ID: 432708
Sample Name: SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
Cookbook: default.jbs
Time: 17:30:18
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report SAUDI ARAMCO Tender Documents - B…

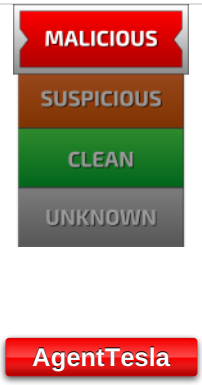
Overview

General Information

Sample Name:	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
Analysis ID:	432708
MD5:	d482d04bd4113f1.
SHA1:	783f25f265c3468..
SHA256:	9973c00cf203198..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection



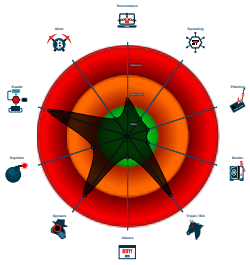
AgentTesla

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…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



- **System is w10x64**
- SAUDI ARAMCO Tender Documents - BOQ and ITB.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe' MD5: D482D04BD4113F1F9F08E39BCA4A3F27)
  - schtasks.exe (PID: 6824 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sXNiyYIFndkxd' /XML 'C:\Users\user\AppData\Local\Temp\tmp2894.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6904 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "admin@dangotesugars.com08102186737CEOus2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.370688660.00000000041A9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.370688660.00000000041A9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.367493021.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.367493021.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.369670905.00000000031E1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.SAUDI ARAMCO Tender Documents - BOQ and ITB.exe.43a6a70.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.SAUDI ARAMCO Tender Documents - BOQ and ITB.exe.43a6a70.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Signature Overview

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

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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

Writes to foreign memory regions

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:

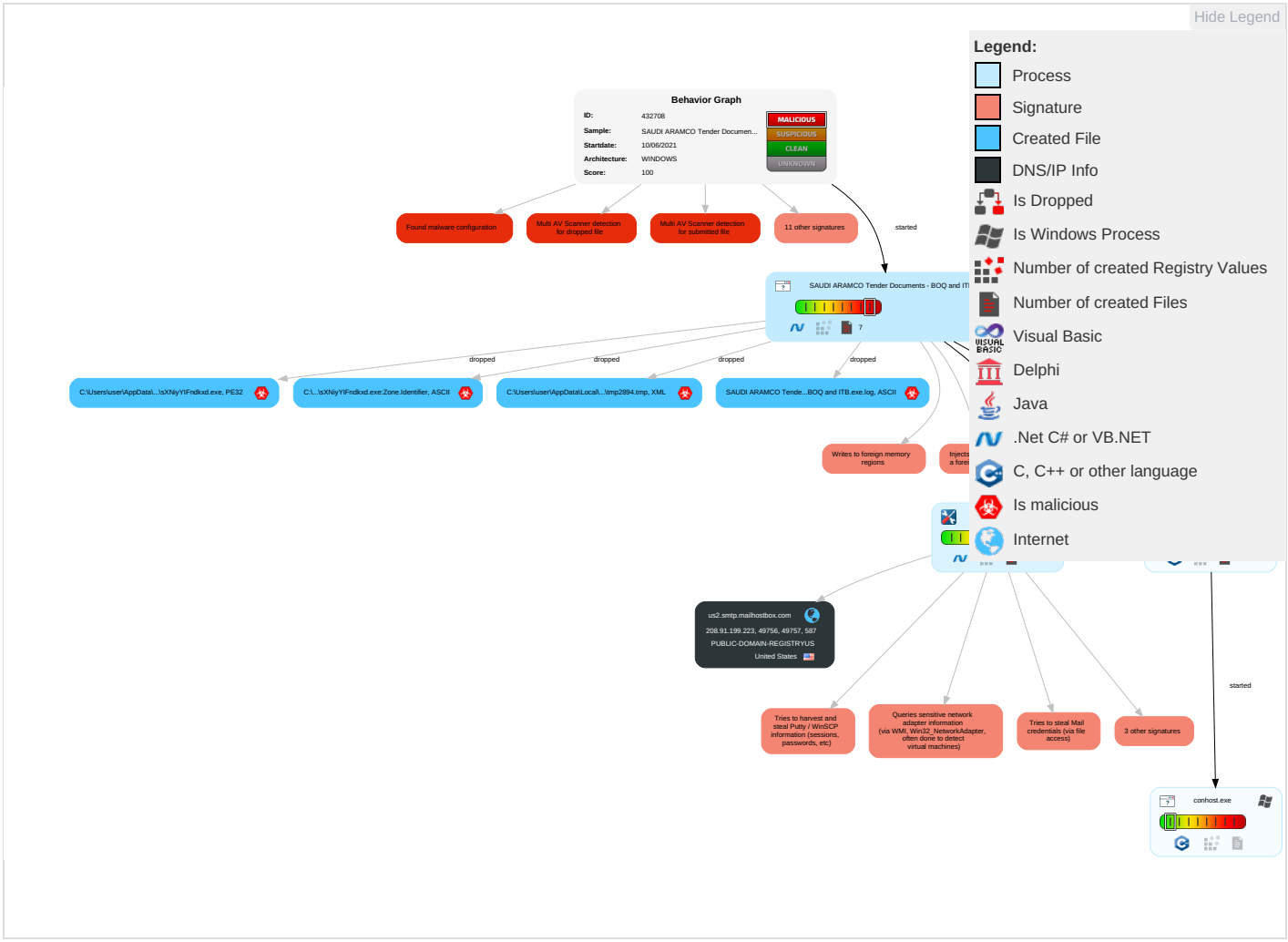
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 2 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 4	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

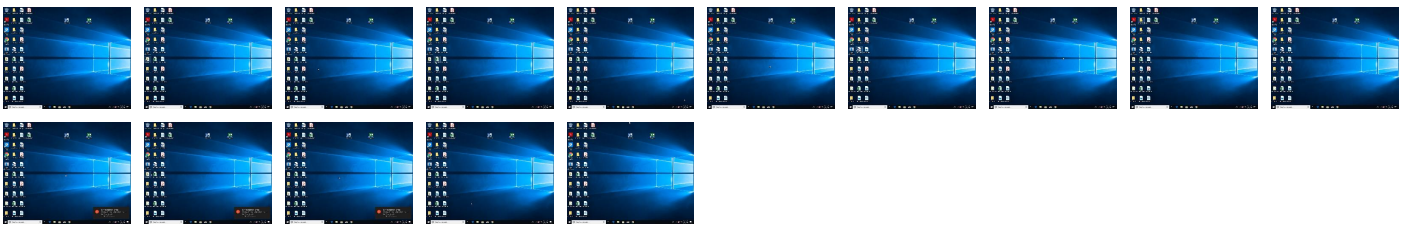
Behavior Graph



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
SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	30%	Virustotal		Browse
SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	
SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sXNiyYIFndkxd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sXNiyYIFndkxd.exe	15%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	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://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://Tw98FI5QiWYWE4R7ojW.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	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://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://xaqngD.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432708
Start date:	10.06.2021
Start time:	17:30:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SAUDI ARAMCO Tender Documents - BOQ and ITB.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:	21
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@6/5@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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

Simulations

Behavior and APIs

Time	Type	Description
17:31:18	API Interceptor	1x Sleep call for process: SAUDI ARAMCO Tender Documents - BOQ and ITB.exe modified
17:31:38	API Interceptor	670x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	
	order 4806125050.xlsx	Get hash	malicious	Browse	
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	
	FXDmHliz25.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	
	003BC09180600189.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Scr.Malcodegdn30.30554.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER_____.exe	Get hash	malicious	Browse	
	YR1eBxhF96.exe	Get hash	malicious	Browse	
	Quote SEQTE00311701.xlsx	Get hash	malicious	Browse	
	sqQyO37l3c.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	
	INVOICE FOR PAYMENT_pdf_____ _____.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	
	Txw9tCLc1Q.exe	Get hash	malicious	Browse	
	E8aAJC09lVhRGbK.exe	Get hash	malicious	Browse	
	payment confirmation copy.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Trojan.PackedNET.831.28325.exe	Get hash	malicious	Browse	• 208.91.199.225
	G8mumaTxk5kFdBG.exe	Get hash	malicious	Browse	• 208.91.198.143
	Trial order 20210609.exe	Get hash	malicious	Browse	• 208.91.199.224
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	• 208.91.199.223
	4It7P3KCyYHUWHU.exe	Get hash	malicious	Browse	• 208.91.199.225
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	Bestil 5039066002128.exe	Get hash	malicious	Browse	• 208.91.199.224
	COMPANY DOCUMENTS.exe	Get hash	malicious	Browse	• 208.91.199.225
	FXDmHliz25.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Trojan.MalPack.ADC.15816.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.174.212.247
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Order10 06 2021.doc	Get hash	malicious	Browse	• 162.215.241.145
	PO187439.exe	Get hash	malicious	Browse	• 119.18.54.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	Bank Swift.doc	Get hash	malicious	Browse	• 162.215.241.145
	SecuriteInfo.com.Trojan.PackedNET.831.28325.exe	Get hash	malicious	Browse	• 208.91.199.225
	Trial order 20210609.exe	Get hash	malicious	Browse	• 208.91.199.224
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	• 208.91.199.223
	4It7P3KCyYHUWHU.exe	Get hash	malicious	Browse	• 208.91.199.225
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	Bestil 5039066002128.exe	Get hash	malicious	Browse	• 208.91.199.224
	Doc2000120201.xls	Get hash	malicious	Browse	• 103.21.59.173

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe.log

Process:	C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe.log	
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2894.tmp	
Process:	C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.165150822696325
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3+Otn:cbha7JlNQV/rydbz9I3YODOLNdq3n
MD5:	3D4A4232313A8C77051BC8881B947A49
SHA1:	56E98C5408F3D45EC82B03C3CCF511C8A972AE49
SHA-256:	7124E726CC2893A43A14639936466452A4656D461D34F5C41EADA3F5B22E4EAE
SHA-512:	43A7C2FCD3B29B73986215E72BF6E68E62D6EA94D2693C7A990A89076352DCBFD71FBA96DEC0991D306153603EE513BDDDA8361C7D41280045AC2325C0F5FB
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\djtasvra.svm\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\sXNiyYIFndkxd.exe	
Process:	C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	979968
Entropy (8bit):	7.860191369488232
Encrypted:	false

C:\Users\user\AppData\Roaming\sXNiyYIFndkxd.exe	
SSDEEP:	12288:zMRIOXqxYM9iIfFKfffFZgK5tRevE7I/JUKg1PEGdvGM62zn1XuyvqwcgabMNLYE:YtDtRPI/Ff152z8iq9gVnNeBUdt
MD5:	D482D04BD4113F1F9F08E39BCA4A3F27
SHA1:	783F25F265C34681FFCA9E5C8AC5BEBECC71BBC6
SHA-256:	9973C00CF203198A16D3D897FA85D46896F04EA9D58B23917EAEA32A3DE4D5E4
SHA-512:	A5E65F1145AF4FDF8E0BD57602918F31EF80E2E9061BEDA08DEDB9E3CDDDF7A8C704FA968B9BF809AD53AD60B14796DB7590C71D5FEC12ED54BC3B5F1F93987
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\..`.....P.....f.... ... ....@.. .....`..... ..@.....O.... .....@..... ....H.....text...l.... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....H.....T..p.....<X.....0.....(!...(".....(.....o#....*.....($.....(%.....(&.....('.....((....*N..(. ...o....()....*&..(*....*.s+.....s,.....s-.....s.....s/.....*....0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*&..(5....* ...0..<.....~.....(6.....,lr...p.....(7...o8...s9.....~.....

C:\Users\user\AppData\Roaming\sXNiyYIFndkxd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.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
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.860191369488232
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:	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
File size:	979968
MD5:	d482d04bd4113f1f9f08e39bca4a3f27
SHA1:	783f25f265c34681ffca9e5c8ac5bebecc71bbc6
SHA256:	9973c00cf203198a16d3d897fa85d46896f04ea9d58b23917eaea32a3de4d5e4
SHA512:	a5e65f1145af4fdf8e0bd57602918f31ef80e2e9061beda08dedb9e3cdddf7a8c704fa968b9bf809ad53ad60b14796db7590c71d5fec12ed54bc3b5f1f939287
SSDEEP:	12288:zMRIOXqxYM9iIfFKfffFZgK5tRevE7I/JUKg1PEGdvGM62zn1XuyvqwcgabMNLYE:YtDtRPI/Ff152z8iq9gVnNeBUdt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\..`.....P.....f.... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f0766
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:	0x60C1CE5C [Thu Jun 10 08:33:32 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xee76c	0xee800	False	0.881842079403	data	7.86709142883	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf2000	0x680	0x800	False	0.34423828125	data	3.58292180879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 17:33:10.290950060 CEST	192.168.2.6	8.8.8.8	0xb231	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 17:33:15.963887930 CEST	192.168.2.6	8.8.8.8	0x3f46	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
Jun 10, 2021 17:33:10.355426073 CEST	8.8.8.8	192.168.2.6	0xb231	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:10.355426073 CEST	8.8.8.8	192.168.2.6	0xb231	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:10.355426073 CEST	8.8.8.8	192.168.2.6	0xb231	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:10.355426073 CEST	8.8.8.8	192.168.2.6	0xb231	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:16.025271893 CEST	8.8.8.8	192.168.2.6	0x3f46	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:16.025271893 CEST	8.8.8.8	192.168.2.6	0x3f46	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:16.025271893 CEST	8.8.8.8	192.168.2.6	0x3f46	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 10, 2021 17:33:16.025271893 CEST	8.8.8.8	192.168.2.6	0x3f46	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 10, 2021 17:33:10.976522923 CEST	587	49756	208.91.199.223	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 10, 2021 17:33:10.976864100 CEST	49756	587	192.168.2.6	208.91.199.223	EHLO 651689
Jun 10, 2021 17:33:11.146632910 CEST	587	49756	208.91.199.223	192.168.2.6	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
Jun 10, 2021 17:33:11.146975994 CEST	49756	587	192.168.2.6	208.91.199.223	STARTTLS
Jun 10, 2021 17:33:11.316747904 CEST	587	49756	208.91.199.223	192.168.2.6	220 2.0.0 Ready to start TLS
Jun 10, 2021 17:33:16.371243954 CEST	587	49757	208.91.199.223	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 10, 2021 17:33:16.371661901 CEST	49757	587	192.168.2.6	208.91.199.223	EHLO 651689
Jun 10, 2021 17:33:16.541405916 CEST	587	49757	208.91.199.223	192.168.2.6	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
Jun 10, 2021 17:33:16.541645050 CEST	49757	587	192.168.2.6	208.91.199.223	STARTTLS
Jun 10, 2021 17:33:16.711458921 CEST	587	49757	208.91.199.223	192.168.2.6	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SAUDI ARAMCO Tender Documents - BOQ and ITB.exe PID: 6556 Parent PID: 6088

General

Start time:	17:31:09
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SAUDI ARAMCO Tender Documents - BOQ and ITB.exe'
Imagebase:	0xde0000
File size:	979968 bytes
MD5 hash:	D482D04BD4113F1F9F08E39BCA4A3F27
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: 00000001.00000002.370688660.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.370688660.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.369670905.00000000031E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6824 Parent PID: 6556

General

Start time:	17:31:22
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sXNiyYIFndkxd' /XML 'C:\Users\user\AppData\Local\Temp\tmp2894.tmp'
Imagebase:	0xb90000
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 Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6836 Parent PID: 6824

General

Start time:	17:31:25
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: RegSvcs.exe PID: 6904 Parent PID: 6556

General

Start time:	17:31:27
Start date:	10/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xa10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.367493021.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.367493021.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.600007572.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.600007572.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.602052323.0000000002CC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.602052323.0000000002CC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis