..}...A.^..?.?.X....?.s?.}7..l..?.....?.Hs?..?.0s?....0.....l>.?..R.Ce..s<..sL...?..R.C...s<..sL...R.R.@e...<...P^..i.....s?....?..o..2 ...s?.}7..l.}_....?.....?.....O..}.H.A.^..?.?.....?.s?.}7..l..?.....?.Hs?..?.0s?.....|r....?..R.Ce..s<..sL...?..R.C...s<..sL...?X.R.C..s<..sL...?.-.R.Be..s<..sD...?.R.C...s<..sL..R.R. @e...<..P..i.....s?.}7..l..?.G.s....o..o..oX.o..o..#...s?.}7..l.}_....?.....?.....O..}.T.?.X....?.s?.}7..l..?.....?.Hs?..?.0s?.....l>.?..R.Ce..s<..sL..?..R.C...s<..sL..R.R.@e...<..P...i..... ..$...s?....o..o....

C:\Users\user\AppData\Local\Temp\ka5y543suvwo

Process:	C:\Users\user\Desktop\#U00d6DEME FORMU.exe
File Type:	data
Category:	dropped
Size (bytes):	189951
Entropy (8bit):	**7.990465363694904**
Encrypted:	**true**
SSDEEP:	3072:idfJQ4gfu2P+FGvM99Z1MG/ZtaEwV74jIFaRVIm53ZvUs1tFbdKKabXj2:idRku2SG4vlZtaqI8RWm53RUivBYXK
MD5:	D922F036AA538A949728682FE98BF835
SHA1:	A850EDF8BFA9EC5694F512062DAFB58929215DEE
SHA-256:	5B6B55B1FA6DEC84C11C4127725ED66FB32394D8C09BE7C3771B43E12C6BFBC3
SHA-512:	14C2188E46699A4268A157E2B8D1C40EFFC8B915916E479CE5C04900A1DBBB8E995561E63A5AEF162F986165EBD1CA7CF5A975488046A524C2498282DECB0A6B
Malicious:	false
Reputation:	low
Preview:	..k&..c.w..=.`....Zt..~O\\.Cw.C.4A.$g..-.uo.2t...a.4.4/.tSA..T....'#).`...e.._.#....n..9..!(;H#.%...3...E".4.!..XF.....0..1.g..R.0.@..'.#.E...p7=r.m..r..H;17...+N=..xM..r.....R...$..K...Uo. ..{.....s.b..l..XX`d.3.pk(Ar.(.....)..voX..|B.{&V0x3....O..c....g..>F.f.t.."......F4A..$j..-.*o..t...a..4/.tSA'.T....I'...svN..*Z...I...!.].@.....\T...j.uv./a>..}.t.O.....0....b...{....a.h...K7.....n. ;.99.$...0R.OV.r.....R.....RK...cRo.).{.....s.b...[<.o`.L^.pk(Ar.(.>...)..vo9S....B..&V0g3.i.gO..c.w.ug..>F..et.l."".....C.4A.$g..-.uo.2t...a.4.4/.tSA'.T....I'...svN..*Z...I...!.].@..... \T...j.uv./a>..}.t.O.....0....b...{....a.h...K7.....n.;.99.$...0R.OV.r.....R...$..K..!.Uo.U.{.....s.b...[<.o`dL^.pk(Ar.(.>...)..vo9S....B..&V0g3.i.gO..c.w.ug..>F..et.l."".....C.4A.$g..-.uo.2t...a.4.4/.tSA'.T....I'...svN..*Z...I...!.].@.....\T...j.uv./a>..}.t.O.....0....b...{....a.h...K7.....n.;.99.$...0R.OV.r.....R...$..K..!.Uo.U.{.....s.b...[<.o`dL^.pk(Ar.(.

C:\Users\user\AppData\Local\Temp\nsz96AE.tmp

Process:	C:\Users\user\Desktop\#U00d6DEME FORMU.exe
File Type:	data
Category:	dropped
Size (bytes):	335245
Entropy (8bit):	7.531798748691562
Encrypted:	false
SSDEEP:	6144:HJPdRku2SG4vlZtaqI8RWm53RUivBYXpZpvncWMElGC:8WNSqHRWm53RdZYXp/cWMEl
MD5:	9D1B5193868454C6C8B9F0FEA6AA7C8E
SHA1:	02818918499AF004548E0C1F641AE9965F27AD13
SHA-256:	BFFEBF62D8473D23F0BA2001738071F94D53532D97D8D3A9B35CA272A8FBDFA5

SHA-512:	562776614426BC11294FC7DD8599AEE68FE14ACCA1F8DE671F3A33299A2225EE2735AA2BE3C569BC3EAB3733F4C34FB80187FCD4361DE844E41FABED250A58B5
Malicious:	false
Reputation:	low
Preview:	.....,.....?..... .....B.....*...j..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.940379937299889
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	#U00d6DEME FORMU.exe
File size:	278482
MD5:	0204546cc8568a60d97947c5fd6ccd49
SHA1:	ff7c492dd728279cd763af6fa525606431fc8db0
SHA256:	eddc1ee1fafda4fe7cf6d114276c992806f33d7527d346464bad7033875fbd66
SHA512:	24fb62695c5455d362fbc157446a2cb2a7ae248268c0786cbd91a79a40fa32baa4f984cbbb45a6dd9f678f26cde7b6a7eb31cf1146f0fbaf17f060b58fa5d077
SSDEEP:	6144:B0YuB3ZgxdaCVG/RF5JUVu0dXet0ojX1nQcznQ:eB3AdaC8/RFYTQ0QDQ
TLSH:	FB441247B7F054F7D1729E3215A3E699F232A34619A191C71FB0AEB9B03E9C1048B74B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qJ...$...$...$./. {...$...%.;.$.".y...$..3....$.f."...$.Rich..$.....PE..L.....iF.....Z.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4032fa
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:	
Time Stamp:	0x4669CEB6 [Fri Jun 8 21:48:38 2007 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:	55f3dfd13c0557d3e32bcbc604441dd3

Entrypoint Preview

Instruction
sub esp, 00000180h

Instruction
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409170h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push ebx
call dword ptr [00407278h]
mov dword ptr [00423FD4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F4E8h
call dword ptr [00407154h]
push 0040922Ch
push 00423720h
call 00007F2BD1003B38h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007F2BD1003B26h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007F2BD100139Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F2BD1003619h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007F2BD10013F5h
cmp cl, 00000020h
jne 00007F2BD1001398h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F2BD100138Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007F2BD1001398h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007F2BD10013C5h
inc eax
cmp byte ptr [eax], 00000053h
jne 00007F2BD10013A0h

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	0x73a0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	0x7000	0x288	.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	0x59ac	0x5a00	False	0.668142361111	data	6.45807821776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x117a	0x1200	False	0.4453125	data	5.17513527374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1afd8	0x400	False	0.6015625	data	4.98110806401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94448786242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, CreateFileA, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, CloseHandle, ExitProcess, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

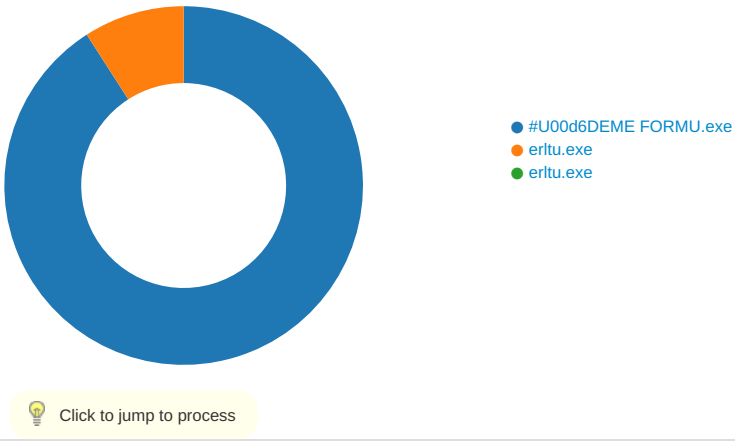
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: #U00d6DEME FORMU.exe PID: **6304**, Parent PID: **2776**

