ID: 321396
Sample Name:
DOC04121993.exe
Cookbook: default.jbs
Time: 10:35:20
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

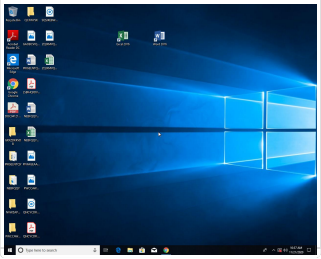
Analysis Report DOC04121993.exe

Overview

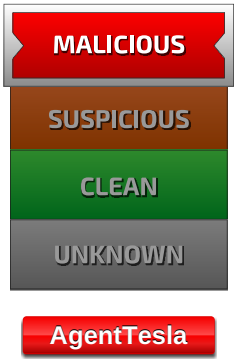
General Information

Sample Name:	DOC04121993.exe
Analysis ID:	321396
MD5:	710843b45a8e65..
SHA1:	909799ac70c5a8..
SHA256:	d0ea8610ecee6c..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

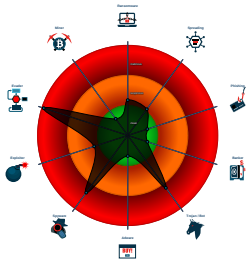


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Drops script at star…
- Yara detected AgentTesla
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Contains functionality to detect slee…
- Delayed program exit found

Classification



Startup

- **System is w10x64**
- DOC04121993.exe (PID: 2576 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' MD5: 710843B45A8E65C939D3AB4FB96D73E4)
  - notepad.exe (PID: 4472 cmdline: C:\Windows\system32\notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
  - DOC04121993.exe (PID: 1000 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' MD5: 710843B45A8E65C939D3AB4FB96D73E4)
  - DOC04121993.exe (PID: 1832 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' 2 1000 3714343 MD5: 710843B45A8E65C939D3AB4FB96D73E4)
- wscript.exe (PID: 2168 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - DOC04121993.exe (PID: 5080 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' MD5: 710843B45A8E65C939D3AB4FB96D73E4)
    - notepad.exe (PID: 780 cmdline: C:\Windows\system32\notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
    - DOC04121993.exe (PID: 1956 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' MD5: 710843B45A8E65C939D3AB4FB96D73E4)
    - DOC04121993.exe (PID: 5320 cmdline: 'C:\Users\user\Desktop\DOC04121993.exe' 2 1956 3726421 MD5: 710843B45A8E65C939D3AB4FB96D73E4)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "bq6qu",
  "URL: ": "http://vd2JBRKVM6n.net",
  "To: ": "info@hybridgroupco.com",
  "ByHost: ": "mail.hybridgroupco.com:587",
  "Password: ": "IhNKJa9",
  "From: ": "info@hybridgroupco.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.229601884.00000000027C5000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.462629290.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.464088936.00000000009E2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.199767698.000000000270500.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.464255746.000000000224000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

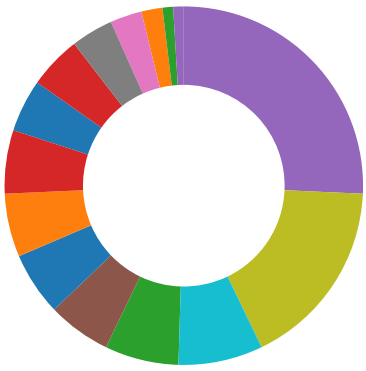
Source	Rule	Description	Author	Strings
7.2.DOC04121993.exe.2290000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.DOC04121993.exe.2240000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.DOC04121993.exe.2150000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.DOC04121993.exe.980000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.DOC04121993.exe.21b0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: Drops script at startup location

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (creates a PE file in dynamic memory)
- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker

Boot Survival:

- Drops VBS files to the startup folder

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications
- Delayed program exit found
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

Remote Access Functionality:

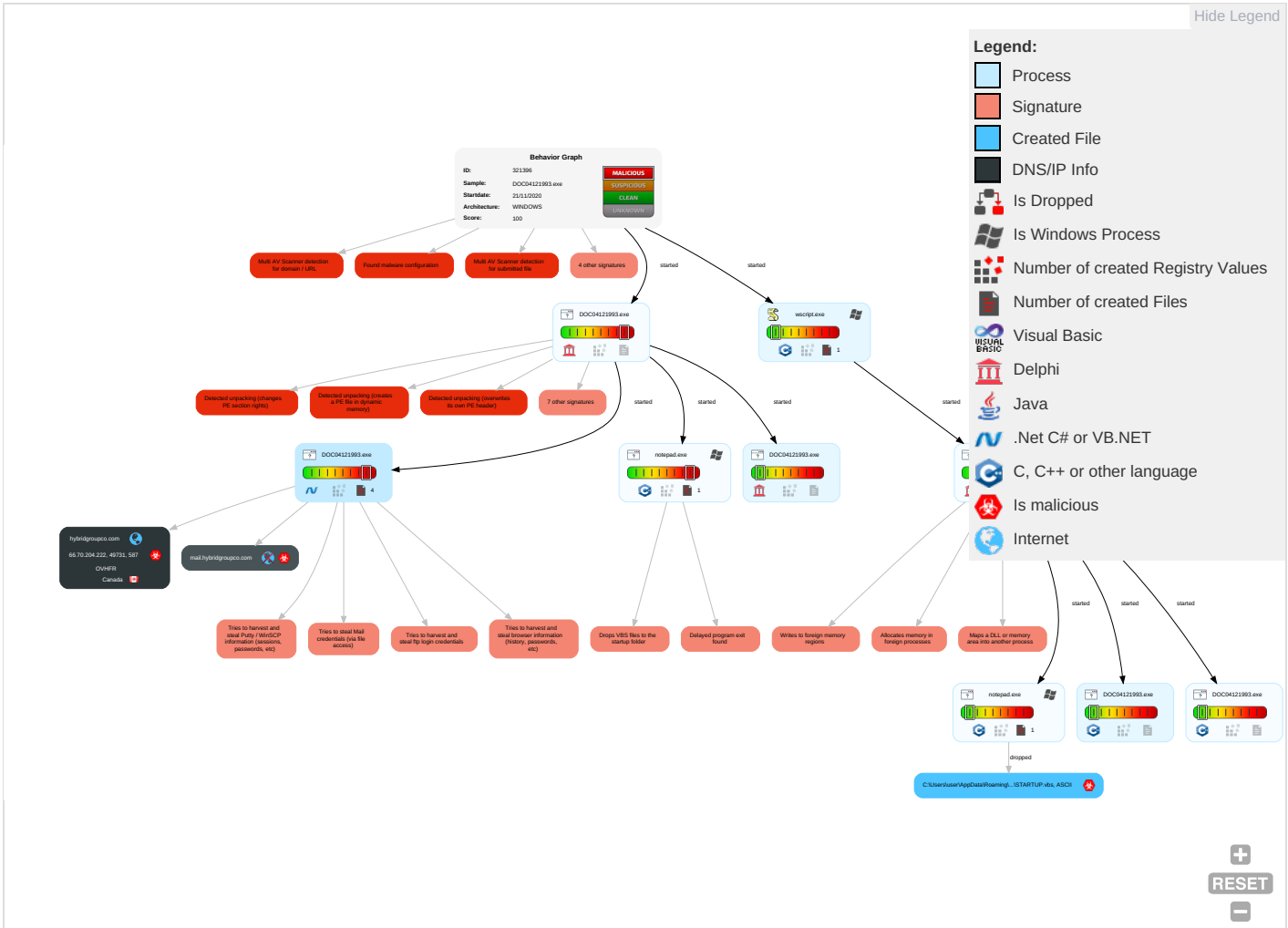
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Othe Network Medium
Default Accounts	Scripting 1 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Scripting 1 1 1	Credentials in Registry 1	File and Directory Discovery 3	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltratio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 4 1 2	Obfuscated Files or Information 2	NTDS	System Information Discovery 1 2 8	Distributed Component Object Model	Email Collection 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Software Packing 4 1	LSA Secrets	Query Registry 1	SSH	Input Capture 2 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Security Software Discovery 2 7 1	VNC	Clipboard Data 2	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 5	DCSync	Virtualization/Sandbox Evasion 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypte Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusca Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

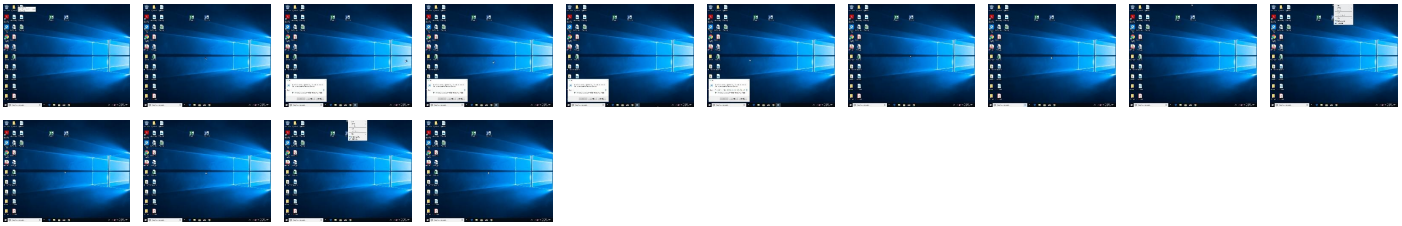
Behavior Graph



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
DOC04121993.exe	69%	Virustotal		Browse
DOC04121993.exe	81%	ReversingLabs	Win32.Trojan.LokiBot	
DOC04121993.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.1.DOC04121993.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.DOC04121993.exe.2240000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.DOC04121993.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
7.2.DOC04121993.exe.21b0000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.DOC04121993.exe.2290000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.DOC04121993.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
5.2.DOC04121993.exe.2750000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.DOC04121993.exe.2690000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
5.2.DOC04121993.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
0.2.DOC04121993.exe.22e0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.1.DOC04121993.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.DOC04121993.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
2.2.DOC04121993.exe.9e0000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.DOC04121993.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
hybridgroupco.com	0%	Virustotal		Browse
mail.hybridgroupco.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:	0%	Virustotal		Browse
http://127.0.0.1:	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://vd2JBRKVM6n.net	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://vd2JBRKVM6n.net$	0%	Avira URL Cloud	safe	

Domains and IPs

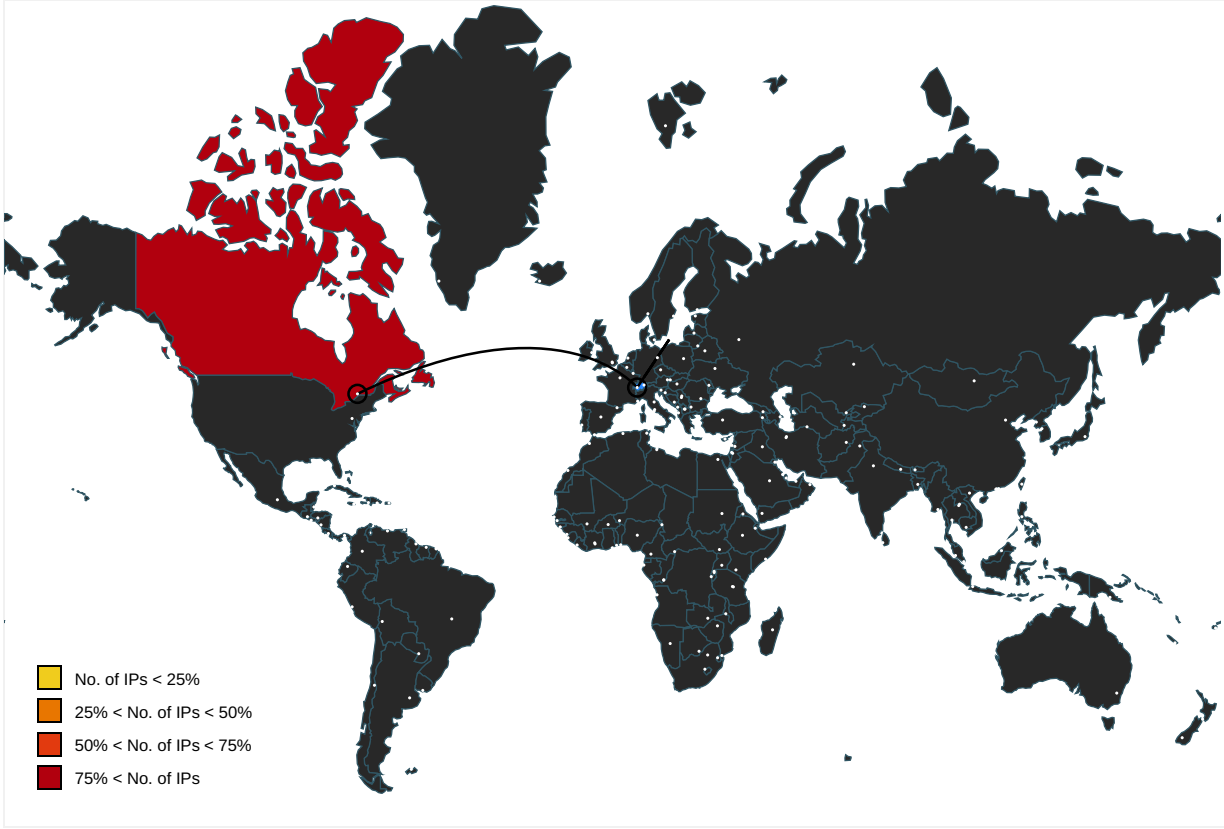
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hybridgroupco.com	66.70.204.222	true	true	• 0%, Virustotal, Browse	unknown
mail.hybridgroupco.com	unknown	unknown	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:	DOC04121993.exe, DOC04121993.exe, 00000007.00000002.22371228 0.0000000000475000.00000040.00 000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/	DOC04121993.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	DOC04121993.exe, 00000000.0000 0002.199767698.000000000270500 0.00000040.00000001.sdmp, DOC0 4121993.exe, 00000002.00000002 .462629290.0000000000402000.00 000040.00000001.sdmp, DOC04121 993.exe, 00000005.00000002.229 601884.00000000027C5000.000000 40.00000001.sdmp, DOC04121993.exe, 00000007.00000002.2237122 80.0000000000475000.00000040.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vd2JBRKVM6n.net	DOC04121993.exe, 00000002.0000 0002.467888799.0000000002B7000 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	DOC04121993.exe, 00000002.0000 0002.468167788.0000000002C9E00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	DOC04121993.exe, DOC04121993.exe, 00000007.00000002.22371228 0.0000000000475000.00000040.00 000001.sdmp	false		high
http://cert.int-x3.letsencrypt.org/0	DOC04121993.exe, 00000002.0000 0002.468167788.0000000002C9E00 0.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DOC04121993.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.int-x3.letsencrypt.org0/	DOC04121993.exe, 00000002.0000 0002.468167788.0000000002C9E00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	DOC04121993.exe, 00000002.0000 0002.468167788.0000000002C9E00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vd2JBRKVM6n.net$	DOC04121993.exe, 00000002.0000 0002.467655668.0000000002A9200 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321396
Start date:	21.11.2020
Start time:	10:35:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOC04121993.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:	32
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@16/2@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 90.3% (good quality ratio 87.7%) • Quality average: 84.7% • Quality standard deviation: 25%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 52.255.188.83, 104.42.151.234, 51.104.139.180, 92.122.213.247, 92.122.213.194, 92.122.144.200, 20.54.26.129, 51.104.144.132, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing disassembly code. • 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
10:36:07	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs
10:36:22	API Interceptor	824x Sleep call for process: DOC04121993.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	PI.exe	Get hash	malicious	Browse	
	d9f83622ec1564600202a937d2414af8.exe	Get hash	malicious	Browse	
	Image001.exe	Get hash	malicious	Browse	
	mEPbT6Dbzc.exe	Get hash	malicious	Browse	
	b32sUgpVdT.exe	Get hash	malicious	Browse	
	ZXeB2BO1Lq.exe	Get hash	malicious	Browse	
	kiGANMAmR3.exe	Get hash	malicious	Browse	
	QM34U1x8l6.exe	Get hash	malicious	Browse	
	Y2UrKCOaJm.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SJAOO8OCe3.exe	Get hash	malicious	Browse	
	zh7966Pn0l.exe	Get hash	malicious	Browse	
	o7B4zT1WNb.exe	Get hash	malicious	Browse	
	emMAbUc8Xg.exe	Get hash	malicious	Browse	
	a2onj1GOHs.exe	Get hash	malicious	Browse	
	RDp6VoVSfQ.exe	Get hash	malicious	Browse	
	DUE_INVOICE.exe	Get hash	malicious	Browse	
	2M3ZdRze7b.exe	Get hash	malicious	Browse	
	36n0FgVGxo.exe	Get hash	malicious	Browse	
	ErKsKTqlS4.exe	Get hash	malicious	Browse	
	yrPgLCinv1.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	PI.exe	Get hash	malicious	Browse	• 66.70.204.222
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 167.114.119.127
	http://https://coralcliffs.com.do/review/	Get hash	malicious	Browse	• 188.165.231.37
	http://https://rugbysacele.ro/zz/lK/of1/nhctfwp4x278qkbusvijl6z39y5ema1o0gdr597irqhw4x0fk3uevzlaoj12bdmpsnt8g6yce40h6iv7bprsowxd3z2nmu8kal5gcj1yf9qt?data=dmluY2VudC5kdXNvcmRldEBpbWQub3Jn#aHR0cHM6Ly9ydWdieXNhY2VsZS5yby96ei9JSy9vZjEvNDUzMjY3NzY4JmVtYWlsPXZpbmNlbnQuZHVzb3JkZXRAaW1kLm9yZw==	Get hash	malicious	Browse	• 51.195.133.190
	http://flossdental.com.au	Get hash	malicious	Browse	• 46.105.201.240
	http://https://bit.ly/2UDM1To	Get hash	malicious	Browse	• 54.38.220.151
	inquiry-010.14.2020.doc	Get hash	malicious	Browse	• 94.23.162.163
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 51.89.9.253
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 51.89.9.253
	http://https://winnersoft.lu/systemadmin/?12=	Get hash	malicious	Browse	• 91.121.74.46
	http://https://carolearmstrongrealestate.com/wpe/14ea332d0684051d9fef033a5f1607dd?usr=cnBlbmRsZXRvbkBkYXRlc3dlaXNlci5jb20=	Get hash	malicious	Browse	• 51.38.157.153
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 51.195.43.214
	QUOTE.exe	Get hash	malicious	Browse	• 51.89.1.123
	ORDER INQUIRY.exe	Get hash	malicious	Browse	• 51.91.236.193
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 51.79.191.17
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 188.165.53.185
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 188.165.53.185
	d9f83622ec1564600202a937d2414af8.exe	Get hash	malicious	Browse	• 66.70.204.222
	direct_010.20.doc	Get hash	malicious	Browse	• 94.23.162.163
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 51.210.112.130

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs

Process:	C:\Windows\SysWOW64\notepad.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	
Size (bytes):	122
Entropy (8bit):	5.36354376778109
Encrypted:	false
SSDEEP:	3:7gwJMr/vtVlmEHhA1FWXp5vhqm77trinRkn:UzPldBA7WXpF8m71i2n
MD5:	863B251962DCEFF8DC4CF0794C51DBD7
SHA1:	639371523C3274C4B3CED14564213AE2AC5F67E7
SHA-256:	A2755DC8A8AD6573A09C4E3CD83265747842802D9AA9CD7AF16939FCFF8B17BF
SHA-512:	F10460F89A54CF00E9BDE282C776B586901D92921C42B3FC26AA2FBAD4AD5B553DB8F9DC476BEFADCDC6F83838C9A0AB2AF25CEB99F7766CFDE335AB042ED96D
Malicious:	**true**
Reputation:	low
Preview:	seT ODikjwDxemlA = cREAtEobJect("wsCrIpt.ShEll")..OdIkjWdxemlA.run """C:\Users\user\Desktop\DOC04121993.exe""", 0, False.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.879727497186752
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	DOC04121993.exe
File size:	978432
MD5:	710843b45a8e65c939d3ab4fb96d73e4
SHA1:	909799ac70c5a8a472b40579ff0c5bc982979676
SHA256:	d0ea8610ecee6c92c50af51c37a0a49f8550768609a08a5a2dcaf98bb06dcff3
SHA512:	04508620bcb1d8406cddcd0ae1dd9f0c31f27ad6e5c140fba402a0c5951901ae62e0f006a35e897f101cac36849981b8379585f906c5db0ef8f4686e7fb8acbc
SSDEEP:	12288:NuhWgv/dKx2k3bue05YyZVr0ZEs+ihR6JL4o9YWg/XLq7XJK/hmlYpOo5WpxIp:Nwz1Kx2k3T0jZGOL7JLBiWgk508lGQKp
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General

Entrypoint:	0x470d00
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	429b4d8f1079c5bb87cad5efdb4eabf0

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00470B08h
call 00007F0B54E286EDh
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
call 00007F0B54E7D715h
mov ecx, dword ptr [0048A0A4h]
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
mov edx, dword ptr [004705ACh]
call 00007F0B54E7D715h
mov eax, dword ptr [00489FACh]
mov eax, dword ptr [eax]
call 00007F0B54E7D789h
call 00007F0B54E261E4h
lea eax, dword ptr [eax+00h]
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8c000	0x2496	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x99000	0x5b424	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x91000	0x7b70	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x90000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x6fd48	0x6fe00	False	0.517266061453	data	6.51621253086	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x71000	0x19130	0x19200	False	0.189841806592	data	2.85009273727	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x8b000	0xcb1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x8c000	0x2496	0x2600	False	0.352796052632	data	4.9419643729	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x8f000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x90000	0x18	0x200	False	0.048828125	data	0.186582516435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x91000	0x7b70	0x7c00	False	0.575321320565	data	6.64623366609	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x99000	0x5b424	0x5b600	False	0.776162790698	data	7.33023350526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x99ed8	0x134	data		
RT_CURSOR	0x9a00c	0x134	data		
RT_CURSOR	0x9a140	0x134	data		
RT_CURSOR	0x9a274	0x134	data		
RT_CURSOR	0x9a3a8	0x134	data		
RT_CURSOR	0x9a4dc	0x134	data		
RT_CURSOR	0x9a610	0x134	data		
RT_BITMAP	0x9a744	0x1d0	data		
RT_BITMAP	0x9a914	0x1e4	data		
RT_BITMAP	0x9aaf8	0x1d0	data		
RT_BITMAP	0x9acc8	0x1d0	data		
RT_BITMAP	0x9ae98	0x1d0	data		
RT_BITMAP	0x9b068	0x1d0	data		
RT_BITMAP	0x9b238	0x1d0	data		
RT_BITMAP	0x9b408	0x1d0	data		
RT_BITMAP	0x9b5d8	0x472f5	data	English	United States
RT_BITMAP	0xe28d0	0x1d0	data		
RT_BITMAP	0xe2aa0	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe2b60	0xd8	data		
RT_BITMAP	0xe2c38	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe2d18	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe2df8	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe2ed8	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe2f98	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe3058	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe3138	0xd8	data		
RT_BITMAP	0xe3210	0xd8	data		
RT_BITMAP	0xe32e8	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe33a8	0xd8	data		
RT_BITMAP	0xe3480	0xe0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe3560	0xd8	data		
RT_BITMAP	0xe3638	0xe8	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe3720	0xc0	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xe37e0	0xe0	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe38c0	0xd228	data		
RT_ICON	0xf0ae8	0x8a8	data	English	United States
RT_DIALOG	0xf1390	0x52	data		
RT_STRING	0xf13e4	0x194	data		
RT_STRING	0xf1578	0x2b0	data		
RT_STRING	0xf1828	0xdc	data		
RT_STRING	0xf1904	0x17c	data		
RT_STRING	0xf1a80	0x1f0	data		
RT_STRING	0xf1c70	0x4ac	data		
RT_STRING	0xf211c	0x39c	data		
RT_STRING	0xf24b8	0x378	data		
RT_STRING	0xf2830	0x418	data		
RT_STRING	0xf2c48	0xf4	data		
RT_STRING	0xf2d3c	0xc4	data		
RT_STRING	0xf2e00	0x2e0	data		
RT_STRING	0xf30e0	0x35c	data		
RT_STRING	0xf343c	0x2b4	data		
RT_RCDATA	0xf36f0	0x10	data		
RT_RCDATA	0xf3700	0x280	data		
RT_RCDATA	0xf3980	0x841	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xf41c4	0x14	Lotus unknown worksheet or configuration, revision 0x1		

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0xf41d8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf41ec	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf4200	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf4214	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf4228	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf423c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xf4250	0x14	data	English	United States
RT_GROUP_ICON	0xf4264	0x14	data		
RT_HTML	0xf4278	0x1a9	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCurrentDirectoryA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVolumeInformationA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLogicalDrives, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDriveTypeA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
mpr.dll	WNetGetConnectionA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, Polyline, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtTextOutA, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreateWindowExA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayRedim, SafeArrayCreate, VariantChangeTypeEx, VariantCopyInd, VariantCopy, VariantClear, VariantInit

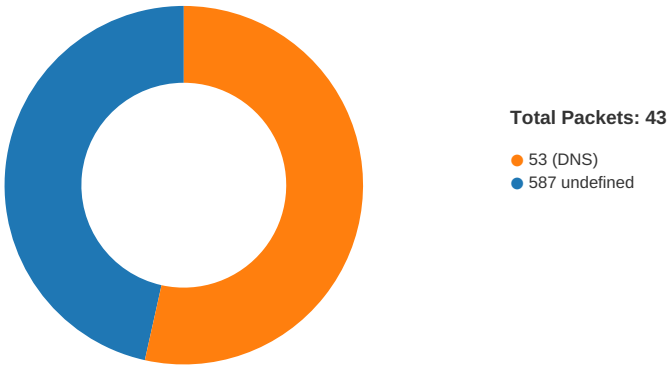
DLL	Import
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
kernel32.dll	MulDiv

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 10:36:43.006767035 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.110047102 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.110234022 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.337428093 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.338118076 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.441622019 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.442186117 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.547034979 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.597945929 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.611474037 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.720846891 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.720907927 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.720932961 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.721205950 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.733109951 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.836888075 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:43.879349947 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:43.923821926 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.027242899 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.028197050 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.131588936 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.132076025 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.235878944 CET	587	49731	66.70.204.222	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 10:36:44.236903906 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.340192080 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.341260910 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.444878101 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.445885897 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.549367905 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.552282095 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.552587986 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.552819014 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.553050995 CET	49731	587	192.168.2.3	66.70.204.222
Nov 21, 2020 10:36:44.655755043 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.655802965 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.655822992 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.656056881 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.658006907 CET	587	49731	66.70.204.222	192.168.2.3
Nov 21, 2020 10:36:44.707648993 CET	49731	587	192.168.2.3	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 10:35:59.611641884 CET	58361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:35:59.647598028 CET	53	58361	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:00.476222038 CET	63492	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:00.503604889 CET	53	63492	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:01.211216927 CET	60831	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:01.238569975 CET	53	60831	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:01.956403017 CET	60100	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:01.983720064 CET	53	60100	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:02.867257118 CET	53195	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:02.894689083 CET	53	53195	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:03.809859991 CET	50141	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:03.837081909 CET	53	50141	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:04.494957924 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:04.530426025 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:05.522062063 CET	49563	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:05.549319029 CET	53	49563	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:07.763705015 CET	51352	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:07.791035891 CET	53	51352	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:09.928251982 CET	59349	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:09.955519915 CET	53	59349	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:11.010195971 CET	57084	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:11.037492990 CET	53	57084	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:11.758013010 CET	58823	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:11.785459042 CET	53	58823	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:12.388540030 CET	57568	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:12.415865898 CET	53	57568	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:13.139347076 CET	50540	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:13.175124884 CET	53	50540	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:25.613919020 CET	54366	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:25.641292095 CET	53	54366	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:30.761260033 CET	53034	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:30.798211098 CET	53	53034	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:37.193355083 CET	57762	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:37.231781960 CET	53	57762	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:40.813800097 CET	55435	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:40.857342958 CET	53	55435	8.8.8.8	192.168.2.3
Nov 21, 2020 10:36:42.922708035 CET	50713	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:36:42.969963074 CET	53	50713	8.8.8.8	192.168.2.3
Nov 21, 2020 10:37:01.039278984 CET	56132	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:37:01.066524982 CET	53	56132	8.8.8.8	192.168.2.3
Nov 21, 2020 10:37:03.973825932 CET	58987	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:37:04.022171974 CET	53	58987	8.8.8.8	192.168.2.3
Nov 21, 2020 10:37:35.499826908 CET	56579	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:37:35.527122974 CET	53	56579	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 10:37:37.098423958 CET	60633	53	192.168.2.3	8.8.8.8
Nov 21, 2020 10:37:37.125749111 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 10:36:42.922708035 CET	192.168.2.3	8.8.8.8	0xd70b	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 10:36:42.969963074 CET	8.8.8.8	192.168.2.3	0xd70b	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 10:36:42.969963074 CET	8.8.8.8	192.168.2.3	0xd70b	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)

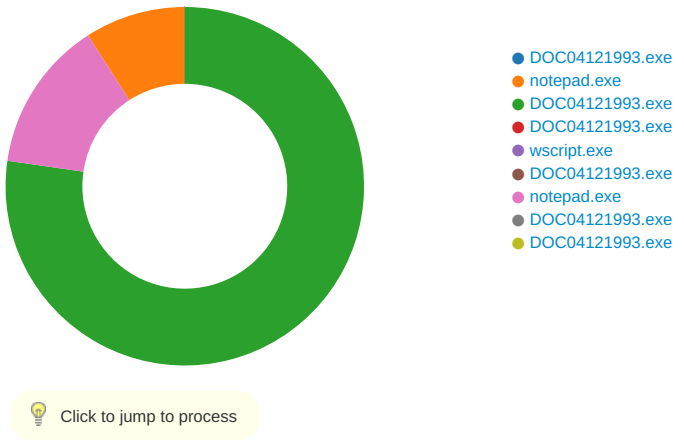
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 21, 2020 10:36:43.337428093 CET	587	49731	66.70.204.222	192.168.2.3	220-host.theserver.live ESMTP Exim 4.93 #2 Sat, 21 Nov 2020 13:36:43 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 21, 2020 10:36:43.338118076 CET	49731	587	192.168.2.3	66.70.204.222	EHLO 141700
Nov 21, 2020 10:36:43.441622019 CET	587	49731	66.70.204.222	192.168.2.3	250-host.theserver.live Hello 141700 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Nov 21, 2020 10:36:43.442186117 CET	49731	587	192.168.2.3	66.70.204.222	STARTTLS
Nov 21, 2020 10:36:43.547034979 CET	587	49731	66.70.204.222	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

System Behavior

Analysis Process: DOC04121993.exe PID: 2576 Parent PID: 5556

General

Start time:	10:36:04
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe'
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.199767698.0000000002705000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.199649349.0000000002692000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: notepad.exe PID: 4472 Parent PID: 2576

General

Start time:	10:36:05
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\notepad.exe
Imagebase:	0xa70000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A3010A	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	unknown	122	73 65 54 20 4f 44 69 6b 6a 77 44 78 65 6d 6c 41 20 3d 20 63 52 45 41 74 45 6f 62 4a 65 63 74 28 22 77 73 43 72 49 70 74 2e 53 68 45 6c 6c 22 29 0d 0a 4f 64 49 6b 6a 57 64 78 65 6d 6c 41 2e 72 75 6e 20 22 22 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 44 4f 43 30 34 31 32 31 39 39 33 2e 65 78 65 22 22 22 2c 20 30 2c 20 46 61 6c 73 65 00	seT ODikjwDxemlA = cREAtEobJect("wscr ipt.ShEll")..OdIkjWdxemlA. run "" "C:\Users\user\Desktop\D OC04121993.exe""", 0, False.	success or wait	1	A3012F	WriteFile

Analysis Process: DOC04121993.exe PID: 1000 Parent PID: 2576

General

Start time:	10:36:05
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe'
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
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: 00000002.00000002.462629290.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.464088936.00000000009E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.464255746.0000000002242000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.467655668.0000000002A92000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.464010082.0000000000980000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.462860776.0000000000475000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.467418503.00000000029D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.467888799.0000000002B70000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	55D0E3F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	55D0E3F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	55D0E3F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	55D0E3F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c201986d-829f-484f-befe-c316546d39a8	unknown	4096	success or wait	1	55D0E3F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	55D0E3F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	55D0E3F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	55D0E3F	ReadFile

Analysis Process: DOC04121993.exe PID: 1832 Parent PID: 2576

General

Start time:	10:36:06
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe' 2 1000 3714343
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: wscript.exe PID: 2168 Parent PID: 3388

General

Start time:	10:36:15
Start date:	21/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs'
Imagebase:	0x7ff6149f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: DOC04121993.exe PID: 5080 Parent PID: 2168

General

Start time:	10:36:16
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe'
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.229601884.00000000027C5000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: notepad.exe PID: 780 Parent PID: 5080

General

Start time:	10:36:17
Start date:	21/11/2020
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\notepad.exe
Imagebase:	0xa70000
File size:	236032 bytes
MD5 hash:	D693F13FE3AA2010B854C4C60671B8E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3F010A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	success or wait	1	3F01E1	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\STARTUP.vbs	unknown	122	73 65 54 20 4f 44 69 6b 6a 77 44 78 65 6d 6c 41 20 3d 20 63 52 45 41 74 45 6f 62 4a 65 63 74 28 22 77 73 43 72 49 70 74 2e 53 68 45 6c 6c 22 29 0d 0a 4f 64 49 6b 6a 57 64 78 65 6d 6c 41 2e 72 75 6e 20 22 22 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 44 4f 43 30 34 31 32 31 39 39 33 2e 65 78 65 22 22 22 2c 20 30 2c 20 46 61 6c 73 65 00	seT ODikjwDxemlA = cREAtEobJect("wscript.ShEll")..OdIkjWdxemlA.run """"C:\Users\user\Desktop\DOC04121993.exe""""", 0, False.	success or wait	1	3F012F	WriteFile

Analysis Process: DOC04121993.exe PID: 1956 Parent PID: 5080

General

Start time:	10:36:17
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe'
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.223712280.0000000000475000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.224265072.0000000002150000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.224575545.0000000002292000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000001.223334796.0000000000499000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.224389648.00000000021B2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: DOC04121993.exe PID: 5320 Parent PID: 5080

General

Start time:	10:36:18
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\DOC04121993.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\DOC04121993.exe' 2 1956 3726421
Imagebase:	0x400000
File size:	978432 bytes
MD5 hash:	710843B45A8E65C939D3AB4FB96D73E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis