ID: 562159
Sample Name: overdue invoices.exe
Cookbook: default.jbs
Time: 15:17:55
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

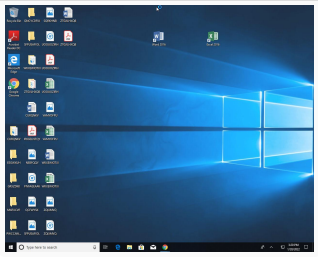
Windows Analysis Report

overdue invoices.exe

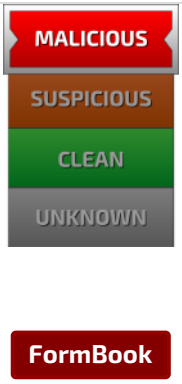
Overview

General Information

Sample Name:	overdue invoices.exe
Analysis ID:	562159
MD5:	e53e6bdf25f7c3b..
SHA1:	3c91623488f8e6..
SHA256:	a2e21d596824ac..
Tags:	exe Formbook xloader
Infos:	



Detection



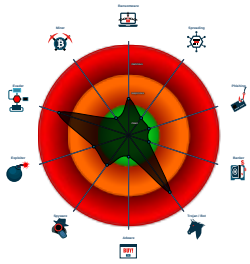
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for drop…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Machine Learning detection for sam…
- Self deletion via cmd delete
- Sigma detected: Suspicious Svchos…

Classification



Process Tree

- **System is w10x64**
- overdue invoices.exe (PID: 5240 cmdline: "C:\Users\user\Desktop\overdue invoices.exe" MD5: E53E6BDF25F7C3BCA385A3021E373061)
  - overdue invoices.exe (PID: 6680 cmdline: "C:\Users\user\Desktop\overdue invoices.exe" MD5: E53E6BDF25F7C3BCA385A3021E373061)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - svchost.exe (PID: 7072 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
      - cmd.exe (PID: 5964 cmdline: /c del "C:\Users\user\Desktop\overdue invoices.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - explorer.exe (PID: 4768 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.storenight.store/rh64/"
  ],
  "decoy": [
    "apx-consultoria.com",
    "naweekjanel.quest",
    "redcrossedgames.com",
    "braswellrestaurantgroup.com",
    "kakazaixian.com",
    "northernnightsky.com",
    "pauschalreisen.xyz",
    "getloyalclients.com",
    "fuckinggril.xyz",
    "kovtor.com",
    "harshalkadam.com",
    "lihsin.com",
    "blablacar-official.online",
    "zaratepsicologia.online",
    "taijaswanston.com",
    "babytono.com",
    "sunnycraftsman.com",
    "shicharroz.com",
    "dollytrailer.com",
    "vende-digital.com",
    "isaacsrealestate.net",
    "crecerspa.com",
    "themeraptor.com",
    "ptjl888.com",
    "iwanster.com",
    "shallmavis.com",
    "myowncorks.com",
    "centscert.com",
    "mysalonphotography.com",
    "goetzerehnstiftung.net",
    "hsee-sl.com",
    "bestuk-fixedrates.com",
    "atspom.com",
    "clashofclansapk.net",
    "pipszone.com",
    "graburballz.com",
    "petektemizlemehizmeti.com",
    "balancebybita.com",
    "cfdphind.com",
    "fsg-trading.com",
    "christinascleaningsvcsfl.com",
    "textile.wiki",
    "446321.com",
    "radiomuskan.com",
    "crystaltopagent.net",
    "andrewspellman.xyz",
    "afroonline.net",
    "shurommo.com",
    "obesite-morlaix.com",
    "encodexbd.com",
    "novemed.com",
    "perfumeghor.com",
    "dharma33.com",
    "potoobrant.com",
    "pravozachitapotreb.store",
    "enrevologix.net",
    "animositiesscale.info",
    "webgem-strategies.com",
    "ruralspices.com",
    "bibipopiah.com",
    "livebtctrades.com",
    "cannabisconnectionmt.com",
    "ammarus.com",
    "buildandrise.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.385434941.000000000F71F000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.385434941.000000000F71F000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.overdue invoices.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.overdue invoices.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.overdue invoices.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
1.0.overdue invoices.exe.400000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.0.overdue invoices.exe.400000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Overview

System Summary

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

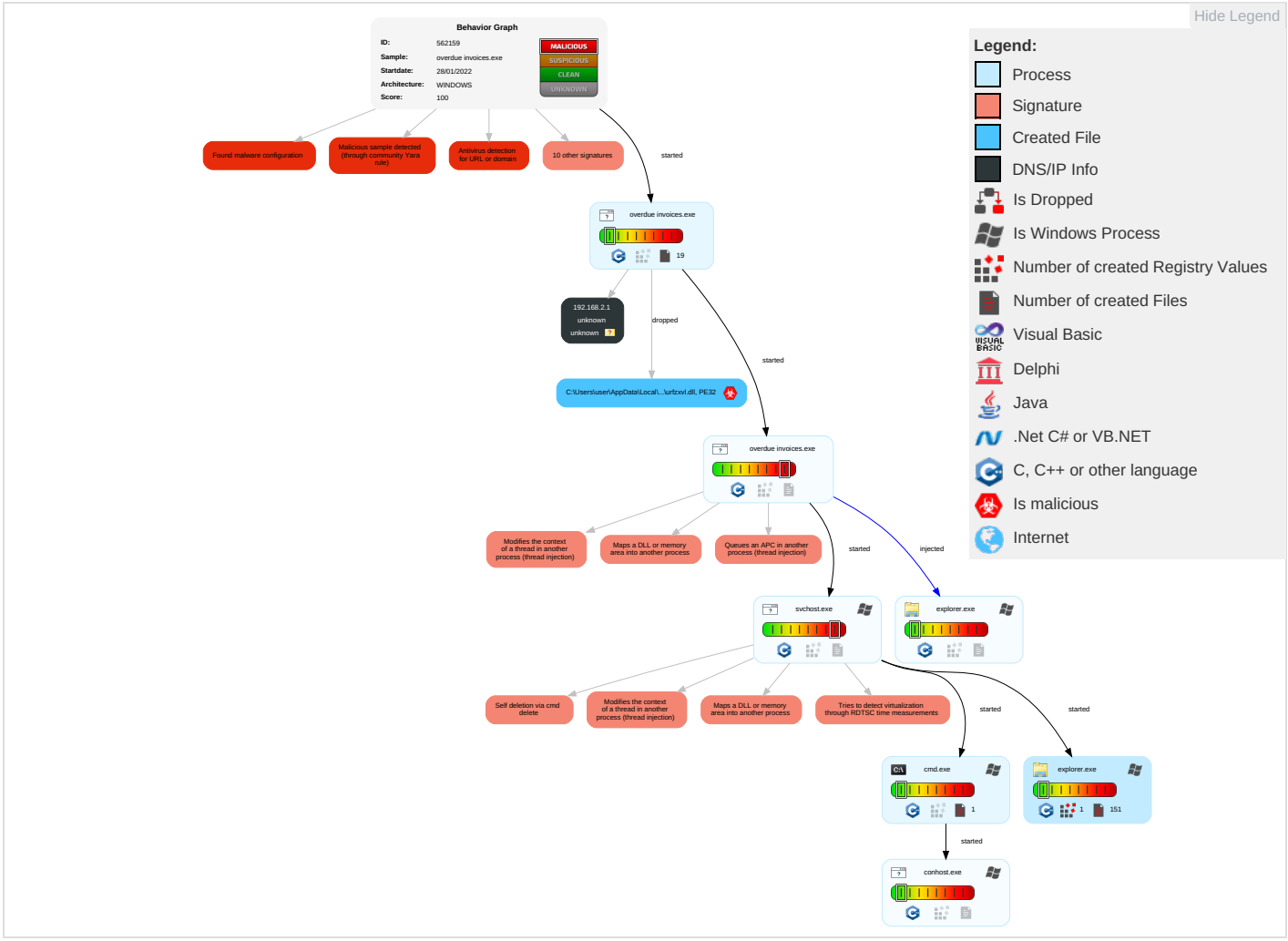
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	3 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Virtualization/Sandbox Evasion	LSASS Memory	2 4 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 2 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

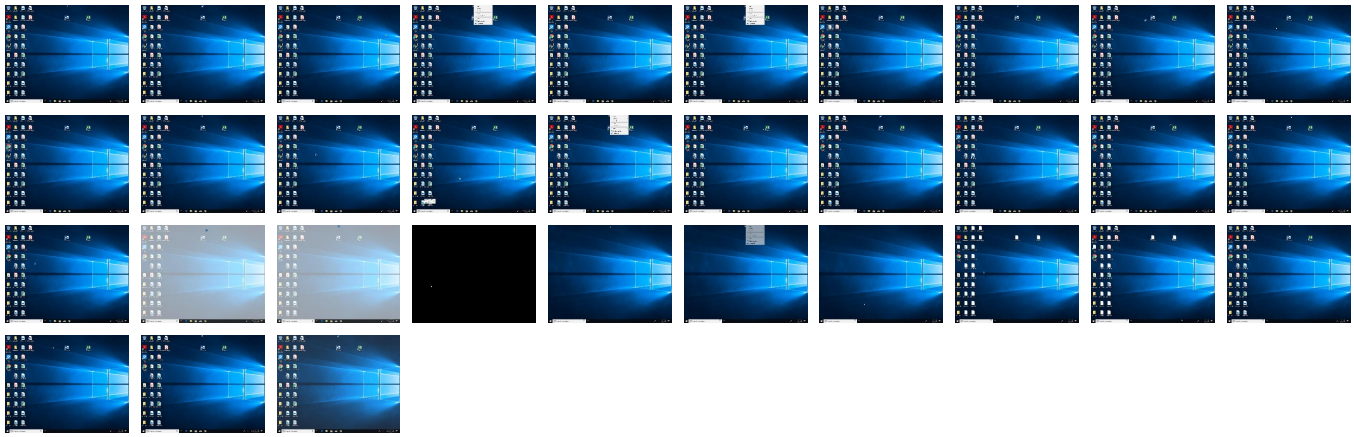
Behavior Graph



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
overdue invoices.exe	36%	Virustotal		Browse
overdue invoices.exe	26%	ReversingLabs	Win32.Trojan.Risis	
overdue invoices.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsz4671.tmp\urfzxvl.dll	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsz4671.tmp\urfzxvl.dll	16%	ReversingLabs	Win32.Trojan.Sdum	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.explorer.exe.88e796c.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.overdue invoices.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
20.0.explorer.exe.88e796c.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.0.explorer.exe.88e796c.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.overdue invoices.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.overdue invoices.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.overdue invoices.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.overdue invoices.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.overdue invoices.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
20.0.explorer.exe.88e796c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.svchost.exe.2c16000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.overdue invoices.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
11.2.svchost.exe.383796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.overdue invoices.exe.21a0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.overdue invoices.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.storenight.store/rh64/	3%	Virustotal		Browse
www.storenight.store/rh64/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

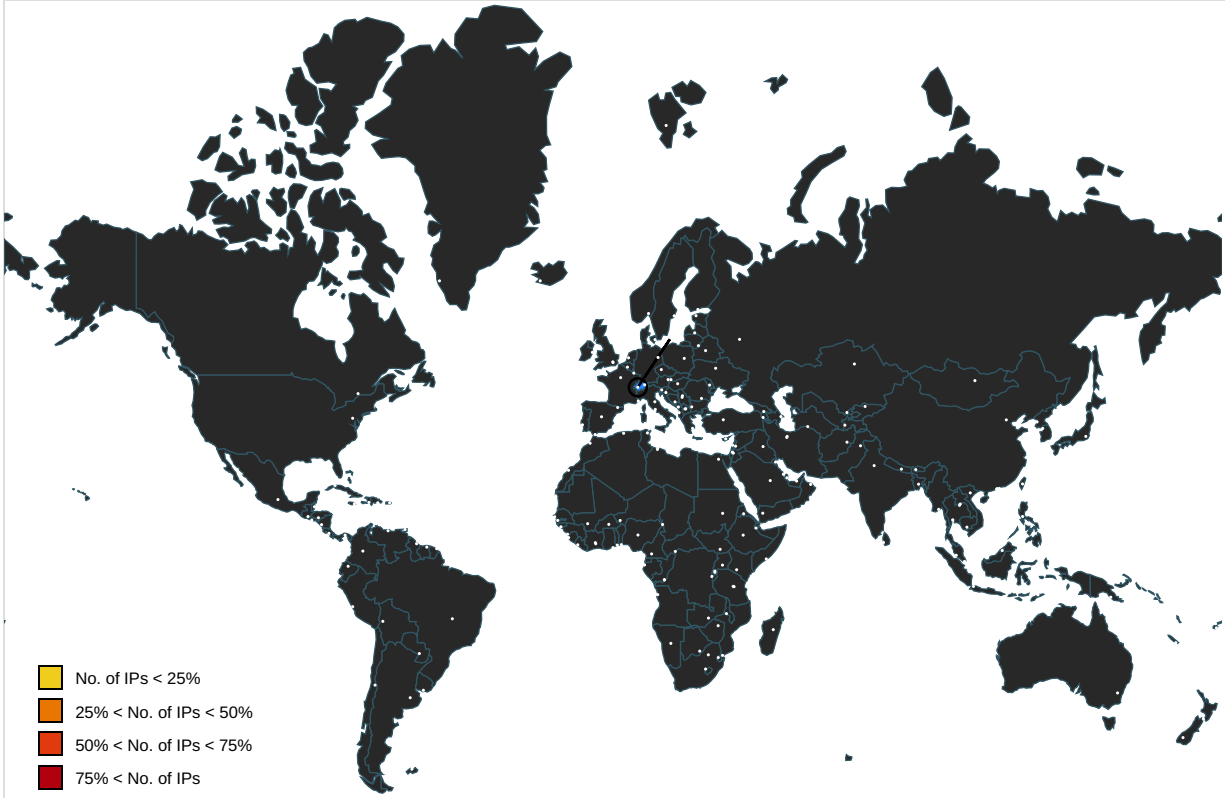
Name	Malicious	Antivirus Detection	Reputation
www.storenight.store/rh64/	true	• 3%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000005.00000000.38988029 0.000000000095C000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 005.00000000.357320779.000000000095C000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000005.00000000.420908981.000000 000095C000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000005.0000 0000.371882109.000000000095C000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	overdue invoices.exe, overdue invoices.exe, 000000 00.00000000.342336809.0000000000409000.0 0000008.00000001.01000000.00000003.sdmp, overdue invoices.exe, 00000000.00000002.353122481 .0000000000409000.00000004.00000001.0100 0000.00000003.sdmp, overdue invoices.exe, 00000001.00000000.346609456.0000000000 409000.00000008.00000001.01000000.000000 03.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	overdue invoices.exe, 00000000.00000000.342336809.0000000000409000.00000008.00000001.01000000.00000003.sdmp, overdue invoices.exe, 00000000.00000002.353122481.000000000409000.00000004.00000001.01000000.00000003.sdmp, overdue invoices.exe, 00000001.00000000.346609456.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562159
Start date:	28.01.2022
Start time:	15:17:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	overdue invoices.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/4@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65.2% (good quality ratio 59.7%) • Quality average: 72.2% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, conhost.exe, svchost.exe, mobsync.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:20:17	API Interceptor	133x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\8y4ukil5ffpt2o

Process:	C:\Users\user\Desktop\overdue invoices.exe
File Type:	data
Category:	dropped
Size (bytes):	218569
Entropy (8bit):	**7.994840241040685**
Encrypted:	**true**
SSDEEP:	6144:JzkhtuwSrhQwHd/yprd9NGAOhxr9xN+abfRzyqtgR71GO:wtutltdCB/TO7PN+UfRzyx1GO
MD5:	A2B4716C51728E07EE484B239DE63E38
SHA1:	ABD1539EBA912CD443BACBDC6F4AB5B5DD9297ED
SHA-256:	97E5CD0634551C8FFBBF5CAE36DC4477AE7477EDE0B21F55887FF703C6DB5BF3
SHA-512:	92BF047D0AC3B6D8F4CC6AA48DD88A815346B9879DE26A746ED70B12C57280CBEED3CD1782BCE75CDFC5F5E11E11EFF2D14A814E8441C7A6B3A961B2A9A1E8A0
Malicious:	false
Reputation:	low
Preview:	..h._c.-...XJq.V.........S?.G._.h.....+q...K*.j.X.8f........v.....g*,.7..u|w(2.6..E....I..|.Z..[y....q ...Z.r...s1R.L.. .w....#.X....J\.....J]...5..|.I.KE~e...C...|I.@;....p...".U..v..U...In.N6vm.$..*..s...Q..f.....~>.....N50`TQDm.G../. U.j.]/..Ec.-..P.R....!..M...<..>hG._.....+qf..K*.j.X.8f....K...&.5.;\.]..<.v.Y.;?........5W..u*.o...X.p.....>....e.1R.L.. ..A..B...n.[..&.'b.*..i.....-N4ko.J@.V.~c[....R...\|..p...)OU.~... I...n.N6vmY$..=...r.LdQ..f.....>.....N50.TQ.m.G../. ..j../..Ec.-..\.R.....!..M.".<..>.G._.h.....+q...K*.j.X.8f....K...&.5.;\.]..<.v.Y.;?........5W..u*.o...X.p.....>....e.1R.L.. ..A..B...n.[..&.'b.*..i.....-N4ko.J@.V.~c[....R.;....p.....U.J...t...In.N6vmY$..=...s.L.Q..f.....>....N50.TQ.m.G../. ..j../..Ec.-..\.R.....!..M.".<..>.G._.h.. ...+q...K*.j.X.8f....K...&.5.;\.]..<.v.Y.;?........5W..u*.o...X.p.....>....e.1R.L.. ..A..B...n.[..&.'b.*..i.....-N4ko.J@.V.~c[....R.;....p.....U.J...t...In.N6vmY$..=...s.L.Q..f.....>....

C:\Users\user\AppData\Local\Temp\beukyly

Process:	C:\Users\user\Desktop\overdue invoices.exe
File Type:	data
Category:	dropped
Size (bytes):	4881
Entropy (8bit):	6.16370682106836
Encrypted:	false
SSDEEP:	96:NtYlIQFqs1Tjge1qVOERr//qaQcaEi6o6qKfNfdbN9udv8N+6aym86BUecxC:wXg6Tjg6sF5/qLJ6XqKZdOdv/6y863
MD5:	EEA52E8D3BE9A6E4268857A90F646400
SHA1:	4A3F1D30AAEE7CBE4F89E8098C1120B9D79B86A9
SHA-256:	4404F10E023A62DB4445FF0BCE7118B4A8CFB4DBA282D1BF3145F07901620B91
SHA-512:	C54C0F48738D52FDD101E1B9EA98FAEDF723EAA59260DDD7F3C36AEF9C0351B50D2A6EAC5627D28FEA73B0EBD52433A45988DB25F8633B373545AFCA5218B883
Malicious:	false
Reputation:	low
Preview:	bC@;;.....;..{...,[..{..,....#;..'s;;;..O;(..(.+..#.&;;;..C..G(..(.+..#.;;;..k..o(..(.+..#.l;;;..S..W(..(.+..#.i;;;..{.....+?..5..4{<<.....[..._..+..?.....'.?j.m5+.P....<.'.?}..'....O._.5..;;;;.?.>Tt.'(.C.(.k.(.S..(.{..(.[.(..Q.+...P....O...*..(.C.....>...<.',;;;;...?.;;;.?..T..O.....^.},.....{...,#....;...L.....;..+./j..#..j?..'....;.....*..#..'.^.}.;31%....=;;.9=;;}/;3.(H...=;;..=;;},.;3.....=;;..=;;}.;...s..{..,....#+;;;..C..'..#;.1..',;;..'...'..#...#._/>;;;{.....5..4.;...C...G....5..jJ;...C...G5=5..4{;..>C.3.(H..Z*;;.Y&((..O.....(....(((..O..O;.A...;.@...*;;;...^.}?;.....{.....#s;;;..{..'..#;.1..',;;..'...'..#...#._..?;;.{...;;;....5..4.;...{.....5..jJ;...{.....+.5..ZJ...{...../..5..4m<...{.....5..jJ=...{....5>5..4{;..>{.31%...a;;;.\'((..O...;.....*.0(..(./(.+(..(....)((..O..O;.A...;.@...*;;;...^.}/;.....#+;;;..._..'..#;.1..',;;..'..'..#...#._.5<;;.{.....5..4.;...._.....5..jJ;..._....5=5..4{;..>_.3.... ;;;..'((..O..(.

C:\Users\user\AppData\Local\Temp\nsz4670.tmp

Process:	C:\Users\user\Desktop\overdue invoices.exe
File Type:	data
Category:	dropped
Size (bytes):	269344
Entropy (8bit):	7.673336729910951
Encrypted:	false
SSDEEP:	6144:LX6zkhtuwSrhQwHd/yprd9NGAOhxr9xN+abfRzyqtgR71GHDw:5tutltdCB/TO7PN+UfRzyx1GH
MD5:	42D350914397CBD208C16387FA16F6C8
SHA1:	48196391E4E3B34D993031BC5E2F9D41101F524A
SHA-256:	E74B59373153E10A79B5F842A6AA0A5E81C791308A2C68E4EF891A683B1E6C7C

SHA-512:	3909EDDE6DD3C9D308B3B0A52A1CB01ABCDB051F96BADAA2C69E5FF0FDDE1F8E1E7E8DA3E2014140259340E1CC7DC827AAA5CE559BBBC4A28E4E7E91FFF69FBE
Malicious:	false
Reputation:	low
Preview:	6a.....0...4K.....P`.....a.....J.....j.....

C:\Users\user\AppData\Local\Temp\nsz4671.tmp\urfzxvl.dll

Process:	C:\Users\user\Desktop\overdue invoices.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.7440203845912166
Encrypted:	false
SSDEEP:	384:96PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhbofub8:9G1albrXY0HwinMdZeUhbomb
MD5:	13A034A08CE0C32CCD5F18F71518DB26
SHA1:	DFD650892733715B3172CBBCC2456D87C0C5C6D4
SHA-256:	598452578751D1C75F6C6F945D814DBAA104FFF2BFC3D37E125CDDB0F434450F
SHA-512:	F3247A0CF9E3304E86E5FF9496FF70D10DBA2584F28651225CAD320D07821E16D952AE2D93FDF308869A1787FEBA6425C5F9D39FF1ED5814A6EA648BB9F0E25
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 16%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0.....PE..L....-.a.....!.....@.....P.....@.....0Q..H...xQ.....`.....p.....P..0....text....>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.930922900924507
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	overdue invoices.exe
File size:	256415
MD5:	e53e6bdf25f7c3bca385a3021e373061
SHA1:	3c91623488f8e645d8f55b802c78c46a86e968da
SHA256:	a2e21d596824ac07de0a0835065fdf00bce5b233c537355edc49e7c10f7b8667
SHA512:	a54df3b4f56156b00fb1799caf305e1384b9d0f2c489f7e66baa921c70ec0ebbd251c049fa6ecea06f81f94f90cccc0154da82e4716fc58e0b528f4d766c610a
SSDEEP:	6144:owfSTftYMNfs8em/DkuBvGwsBQJb4veqz:7glTN08emod9F2qz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007FD078B84290h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007FD078B83F47h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007FD078B83F35h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007FD078B8175Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h

Instruction
push dword ptr [esp+14h]
push eax
call 00007FD078B83A28h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FD078B817B5h
cmp cl, 00000020h
jne 00007FD078B81758h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FD078B8174Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

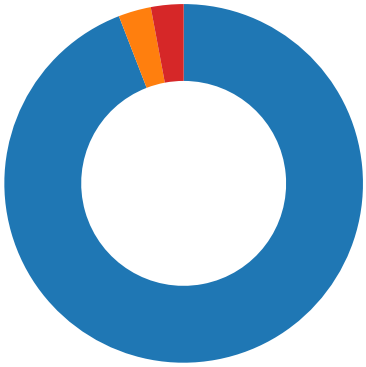
Network Behavior

No network behavior found

Statistics

Behavior

- overdue invoices.exe
- overdue invoices.exe
- explorer.exe
- svchost.exe
- cmd.exe
- conhost.exe
- explorer.exe



Click to jump to process

System Behavior

Analysis Process: overdue invoices.exe PID: **5240**, Parent PID: **5480**

General

Target ID:	0
Start time:	15:18:52
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\overdue invoices.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\overdue invoices.exe"
Imagebase:	0x400000
File size:	256415 bytes
MD5 hash:	E53E6BDF25F7C3BCA385A3021E373061
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: 00000000.00000002.353489816.00000000021A0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.353489816.00000000021A0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.353489816.00000000021A0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: overdue invoices.exe PID: **6680**, Parent PID: **5240**

General

Target ID:	1
Start time:	15:18:54
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\overdue invoices.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\overdue invoices.exe"
Imagebase:	0x400000
File size:	256415 bytes
MD5 hash:	E53E6BDF25F7C3BCA385A3021E373061
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: 00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.442760136.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.443132188.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.443132188.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.443132188.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.351727367.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.351727367.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.351727367.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.350667334.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.350667334.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.350667334.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.443082963.00000000008B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.443082963.00000000008B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.443082963.00000000008B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186D7	NtReadFile

Analysis Process: explorer.exe PID: **3440**, Parent PID: **6680**

General

Target ID:	5
Start time:	15:18:59
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.385434941.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.385434941.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.385434941.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.399598391.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.399598391.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.399598391.000000000F71F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: svchost.exe PID: **7072**, Parent PID: **6680**

General

Target ID:	11
Start time:	15:19:38
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x7ff6b7590000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.625777467.0000000002990000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.625777467.0000000002990000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.625777467.0000000002990000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.625289647.0000000002890000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.625289647.0000000002890000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.625289647.0000000002890000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.625199812.0000000000710000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.625199812.0000000000710000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.625199812.0000000000710000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	29A86D7	NtReadFile

Analysis Process: cmd.exe PID: **5964**, Parent PID: **7072**

General

Target ID:	12
Start time:	15:19:41
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\overdue invoices.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6196**, Parent PID: **5964**

General

Target ID:	14
Start time:	15:19:42
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **4768**, Parent PID: **3424**

General

Target ID:	20
Start time:	15:20:16
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly