ID: 483687
Sample Name: gLO4rDsniT
Cookbook: default.jbs
Time: 11:35:23
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

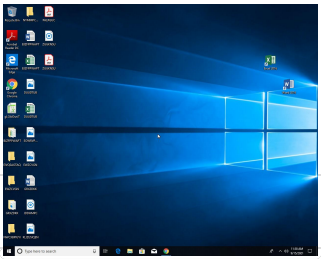
Windows Analysis Report gLO4rDsniT

Overview

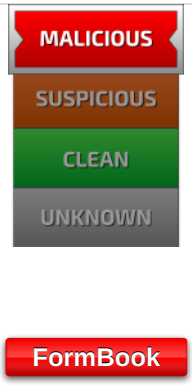
General Information

Sample Name:	gLO4rDsniT (renamed file extension from none to exe)
Analysis ID:	483687
MD5:	ebcd5648eab5a3..
SHA1:	b2a43a1489ce76..
SHA256:	bef7f97dcb40fd7…
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



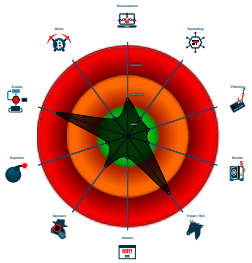
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- Tries to detect virtualization through…
- Machine Learning detection for dropp…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- gLO4rDsniT.exe (PID: 6308 cmdline: 'C:\Users\user\Desktop\gLO4rDsniT.exe' MD5: EBCD5648EAB5A3214EC61D4BED956A36)
  - powershell.exe (PID: 6740 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 20 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gLO4rDsniT.exe (PID: 3880 cmdline: C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe MD5: EBCD5648EAB5A3214EC61D4BED956A36)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.inboundtechnology.net/b9qq/"
  ],
  "decoy": [
    "tmalborz.com",
    "jiutianbath.com",
    "yazdir.info",
    "budget.sucks",
    "harman-enterprises.com",
    "kedaidaging.com",
    "exiteight.com",
    "urpropertymanager.com",
    "tomorrowsrider.com",
    "otlpro.com",
    "shopfunda.com",
    "xinhaojc1998.com",
    "fyqyzs.com",
    "legal-plaza.net",
    "bonmarchefr.net",
    "3bestrehab.com",
    "riyadhalnarjes.com",
    "bharateeyaswasrayadarshan.com",
    "inchingforhelp.com",
    "lojongdev.com",
    "jonathanbrowndrums.com",
    "rongnhonhatban.online",
    "gelora.site",
    "shirleyswigsinc.com",
    "pepsi-vm.com",
    "lovabubble.com",
    "wwwburlingtontownshipcourts.com",
    "findousd.com",
    "santavitrine.com",
    "sabaidiver.com",
    "actionclassiccars.com",
    "comdevfund.info",
    "geomasala.com",
    "leviathanpursuits.net",
    "fenrirnoise.com",
    "planeadvisory.com",
    "goehub.com",
    "greyriverstay.com",
    "monikalupaczewska.com",
    "yournorwegiancourse.com",
    "xn--hgbque4i.com",
    "topdex.info",
    "canvasgoogle.com",
    "leal-am.com",
    "peach-dev.finance",
    "us-phoneprotection.com",
    "nek.cool",
    "oraclenailstucson.com",
    "bloortoqueen.com",
    "hfhscn.com",
    "grooveautohacking.com",
    "getallentownpets.com",
    "storiesofablonde.com",
    "assistance-habitation.com",
    "aandzauto.services",
    "eating4mentalhealth.com",
    "getcareerpower.com",
    "hayokapan.com",
    "georgestuff.com",
    "manage-autpypl-account.com",
    "cjbwxs.com",
    "goodgly.com",
    "toptoffee.com",
    "salonefestival.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x4695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x4797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x33fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xa82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x66b9:$sqlite3step: 68 34 1C 7B E1 • 0x67cc:$sqlite3step: 68 34 1C 7B E1 • 0x66e8:$sqlite3text: 68 38 2A 90 C5 • 0x680d:$sqlite3text: 68 38 2A 90 C5 • 0x66fb:$sqlite3blob: 68 53 D8 7F 8C • 0x6823:$sqlite3blob: 68 53 D8 7F 8C
00000018.00000002.545104364.0000000001700000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000018.00000002.545104364.0000000001700000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.gLO4rDsniT.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
24.2.gLO4rDsniT.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
24.2.gLO4rDsniT.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
24.2.gLO4rDsniT.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
24.2.gLO4rDsniT.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning 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:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

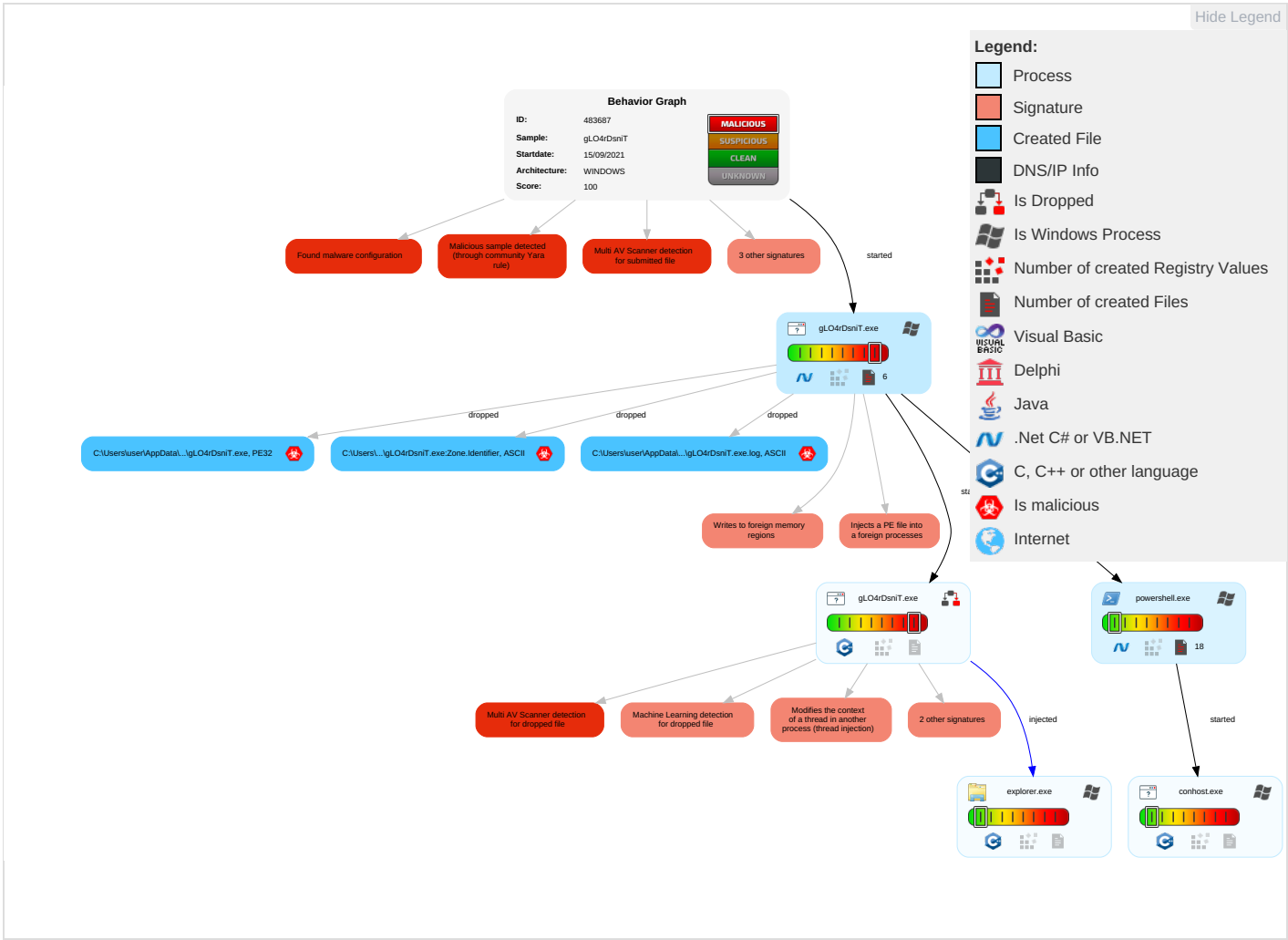
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 4 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

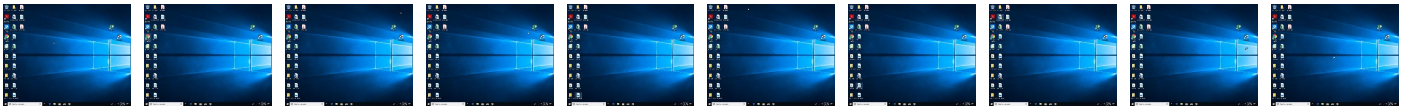
Behavior Graph



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
gLO4rDsniT.exe	32%	Virustotal		Browse
gLO4rDsniT.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
gLO4rDsniT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe	32%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.gLO4rDsniT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.inboundtechnology.net/b9qq/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.inboundtechnology.net/b9qq/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483687
Start date:	15.09.2021
Start time:	11:35:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gLO4rDsniT (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:	mal100.troj.evad.winEXE@6/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 3.6%) • Quality average: 80.3% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:36:51	API Interceptor	29x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\gLO4rDsniT.exe.log	
Process:	C:\Users\user\Desktop\gLO4rDsniT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D 8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17216
Entropy (8bit):	5.282642528769125
Encrypted:	false
SSDEEP:	384:3t9/p718YkTnTnArc0/I1rpdmRNkxOAFaF:1HaAw0AN3xc
MD5:	DEC1CE107BF9A1348958A864D173BC63
SHA1:	F5EFAD01E6074887E7237ABDEA0AC0193D11370C
SHA-256:	395FBB79E6D4032BF5E166A1215E89985158E92BF598A3CBC2FED792ED8F1A6A
SHA-512:	27E443924658B6F1D9AA9368DAEB588159CA1F0E68015AFE6D190E4155FC25655D68394977211A95CDE09C13668E0AA7710909BAF6352C99C73AE8C11925F467
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....d.Z.W.....@.....D.....fZve...F.....x.)T.....System.Management.AutomationH.....<@.^.L."My...:)..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fwacnx5e.wgs.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lmgobnyv.q3r.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe	
Process:	C:\Users\user\Desktop\gLO4rDsniT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	827904
Entropy (8bit):	7.113226060715182
Encrypted:	false
SSDEEP:	12288:t/gecNU2zqX6lUB2AkegSpxGrsM+qFeWRs:yDNgWUB2AkegSp0hZRs
MD5:	EBCD5648EAB5A3214EC61D4BED956A36
SHA1:	B2A43A1489CE76373DF3BA5E4BA54172A6CC92F4
SHA-256:	BEF7F97DCB40FD71E9A9FCA6F43389749245F17E7A3092219D20217B8AD8E36A
SHA-512:	9FB5A58AEF41AC0B54916742DEF94A2C8CEE88DA3C7D550CE01B667285FDF21A00EB8266A8288E52A652E82A2C40B845AF0A237538AE5B74DE0F6D41F46BAB(E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n=@a..... ....@.. ....@.....T...W.....P..... ....H.....text..... ....`.rsrc...P.....@..@.rel oc.....@..B.....H.....8.....(..0Y.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....(.....-.&+. (....+.*....0..*.....-.&r...p%.-.&..-.&&(....+..+..+.(....+.*...0..'.....,.{.....{....o.....-.&&+.(....+.*..0.....:....&."...A"...As.....-v&&...-v&&. ".. ....s....(.....(.....(.....(.....s....(.....r ...p(.....r...po .....s!...("....(#...+.($...8w...(%...+.(&...+.*.0.....

C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\gLO4rDsniT.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe:Zone.Identifier	
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210915\PowerShell_transcript.841618.Y+XpuZo3.20210915113633.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	941
Entropy (8bit):	5.0117760090308785
Encrypted:	false
SSDEEP:	24:BxSASDvBB8x2DOXUWM1W4yHjeTKKjX4CIym1ZJXzxOnxSAZ83:BZqv/8oOZRqDYB1ZpxgZZ83
MD5:	FF931FCCE8FDC4A6F721FFE72FF853C8
SHA1:	D616C4CBEC7C8B55BF38EA18447B1173019A1637
SHA-256:	077C0652C040C77E5E578A791540C6AF2B02E48F3500580EFB770C10B41F9560
SHA-512:	8B317B831F7C3E03F53E5DE162EC00DD4E59D244F9D76C1FD213C17807DDC303943C113FA328379B64292CD2103DD02F65EF47A2F4E044C3F1942B8BE1E44AE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915113647..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Sleep -s 20..Process ID: 6740..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30 319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 2021 0915113647..**********..PS>Start-Sleep -s 20..**********..Command start time: 20210915114051..**********..PS>$global:?..True..******** **********..Windows PowerShell transcript end..End time: 20210915114052..**********..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.113226060715182
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	gLO4rDsniT.exe
File size:	827904
MD5:	ebcd5648eab5a3214ec61d4bed956a36
SHA1:	b2a43a1489ce76373df3ba5e4ba54172a6cc92f4
SHA256:	bef7f97dcb40fd71e9a9fca6f43389749245f17e7a3092219d20217b8ad8e36a
SHA512:	9fb5a58aef41ac0b54916742def94a2c8cee88da3c7d550ce01b667285fdf21a00eb8266a8288e52a652e82a2c40b845af0a237538ae5b74de0f6d41f46bab6e
SSDEEP:	12288:t/gecNU2zqX6lUB2AkegSpxGrsM+qFeWRs:yDNgWUB2AkegSp0hZRs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n=@a..... ....@.. .....@.....

File Icon

Icon Hash:	d0d4d2dadadadae4

Static PE Info

General

Entrypoint:	0x4c9fae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61403D6E [Tue Sep 14 06:13:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc7fb4	0xc8000	False	0.638974609375	data	7.11687874343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x1c50	0x1e00	False	0.450130208333	data	5.85410682241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xcc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: gLO4rDsniT.exe PID: 6308 Parent PID: 5036

General

Start time:	11:36:19
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\gLO4rDsniT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\gLO4rDsniT.exe'
Imagebase:	0x6f0000
File size:	827904 bytes
MD5 hash:	EBCD5648EAB5A3214EC61D4BED956A36
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.466649182.0000000003B59000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.466649182.0000000003B59000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.466649182.0000000003B59000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.467041262.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.467041262.0000000003C49000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.467041262.0000000003C49000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.466807357.0000000003BB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.466807357.0000000003BB4000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.466807357.0000000003BB4000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: powershell.exe PID: 6740 Parent PID: 6308

General

Start time:	11:36:30
Start date:	15/09/2021

Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 20
Imagebase:	0x1280000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6748 Parent PID: 6740

General

Start time:	11:36:31
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: gLO4rDsniT.exe PID: 3880 Parent PID: 6308

General

Start time:	11:38:03
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\gLO4rDsniT.exe
Imagebase:	0x960000
File size:	827904 bytes
MD5 hash:	EBCD5648EAB5A3214EC61D4BED956A36
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: 00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.545335617.0000000001800000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.545104364.0000000001700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.545104364.0000000001700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.545104364.0000000001700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.543592754.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.543592754.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.543592754.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, Virustotal, Browse • Detection: 41%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3880

General

Start time:	11:38:06
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000019.00000000.493656809.0000000006740000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000019.00000000.493656809.0000000006740000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000019.00000000.493656809.0000000006740000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000019.00000002.529006238.0000000006740000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000019.00000002.529006238.0000000006740000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000019.00000002.529006238.0000000006740000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Disassembly

Code Analysis