ID: 680430
Sample Name: vbc.exe
Cookbook: default.jbs
Time: 15:48:12
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

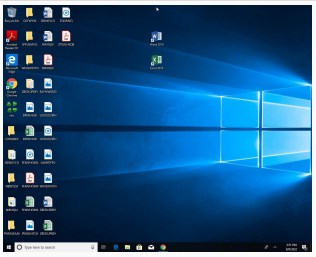
Windows Analysis Report

vbc.exe

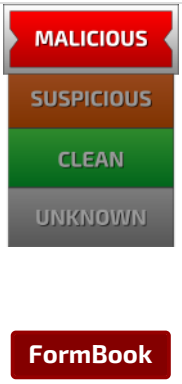
Overview

General Information

Sample Name:	vbc.exe
Analysis ID:	680430
MD5:	2fd70987e440c0..
SHA1:	1fbf7460b77d633.
SHA256:	46b08ac7a1a467..
Tags:	exe
Infos:	



Detection



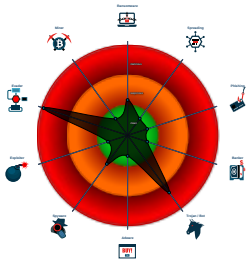
FormBook

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
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- vbc.exe (PID: 6192 cmdline: "C:\Users\user\Desktop\vbc.exe" MD5: 2FD70987E440C0351B1CE6BA45568868)
  - powershell.exe (PID: 6492 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6508 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\svyewSjGVGtgt" /XML "C:\Users\user\AppData\Local\Temp\tmp8F67.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vbc.exe (PID: 6748 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 6432 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.danetsystem.com/x8ut/"
  ],
  "decoy": [
    "mUYLEBuVKFsO",
    "Bi9gZRFSHUmFLCtq/7U=",
    "FbmmfzSUYXSePwRymyniT3oEeK79",
    "udVNLrDQnqjROz4uqn9FqdOIYA==",
    "W0IuGtY0/QXuXQlo6ZRWeMvJhq31",
    "q7sxIMoN9y2Sjda8WFtJqdOIYA==",
    "wUCsjyxXWHJujLSbJQn3ImshLMYdSfw=",
    "YpHPPzxXNnlwnTzt0BbJ+Gjk",
    "YZTMKoDNnNdjWIFKPH3rXqns",
    "bxHZySMSzymSNA==",
    "znV02t/6orjqlYeiGr8=",
    "eygnfJgRpsibwQz6pg==",
    "Hkt+9xJAGS3rTUoouw==",
    "z/Fq9d3ksMa/rlCa",
    "ALeXgBFSDRF6Y45Q+wR8neDWE+8=",
    "u2QZIK+8sOklBZ34rw==",
    "ex3XYKf3ts9aBPnUV086qdOIYA==",
    "ttMVj0CBfsW/rlCa",
    "AydNsr7ejaGWvyGUJxB0oPU=",
    "fyo5sLzbrL+LoUYbsg==",
    "TmpyUx16WZvOfTouuA==",
    "f2ynAEXel84KdWYxtmAnVsQGYniCS3DM",
    "Zfzu7VZxWY/OfTouuA==",
    "iX+zJSo39iLyFrcIILqnyDS8Tx27dQ==",
    "35RMMbTZuedQA1YWqrG+81cNyiWoIOJwxA==",
    "b4P0Wpj+tMa/rlCa",
    "ZgB2UP1xPsqI7j/w70o8qdOIYA==",
    "0PN1YODem705EyNKc9KSwf0=",
    "KhvWi6bMp/UxYSc=",
    "DCx4mMdtzloIgDg=",
    "mAa2j+gmr9VD5u/2x4Vwkg==",
    "wKyp/gqNP18T",
    "PxUPcIGYd6eavi6fuC7rXqns",
    "03x33AUsGmpV0u3/Xn05mvM=",
    "O2+Z/P4Y8icXike0KxB0oPU=",
    "kge9qTmWeMa2SoeiGr8=",
    "AC9QRQ5zHYN69b4wWbc=",
    "G0d95OYE4loIgDg=",
    "Og0cip/Yj6/oklGuvysuRbsrOMS1DPQ=",
    "fOloUMXKx/koBZ34rw==",
    "AyNYruhCG1QLLmqFB71/",
    "OGOK8gcyAT1pEjUMx4Vwkg==",
    "0fd+BEOuhM/V8mC40g7OPUK+eQ==",
    "bxgH4qb2trOk4oeiGr8=",
    "xjKwL1qcX2vRyGr91Gto",
    "xjCeFGLgrMOLoUYbsg==",
    "gZ8Tgsw3DET86p2yzWpq",
    "VL9udRpGzymSNA==",
    "07D5V6EvzymSNA==",
    "z3sjDrwI+SdrIPdh4pNKqNLLXGy7HfQ=",
    "eLHjUiyXeLfZfV791Gto",
    "EEdy5PwP1uqjwfK8WEcEYZdVLb+afQ==",
    "cG6wIP7vzhCcOST6x4Vwkg==",
    "JiEkhou0n8a/rlCa",
    "MaJQKY6IRvS/rlCa",
    "/uvi2Z4G8DFb/xNT5KY=",
    "DTlm3fpB7gAy26A3FpaSzP0=",
    "cRPDizBcKjfwIcY5ZPXnGo7O6zFHPm7K",
    "B7dhSMi6kc0x5vP0x4Vwkg==",
    "y7zoUktTNl0Qb2A74r9g",
    "DQpAv9TzwMm/rlCa",
    "4VH0zD4z+wgXwjWQ",
    "jKP03nOMcHi1lAFkZrc=",
    "kTfm0oHkyfN2Jg3g1ge02lD8vSGlIOJwxA=="
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
vbc.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.433034346.0000000002ADD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d7a0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa93f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16b67:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16965:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16411:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16a67:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16bdf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa50a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1565c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb252:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c3e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18e49:$sqlite3step: 68 34 1C 7B E1 • 0x18f7c:$sqlite3step: 68 34 1C 7B E1 • 0x18e8b:$sqlite3text: 68 38 2A 90 C5 • 0x18fd3:$sqlite3text: 68 38 2A 90 C5 • 0x18ea2:$sqlite3blob: 68 53 D8 7F 8C • 0x18ff5:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.vbc.exe.3b73cf8.7.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.vbc.exe.3b73cf8.7.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x33421:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x5e441:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x88461:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x4a5c0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x755e0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9f600:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x3775f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x6277f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x8c79f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x43987:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83 • 0x6e9a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83 • 0x989c7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0.2.vbc.exe.3b73cf8.7.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x43785:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x6e7a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x987c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x43231:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x6e251:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x98271:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x43887:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x6e8a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x988c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x439ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x6ea1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x98a3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x3732a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x6234a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x8c36a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x4247c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x6d49c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x974bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x38072:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x63092:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x8d0b2:$sequence_7: 66 89 0C 02 5B 8B E5 5D
0.2.vbc.exe.3b73cf8.7.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x45c69:$sqlite3step: 68 34 1C 7B E1 • 0x45d9c:$sqlite3step: 68 34 1C 7B E1 • 0x70c89:$sqlite3step: 68 34 1C 7B E1 • 0x70dbc:$sqlite3step: 68 34 1C 7B E1 • 0x9aca9:$sqlite3step: 68 34 1C 7B E1 • 0x9addc:$sqlite3step: 68 34 1C 7B E1 • 0x45cab:$sqlite3text: 68 38 2A 90 C5 • 0x45df3:$sqlite3text: 68 38 2A 90 C5 • 0x70ccb:$sqlite3text: 68 38 2A 90 C5 • 0x70e13:$sqlite3text: 68 38 2A 90 C5 • 0x9aceb:$sqlite3text: 68 38 2A 90 C5 • 0x9ae33:$sqlite3text: 68 38 2A 90 C5 • 0x45cc2:$sqlite3blob: 68 53 D8 7F 8C • 0x45e15:$sqlite3blob: 68 53 D8 7F 8C • 0x70ce2:$sqlite3blob: 68 53 D8 7F 8C • 0x70e35:$sqlite3blob: 68 53 D8 7F 8C • 0x9ad02:$sqlite3blob: 68 53 D8 7F 8C • 0x9ae55:$sqlite3blob: 68 53 D8 7F 8C
0.0.vbc.exe.660000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 4 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

Multi AV Scanner detection for dropped file

Networking

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

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

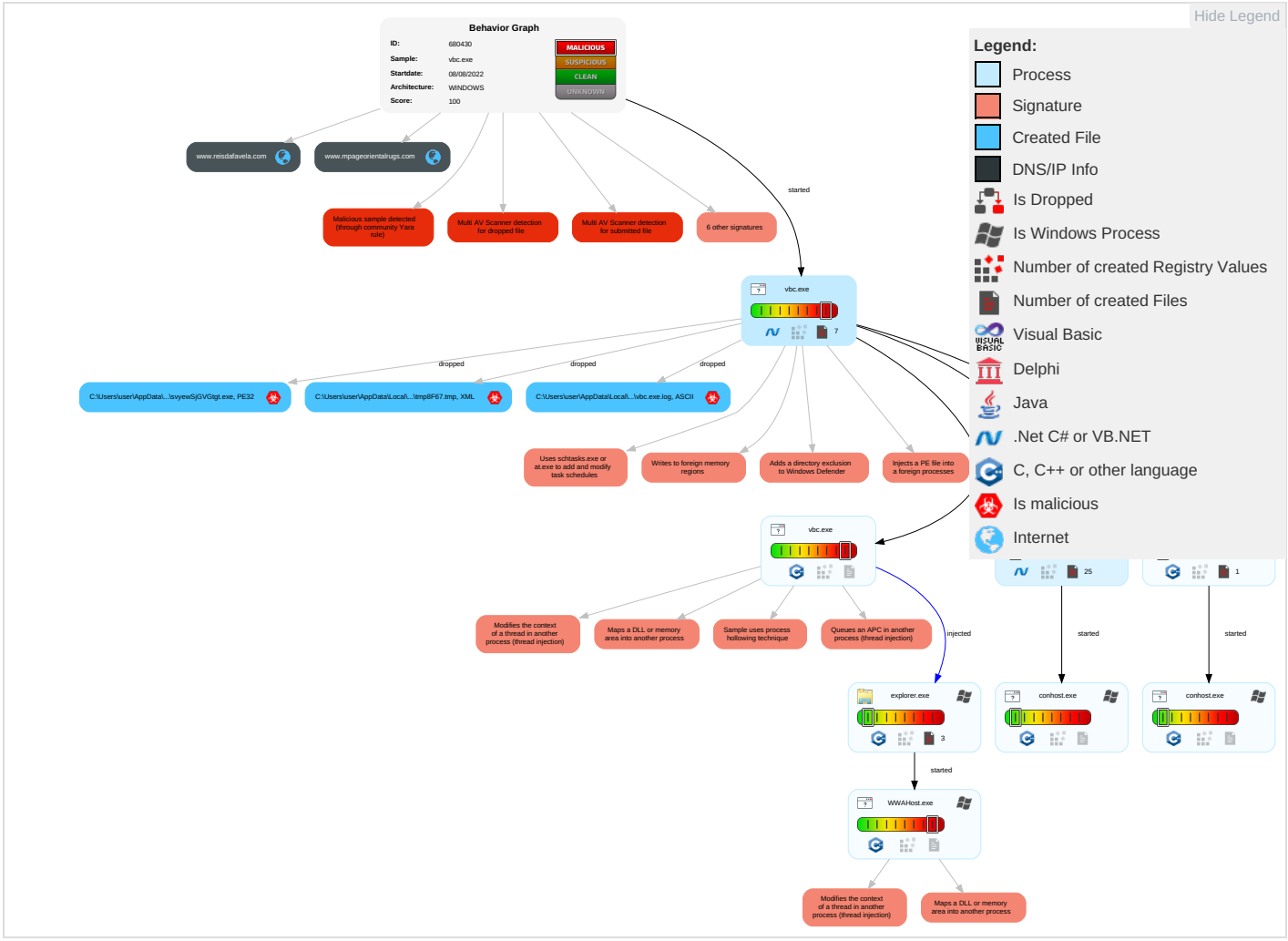
Yara detected FormBook

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	6 1 2 Process Injection	1 Masqueradi ng	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initializatio n Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualizatio n/Sandbox Evasion	Security Account Manager	3 1 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati on	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscat e/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.commo n	Rc.commo n	3 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic ation	Jamming or Denial of Service		Abuse Accessibilit y Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Manageme nt	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

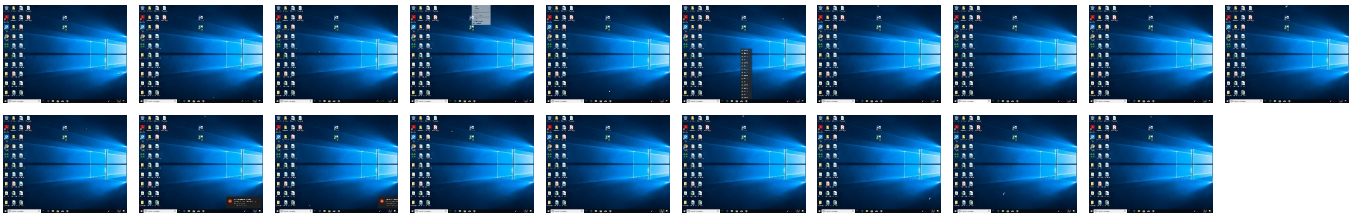
Behavior Graph



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
vbc.exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

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

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.com=	0%	Avira URL Cloud	safe	
http://ns.adobY	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.danetsystem.com/x8ut/	0%	Avira URL Cloud	safe	
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://boards.4chan.org3Retrieving	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.reisdafavela.com	198.50.252.64	true	false		unknown
www.mpageorientalrugs.com	199.59.243.220	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.danetsystem.com/x8ut/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com=	vbc.exe, 00000000.00000003.362484787.000000000110C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobY	explorer.exe, 0000000D.00000000.48269449 0.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000D.00000000.437285891.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000D.00000000.514496245.00000000026D0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000D.00000000.582671646.00000000026D0000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://boards.4chan.org/b/	vbc.exe, svyewSjGVGtgt.exe.0.dr	false		high
http://www.fontbureau.com/designers?	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000000.00000003.362484787.000000000110C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://boards.4chan.org3Retrieving	vbc.exe, svyewSjGVGtgt.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://images.4chan.org/	vbc.exe, svyewSjGVGtgt.exe.0.dr	false		high
http://www.urwpp.deDPlease	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000000.00000002.433034346.0000000002ADD000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000000.00000002.435077515.0000000002D26000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	vbc.exe, 00000000.00000002.441794995.0000000006B22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680430
Start date and time: 08/08/202215:48:12	2022-08-08 15:48:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vbc.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:	27
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@10/8@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 89.4% (good quality ratio 78%) • Quality average: 72% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 97% • 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, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior 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.

Simulations

Behavior and APIs

Time	Type	Description
15:49:44	API Interceptor	1x Sleep call for process: vbc.exe modified
15:49:52	API Interceptor	17x 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\vbc.exe.log

Process:	C:\Users\user\Desktop\vbc.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**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	22044
Entropy (8bit):	5.605422146552003
Encrypted:	false
SSDEEP:	384:ltCDL7LAR404OYSBKnEjsE7nvGL3Ss3YcMtEm+y+AV7gMWIwLYI++zyv:CS409Y4KEozDSKEsy1
MD5:	8838823AC054A0478910CFA8271674A2
SHA1:	C98923EA621F79B96994728D3B46EC2E88C58A22
SHA-256:	DB299AC84ED574EE9514A2CD374189118D69A619D506B0A35350165AD163B2EF
SHA-512:	34AD80087C4C3878C55099B0AE860BD273C11A464EB35E212DAF58DFE5FD79288811BB79528069BD00D48B552295ACD435DA174EBE4867FE2D732E241AD9A671
Malicious:	false
Reputation:	low
Preview:	@...e.....?.....m.:.2.....@.X.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.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.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ifas2zv3.1tq.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__PSScriptPolicyTest_yvgpjfng.m1e.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\tmp8F67.tmp

Process:	C:\Users\user\Desktop\vbc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1616
Entropy (8bit):	5.137169455237211
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtTxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTNv
MD5:	FF07B22E748EA6A46D61392F077BB03C
SHA1:	41A9F6631C8124F65DBB1DE38E916B227F2BB7DF
SHA-256:	97360A802B86E1ED2E15B9D5CEA6795ABC8D4078F7A9DC411428687E4CC6267D

SHA-512:	FDD6061FBC633442B66AB51264BCB24F24C15FAFD885242F0653A87E8422FA2939363F2B38B21D7CE6694B5B48ECACF7E803BEAFE723C4A531D129D7D6E61D0
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</StartWhenAvai

C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe

Process:	C:\Users\user\Desktop\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	980480
Entropy (8bit):	7.45173526736637
Encrypted:	false
SSDEEP:	24576:Ki6ry6N+Io9b2VyRRptoX82u4nTDe9IbUDHDlC:KiN6NTMrRRy1ue7UI
MD5:	2FD70987E440C0351B1CE6BA45568868
SHA1:	1FBF7460B77D6335CA56F5DD0BF274049436AB62
SHA-256:	46B08AC7A1A467F9D8053AAF6853500A32FD5C4B1ACD747A9A83134F59115424
SHA-512:	D23242DE267CDEB1C7E08955725ADDC560D441D1181F04885C9813157AF3A94639AA463EAA21456C5518A2F71FEB6AB40FE7C2A596D5FC75759D941D5EFDFD8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....i.b.....0.....B(... ...@....@.. .....@.....@.....'..O....@..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc..... .....@..B.....$(.....H.....<+.....X....+.....0..V.....~....~*...(+.....,5.(....&r...p(,....+...r...p(....%.....~*...(+.....-..~.....(....&*...0..!.....~....~*...(-.....,-.....(....&*....0..\.....s.....~....r/..p(/.....,.(0.....~....(1...o2...&..r1..po2...&..o2...&..o2...&.o3...(.....*:..r]..p(.....*..0..\.....s.....~....r/..p(/.....,.(0.....~....(1...o2...&.ra..po2...&..o2...&..o2...&.o3...(.....*:..r]..p(.....*..0..\.....s.....~

C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\vbc.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220808\PowerShell_transcript.124406.zAYrvPjT.20220808154951.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):	5841
Entropy (8bit):	5.399056258409197
Encrypted:	false
SSDEEP:	96:BZIA6FNEqDo1ZuMZ96FNEqDo1Zg5XBjZ96FNEqDo1Z38RRvZo:0hn
MD5:	7F9D4AF83AFC9696935D6A5C85E861EC
SHA1:	0DBD97C17C16B00E10D0E976DB641EAED4234FF9
SHA-256:	17A265782A76ED320328F53D902AF79B3E9F991DAD11681E6FEAF078E0BD0366
SHA-512:	3EB43C3491D0080D188961EFA1707508FE216273AE57130E34673FDB0576BB829F368DAD2B105D9E9DC12BFBBC93067CE37B3F7CB06B2378955ED4B2CFF3E3AC
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220808154952..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (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\svyewSjGVGtgt.exe..Process ID: 6492..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: 20220808154952..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\svyewSjGVGtgt.exe..**********..Windows PowerShell transcript start..Start time: 20220808155212..Username: computer\user..RunAs

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.45173526736637
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:	vbc.exe
File size:	980480
MD5:	2fd70987e440c0351b1ce6ba45568868
SHA1:	1fbf7460b77d6335ca56f5dd0bf274049436ab62
SHA256:	46b08ac7a1a467f9d8053aaf6853500a32fd5c4b1acd747a9a83134f59115424
SHA512:	d23242de267cdeb1c7e08955725addc560d441d1181f04885c9813157af3a94639aa463eaa21456c5518a2f71feb6ab40fe7c2a596d5fc75759d941d5efdfde8
SSDEEP:	24576:Ki6ry6N+Io9b2VyRRptoX82u4nTDe9IbUDHDlC:KiN6NTMrRRy1ue7UI
TLSH:	C125AD17AFA07708E4F75BB8DD6B686183F63809617ED2792E905C9F2DFA300D50162B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....i.b.....0.....B(... ...@....@.. .....@.....@.....

File Icon

Icon Hash:	c68ce86ecc8c8ac8

Static PE Info

General

Entrypoint:	0x4e2842
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F069A6 [Mon Aug 8 01:40:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
mov bh, 1Dh

Instruction
rol dword ptr [esi+ebp*2], 3Bh
or byte ptr [ecx], FFFFFFD9h
inc ebx
or eax, 130476DCh
imul ebp, dword ptr [ebx-3Bh], 17h
mov dl, 4Dh
xchg byte ptr [edx], bl
add eax, B81E4750h
in eax, dx
or byte ptr [esi], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe27f0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0xd4bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf2000	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	0xe1bc0	0xe1c00	False	0.7346626695736435	data	7.58951432122368	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0xd4bc	0xd600	False	0.2766683703271028	data	3.757541169308502	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf2000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe4128	0x94a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xed5e0	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xefb98	0x10a8	data		
RT_ICON	0xf0c50	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf10c8	0x3e	data		
RT_VERSION	0xf1118	0x3a0	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 15:51:43.529246092 CEST	53907	53	192.168.2.7	8.8.8.8
Aug 8, 2022 15:51:43.554703951 CEST	53	53907	8.8.8.8	192.168.2.7
Aug 8, 2022 15:51:48.779010057 CEST	63852	53	192.168.2.7	8.8.8.8
Aug 8, 2022 15:51:48.888549089 CEST	53	63852	8.8.8.8	192.168.2.7

DNS Queries

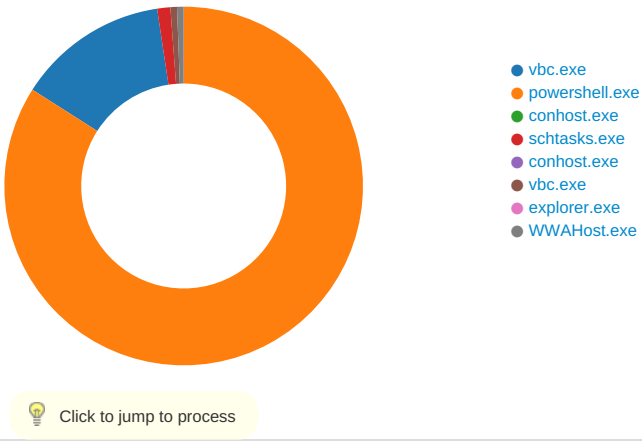
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 15:51:43.529246092 CEST	192.168.2.7	8.8.8.8	0x1b2f	Standard query (0)	www.reisdafavela.com	A (IP address)	IN (0x0001)
Aug 8, 2022 15:51:48.779010057 CEST	192.168.2.7	8.8.8.8	0x1653	Standard query (0)	www.mpageorientalrugs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 15:51:43.554703951 CEST	8.8.8.8	192.168.2.7	0x1b2f	No error (0)	www.reisdafavela.com		198.50.252.64	A (IP address)	IN (0x0001)
Aug 8, 2022 15:51:48.888549089 CEST	8.8.8.8	192.168.2.7	0x1653	No error (0)	www.mpageorientalrugs.com		199.59.243.220	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: vbc.exe PID: **6192**, Parent PID: **968**

General

Target ID:	0
Start time:	15:49:24
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vbc.exe"
Imagebase:	0x660000

File size:	980480 bytes
MD5 hash:	2FD70987E440C0351B1CE6BA45568868
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.433034346.0000000002ADD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.435077515.0000000002D26000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.437207129.0000000003B73000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.437207129.0000000003B73000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.437207129.0000000003B73000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.437207129.0000000003B73000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **6492**, Parent PID: **6192**

General

Target ID:	4
Start time:	15:49:49
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\svyewSjGVGtgt.exe
Imagebase:	0xf0000
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:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BDE5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BDE5B28	unknown
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	6D03CF06	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	6D03CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ifas2zv3.1tq.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE81E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yvgpjfng.m1e.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE81E60	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	6BE8BEFF	CreateDirectoryW
C:\Users\user\Documents\20220808\PowerShell_transcript.124406.zAYrvPjT.20220808154951.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BE81E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ifas2zv3.1tq.ps1	success or wait	1	6BE86A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yvgpjfng.m1e.psm1	success or wait	1	6BE86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDE5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ifas2zv3.1tq.ps1	0	1	31	1	success or wait	1	6BE81B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yvgpjfng.m1e.psm1	0	1	31	1	success or wait	1	6BE81B4F	WriteFile
C:\Users\user\Documents\20220808\PowerShell_transcript.124406.zAYrvPjT.20220808154951.txt	0	3	ff		success or wait	1	6BE81B4F	WriteFile
C:\Users\user\Documents\20220808\PowerShell_transcript.124406.zAYrvPjT.20220808154951.txt	3	692	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 38 30 38 31 35 34 39 35 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********Windows PowerShell transcript startStart time: 20220808154952Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 124406 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	44	6BE81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 3f 14 00 00 19 00 00 00 fd 0e 6d 05 3a 09 32 09 fd 08 00 00 40 01 58 00 08 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e?m:2@X@	success or wait	1	6D3076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	6D3076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D3076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D3076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D3076FC	WriteFile
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 40 01 3f 4d 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 35 26 40 01 37 26 40	T@>@@V@H@X@[@NT@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@?M@BM@D@mE@EM@q@q@S@%@n@4&@5&@7&@	success or wait	11	6D3076FC	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	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D01CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D01CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D01CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D015705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	6D021F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	22408	success or wait	1	6D02203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6CF703DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	62	success or wait	1	6BE81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	990	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	990	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker \AppLocker.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClien t\AppvClient.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClien t\AppvClient.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClien t\AppvClient.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClien t\AppvClient.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6CF703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx .psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx .psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker \BitLocker.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker \BitLocker.psd1	unknown	368	end of file	1	6BE81B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D015705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE81B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6BE81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BE81B4F	ReadFile

Analysis Process: conhost.exe PID: **6500**, Parent PID: **6492**

General

Target ID:	5
Start time:	15:49:49
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: **6508**, Parent PID: **6192**

General

Target ID:	6
Start time:	15:49:49
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\svyewSjGVGtgt" /XML "C:\Users\user\AppData\Local\Temp\tmp8F67.tmp
Imagebase:	0xf70000
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\tmp8F67.tmp	unknown	2	success or wait	1	F7AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8F67.tmp	unknown	1617	success or wait	1	F7ABD9	ReadFile

Analysis Process: conhost.exe PID: **6608**, Parent PID: **6508**

General

Target ID:	7
Start time:	15:49:51
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: vbc.exe PID: **6748**, Parent PID: **6192**

General

Target ID:	9
Start time:	15:49:58
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xd70000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
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: 00000009.00000000.426521887.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.426521887.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.426521887.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.426521887.0000000000401000.00000040.00000400.00020000.00000000.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	41AE47	NtReadFile

Analysis Process: explorer.exe PID: **3808**, Parent PID: **6748**

General

Target ID:	13
Start time:	15:50:03
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
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: 0000000D.00000000.501771022.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.501771022.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.501771022.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.501771022.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000000.535893743.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000000.535893743.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000000.535893743.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000000.535893743.000000000B529000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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: WWAHost.exe PID: **6432**, Parent PID: **3808**

General

Target ID:	20
Start time:	15:50:56
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0xde0000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.623504800.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.625773894.0000000002F80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000002.625773894.0000000002F80000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.625773894.0000000002F80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.625773894.0000000002F80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.626309765.0000000003440000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000002.626309765.0000000003440000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.626309765.0000000003440000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.626309765.0000000003440000.00000040.80000000.00040000.00000000.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	345AE47	NtReadFile

Disassembly

No disassembly