ID: 510600
Sample Name:
PO_101&102.exe
Cookbook: default.jbs
Time: 00:35:11
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

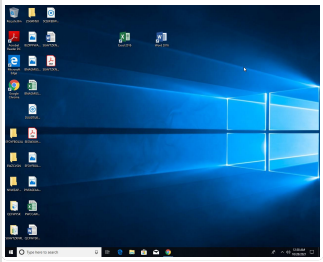
Windows Analysis Report PO_101&102.exe

Overview

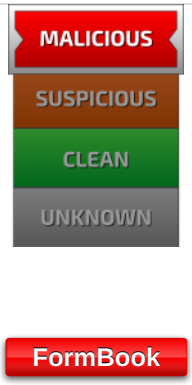
General Information

Sample Name:	PO_101&102.exe
Analysis ID:	510600
MD5:	c8a5346cb632c9…
SHA1:	a671570c31428e..
SHA256:	46a0a8595dccf13..
Tags:	exe formbook
Infos:	

Most interesting Screenshot:



Detection

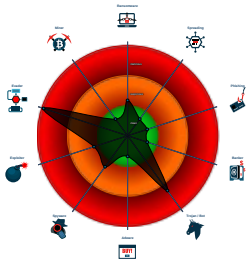


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- PO_101&102.exe (PID: 7016 cmdline: 'C:\Users\user\Desktop\PO_101&102.exe' MD5: C8A5346CB632C91E0006252FD2C47BEC)
  - PO_101&102.exe (PID: 5268 cmdline: {path} MD5: C8A5346CB632C91E0006252FD2C47BEC)
  - PO_101&102.exe (PID: 5964 cmdline: {path} MD5: C8A5346CB632C91E0006252FD2C47BEC)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 5580 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 6216 cmdline: /c del 'C:\Users\user\Desktop\PO_101&102.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.reynbetgirisi.com/snr6/"
  ],
  "decoy": [
    "jjglassmi1.com",
    "vpsseattle.com",
    "drfllc.top",
    "staycoolonline.com",
    "eptlove.com",
    "solusimatasehat.site",
    "ionrarecharlestonproperties.com",
    "b3eflucg.xyz",
    "tvchosun-usa.com",
    "mmahzxwzsadqlshop.life",
    "gospelimport.com",
    "demoapps.website",
    "jackburst54.com",
    "99rocket.education",
    "ccbwithbri.com",
    "trapperairsoft.com",
    "useroadly.com",
    "ralphlaurenonline-nl.com",
    "loanmaster4u.com",
    "champ-beauty-tomigaoka-nail.com",
    "theripemillennial.com",
    "123intan.net",
    "typopendant.com",
    "coruscant.holdings",
    "bio-intelligenz-therapie.com",
    "reprv.com",
    "directreport.net",
    "phinespe.xyz",
    "xuvedae.site",
    "idilikproperties.info",
    "wakigaggenin.com",
    "mal2tech.com",
    "nftwhaler.xyz",
    "gxhnjssx.com",
    "ozba.xyz",
    "lecupcake.net",
    "lucid.quest",
    "kaleoslawncare.com",
    "tiew.store",
    "texcommercialpainting.com",
    "2152351.com",
    "likewize-xl.com",
    "dacooligans.com",
    "manuelmartinezs.com",
    "beancusp.com",
    "barbershopvalleyvillage.com",
    "southwickfunerals.com",
    "briellebaeslay.info",
    "rebeccarye.com",
    "unitedstateswelders.com",
    "saudiarabiavegan.com",
    "testcarona.com",
    "serverapsd.com",
    "crickx.email",
    "hdszbj.com",
    "bennettmountainoutfitter.com",
    "leileilei1999.xyz",
    "baroquefolke.com",
    "francinegeorges.com",
    "horpces.online",
    "resolutionfix.com",
    "mike-schultz.xyz",
    "sohutobankueahomupezinkv.xyz",
    "flowerseedqueen.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.371409464.0000000001530000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.371409464.0000000001530000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.PO_101&102.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.PO_101&102.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.PO_101&102.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
10.0.PO_101&102.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.0.PO_101&102.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