General

Target ID:	0
Start time:	18:24:13
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\#U00d6DEME FORMU.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\#U00d6DEME FORMU.exe"
Imagebase:	0x400000
File size:	278482 bytes
MD5 hash:	0204546CC8568A60D97947C5FD6CCD49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	4032ED	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz96AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsz96AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz96AF.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	4015E9	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
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	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ka5y543suvwo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\fvcshciph	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\erltu.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz96AD.tmp	success or wait	1	40345C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsz96AF.tmp	success or wait	1	40544C	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	0	26500	fd 16 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 09 00 00 3f 00 00 00 fd 10 00 00 00 00 00 00 fd 15 00 00 01 00 00 00 fd 16 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 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 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 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	,?	success or wait	17	4031E9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ka5y543suvwo	0	16384	fd fd 6b 26 06 fd 63 fd 77 fd fd 3d 05 60 09 fd fd fd 5a 74 17 fd 7e 4f 5c 5c fd 43 77 fd 43 fd 34 41 fd 24 67 fd 18 2d 1b 75 6f fd 32 74 2e 19 fd 61 fd 34 fd 34 2f 0b 74 53 41 1f fd 54 05 0a 29 1f 27 23 29 fd 60 fd fd 14 65 a0 fd 5f fd 23 fd fd 18 fd 6e fd fd 39 08 fd 21 28 3b 48 23 fd 25 fd fd fd 33 09 fd 1d 45 22 fd 34 fd 21 08 fd 58 46 fd 09 fd fd fd 08 30 12 fd 31 fd 67 fd fd 52 fd 30 fd 40 fd fd 27 fd 23 fd 45 fd fd 46 70 37 3d 72 11 6d fd fd 72 fd 1c 48 3b 31 37 fd fd fd 2b 4e 3d fd 1a 78 4d fd fd 72 fd fd fd fd 09 52 fd fd fd 24 fd fd 4b fd fd 20 55 6f fd fd fd 7b fd fd 0b 13 fd 0c 15 03 fd 73 fd 62 7f fd 6c fd 17 58 58 60 64 fd 33 05 70 6b 28 41 72 fd 28 fd fd fd fd fd 29 fd fd 76 6f 58 61 1f 7c 42 fd 7b 26 56 30 78 33	k&cw=`Zt~O\\CwC4A$g-uo2t.a44/tSAT'#)`e_#n9!(;H#%3E"4!XF01gR0@'#Ep7=rmrH;17+N=xMrR$KUo{sblXX`d3pk(Ar()voX|B{&V0x3	success or wait	12	40303D	WriteFile
C:\Users\user\AppData\Local\Temp\fvcshciph	0	5310	fd fd fd 08 08 4f fd fd 7d fd 48 4d 4e 41 7d 5f fd 08 fd 41 fd 5e fd 0d 3f fd fd 41 fd 5e fd 0d 3f fd 7d 5f fd 08 fd 3f fd 10 08 08 08 7d 5f fd 08 fd 6f 04 fd 6f 58 fd 3f fd fd 35 08 08 08 73 3f fd 73 4f 14 fd 6f 04 fd 6f 58 fd 3f fd fd fd fd 08 08 08 73 3f 18 73 4f fd fd 6f 04 fd 6f 58 fd 3f fd fd fd 1b 08 08 08 73 3f fd 73 4f fd fd 6f 04 fd 6f 58 fd 3f fd fd fd 74 08 08 08 73 3f fd 73 4f fd 7d 37 58 fd 6e 22 52 fd 40 65 fd fd fd 3f 04 fd 73 3f fd 73 4f 05 3f 58 7d fd fd 2d fd 73 3f fd 73 47 fd 3f 05 47 fd fd fd fd 2d 1a 52 58 43 c5 3f fd fd 4f fd fd fd fd 73 3f fd 41 4e 73 5f fd 7d 38 52 2d fd 08 08 08 08 7d fd 1c fd fd 25 5f fd fd 6f fd 43 fd 6f 18 42 fd 6f fd 4b 40 fd 6f fd 4b 43 fd 6f fd 49 fd 6f 16 7f fd 6c 58 51 30 fd 04 fd	O}HMNA}_A^?A^?}_?}_ooX?s?sOooX?s?sOooX?s?sOooX?ts?sO}7Xn"R@e?s?sO?X}-s?sG?G-RXC?Os?ANs_}R-}%_oCoBoK@oKCololXQ0	success or wait	1	40303D	WriteFile
C:\Users\user\AppData\Local\Temp\erltu.exe	0	16384	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 fd 1c 0d 28 fd 7d 63 7b fd 7d 63 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b 28 0f 62 7a fd 7d 63 7b fd 7d 62 7b fd 7d 63 7b 79 04 67 7a fd 7d 63 7b 79 04 fd 7b fd 7d 63 7b 79 04 61 7a fd 7d 63 7b 52 69 63 68 fd 7d 63 7b 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 50 45 00 00 4c 01 05 00 1b fd fd 62 00 00 00	MZ@!L!This program cannot be run in DOS mode.$(}c{}c{}c{/{}c{/{}c{/{}c{(bz}c{}b{}c{ygz}c{y{}c{yaz}c{Rich}c{PELb	success or wait	9	40303D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\#U00d6DEME FORMU.exe	unknown	512	success or wait	64	40329A	ReadFile
C:\Users\user\Desktop\#U00d6DEME FORMU.exe	unknown	16384	success or wait	16	40329A	ReadFile
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	unknown	4	success or wait	1	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	unknown	5824	success or wait	1	40307D	ReadFile
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	unknown	4	success or wait	3	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsz96AE.tmp	unknown	16384	success or wait	22	403021	ReadFile

Analysis Process: erltu.exe PID: **6336**, Parent PID: **6304**

General

Target ID:	1
Start time:	18:24:15
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\erltu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\erltu.exe C:\Users\user\AppData\Local\Temp\fvcshciph
Imagebase:	0x1010000
File size:	134144 bytes
MD5 hash:	2603B527A791BAA25AC589C33B254470
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.280690320.0000000000B40000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 48%, Virustotal, Browse • Detection: 44%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fvcshciph	unknown	4096	success or wait	1	101F88C	ReadFile
C:\Users\user\AppData\Local\Temp\fvcshciph	unknown	4096	success or wait	1	101F88C	ReadFile
C:\Users\user\AppData\Local\Temp\ka5y543suvwo	unknown	189951	success or wait	1	7F09F4	ReadFile

Analysis Process: erltu.exe PID: **6356**, Parent PID: **6336**

General

Target ID:	2
Start time:	18:24:16
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\erltu.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\erltu.exe C:\Users\user\AppData\Local\Temp\fvcshciph
Imagebase:	
File size:	134144 bytes
MD5 hash:	2603B527A791BAA25AC589C33B254470
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Disassembly

No disassembly