

JoeSandbox Cloud BASIC



ID: 680485

Sample Name: 6109238.exe

Cookbook: default.jbs

Time: 17:24:07

Date: 08/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report 6109238.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Signatures	6
Memory Dumps	6
Unpacked PEs	6
Sigma Signatures	7
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
E-Banking Fraud	7
System Summary	7
Boot Survival	7
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	11
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6109238.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_djzcf1.bda.psm1	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kmqndebx.s0u.ps1	15
C:\Users\user\AppData\Local\Temp\tmp1585.tmp	15
C:\Users\user\AppData\Roaming\leHkVrJJ.exe	15
C:\Users\user\AppData\Roaming\leHkVrJJ.exe:Zone.Identifier	16
C:\Users\user\Documents\20220808\PowerShell_transcript.841675.UFIE9n5j.20220808172536.txt	16
Static File Info	16
General	16
File Icon	16
Static PE Info	17
General	17
Entrypoint Preview	17
Data Directories	19
Sections	19
Resources	19
Imports	19
Network Behavior	19
Code Manipulations	19
User Modules	20
Hook Summary	20

Processes	20
Statistics	20
Behavior	20
System Behavior	20
Analysis Process: 6109238.exePID: 1980, Parent PID: 5768	20
General	20
File Activities	21
Analysis Process: powershell.exePID: 5756, Parent PID: 1980	21
General	21
File Activities	21
File Created	21
File Deleted	21
File Written	22
File Read	23
Analysis Process: conhost.exePID: 5064, Parent PID: 5756	26
General	26
Analysis Process: schtasks.exePID: 2276, Parent PID: 1980	26
General	26
File Activities	27
File Read	27
Analysis Process: conhost.exePID: 1384, Parent PID: 2276	27
General	27
Analysis Process: 6109238.exePID: 5392, Parent PID: 1980	27
General	27
File Activities	27
File Read	27
Analysis Process: explorer.exePID: 3688, Parent PID: 5392	28
General	28
Analysis Process: help.exePID: 2056, Parent PID: 3688	28
General	28
File Activities	29
File Read	29
Analysis Process: cmd.exePID: 5596, Parent PID: 2056	29
General	29
File Activities	29
Analysis Process: conhost.exePID: 6112, Parent PID: 5596	29
General	29
Disassembly	30

Windows Analysis Report

6109238.exe

Overview

General Information

Sample Name:

6109238.exe

Analysis ID:

680485

MD5:

2aeb09e3b19012..

SHA1:

0364e572469a4b..

SHA256:

917e03484856f0..

Tags:

exe formbook

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

FormBook

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Yara detected FormBook

Malicious sample detected (through...

Yara detected AntiVM3

Antivirus detection for URL or domain

Multi AV Scanner detection for drop...

Sample uses process hollowing tech...

Maps a DLL or memory area into an...

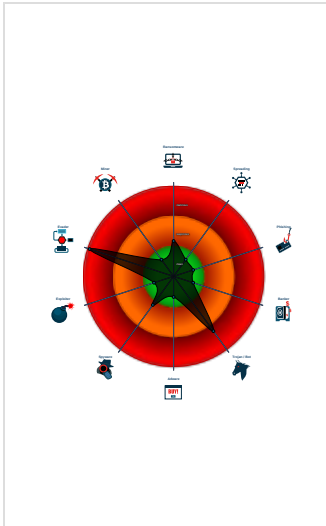
Tries to detect sandboxes and other...

Machine Learning detection for sam...

Modifies the prolog of user mode fun...

Injects a PE file into a foreign proce...

