ID: 562156
Sample Name:
H4vBtZsi8xAKaMm.exe
Cookbook: default.jbs
Time: 15:14:32
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report H4vBtZsi8xAKaMm.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 6
System Summary 6
Jbx Signature Overview 6
AV Detection 6
Networking 6
E-Banking Fraud 6
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 23
Public IPs 23
General Information 23
Warnings 24
Simulations 24
Behavior and APIs 24
Joe Sandbox View / Context 25
IPs 25
Domains 25
ASNs 25
JA3 Fingerprints 25
Dropped Files 25
Created / dropped Files 25
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\H4vBtZsi8xAKaMm.exe.log 25
Static File Info 25
General 25
File Icon 26
Static PE Info 26
General 26
Entrypoint Preview 26
Data Directories 28
Sections 28
Resources 28
Imports 29
Version Infos 29
Network Behavior 29
Snort IDS Alerts 29
Network Port Distribution 29
TCP Packets 29
UDP Packets 30
ICMP Packets 30
DNS Queries 31
DNS Answers 31
HTTP Request Dependency Graph 31
HTTP Packets 32
Statistics 33
Behavior 33

System Behavior 34
Analysis Process: H4vBtZsi8xAKaMm.exePID: 6364, Parent PID: 5436 34
General 34
File Activities 34
Analysis Process: MSBuild.exePID: 6100, Parent PID: 6364 34
General 34
File Activities 35
File Read 35
Analysis Process: explorer.exePID: 3292, Parent PID: 6100 35
General 35
Analysis Process: rundll32.exePID: 4480, Parent PID: 3292 36
General 36
File Activities 36
File Read 36
Analysis Process: cmd.exePID: 6880, Parent PID: 4480 36
General 36
File Activities 36
Analysis Process: conhost.exePID: 6872, Parent PID: 6880 37
General 37
Analysis Process: explorer.exePID: 4704, Parent PID: 568 37
General 37
File Activities 37
Registry Activities 37
Analysis Process: explorer.exePID: 4104, Parent PID: 568 38
General 38
File Activities 38
Registry Activities 38
Disassembly 38

Windows Analysis Report

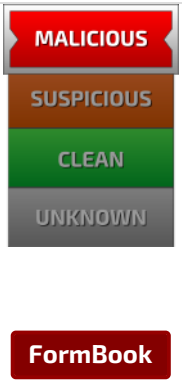
H4vBtZsi8xAKaMm.exe

Overview

General Information

Sample Name:	H4vBtZsi8xAKaMm.exe
Analysis ID:	562156
MD5:	7eabab04e4a6fd..
SHA1:	e0e1dc469746f5..
SHA256:	b79d2d02fe777c..
Tags:	exe
Infos:	

Detection



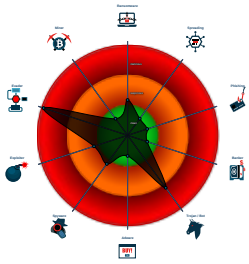
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- H4vBtZsi8xAKaMm.exe (PID: 6364 cmdline: "C:\Users\user\Desktop\H4vBtZsi8xAKaMm.exe" MD5: 7EABAB04E4A6FDD45238E32ED81E222C)
  - MSBuild.exe (PID: 6100 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 4480 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6880 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 4704 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - explorer.exe (PID: 4104 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x18839:$sqlite3step: 68 34 1C 7B E1 0x1894c:$sqlite3step: 68 34 1C 7B E1 0x18868:$sqlite3text: 68 38 2A 90 C5 0x1898d:$sqlite3text: 68 38 2A 90 C5 0x1887b:$sqlite3blob: 68 53 D8 7F 8C 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.401760345.0000000000E90000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.401760345.0000000000E90000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.MSBuild.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
14.2.MSBuild.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
14.2.MSBuild.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x18839:$sqlite3step: 68 34 1C 7B E1 0x1894c:$sqlite3step: 68 34 1C 7B E1 0x18868:$sqlite3text: 68 38 2A 90 C5 0x1898d:$sqlite3text: 68 38 2A 90 C5 0x1887b:$sqlite3blob: 68 53 D8 7F 8C 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
14.0.MSBuild.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
14.0.MSBuild.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Sigma Overview

System Summary

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

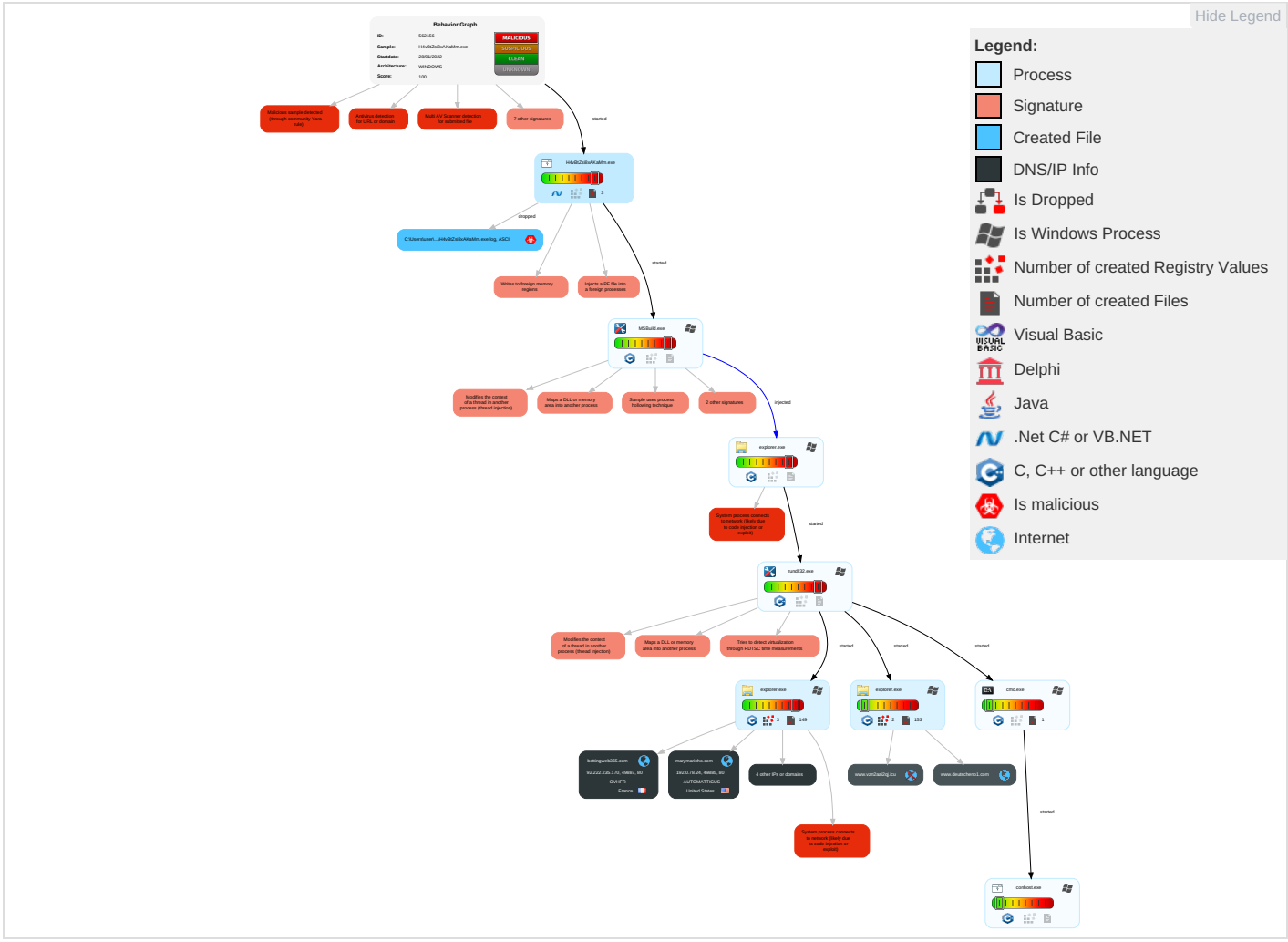
Yara detected FormBook

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	7 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	7 1 2 Process Injection	NTDS	4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	1 1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

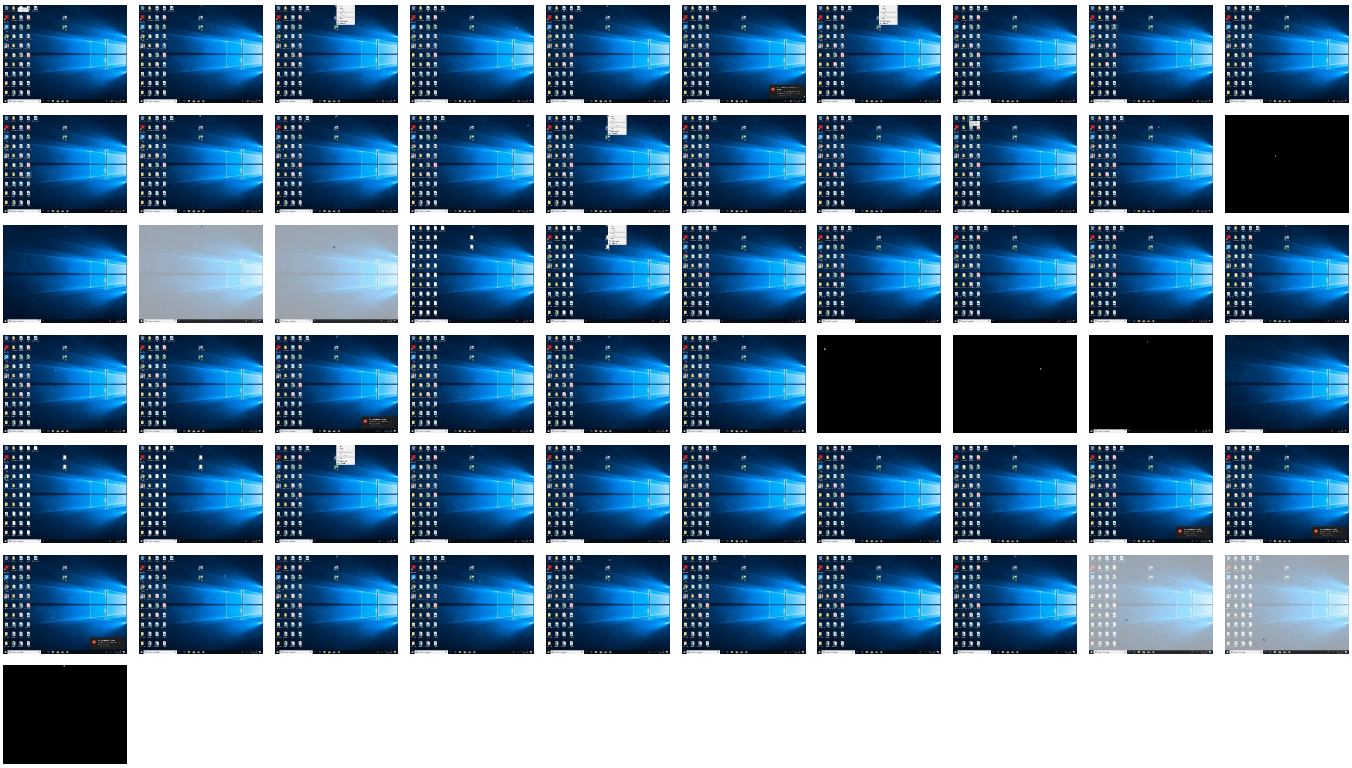
Behavior Graph

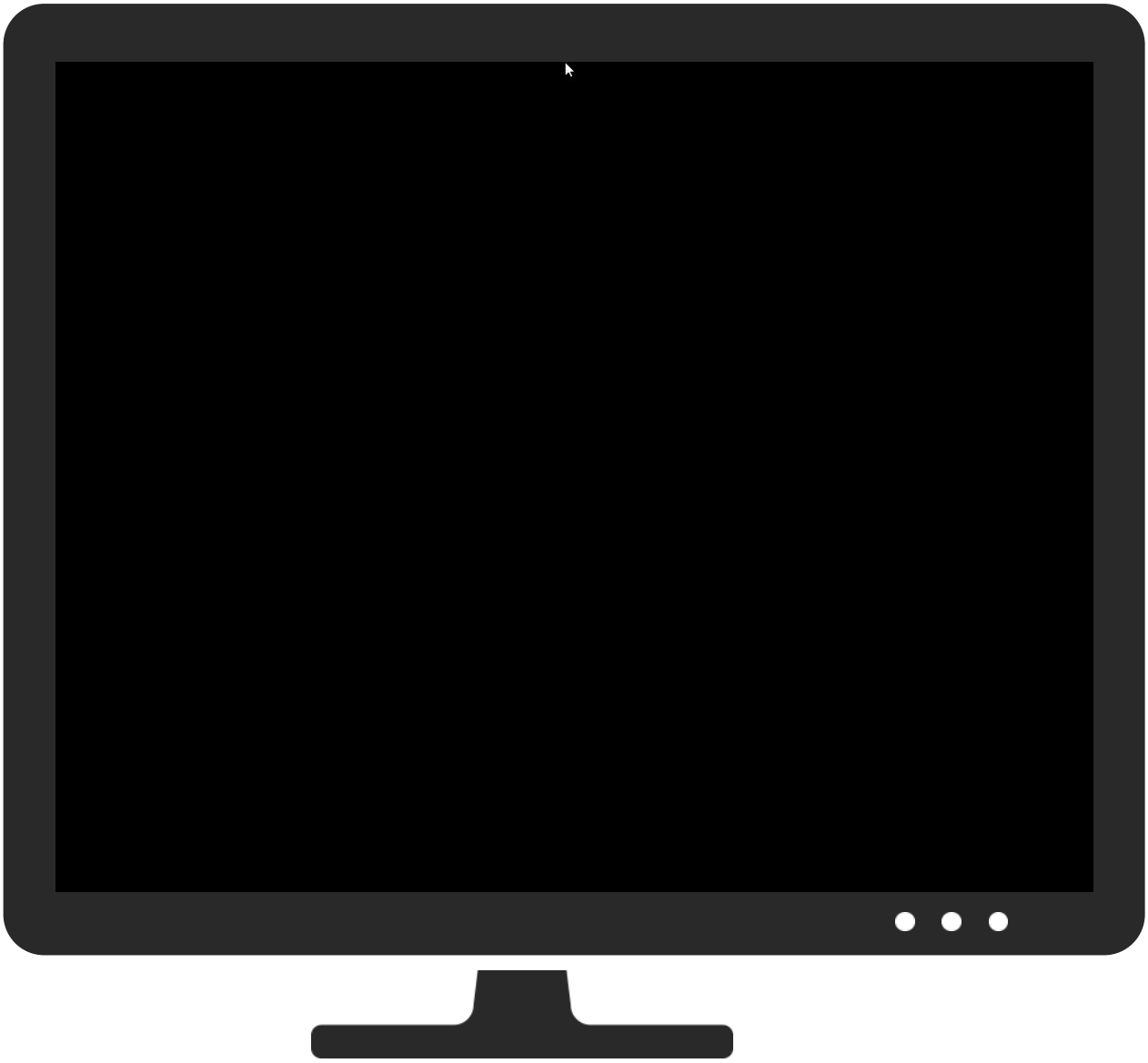


Screenshots

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
H4vBtZsi8xAKaMm.exe	65%	Virustotal		Browse
H4vBtZsi8xAKaMm.exe	47%	Metadefender		Browse
H4vBtZsi8xAKaMm.exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
H4vBtZsi8xAKaMm.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.vinewineltd.com	0%	Avira URL Cloud	safe	
http://www.hornnbach.comReferer:	0%	Avira URL Cloud	safe	
http://www.verifyaxcx.com/u1p5/www.agengrosirfashion.com	0%	Avira URL Cloud	safe	
http://www.freeclothesonline.com/u1p5/	1%	Virustotal		Browse
http://www.freeclothesonline.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.piertrafesa.com/u1p5/www.vinewineltd.com	0%	Avira URL Cloud	safe	
http://www.freeclothesonline.com/u1p5/www.apeutah.com	100%	Avira URL Cloud	malware	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.rhoads-music.comReferer:	0%	Avira URL Cloud	safe	
http://www.kailibianminwang.comReferer:	0%	Avira URL Cloud	safe	
http://www.pbcgotv.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.piertrafesa.com	0%	Avira URL Cloud	safe	
http://www.yannickrast.com/u1p5/www.rhoads-music.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.rhoads-music.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.apeutah.com/u1p5/www.jovam.xyz	100%	Avira URL Cloud	malware	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://bettingweb365.com/u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD	0%	Avira URL Cloud	safe	
http://www.yannickrast.com/u1p5/	0%	Avira URL Cloud	safe	
http://www.pbcgotv.com/u1p5/www.kailibianminwang.com	100%	Avira URL Cloud	malware	
http://www.verifyaxcx.comReferer:	0%	Avira URL Cloud	safe	
http://www.apeutah.com	0%	Avira URL Cloud	safe	
http://www.dasmonica.comReferer:	0%	Avira URL Cloud	safe	
http://www.hokabrazil.com/u1p5/www.hornnbach.com	100%	Avira URL Cloud	phishing	
http://www.hornnbach.com/u1p5/www.piertrafesa.com	0%	Avira URL Cloud	safe	
http://www.dasmonica.com/u1p5/www.freeclothesonline.com	0%	Avira URL Cloud	safe	
http://www.marymarinho.com/u1p5/?y4Mp=jmW97e0DcxHZsiDt+DmiFhziWrO1jPfkTbEIn6OHXnuLtYKLIrDwNEu/EQYt2xDuBHghXZP9DQ==&D0GHx=5jNT	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.piertrafesa.com/u1p5/	0%	Avira URL Cloud	safe	
http://www.jovam.xyz/u1p5/www.hokabrazil.com	100%	Avira URL Cloud	phishing	
http://www.jovam.xyz	0%	Avira URL Cloud	safe	
http://www.apeutah.comReferer:	0%	Avira URL Cloud	safe	
http://www.pbcgotv.comReferer:	0%	Avira URL Cloud	safe	
http://www.kailibianminwang.com	0%	Avira URL Cloud	safe	
http://www.vzn2aai2qj.icuReferer:	0%	Avira URL Cloud	safe	
http://www.vinewineltd.com/u1p5/www.pbcgotv.com	100%	Avira URL Cloud	malware	
http://www.dasmonica.com/u1p5/	0%	Avira URL Cloud	safe	
http://www.vzn2aai2qj.icu/u1p5/www.deutscheno1.com	0%	Avira URL Cloud	safe	
http://www.agengrosirfashion.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.freeclothesonline.comReferer:	0%	Avira URL Cloud	safe	
http://www.hokabrazil.comReferer:	0%	Avira URL Cloud	safe	
http://www.jovam.xyz/u1p5/	100%	Avira URL Cloud	phishing	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jovam.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.verifyaxcx.com	0%	Avira URL Cloud	safe	
http://www.deutscheno1.com/u1p5/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.pbcgotv.com	0%	Avira URL Cloud	safe	
http://www.piertrafesa.comReferer:	0%	Avira URL Cloud	safe	
http://www.yannickrast.comReferer:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.dasmonica.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.kailibianminwang.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.agengrosirfashion.com/u1p5/www.dasmonica.com	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.agengrosirfashion.comReferer:	0%	Avira URL Cloud	safe	
http://www.apeutah.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.hokabrazil.com/u1p5/	100%	Avira URL Cloud	phishing	
http://www.freeclothesonline.com	0%	Avira URL Cloud	safe	
http://www.vinewineltd.comReferer:	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.rhoads-music.com/u1p5/www.verifyaxcx.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.hokabrazil.com	100%	Avira URL Cloud	phishing	
http://www.yannickrast.com	0%	Avira URL Cloud	safe	
http://www.agengrosirfashion.com	0%	Avira URL Cloud	safe	
http://www.vinewineltd.com/u1p5/	100%	Avira URL Cloud	malware	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.bettingweb365.com/u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD+HvWaQ2ttROlxFaz7G4unDmw6qRWL3K2g==&D0GHx=5jNT	0%	Avira URL Cloud	safe	
http://www.verifyaxcx.com/u1p5/	0%	Avira URL Cloud	safe	
http://www.vzn2aai2qj.icu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.hornnbach.com/u1p5/	0%	Avira URL Cloud	safe	
http://www.deutscheno1.com/u1p5/www.yannickrast.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.kailibianminwang.com/u1p5/.	100%	Avira URL Cloud	malware	
http://www.hornnbach.com	0%	Avira URL Cloud	safe	
http://www.vzn2aai2qj.icu/u1p5/	0%	Avira URL Cloud	safe	
http://www.deutscheno1.com	0%	Avira URL Cloud	safe	
http://www.shitcoin.team/u1p5/?y4Mp=vL5j7Eq3si3+pqkwq9GVQc9zWaxA/P/bTusMaerk9f3EW+lc0CCc1NhXRSl0Kt4KYFMx8zSAYw==&D0GHx=5jNT	0%	Avira URL Cloud	safe	
http://www.rhoads-music.com/u1p5/	0%	Avira URL Cloud	safe	
http://crl.v	0%	URL Reputation	safe	
http://www.deutscheno1.comReferer:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bettingweb365.com	92.222.235.170	true	false		high
www.deutscheno1.com	34.149.59.90	true	false		high
marymarinho.com	192.0.78.24	true	false		high
shitcoin.team	107.180.34.104	true	false		high
www.shitcoin.team	unknown	unknown	false		high
www.bettingweb365.com	unknown	unknown	false		high
www.vzn2aai2qj.icu	unknown	unknown	false		high
www.marymarinho.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.marymarinho.com/u1p5/?y4Mp=jmW97e0DcxHZsiDt+DmiFhziWrO1jPfkTbEIn6OHXnuLtYKLIrDwNEu/EQYt2xDuBHghXZP9DQ==&D0GHx=5jNT	true	• Avira URL Cloud: safe	unknown
http://www.bettingweb365.com/u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD+HvWaQ2ttROIxFaz7G4unDmw6qRWL3K2g==&D0GHx=5jNT	true	• Avira URL Cloud: safe	unknown
http://www.shitcoin.team/u1p5/?y4Mp=vL5j7Eq3si3+pqkwq9GVQc9zWaxA/P/bTusMaerk9f3EW+lc0CCc1NhXRSl0Kt4KYFMx8zSAYw==&D0GHx=5jNT	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.vinewineltd.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hornnbach.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.verifyaxcx.com/u1p5/www.agengrosirfashion.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.freeclothesonline.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.fontbureau.com/designers	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.piertrafesa.com/u1p5/www.vinewineltd.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.freeclothesonline.com/u1p5/www.apeutah.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.sajatypeworks.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rhoads-music.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kailibianminwang.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pbcgotv.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piertrafesa.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yannickrast.com/u1p5/www.rhoads-music.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.rhoads-music.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apeutah.com/u1p5/www.jovam.xyz	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.zhongyicts.com.cn	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 40630386.00000000032D1000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://bettingweb365.com/u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD	rundll32.exe, 00000013.00000002.80114715 5.000000000541F000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yannickrast.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000F.00000000.36349862 1.0000000006840000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00F.00000000.434119185.0000000006840000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000F.00000000.348701953.000000 0006840000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 0000000F.0000 0000.382832125.0000000006840000.00000004 .00000001.00020000.00000000.sdmp	false		high
http://www.pbcgotv.com/u1p5/www.kailibianminwang.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.verifyaxcx.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apeutah.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dasmonica.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hokabrazil.com/u1p5/www.hornnbach.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.hornnbach.com/u1p5/www.piertrafesa.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dasmonica.com/u1p5/www.freeclothesonline.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piertrafesa.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jovam.xyz/u1p5/www.hokabrazil.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.jovam.xyz	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.apeutah.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pbcgotv.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kailibianminwang.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vzn2aai2qj.icuReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.vinewineltd.com/u1p5/www.pbcgotv.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.dasmonica.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vzn2aai2qj.icu/u1p5/www.deutscheno1.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agengrosirfashion.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.freeclothesonline.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hokabrazil.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.jovam.xyz/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jovam.xyzReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.verifyaxcx.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.deutscheno1.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.pbcgotv.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piertrafesa.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yannickrast.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.344172860.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.dasmonica.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.547185331.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000002.605753467.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	H4vBtZsi8xAKaMm.exe, 00000001.00000002.344172860.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.kailibianminwang.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.547185331.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000002.605753467.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.typography.netD	H4vBtZsi8xAKaMm.exe, 00000001.00000002.344172860.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agengrosirfashion.com/u1p5/www.dasmonica.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.547185331.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000002.605753467.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.galapagosdesign.com/staff/dennis.htm	H4vBtZsi8xAKaMm.exe, 00000001.00000002.344172860.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.344172860.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agengrosirfashion.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.547185331.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000002.605753467.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apeutah.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.547185331.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000002.605753467.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

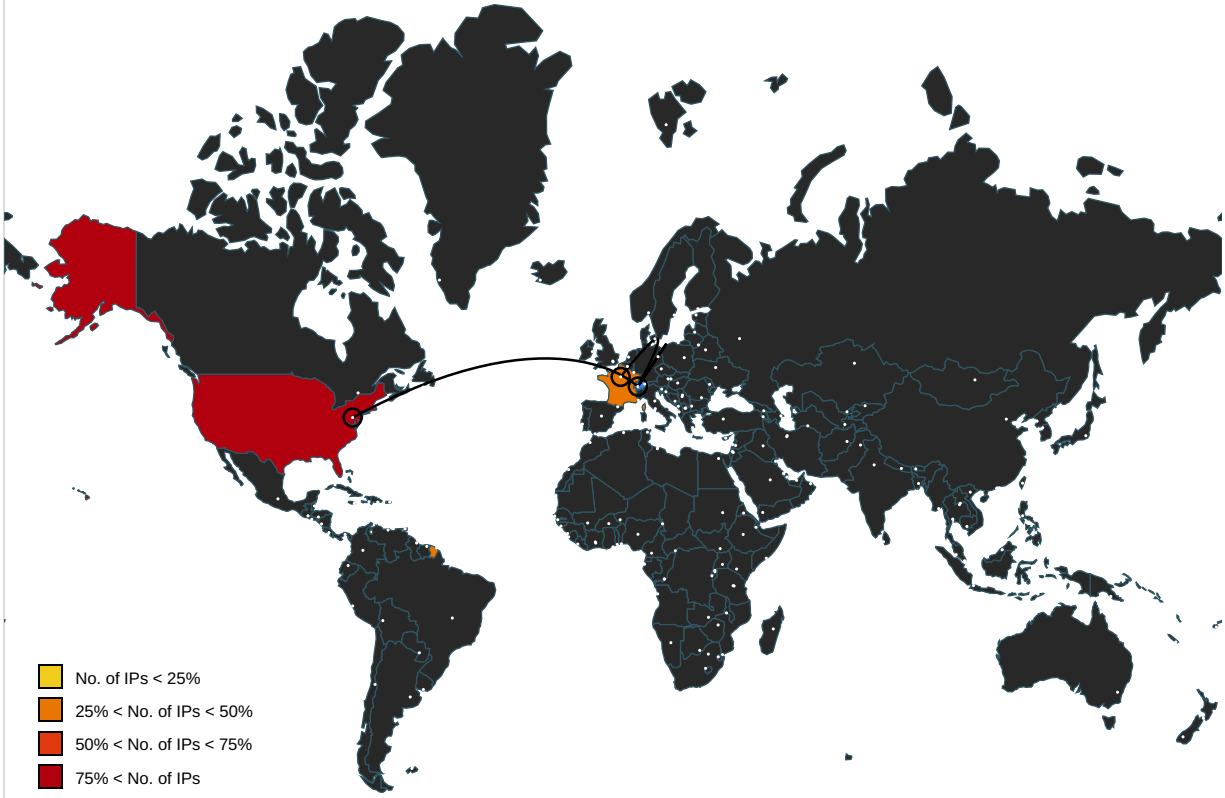
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hokabrazil.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.freeclothesonline.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vinewineltd.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rhoads-music.com/u1p5/www.verifyaxcx.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hokabrazil.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.yannickrast.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.agengrosirfashion.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 40265098.0000000001987000.00000004.00000 020.00020000.00000000.sdmp, H4vBtZsi8xAK aMm.exe, 00000001.00000002.344172860.000 00000074A2000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://www.vinewineltd.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fontbureau.comF	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 40265098.0000000001987000.00000004.00000 020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.verifyaxcx.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.vzn2aai2qj.icu	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hornnbach.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.deutscheno1.com/u1p5/www.yannickrast.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 40265098.0000000001987000.00000004.00000 020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.kailibianminwang.com/u1p5/.	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hornnbach.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	H4vBtZsi8xAKaMm.exe, 00000001.00000002.3 44172860.00000000074A2000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.vzn2aai2qj.icu/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.deutscheno1.com	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rhoads-music.com/u1p5/	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.v	explorer.exe, 0000001E.00000003.56864959 4.000000000A9F8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.565231882.000000000A9F8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.567907070.000000 000A9F8000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.606120571.000000000A9F8000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.deutscheno1.comReferer:	explorer.exe, 0000001E.00000003.54425958 7.000000000A8C1000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01E.00000003.547185331.000000000A8C1000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.541475880.000000 000A8C1000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001E.0000 0002.605753467.000000000A8C1000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001E.00000003.546230815.000000000A8C10 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.24	marymarinho.com	United States		2635	AUTOMATTICUS	false
92.222.235.170	bettingweb365.com	France		16276	OVHFR	false
107.180.34.104	shitcoin.team	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562156
Start date:	28.01.2022
Start time:	15:14:32
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 15m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	H4vBtZsi8xAKaMm.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:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@8/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65.3% (good quality ratio 59.3%) • Quality average: 71.4% • Quality standard deviation: 32%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, dllhost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, mobsync.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.3.108.67, 20.82.209.183, 8.248.143.254, 8.253.95.120, 8.253.207.121, 8.241.126.121, 8.248.133.254, 20.199.120.182, 20.199.120.151, 80.67.82.211, 80.67.82.235, 40.91.112.76, 20.54.7.98, 40.112.88.60, 20.199.120.85, 204.79.197.200, 13.107.21.200, 51.104.136.2
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.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, wus2-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, consumer-displaycatalogrp-aks2aks-uswest.md.mp.microsoft.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, wu-shim.trafficmanager.net, ris-prod.trafficmanager.ne
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:16:07	API Interceptor	1x Sleep call for process: H4vBtZsi8xAKaMm.exe modified
15:17:18	API Interceptor	450x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\H4vBtZsi8xAKaMm.exe.log

Process:	C:\Users\user\Desktop\H4vBtZsi8xAKaMm.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:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180 2B7
Malicious:	**true**
Reputation:	unknown
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):	7.905438661946074
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	H4vBtZsi8xAKaMm.exe

File size:	1304576
MD5:	7eabab04e4a6fdd45238e32ed81e222c
SHA1:	e0e1dc469746f5e2e049ea4a93d9b09a9227b342
SHA256:	b79d2d02fe777cfd64723ad9b3935b30c00cbc75614fcadbf867cce88df4a8fd
SHA512:	eeaa0f02a15a66b3363f94730ad3cf7c533a4bf303cfa0f53b21959a54dc0f65c50b1ac179aa5f992e3e17bbfaaa1b7393da3d1859ddd51932d36bdf0b7fa21b
SSDEEP:	24576:Xn0jA6ehzLFCgTrc1zKViGWIANSCqCmURrOrSO/8dVnJE0RujU88WyPZxG:X96e1d4171NNSCquRiFjD/8WyRk
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...e..a..............P..D...........b... ....@.. ....@.........@................................

File Icon

Icon Hash:	b2b2929292b2b2b2

Static PE Info

General

Entrypoint:	0x5362ea
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:	0x61F09D65 [Wed Jan 26 01:01:25 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x136298	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x138000	0x9f74	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x142000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x136160	0x1c	.text
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	0x1342f0	0x134400	False	0.912575875659	data	7.91694602687	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x138000	0x9f74	0xa000	False	0.159008789062	data	6.8397629142	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x142000	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	0x138120	0x4c28	dBase IV DBT, blocks size 0, block length 18432, next free block index 40, next free block 0, next used block 16777216		
RT_ICON	0x13cd58	0x4c28	dBase IV DBT, blocks size 0, block length 18432, next free block index 40, next free block 0, next used block 16777216		
RT_GROUP_ICON	0x141990	0x22	data		
RT_VERSION	0x1419c4	0x3b0	data		
RT_MANIFEST	0x141d84	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

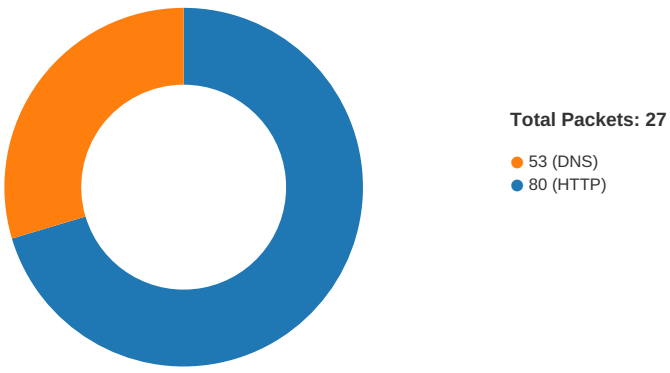
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Francisco Laria 2007
Assembly Version	1.0.0.0
InternalName	760pQ.exe
FileVersion	1.0.0.0
CompanyName	Francisco Laria
LegalTrademarks	
Comments	A .NET version of the classic board game.
ProductName	Simon Says Game
ProductVersion	1.0.0.0
FileDescription	Simon Says Game
OriginalFilename	760pQ.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-15:17:54.685247	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
01/28/22-15:17:55.551640	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
01/28/22-15:17:57.802015	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:16:23.253470898 CET	49686	80	192.168.2.7	173.222.108.210
Jan 28, 2022 15:16:23.270128965 CET	80	49686	173.222.108.210	192.168.2.7
Jan 28, 2022 15:16:23.270261049 CET	49686	80	192.168.2.7	173.222.108.210
Jan 28, 2022 15:16:24.966999054 CET	80	49684	93.184.220.29	192.168.2.7
Jan 28, 2022 15:16:24.967207909 CET	49684	80	192.168.2.7	93.184.220.29
Jan 28, 2022 15:16:27.496630907 CET	80	49692	93.184.220.29	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:16:27.496728897 CET	49692	80	192.168.2.7	93.184.220.29
Jan 28, 2022 15:17:12.899142027 CET	49684	80	192.168.2.7	93.184.220.29
Jan 28, 2022 15:17:12.899296045 CET	49682	80	192.168.2.7	173.222.108.210
Jan 28, 2022 15:17:12.916321039 CET	80	49682	173.222.108.210	192.168.2.7
Jan 28, 2022 15:17:12.916470051 CET	49682	80	192.168.2.7	173.222.108.210
Jan 28, 2022 15:17:12.919374943 CET	80	49684	93.184.220.29	192.168.2.7
Jan 28, 2022 15:17:12.920589924 CET	49684	80	192.168.2.7	93.184.220.29
Jan 28, 2022 15:17:22.192085981 CET	49692	80	192.168.2.7	93.184.220.29
Jan 28, 2022 15:18:48.838774920 CET	49880	80	192.168.2.7	107.180.34.104
Jan 28, 2022 15:18:48.949897051 CET	80	49880	107.180.34.104	192.168.2.7
Jan 28, 2022 15:18:48.949994087 CET	49880	80	192.168.2.7	107.180.34.104
Jan 28, 2022 15:18:48.952475071 CET	49880	80	192.168.2.7	107.180.34.104
Jan 28, 2022 15:18:49.070127010 CET	80	49880	107.180.34.104	192.168.2.7
Jan 28, 2022 15:18:49.070324898 CET	49880	80	192.168.2.7	107.180.34.104
Jan 28, 2022 15:18:49.070355892 CET	49880	80	192.168.2.7	107.180.34.104
Jan 28, 2022 15:18:49.182204008 CET	80	49880	107.180.34.104	192.168.2.7
Jan 28, 2022 15:19:12.004883051 CET	49885	80	192.168.2.7	192.0.78.24
Jan 28, 2022 15:19:12.021564960 CET	80	49885	192.0.78.24	192.168.2.7
Jan 28, 2022 15:19:12.024972916 CET	49885	80	192.168.2.7	192.0.78.24
Jan 28, 2022 15:19:12.066575050 CET	49885	80	192.168.2.7	192.0.78.24
Jan 28, 2022 15:19:12.083214998 CET	80	49885	192.0.78.24	192.168.2.7
Jan 28, 2022 15:19:12.220340014 CET	80	49885	192.0.78.24	192.168.2.7
Jan 28, 2022 15:19:12.220377922 CET	80	49885	192.0.78.24	192.168.2.7
Jan 28, 2022 15:19:12.220552921 CET	49885	80	192.168.2.7	192.0.78.24
Jan 28, 2022 15:19:12.220606089 CET	49885	80	192.168.2.7	192.0.78.24
Jan 28, 2022 15:19:12.239855051 CET	80	49885	192.0.78.24	192.168.2.7
Jan 28, 2022 15:19:35.543049097 CET	49887	80	192.168.2.7	92.222.235.170
Jan 28, 2022 15:19:35.572104931 CET	80	49887	92.222.235.170	192.168.2.7
Jan 28, 2022 15:19:35.572236061 CET	49887	80	192.168.2.7	92.222.235.170
Jan 28, 2022 15:19:35.623141050 CET	49887	80	192.168.2.7	92.222.235.170
Jan 28, 2022 15:19:35.652195930 CET	80	49887	92.222.235.170	192.168.2.7
Jan 28, 2022 15:19:35.810760975 CET	80	49887	92.222.235.170	192.168.2.7
Jan 28, 2022 15:19:35.810784101 CET	80	49887	92.222.235.170	192.168.2.7
Jan 28, 2022 15:19:35.811115026 CET	49887	80	192.168.2.7	92.222.235.170
Jan 28, 2022 15:19:35.813723087 CET	49887	80	192.168.2.7	92.222.235.170
Jan 28, 2022 15:19:35.842775106 CET	80	49887	92.222.235.170	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 15:17:48.665153027 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:17:49.667907953 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:17:50.688549042 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:17:52.785115004 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:17:53.681818962 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 15:17:54.685043097 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 15:17:55.550877094 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 15:17:57.801929951 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 15:18:17.763120890 CET	60983	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:18:17.798033953 CET	53	60983	8.8.8.8	192.168.2.7
Jan 28, 2022 15:18:48.755186081 CET	52286	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:18:48.784271955 CET	53	52286	8.8.8.8	192.168.2.7
Jan 28, 2022 15:19:11.739278078 CET	61457	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:19:11.762356997 CET	53	61457	8.8.8.8	192.168.2.7
Jan 28, 2022 15:19:34.159179926 CET	60599	53	192.168.2.7	8.8.8.8
Jan 28, 2022 15:19:34.193367958 CET	53	60599	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 28, 2022 15:17:54.685246944 CET	192.168.2.7	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Jan 28, 2022 15:17:55.551640034 CET	192.168.2.7	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Jan 28, 2022 15:17:57.802015066 CET	192.168.2.7	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 15:17:48.665153027 CET	192.168.2.7	8.8.8.8	0xa4f9	Standard query (0)	www.vzn2aai2qj.icu	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:49.667907953 CET	192.168.2.7	8.8.8.8	0xa4f9	Standard query (0)	www.vzn2aai2qj.icu	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:50.688549042 CET	192.168.2.7	8.8.8.8	0xa4f9	Standard query (0)	www.vzn2aai2qj.icu	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:52.785115004 CET	192.168.2.7	8.8.8.8	0xa4f9	Standard query (0)	www.vzn2aai2qj.icu	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:17.763120890 CET	192.168.2.7	8.8.8.8	0xd8e4	Standard query (0)	www.deutscheno1.com	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:48.755186081 CET	192.168.2.7	8.8.8.8	0x66b7	Standard query (0)	www.shitcoin.team	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:11.739278078 CET	192.168.2.7	8.8.8.8	0xfa76	Standard query (0)	www.marymarinho.com	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:34.159179926 CET	192.168.2.7	8.8.8.8	0xfdb5	Standard query (0)	www.bettingweb365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 15:17:53.681818962 CET	8.8.8.8	192.168.2.7	0xa4f9	Server failure (2)	www.vzn2aai2qj.icu	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:54.685043097 CET	8.8.8.8	192.168.2.7	0xa4f9	Server failure (2)	www.vzn2aai2qj.icu	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:55.550877094 CET	8.8.8.8	192.168.2.7	0xa4f9	Server failure (2)	www.vzn2aai2qj.icu	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 15:17:57.801929951 CET	8.8.8.8	192.168.2.7	0xa4f9	Server failure (2)	www.vzn2aai2qj.icu	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:17.798033953 CET	8.8.8.8	192.168.2.7	0xd8e4	No error (0)	www.deutscheno1.com		34.149.59.90	A (IP address)	IN (0x0001)
Jan 28, 2022 15:18:48.784271955 CET	8.8.8.8	192.168.2.7	0x66b7	No error (0)	www.shitcoin.team	shitcoin.team		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 15:18:48.784271955 CET	8.8.8.8	192.168.2.7	0x66b7	No error (0)	shitcoin.team		107.180.34.104	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:11.762356997 CET	8.8.8.8	192.168.2.7	0xfa76	No error (0)	www.marymarinho.com	marymarinho.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 15:19:11.762356997 CET	8.8.8.8	192.168.2.7	0xfa76	No error (0)	marymarinho.com		192.0.78.24	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:11.762356997 CET	8.8.8.8	192.168.2.7	0xfa76	No error (0)	marymarinho.com		192.0.78.25	A (IP address)	IN (0x0001)
Jan 28, 2022 15:19:34.193367958 CET	8.8.8.8	192.168.2.7	0xfdb5	No error (0)	www.bettingweb365.com	bettingweb365.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 15:19:34.193367958 CET	8.8.8.8	192.168.2.7	0xfdb5	No error (0)	bettingweb365.com		92.222.235.170	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.shitcoin.team
- www.marymarinho.com
- www.bettingweb365.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49880	107.180.34.104	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:18:48.952475071 CET	23848	OUT	GET /u1p5/?y4Mp=vL5j7Eq3si3+pqkwq9GVQc9zWaxA/P/bTusMaerk9f3EW+lc0CCc1NhXRSl0Kt4KYFMx8zSAYw==&D0GHx=5jNT HTTP/1.1 Host: www.shitcoin.team Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 15:18:49.070127010 CET	23850	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Fri, 28 Jan 2022 14:18:48 GMT Connection: close Content-Length: 1118 Data Raw: 3c 48 54 4d 4c 3e 0d 0a 3c 48 45 41 44 3e 0d 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 42 41 53 45 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 5f 64 6f 63 73 2f 22 3e 3c 21 2d 2d 5b 69 66 20 6c 74 65 20 49 45 20 36 5d 3e 3c 2f 42 41 53 45 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 2f 48 45 41 44 3e 0d 0a 3c 42 4f 44 59 3e 0d 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0d 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 64 6f 63 75 6d 65 6e 74 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 0d 0a 3c 50 3e 0d 0a 3c 48 52 3e 0d 0a 3c 41 44 44 52 45 53 53 3e 0d 0a 57 65 62 20 53 65 72 76 65 72 20 61 74 20 26 23 31 31 35 3b 26 23 31 30 34 3b 26 23 31 30 35 3b 26 23 31 31 36 3b 26 23 39 39 3b 26 23 31 31 31 3b 26 23 31 30 35 3b 26 23 31 31 30 3b 26 23 34 36 3b 26 23 31 31 36 3b 26 23 31 30 31 3b 26 23 39 37 3b 26 23 31 30 39 3b 0d 0a 3c 2f 41 44 44 52 45 53 53 3e 0d 0a 3c 2f 42 4f 44 59 3e 0d 0a 3c 2f 48 54 4d 4c 3e 0d 0a 0d 0a 3c 21 2d 2d 0d 0a 20 20 20 2d 20 55 6e 66 6f 72 74 75 6e 61 74 65 6c 79 2c 20 4d 69 63 72 6f 73 6f 66 74 20 68 61 73 20 61 64 64 65 64 20 61 20 63 6c 65 76 65 72 20 6e 65 77 0d 0a 20 20 20 2d 20 22 66 65 61 74 75 72 65 22 20 74 6f 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 2e 20 49 66 20 74 68 65 20 74 65 78 74 20 6f 66 0d 0a 20 20 20 2d 20 61 6e 20 65 72 72 6f 72 27 73 20 6d 65 73 73 61 67 65 20 69 73 20 22 74 6f 6f 20 73 6d 61 6c 6c 22 2c 20 73 70 65 63 69 66 69 63 61 6c 6c 79 0d 0a 20 20 20 2d 20 6c 65 73 73 20 74 68 61 6e 20 35 31 32 20 62 79 74 65 73 2c 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 72 65 74 75 72 6e 73 0d 0a 20 20 20 2d 20 69 74 73 20 6f 77 6e 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 2e 20 59 6f 75 20 63 61 6e 20 74 75 72 6e 20 74 68 61 74 20 6f 66 66 2c 0d 0a 20 20 20 2d 20 62 75 74 20 69 74 27 73 20 70 72 65 74 74 79 20 74 72 69 63 6b 79 20 74 6f 20 66 69 6e 64 20 73 77 69 74 63 68 20 63 61 6c 6c 65 64 0d 0a 20 20 20 2d 20 22 73 6d 61 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 22 2e 20 54 68 61 74 20 6d 65 61 6e 73 2c 20 6f 66 20 63 6f 75 72 73 65 2c 0d 0a 20 20 20 2d 20 74 68 61 74 20 73 68 6f 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 61 72 65 20 63 65 6e 73 6f 72 65 64 20 62 79 20 64 65 66 61 75 6c 74 2e 0d 0a 20 20 20 2d 20 49 49 53 20 61 6c 77 61 79 73 20 72 65 74 75 72 6e 73 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 74 68 61 74 20 61 72 65 20 6c 6f 6e 67 68 20 74 6f 20 6d 61 6b 65 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 68 61 70 70 79 2e 20 54 68 65 0d 0a 20 20 20 2d 20 77 6f 72 6b 61 72 6f 75 6e 64 20 69 73 20 70 72 65 74 74 79 20 73 69 6d 70 6c 65 3a 20 70 61 64 20 74 68 65 20 65 72 72 6f 72 0d 0a 20 20 20 2d 20 6d 65 73 73 61 67 65 20 77 69 74 68 20 61 20 62 69 67 20 63 6f 6d 6d 65 6e 74 20 6c 69 6b 65 20 74 68 69 73 20 74 6f 20 70 75 73 68 20 69 74 0d 0a 20 20 20 2d 20 6f 76 65 72 20 74 68 65 20 66 69 76 65 20 68 75 6e 64 72 65 64 20 61 6e 64 20 74 77 65 6c 76 65 20 62 79 74 65 73 20 6d 69 6e 69 6d 75 6d 2e 0d 0a 20 20 20 2d 20 4f 66 20 63 6f 75 72 73 65 2c 20 74 68 61 74 27 73 20 65 78 61 63 74 6c 79 20 77 68 61 74 20 79 6f 75 27 72 65 20 72 65 61 64 69 6e 67 0d 0a 20 20 20 2d 20 72 69 67 68 74 20 6e 6f 77 2e 0d 0a 20 20 20 2d 2d 3e 0d 0a Data Ascii: <HTML><HEAD><TITLE>404 Not Found</TITLE><BASE href="/error_docs/">...[if lte IE 6]></BASE><![endif]--></HEAD><BODY><H1>Not Found</H1>The requested document was not found on this server.<P><HR><ADDRESS>Web Server at shitcoin.team</ADDRESS></BODY></HTML>... - Unfortunately, Microsoft has added a clever new - "feature" to Internet Explorer. If the text of - an error's message is "too small", specifically - less than 512 bytes, Internet Explorer returns - its own error message. You can turn that off, - but it's pretty tricky to find switch called - "smart error messages". That means, of course, - that short error messages are censored by default. - IIS always returns error messages that are long - enough to make Internet Explorer happy. The - workaround is pretty simple: pad the error - message with a big comment like this to push it - over the five hundred and twelve bytes minimum. - Of course, that's exactly what you're reading - right now. -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49885	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:19:12.066575050 CET	23882	OUT	GET /u1p5/?y4Mp=jmW97e0DcxHZsiDt+DmiFhziWrO1jPfkTbEln6OHXnuLtYKLIrDwNEu/EQYt2xDuBHghXZP9DQ==&D0GHx=5jNT HTTP/1.1 Host: www.marymarinho.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

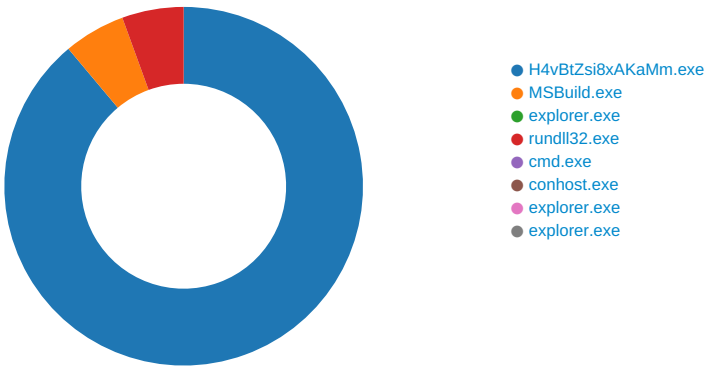
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:19:12.220340014 CET	23883	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 28 Jan 2022 14:19:12 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.marymarinho.com/u1p5/?y4Mp=jmW97e0DcxHZsiDt+DmiFhziWrO1jPfkTbEIn6OHXnuLtYKLIrDwNEu/EQYt2xDuBHghXZP9DQ==&D0GHx=5jNT X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49887	92.222.235.170	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 15:19:35.623141050 CET	23891	OUT	GET /u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD+HvWaQ2ttROIxFaz7G4unDmw6qRWL3K2g==&D0GHx=5jNT HTTP/1.1 Host: www.bettingweb365.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 15:19:35.810760975 CET	23891	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 28 Jan 2022 14:19:35 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://bettingweb365.com/u1p5/?y4Mp=UXBCCV9Hg7LlUlEhFgBZZuvhtrkgDnenbWAOO9JvD+HvWaQ2ttROIxFaz7G4unDmw6qRWL3K2g==&D0GHx=5jNT Vary: Accept-Encoding Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Statistics

Behavior



System Behavior

Analysis Process: H4vBtZsi8xAKaMm.exe PID: **6364**, Parent PID: **5436**

General

Target ID:	1
Start time:	15:15:37
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\H4vBtZsi8xAKaMm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\H4vBtZsi8xAKaMm.exe"
Imagebase:	0xe30000
File size:	1304576 bytes
MD5 hash:	7EABAB04E4A6FDD45238E32ED81E222C
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: 00000001.00000002.341894458.00000000042D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.341894458.00000000042D9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.341894458.00000000042D9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.341173431.000000000363B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: MSBuild.exe PID: **6100**, Parent PID: **6364**

General

Target ID:	14
Start time:	15:16:13
Start date:	28/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4b0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.401541679.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.401760345.0000000000E90000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.401760345.0000000000E90000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.401760345.0000000000E90000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.337332545.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.337332545.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.337332545.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.337090628.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.337090628.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.337090628.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.402488098.0000000001200000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.402488098.0000000001200000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.402488098.0000000001200000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3292**, Parent PID: **6100**

General

Target ID:	15
Start time:	15:16:16
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.388085827.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.388085827.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.388085827.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.375017182.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.375017182.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.375017182.000000000EBE6000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: rundll32.exe PID: **4480**, Parent PID: **3292**

General

Target ID:	19
Start time:	15:16:40
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x1110000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000013.00000002.798933508.00000000010C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.798933508.00000000010C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.798933508.00000000010C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.799622406.00000000046D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.799622406.00000000046D0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.799622406.00000000046D0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.790726113.0000000000AA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.790726113.0000000000AA0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.790726113.0000000000AA0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	ABA447	NtReadFile

Analysis Process: cmd.exe PID: **6880**, Parent PID: **4480**

General

Target ID:	20
Start time:	15:16:46
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6872**, Parent PID: **6880**

General

Target ID:	21
Start time:	15:16:48
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **4704**, Parent PID: **568**

General

Target ID:	30
Start time:	15:17:17
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: explorer.exe PID: **4104**, Parent PID: **568**

General

Target ID:	42
Start time:	15:18:17
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly