ID: 626543
Sample Name: From Richard.exe
Cookbook: default.jbs
Time: 11:57:10
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

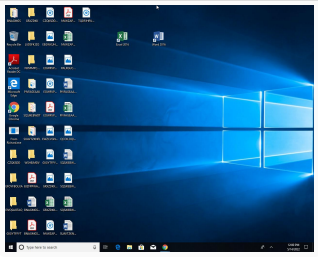
Windows Analysis Report

From Richard.exe

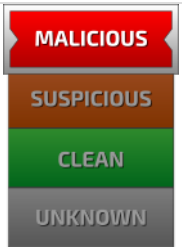
Overview

General Information

Sample Name:	From Richard.exe
Analysis ID:	626543
MD5:	fa530d1cf018a5c..
SHA1:	bbd46bf5bead0b..
SHA256:	fe581076f8a8cd9..
Tags:	agenttesla exe
Infos:	



Detection



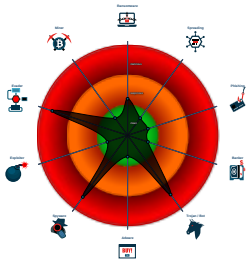
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- From Richard.exe (PID: 6432 cmdline: "C:\Users\user\Desktop\From Richard.exe" MD5: FA530D1CF018A5CC8C8215344B09D2F7)
  - From Richard.exe (PID: 6732 cmdline: C:\Users\user\Desktop\From Richard.exe MD5: FA530D1CF018A5CC8C8215344B09D2F7)
  - From Richard.exe (PID: 6740 cmdline: C:\Users\user\Desktop\From Richard.exe MD5: FA530D1CF018A5CC8C8215344B09D2F7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "btc@imfalert.com",
  "Password": "dontgiveup@2022",
  "Host": "mail.imfalert.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.271694098.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.271694098.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.271208855.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.271208855.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.508749383.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.From Richard.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.From Richard.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.From Richard.exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b21:$s10: logins • 0x32588:$s11: credential • 0x2eb72:$g1: get_Clipboard • 0x2eb80:$g2: get_Keyboard • 0x2eb8d:$g3: get_Password • 0x2fe91:$g4: get_CtrlKeyDown • 0x2fea1:$g5: get_ShiftKeyDown • 0x2feb2:$g6: get_AltKeyDown
5.2.From Richard.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.From Richard.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 34 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

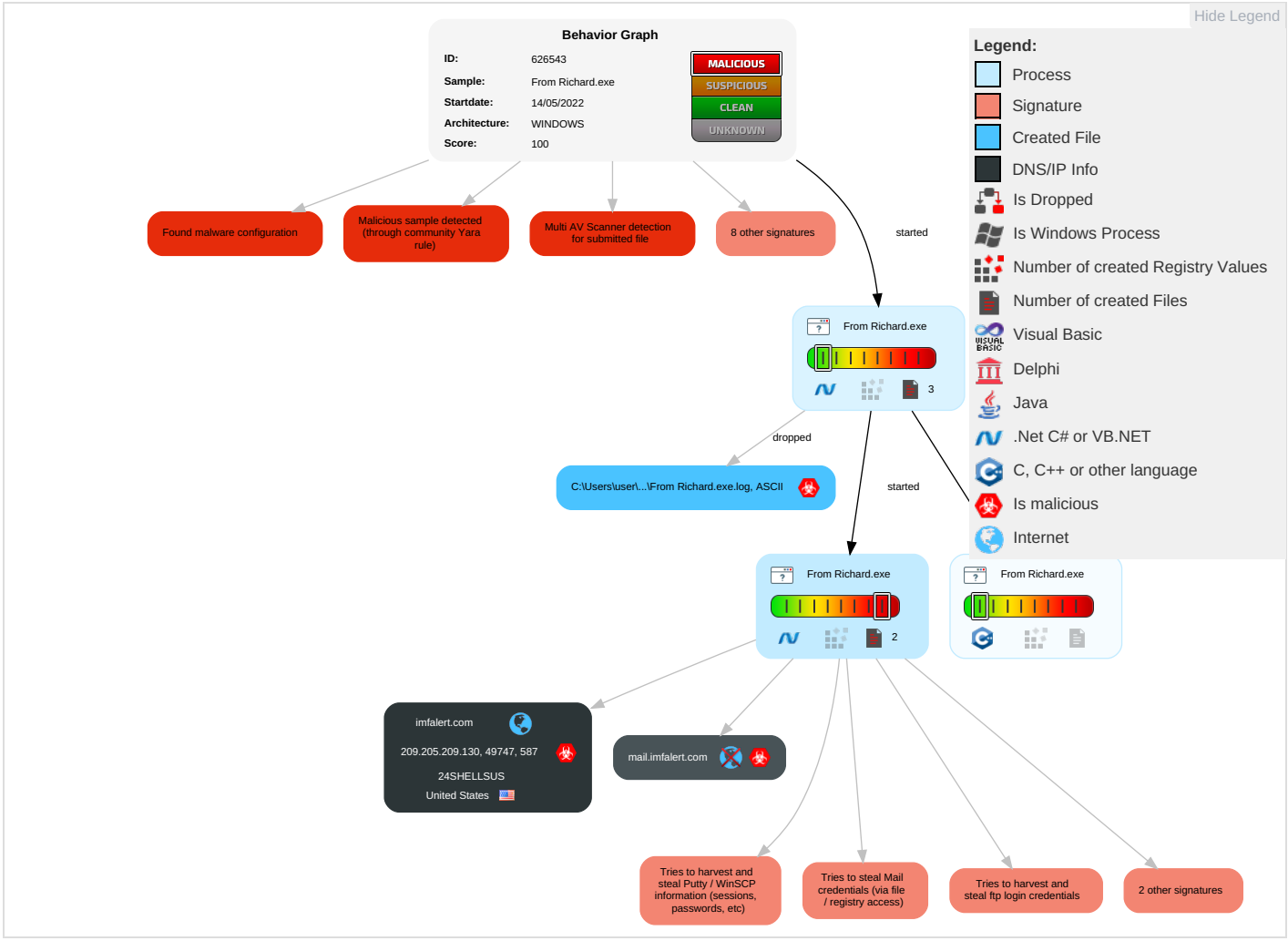
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	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	1 1 1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 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)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

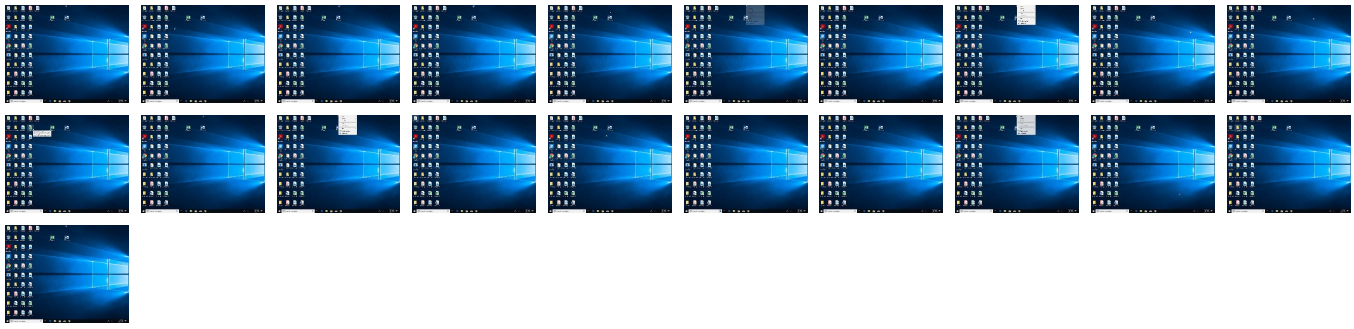
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
From Richard.exe	49%	Virustotal		Browse
From Richard.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
From Richard.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.From Richard.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.From Richard.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.From Richard.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.From Richard.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.From Richard.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.From Richard.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
imfalert.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.sandoll.co.kr-	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/6	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-us;	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://imfalert.com	0%	Avira URL Cloud	safe	
http://mail.imfalert.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://rfVwMD.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmfr-fr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://GJvFKn8SY2mNH.org	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
imfalert.com	209.205.209.130	true	true	• 0%, Virustotal, Browse	unknown
mail.imfalert.com	unknown	unknown	true		unknown

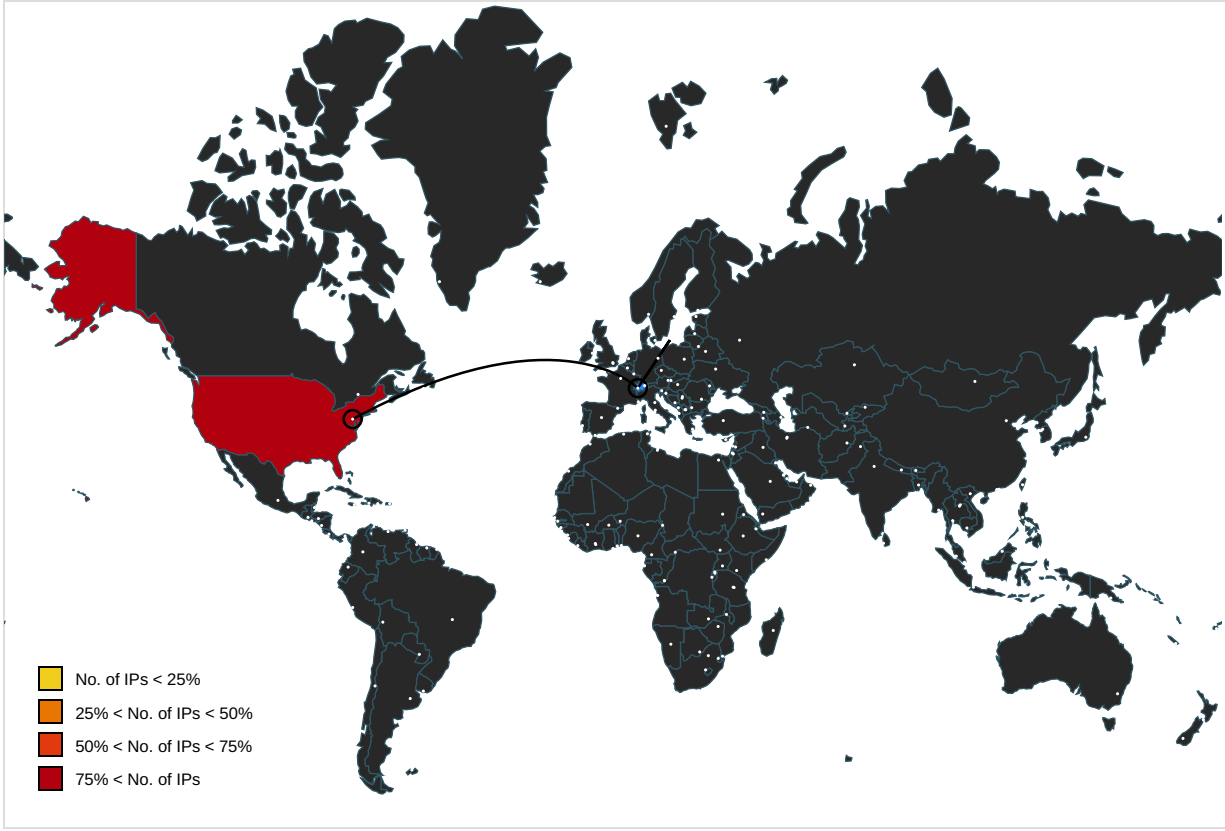
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp, From Richard.exe, 00000000.00000003.248894766.000000000 62E1000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.fontbureau.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	From Richard.exe, 00000005.00000002.5100 99135.000000000164A000.00000004.00000020 .00020000.00000000.sdmp, From Richard.exe, 00000005.00000002.511136148.000000000 3538000.00000004.00000800.00020000.00000 000.sdmp, From Richard.exe, 00000005.000 00003.303178584.0000000001676000.0000000 4.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr-	From Richard.exe, 00000000.00000003.2478 89234.00000000062D6000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp, From Richard.exe, 00000000.00000003.246948322.000000000 62EB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	From Richard.exe, 00000000.00000003.2478 89234.00000000062D6000.00000004.00000800 .00020000.00000000.sdmp, From Richard.exe, 00000000.00000002.282112351.000000000 74E2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/6	From Richard.exe, 00000000.00000003.2509 02150.00000000062D2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	From Richard.exe, 00000000.00000002.2819 59651.00000000062D0000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coml1	From Richard.exe, 00000000.00000002.2819 59651.00000000062D0000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-us;	From Richard.exe, 00000000.00000003.2509 02150.00000000062D2000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://imfalert.com	From Richard.exe, 00000005.00000002.5111 36148.0000000003538000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.imfalert.com	From Richard.exe, 00000005.00000002.5111 36148.0000000003538000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://rfVwMD.com	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htmfr-fr	From Richard.exe, 00000000.00000003.2560 01459.000000000630E000.00000004.00000800 .00020000.00000000.sdmp, From Richard.exe, 00000000.00000003.256123470.000000000 630E000.00000004.00000800.00020000.00000 000.sdmp, From Richard.exe, 00000000.000 00003.256046813.000000000630E000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	From Richard.exe, 00000000.00000002.2819 59651.00000000062D0000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	From Richard.exe, 00000000.00000003.2509 02150.00000000062D2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fonts.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	From Richard.exe, 00000000.00000003.2478 89234.00000000062D6000.00000004.00000800 .00020000.00000000.sdmp, From Richard.exe, 00000000.00000002.282112351.000000000 74E2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://https://GJvFKn8SY2mNH.org	From Richard.exe, 00000005.00000002.5113 06936.000000000355C000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	From Richard.exe, 00000000.00000002.2821 12351.00000000074E2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	From Richard.exe, 00000005.00000002.5103 23471.00000000031E1000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.205.209.130	imfalert.com	United States		55081	24SHELLSUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626543
Start date and time: 14/05/202211:57:10	2022-05-14 11:57:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	From Richard.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@2/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 33.6% • Quality standard deviation: 27.4%

HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target From Richard.exe, PID 6732 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:58:18	API Interceptor	725x Sleep call for process: From Richard.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\From Richard.exe.log

Process:	C:\Users\user\Desktop\From Richard.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ

MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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):	7.897267979651854
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	From Richard.exe
File size:	550912
MD5:	fa530d1cf018a5cc8c8215344b09d2f7
SHA1:	bbd46bf5bead0b503ce045e5d5a856745bca49b9
SHA256:	fe581076f8a8cd90b93b2bca8fde7fa8008c2c1c0962fc0282f785354fcda4a4
SHA512:	1ca23c746e0f98a384e2bc0842c773af9bb9bcac2c2bc2d2b38ebc870f0ea49466957fb1d0661fe5f7ecc3169857e9b250960eed9d222e9612b6f4d5818ffb7f
SSDEEP:	12288:lhWQ1JN/HRCakerytvcHi9sS2Q7oY4J/DP:UWQ1JpRCs20Hid2Qob9
TLSH:	0BC4122932F47B66E8BB9BFC42B4300503F5662B3111F3AE9DC520DB6A65F540741EAB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}b.....0..^.....}... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x487d82
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:	0x627DCBA3 [Fri May 13 03:08:19 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87d30	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x5c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x85d88	0x85e00	False	0.930996877918	data	7.90632247255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x5c4	0x600	False	0.424479166667	data	4.122031579	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	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_VERSION	0x88090	0x334	data		
RT_MANIFEST	0x883d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

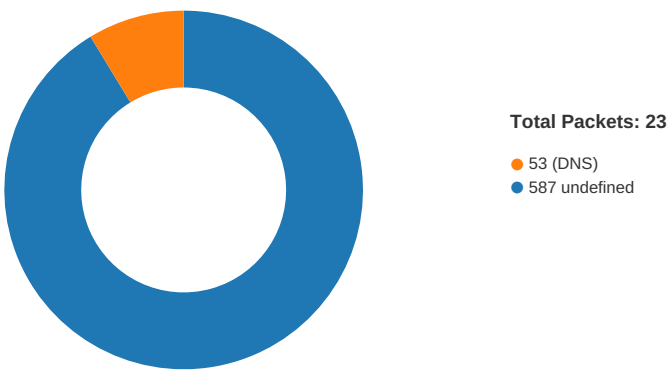
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	PropertyBuil.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	TexasHoldem
ProductVersion	1.0.0.0
FileDescription	TexasHoldem
OriginalFilename	PropertyBuil.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:58:36.338269949 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.441176891 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.441324949 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.595638990 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.598819971 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.702187061 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.702584982 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.807768106 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.865362883 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.974081039 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.974169016 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.974215984 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.974255085 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:36.974255085 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.974313021 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:36.975522995 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.028873920 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.132056952 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.225039959 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.328228951 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.332756996 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.436261892 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.469553947 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.588709116 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.606544971 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.709552050 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.712232113 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.825894117 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.876655102 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.979805946 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:37.981095076 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.981161118 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.981924057 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:37.982029915 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 11:58:38.084068060 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:38.084152937 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:38.084671021 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:38.084703922 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:38.093137980 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 11:58:38.136451006 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 12:00:15.973247051 CEST	49747	587	192.168.2.3	209.205.209.130
May 14, 2022 12:00:16.117870092 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 12:00:16.405720949 CEST	587	49747	209.205.209.130	192.168.2.3
May 14, 2022 12:00:16.407898903 CEST	49747	587	192.168.2.3	209.205.209.130

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 11:58:36.054285049 CEST	55923	53	192.168.2.3	8.8.8.8
May 14, 2022 11:58:36.157443047 CEST	53	55923	8.8.8.8	192.168.2.3
May 14, 2022 11:58:36.216921091 CEST	57723	53	192.168.2.3	8.8.8.8
May 14, 2022 11:58:36.318223953 CEST	53	57723	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 11:58:36.054285049 CEST	192.168.2.3	8.8.8.8	0x7825	Standard query (0)	mail.imfalert.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 11:58:36.216921091 CEST	192.168.2.3	8.8.8.8	0x7190	Standard query (0)	mail.imfalert.com	A (IP address)	IN (0x0001)

DNS Answers

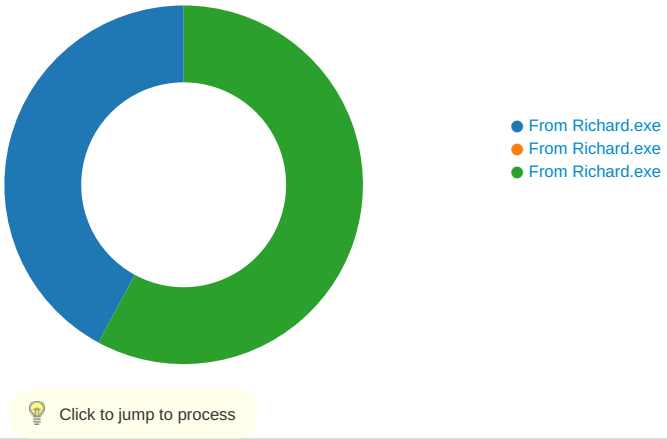
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 11:58:36.157443047 CEST	8.8.8.8	192.168.2.3	0x7825	No error (0)	mail.imfalert.com	imfalert.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:58:36.157443047 CEST	8.8.8.8	192.168.2.3	0x7825	No error (0)	imfalert.com		209.205.209.130	A (IP address)	IN (0x0001)
May 14, 2022 11:58:36.318223953 CEST	8.8.8.8	192.168.2.3	0x7190	No error (0)	mail.imfalert.com	imfalert.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 11:58:36.318223953 CEST	8.8.8.8	192.168.2.3	0x7190	No error (0)	imfalert.com		209.205.209.130	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 11:58:36.595638990 CEST	587	49747	209.205.209.130	192.168.2.3	220-standard8.doveserver.com ESMTP Exim 4.95 #2 Sat, 14 May 2022 10:58:36 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 11:58:36.598819971 CEST	49747	587	192.168.2.3	209.205.209.130	EHLO 585948
May 14, 2022 11:58:36.702187061 CEST	587	49747	209.205.209.130	192.168.2.3	250-standard8.doveserver.com Hello 585948 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
May 14, 2022 11:58:36.702584982 CEST	49747	587	192.168.2.3	209.205.209.130	STARTTLS
May 14, 2022 11:58:36.807768106 CEST	587	49747	209.205.209.130	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: From Richard.exe PID: 6432, Parent PID: 4856

General

Target ID:	0
Start time:	11:58:10
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\From Richard.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\From Richard.exe"
Imagebase:	0xfc0000
File size:	550912 bytes
MD5 hash:	FA530D1CF018A5CC8C8215344B09D2F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.277272933.0000000003481000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.281354781.00000000045DC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.281354781.00000000045DC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\From Richard.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\From Richard.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C151B4F	ReadFile

Analysis Process: From Richard.exe PID: **6732**, Parent PID: **6432**

General

Target ID:	4
Start time:	11:58:20
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\From Richard.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\From Richard.exe
Imagebase:	0x340000
File size:	550912 bytes
MD5 hash:	FA530D1CF018A5CC8C8215344B09D2F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: From Richard.exe PID: **6740**, Parent PID: **6432**

General

Target ID:	5
Start time:	11:58:22
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\From Richard.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\From Richard.exe
Imagebase:	0xec0000
File size:	550912 bytes
MD5 hash:	FA530D1CF018A5CC8C8215344B09D2F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.271694098.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.271694098.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.271208855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.271208855.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.508749383.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.508749383.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.270510923.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.270510923.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.270879293.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.270879293.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.510323471.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.510323471.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C151B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C151B4F	ReadFile

Disassembly

No disassembly