Classification



Process Tree

System is w10x64

6109238.exe (PID: 1980 cmdline: "C:\Users\user\Desktop\6109238.exe" MD5: 2AEB09E3B19012D3D2ADD45559422416)

powershell.exe (PID: 5756 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roamin...

conhost.exe (PID: 5064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

schtasks.exe (PID: 2276 cmdline: C:\Windows\System32\schtasks.exe /Create /TN "Updates\leHkVrJJ" /XML "C:\Users\user\AppData\Local\Temp\tmp1585.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe (PID: 1384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

6109238.exe (PID: 5392 cmdline: C:\Users\user\Desktop\6109238.exe MD5: 2AEB09E3B19012D3D2ADD45559422416)

explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)

help.exe (PID: 2056 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)

cmd.exe (PID: 5596 cmdline: /c del "C:\Users\user\Desktop\6109238.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cleanup

Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2022

Page 4 of 30

```

{
  "C2 list": [
    "www.ruichuo888.com/g2t8/"
  ],
  "decoy": [
    "ziezi.top",
    "vngik.com",
    "alternativaporbenidorn.com",
    "papinahooy.com",
    "aldemyangin.com",
    "943757.com",
    "ayty8.com",
    "rindedwladku.xyz",
    "highwoodcorp.com",
    "tyarx.com",
    "pikkunoita.online",
    "airtaxifl.com",
    "bjbjbfc.com",
    "busan.xyz",
    "ieeeturkeyblog.com",
    "valtuo.store",
    "xinyenet.net",
    "ditral.com",
    "protocolozero.info",
    "newbrunswickcreditunions.com",
    "elainebaby.xyz",
    "koidesignstudio.com",
    "99vin.group",
    "archipel-aventure.com",
    "khademi.group",
    "takaboar.com",
    "rzxx123.net",
    "games-wedding.com",
    "spinhaus.com",
    "51sic.com",
    "3dtouch.asia",
    "tracking173.xyz",
    "febnaklstudio.xyz",
    "cookingshots.com",
    "royaltristate.com",
    "amangift.store",
    "vehicleaccessories.store",
    "kannadasuddi.com",
    "the4weekway.international",
    "asd1118.xyz",
    "cursosparapotenciarte.store",
    "faithsquint.sbs",
    "otom.blue",
    "mamaandpapafoodtruck.com",
    "287by.com",
    "memoryuniverse.com",
    "televizeme.tech",
    "zpw168.com",
    "kayseriozelders.xyz",
    "solytics.xyz",
    "3kidsandahouse.com",
    "020dd.com",
    "shawlco.com",
    "wekiok05.top",
    "zalandashop.com",
    "tenergia.info",
    "nedreptate.net",
    "dentalimplantnearme-sg.space",
    "v pussy.com",
    "katzenglueck.net",
    "leftygolf.online",
    "simplehealthquotes.today",
    "estuidioma.online",
    "aviaboofit.site"
  ]
}

```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.640356208.0000000000EC0000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
0000000A.00000002.640356208.0000000000EC0000.0000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	0x6251:\$a1: 3C 30 50 4F 53 54 74 09 40 0x1cbb0:\$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 0xa9bf:\$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 0x158a7:\$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000A.00000002.640356208.0000000000EC0000.0000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x9908:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b72:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x156a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15191:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x157a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1591f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa58a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 0x1440c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb283:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b917:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c91a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
0000000A.00000002.640356208.0000000000EC0000.0000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x18839:\$sqlite3step: 68 34 1C 7B E1 0x1894c:\$sqlite3step: 68 34 1C 7B E1 0x18868:\$sqlite3text: 68 38 2A 90 C5 0x1898d:\$sqlite3text: 68 38 2A 90 C5 0x1887b:\$sqlite3blob: 68 53 D8 7F 8C 0x189a3:\$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.423502729.0000000000401000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.6109238.exe.400000.0.unpack	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
5.0.6109238.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	0x5451:\$a1: 3C 30 50 4F 53 54 74 09 40 0x1bd0:\$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 0x9bbf:\$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 0x14aa7:\$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
5.0.6109238.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8b08:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8d72:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x148a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14391:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x149a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x14b1f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x978a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 0x1360c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa483:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1ab17:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1bb1a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
5.0.6109238.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x17a39:\$sqlite3step: 68 34 1C 7B E1 0x17b4c:\$sqlite3step: 68 34 1C 7B E1 0x17a68:\$sqlite3text: 68 38 2A 90 C5 0x17b8d:\$sqlite3text: 68 38 2A 90 C5 0x17a7b:\$sqlite3blob: 68 53 D8 7F 8C 0x17ba3:\$sqlite3blob: 68 53 D8 7F 8C
0.2.6109238.exe.43053d8.6.raw.unpack	JoeSecurity_Form Book	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

Sigma Signatures

⊘ No Sigma rule has matched

Snort Signatures

⊘ No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected FormBook

System Summary



Malicious sample detected (through community Yara rule)

Boot Survival



Uses schtasks.exe or at.exe to add and modify task schedules

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



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)
Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information



Yara detected FormBook

Remote Access Functionality



Yara detected FormBook

Mitre Att&ck Matrix

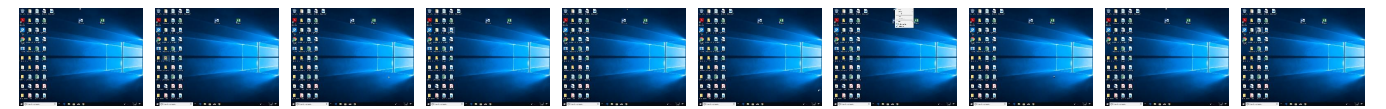
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	5 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	3 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 DLL Side-Loading	1 Scheduled Task/Job	1 Masquerading	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	5 1 2 Process Injection	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

Screenshots

Thumbnails

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

A grid of 14 small thumbnail images showing various Windows 10 desktops. Each thumbnail displays a blue background with a light blue window frame in the center. The taskbar at the bottom of each thumbnail shows different icons and system tray elements, indicating different states or configurations of the desktop environment. The thumbnails are arranged in two rows of seven.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
6109238.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
6109238.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\leHkVrJJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\leHkVrJJ.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.6109238.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

 No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.ruichuo888.com/g2i8/	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.unwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs
Contacted Domains
 No contacted domains info

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
www.ruichuo888.com/g2i8/	true	Avira URL Cloud: malware	low

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.coml	6109238.exe, 00000000.00000002.446511442.0000000007452000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.typography.netD	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.founder.com.cn/cn/cThe	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://fontfabrik.com	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.jiyu-kobo.co.jp/	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.fonts.com	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.sandoll.co.kr	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	6109238.exe, 00000000.00000002.433596561.000000003225000.00000004.00000800.00020000.00000000.sdm, 6109238.exe, 00000000.00000002.439859566.00000000345A000.00000004.00000800.00020000.00000000.sdm	false		high
http://www.sakkal.com	6109238.exe, 00000000.00000002.446511442.000000007452000.00000004.00000800.00020000.00000000.sdm	false	URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information	
Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680485
Start date and time: 08/08/202217:24:07	2022-08-08 17:24:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6109238.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:	15
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@13/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.2% (good quality ratio 80.9%) • Quality average: 71.5% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctdl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: 6109238.exe

Simulations

Behavior and APIs

Time	Type	Description
17:25:31	API Interceptor	1x Sleep call for process: 6109238.exe modified
17:25:38	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files	
	No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\6109238.exe.log 	
Process:	C:\Users\user\Desktop\6109238.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	true
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\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22192
Entropy (8bit):	5.602774286628419
Encrypted:	false
SSDEEP:	384:utCD+0eRZo20g+p3elSBKnEjs/M7nvGL3Ss3YQMtEm+K+AV7bnU5LYI++2YV:QR22H4KEo/bDeKspQ
MD5:	003DA7014349DC14452BB166F8A2AF7D
SHA1:	C493FF8D600C343A36E0C291137DEAF67D37E86E
SHA-256:	4CAF983380A247DA3841CA842458B0A0399B081AC8077E7962533FB371F1FCC
SHA-512:	C0AF534E916D7F7BF51649BDF387847809D61481D86232DFB544010DA3DC3F7A9EB0FAD7E2E82AAEBE3DEE895156701CBE6182B2B910A1C2CAFAD00D3202A7EA
Malicious:	false
Preview:	@...e.....d.....j.=1.....A.y.....@.....H.....<@.^L."My...:P..... Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C...%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5...:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'.....L..}).....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ..H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...\$.1.q.....System.ConfigurationP......./C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<.;nt.1System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_djzcf1e1.bda.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_kmqndebx.s0u.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp1585.tmp 	
Process:	C:\Users\user\Desktop\6109238.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1606
Entropy (8bit):	5.1199910671225615
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiQRvh7hwrgXuNtL0xvn:cgeaYrFdOFzOzN33ODOiDdKrsuTww
MD5:	B2C79088E946DE62D82F2E58E5C4FAE7
SHA1:	0E2C066C76F11AC9667555A595873ABE7F0674D6
SHA-256:	39CB5732D5B565108FD6473E39447FCD86078EAD8C4D01EB33AD3C9D825D516E
SHA-512:	E26983344AE2EA7CFB27AADFF50AA43B7498128A94607BB456AED5E7826F39FDF38D79D5977BB3E3A15505F52F4CECC5FCC287BD55C46858CE0CBDA2AA8F7F42
Malicious:	true
Preview:	<?xml version="1.0" encoding="UTF-16"?><Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\eHkVrJJ.exe  	
Process:	C:\Users\user\Desktop\6109238.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	874496
Entropy (8bit):	7.722977017951353
Encrypted:	false
SSDEEP:	24576:QxgV10/5JdlBRMJ0bi7FbjVte9IbUDHDI:ogVWFIBRc0b4FL7U
MD5:	2AEB09E3B19012D3D2ADD45559422416
SHA1:	0364E572469A4BFB486C982348C7FA62CCB7E818
SHA-256:	917E03484856F0980F2150822A231E0F73E3CEF3F074EA1644DCBD1082590399
SHA-512:	EAC61F118AFEB8F0444EF6623795E4D9201FE13C0EB3C6F4C1800331860E2538A1017B3F09D0B20D6FF8496ADBE3F38BDC7E93C154F82A35A64FB2AAA3C2F77D
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L.....b.....0..P.....n.....@..... ..@.....pn..K......H.....text...N...P.....`..rsrc.....R.....@..@..rel oc.....V.....@..B.....n.....H.....{.....0.....*..0..k.....K...%.f...p..r+..p..%r9..p.).....}.....{.....{.....{.....{..... ...~...t...{...(&*..0.....&l..cmZQa%..^E.....+..(.....Z..%a+*..0.....*..0.....7..a%..^E.....n.....[.....\$.9.....A.....8.....XQZ X...a8w.....-..^q.1%+...q?..%&.. ..

C:\Users\user\AppData\Roaming\ehkVrJJ.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\6109238.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\Documents\20220808\PowerShell_transcript.841675.UFIE9n5j.20220808172536.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5807
Entropy (8bit):	5.375386426126985
Encrypted:	false
SSDEEP:	96:BZPTL/NRqDo1ZdZbTL/NRqDo1Z5I/NjZGTL/NRqDo1ZoQddSZ1:7
MD5:	8E2A47A69E2C42272669F5CA452E2967
SHA1:	F1C2A50D71832BEA952FEB45EBAA57C7B16EDEB2
SHA-256:	234721E3D39262F2111F652946F16B84AA45484C2E9F1F0E48E90AF5204E1391
SHA-512:	9545CE5A9475A3D9474F57FDE7CF9D48C2B34FE30DAE4691437DF33DFF624A876CD8BE0AD10155E2FB1D40609C58934DD52C5DCC327CAB286CB149D7F4D755D
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220808172537..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841675 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\ehkVrJJ.exe..Process ID: 5756..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0 .1..*****.*****.Command start time: 20220808172537..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\ehkVrJJ.exe..*****.Windows PowerShell transcript start..Start time: 20220808173031..Username: computer\user..RunAs User: DESKTOP-716

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.722977017951353
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:	6109238.exe
File size:	874496
MD5:	2aeb09e3b19012d3d2add45559422416
SHA1:	0364e572469a4bfb486c982348c7fa62ccb7e818
SHA256:	917e03484856f0980f2150822a231e0f73e3cef3f074ea1644dcbd1082590399
SHA512:	eac61f118afeb8f0444ef6623795e4d9201fe13c0eb3c6f4c1800331860e2538a1017b3f09d0b20d6ff8496adbe3f38bdc7e93c154f82a35a64fb2aaa3c2f77d
SSDEEP:	24576:QxgV10/5JdlBRMJ0bi7FbjVte9IbUDHDI:ogVWFIbRc0b4FL7U
TLSH:	6C05AE5BBF10324DC9A7A975DE4B7C61A7F22C2E3226D0766517380E8AFF342DA11076
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L.....b.....0..P.....n... ..@.. ..@.....

File Icon

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd6e70	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd4ec4	0xd5000	False	0.7882945459213615	data	7.729019884750608	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x398	0x400	False	0.373046875	data	2.8853098954714	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd8058	0x33c	data		

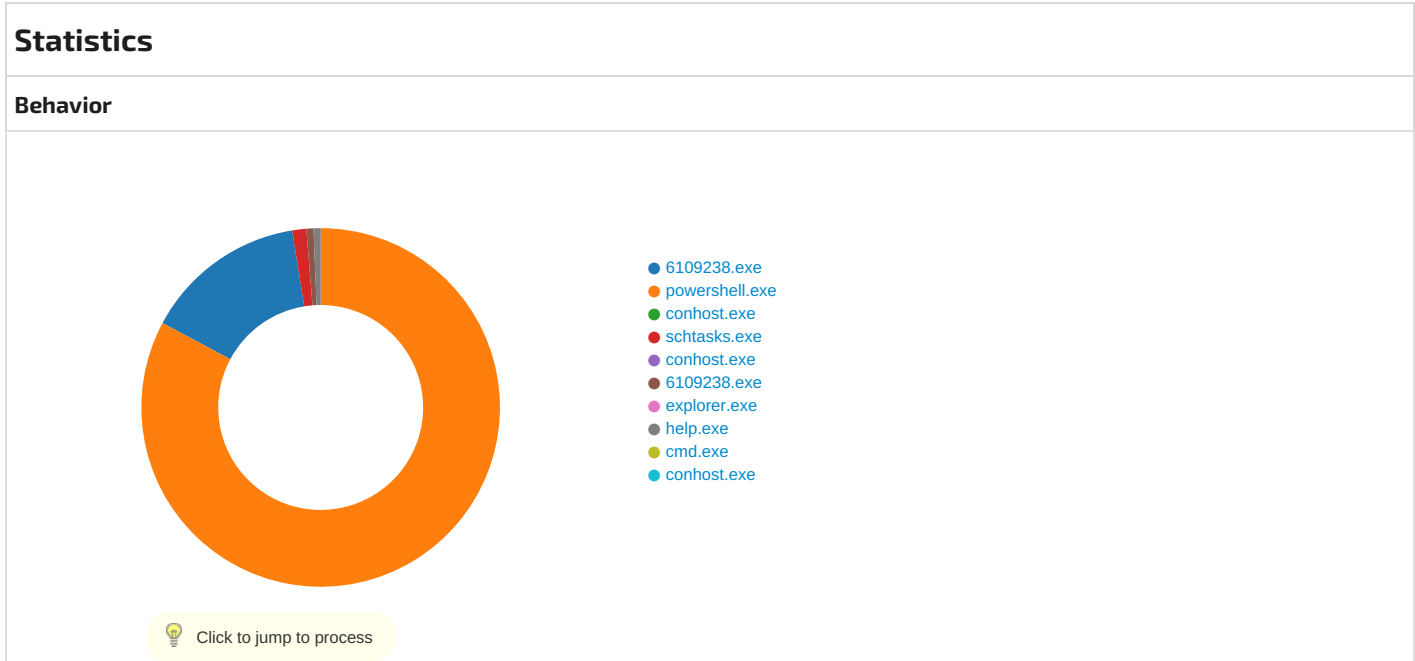
Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior
 No network behavior found

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		
Process: explorer.exe, Module: user32.dll		
Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE8
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE8
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE8
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE8



System Behavior	
Analysis Process: 6109238.exe PID: 1980, Parent PID: 5768	
General	
Target ID:	0
Start time:	17:25:18
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\6109238.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\6109238.exe"
Imagebase:	0xde0000
File size:	874496 bytes
MD5 hash:	2AEB09E3B19012D3D2ADD45559422416
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: 00000000.00000002.442527217.0000000004305000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.442527217.0000000004305000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.442527217.0000000004305000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.442527217.0000000004305000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.433596561.0000000003225000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.439859566.000000000345A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: 5756, Parent PID: 1980

General	
Target ID:	1
Start time:	17:25:34
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HkVrJJ.exe
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CC1CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CC1CF06	unknown	
C:\Users\user\AppData\Local\Temp__PSScripPolicyTest_kmqndebx.s0u.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BA61E60	CreateFileW	
C:\Users\user\AppData\Local\Temp__PSScripPolicyTest_djzcfe1.bda.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BA61E60	CreateFileW	
C:\Users\user\Documents\20220808	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BA6BEFF	CreateDirectoryW	
C:\Users\user\Documents\20220808\PowerShell_transcript.841675.UFIE9n5j.20220808172536.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6BA61E60	CreateFileW	

File Deleted

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@\\@T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;M@D@D@@M @<M@\$M@8M? MBMDmEEMqqS%n4&5 &7&	success or wait	11	6CEE76FC	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBF5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlibb1a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB503DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBFCA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBFCA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBF5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBF5705	unknown	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CC01F73	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BA61B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BA61B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BA61B4F	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	2	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CBF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BA61B4F	ReadFile

Analysis Process: conhost.exe PID: 5064, Parent PID: 5756

General

Target ID:	2
Start time:	17:25:35
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2276, Parent PID: 1980

General

Target ID:	3
Start time:	17:25:35
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\leHkVrJJ" /XML "C:\Users\user\AppData\Local\Temp\tmp1585.tmp
Imagebase:	0xa0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1585.tmp	unknown	2	success or wait	1	AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1585.tmp	unknown	1607	success or wait	1	AABD9	ReadFile

Analysis Process: conhost.exe PID: 1384, Parent PID: 2276

General

Target ID:	4
Start time:	17:25:38
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 6109238.exe PID: 5392, Parent PID: 1980

General

Target ID:	5
Start time:	17:25:41
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\6109238.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6109238.exe
Imagebase:	0xbe0000
File size:	874496 bytes
MD5 hash:	2AEB09E3B19012D3D2ADD45559422416
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: 00000005.00000000.423502729.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.423502729.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.423502729.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.423502729.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: 3688, Parent PID: 5392**General**

Target ID:	9
Start time:	17:25:51
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.498783665.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.498783665.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.498783665.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.498783665.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.519597064.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.519597064.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.519597064.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.519597064.00000000D7E0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: help.exe PID: 2056, Parent PID: 3688**General**

Target ID:	10
Start time:	17:26:32
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x12d0000
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: 0000000A.00000002.640356208.0000000000EC0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.640356208.0000000000EC0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.640356208.0000000000EC0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.640356208.0000000000EC0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.640116150.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.640116150.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.640116150.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.640116150.0000000000E80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.639269207.0000000000C70000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.639269207.0000000000C70000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.639269207.0000000000C70000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.639269207.0000000000C70000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities						
File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	C8A447	NtReadFile

Analysis Process: cmd.exe PID: 5596, Parent PID: 2056	
General	
Target ID:	11
Start time:	17:26:38
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\luser\Desktop\6109238.exe"
Imagebase:	0xed0000
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							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6112, Parent PID: 5596	
General	
Target ID:	12
Start time:	17:26:39
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000

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

 No disassembly