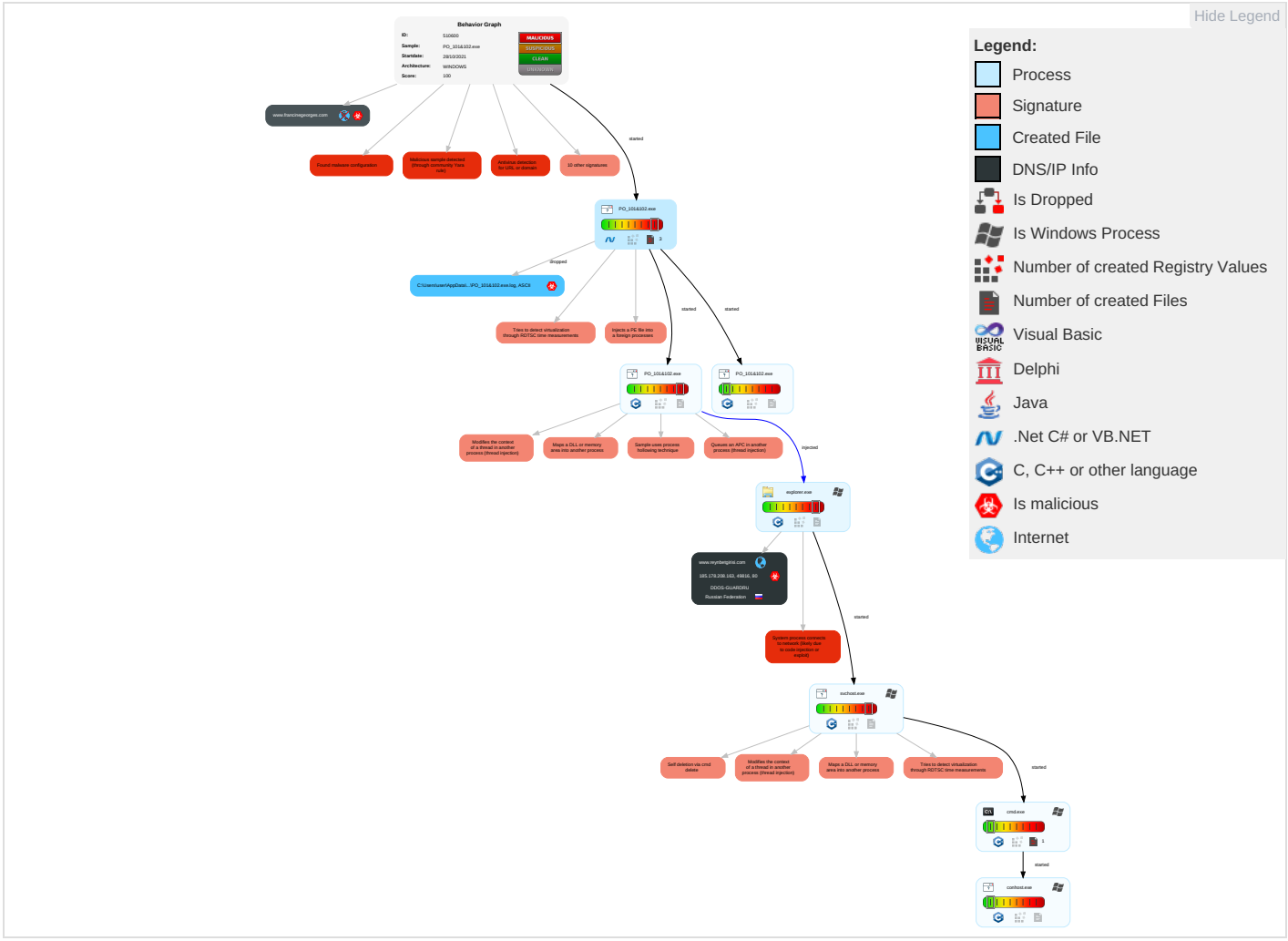
Remote Access Functionality:

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	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 (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	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	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
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-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

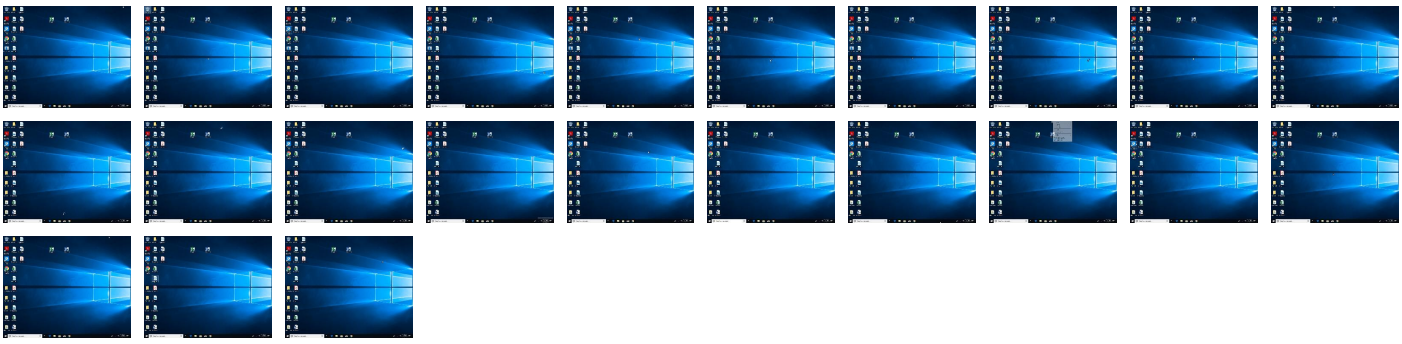
Behavior Graph



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
PO_101&102.exe	36%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
PO_101&102.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.PO_101&102.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.PO_101&102.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.PO_101&102.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.0.PO_101&102.exe.400000.8.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://www.tiro.comy	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://https://www.reynbetgirisi.com/snr6/?jDH8=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.tiro.comF	0%	URL Reputation	safe	
http://www.fonts.com-ul	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	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.jiyu-kobo.co.jp/jp/_	0%	Avira URL Cloud	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	
http://www.reynbetgirisi.com/snr6/?jDH8=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF+l+57NdrJs1Xds1ailiks&l0D0=fJBTE	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
www.reynbetgirisi.com/snr6/	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://tempuri.org/DatabaseDataSet.xsd	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.com5	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krE	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.com-u	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.reynbetgirisi.com	185.178.208.163	true	true		unknown
www.francinegeorges.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.reynbetgirisi.com/snr6/?jDH8=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF+l+57NdrJs1Xds1ailiks&l0D0=fJBTE	true	• Avira URL Cloud: malware	unknown
www.reynbetgirisi.com/snr6/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.178.208.163	www.reynbetgirisi.com	Russian Federation		57724	DDOS-GUARDRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510600
Start date:	28.10.2021
Start time:	00:35:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_101&102.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:	28
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@9/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.2% (good quality ratio 14.5%) • Quality average: 72% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 97% • 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
00:36:12	API Interceptor	2x Sleep call for process: PO_101&102.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.178.208.163	S.O.A.exe	Get hash	malicious	Browse	• www.reynbetgirisi.com/snr6/?Q2JHDn=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF+l+57NdrJs1X3zFqihgss&j0Gh4=5j9l3Fyx

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.reynbetgirisi.com	S.O.A.exe	Get hash	malicious	Browse	• 185.178.208.163

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DDOS-GUARDRU	S.O.A.exe	Get hash	malicious	Browse	• 185.178.208.163
	6xVYuXitGI.exe	Get hash	malicious	Browse	• 185.178.208.148
	vbc.exe	Get hash	malicious	Browse	• 185.129.100.113
	pYXAhd1foP.exe	Get hash	malicious	Browse	• 185.129.100.113
	DeqrlfxzHW.exe	Get hash	malicious	Browse	• 185.129.100.113
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 185.129.100.115
	loligang.x86	Get hash	malicious	Browse	• 185.129.101.234
	APfSnkgVzU	Get hash	malicious	Browse	• 185.129.101.214
	PO650.exe	Get hash	malicious	Browse	• 77.220.207.191
	ABhHk2dXUE.exe	Get hash	malicious	Browse	• 185.178.208.180
	vrTEp3LkwG.exe	Get hash	malicious	Browse	• 185.178.208.180
	sDsPEdoFdb.exe	Get hash	malicious	Browse	• 185.178.208.177
	SEPTEMBER ORDER.xlsx	Get hash	malicious	Browse	• 185.178.208.164
	Decline-331847309-06242021.xlsm	Get hash	malicious	Browse	• 5.253.62.174
	Decline-331847309-06242021.xlsm	Get hash	malicious	Browse	• 5.253.62.174
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_101&102.exe.log	
Process:	C:\Users\user\Desktop\PO_101&102.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):	7.427190609127641
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO_101&102.exe
File size:	684032
MD5:	c8a5346cb632c91e0006252fd2c47bec
SHA1:	a671570c31428ebc9bee30c9a2b9963bf629560a
SHA256:	46a0a8595dccf134213c2e9ae10dd6fdd8e3ff5f0cb1b01014a6b67e31927eec
SHA512:	eb3f2e70339e04821b86ced686a47abec277f59a0f90d03b512d6023d71d24de0ae84c36983291d40ecbb4765b94c146affea45b8d09d0d000633af20cfdf528
SSDEEP:	12288:fhwV/8FumO5ZBLbGZ3EEFdmgTSuAReaSA7hqJFTP:fmV/8FumO/B3GtnmRufo7hq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...7vya.....P..f.....B.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a8542
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61797637 [Wed Oct 27 15:54:31 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	0xa6548	0xa6600	False	0.698281073911	data	7.43588694795	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x5a4	0x600	False	0.418619791667	data	4.06372822623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 00:37:54.252959013 CEST	192.168.2.3	8.8.8.8	0x4941	Standard query (0)	www.reynbetgirisi.com	A (IP address)	IN (0x0001)
Oct 28, 2021 00:38:15.052742004 CEST	192.168.2.3	8.8.8.8	0x80cf	Standard query (0)	www.francinegeorges.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 00:37:54.319506884 CEST	8.8.8.8	192.168.2.3	0x4941	No error (0)	www.reynbetgirisi.com		185.178.208.163	A (IP address)	IN (0x0001)
Oct 28, 2021 00:38:15.117805004 CEST	8.8.8.8	192.168.2.3	0x80cf	Name error (3)	www.francinegeorges.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.reynbetgirisi.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49816	185.178.208.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 00:37:54.376329899 CEST	5185	OUT	GET /snr6/?jDH8=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF+l+57NdrJs1Xds1ailiks&l0D0=fJBTE HTTP/1.1 Host: www.reynbetgirisi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 28, 2021 00:37:54.402657032 CEST	5186	IN	HTTP/1.1 301 Moved Permanently Server: ddos-guard Date: Wed, 27 Oct 2021 22:37:54 GMT Connection: close Location: https://www.reynbetgirisi.com/snr6/?jDH8=E19JCPWLLAvTbcnEEa/roDJkoR1wzkcHqaxLe1hmnUekSrF+l+57NdrJs1Xds1ailiks&l0D0=fJBTE Content-Type: text/html; charset=utf8 Content-Length: 568 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 33 30 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 20 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 20 3a 6e 6f 6e 65 3b 7d 3c 2f 73 74 79 6c 65 3e 3c 70 3e 3c 62 3e 33 30 31 20 2d 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 20 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 52 65 71 75 65 73 74 65 64 20 63 6f 6e 74 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 20 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e Data Ascii: <!DOCTYPE html><html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 301</title><style>*{margin:0;padding:0}html{font:15px/22px arial,sans-serif;background: #fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}p{margin:11px 0 22px;overflow :hidden}ins{color:#777;text-decoration :none;}</style><p>301 - Moved Permanently . <ins>Thats an error.</ins><p>Requested content has been permanently moved. <ins>Thats all we know.</ins>

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: PO_101&102.exe PID: 7016 Parent PID: 5532

General

Start time:	00:36:04
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\PO_101&102.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_101&102.exe'
Imagebase:	0xf90000
File size:	684032 bytes
MD5 hash:	C8A5346CB632C91E0006252FD2C47BEC
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: 00000001.00000002.312254656.0000000004500000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.312254656.0000000004500000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.312254656.0000000004500000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: PO_101&102.exe PID: 5268 Parent PID: 7016

General

Start time:	00:36:14
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\PO_101&102.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x180000
File size:	684032 bytes
MD5 hash:	C8A5346CB632C91E0006252FD2C47BEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO_101&102.exe PID: 5964 Parent PID: 7016

General

Start time:	00:36:15

Start date:	28/10/2021
Path:	C:\Users\user\Desktop\PO_101&102.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaf0000
File size:	684032 bytes
MD5 hash:	C8A5346CB632C91E0006252FD2C47BEC
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: 0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.307243585.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.371409464.0000000001530000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.371409464.0000000001530000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.371409464.0000000001530000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.370759398.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.370759398.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.370759398.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.371246188.0000000001500000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.371246188.0000000001500000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.371246188.0000000001500000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.308236166.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.308236166.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.308236166.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 5964

General

Start time:	00:36:18
Start date:	28/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.352889129.0000000007949000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.352889129.0000000007949000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.352889129.0000000007949000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.335987438.0000000007949000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.335987438.0000000007949000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.335987438.0000000007949000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5580 Parent PID: 3352

General

Start time:	00:36:42
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x100000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.558614233.0000000002E40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.558614233.0000000002E40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.558614233.0000000002E40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.555083742.00000000001A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.555083742.00000000001A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.555083742.00000000001A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.559409706.0000000002F40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.559409706.0000000002F40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.559409706.0000000002F40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6216 Parent PID: 5580

General

Start time:	00:36:47
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO_101&102.exe'
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6076 Parent PID: 6216

General

Start time:	00:36:48
Start date:	28/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis