ID: 510693
Sample Name: SOA pdf.exe
Cookbook: default.jbs
Time: 05:02:03
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

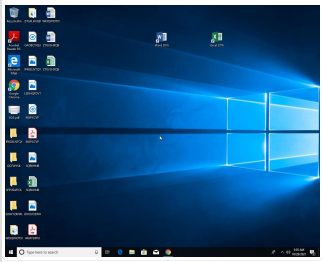
Windows Analysis Report SOA pdf.exe

Overview

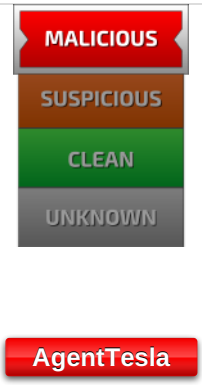
General Information

Sample Name:	SOA pdf.exe
Analysis ID:	510693
MD5:	a4777dd931c6b1..
SHA1:	bac3170333a0c8..
SHA256:	59bb800d65d8c2..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



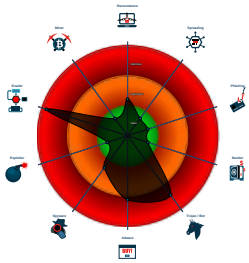
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Hides that the sample has been dow…
- Queries sensitive network adapter in…
- Uses schtasks.exe or at.exe to add …

Classification



Process Tree

- **System is w10x64**
- SOA pdf.exe (PID: 5552 cmdline: 'C:\Users\user\Desktop\SOA pdf.exe' MD5: A4777DD931C6B16901478A2C1888DC27)
  - schtasks.exe (PID: 6392 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF7F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SOA pdf.exe (PID: 6484 cmdline: {path} MD5: A4777DD931C6B16901478A2C1888DC27)
- hgvQCmQ.exe (PID: 240 cmdline: 'C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe' MD5: A4777DD931C6B16901478A2C1888DC27)
  - schtasks.exe (PID: 6344 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmp9A6B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - hgvQCmQ.exe (PID: 5344 cmdline: {path} MD5: A4777DD931C6B16901478A2C1888DC27)
- hgvQCmQ.exe (PID: 396 cmdline: 'C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe' MD5: A4777DD931C6B16901478A2C1888DC27)
  - schtasks.exe (PID: 400 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmpBCF7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - hgvQCmQ.exe (PID: 5868 cmdline: {path} MD5: A4777DD931C6B16901478A2C1888DC27)
  - hgvQCmQ.exe (PID: 6620 cmdline: {path} MD5: A4777DD931C6B16901478A2C1888DC27)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "markhung@jingtai.com.vn",
  "Password": "truongtuyen2209",
  "Host": "Mail.jingtai.com.vn"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000000.553026976.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001A.00000000.553026976.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001A.00000002.629021312.0000000002B11000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001A.00000002.629021312.0000000002B11000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000012.00000000.523738351.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SOA pdf.exe.3f5dab8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.SOA pdf.exe.3f5dab8.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.SOA pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.SOA pdf.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
26.0.hgvQCmQ.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 49 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

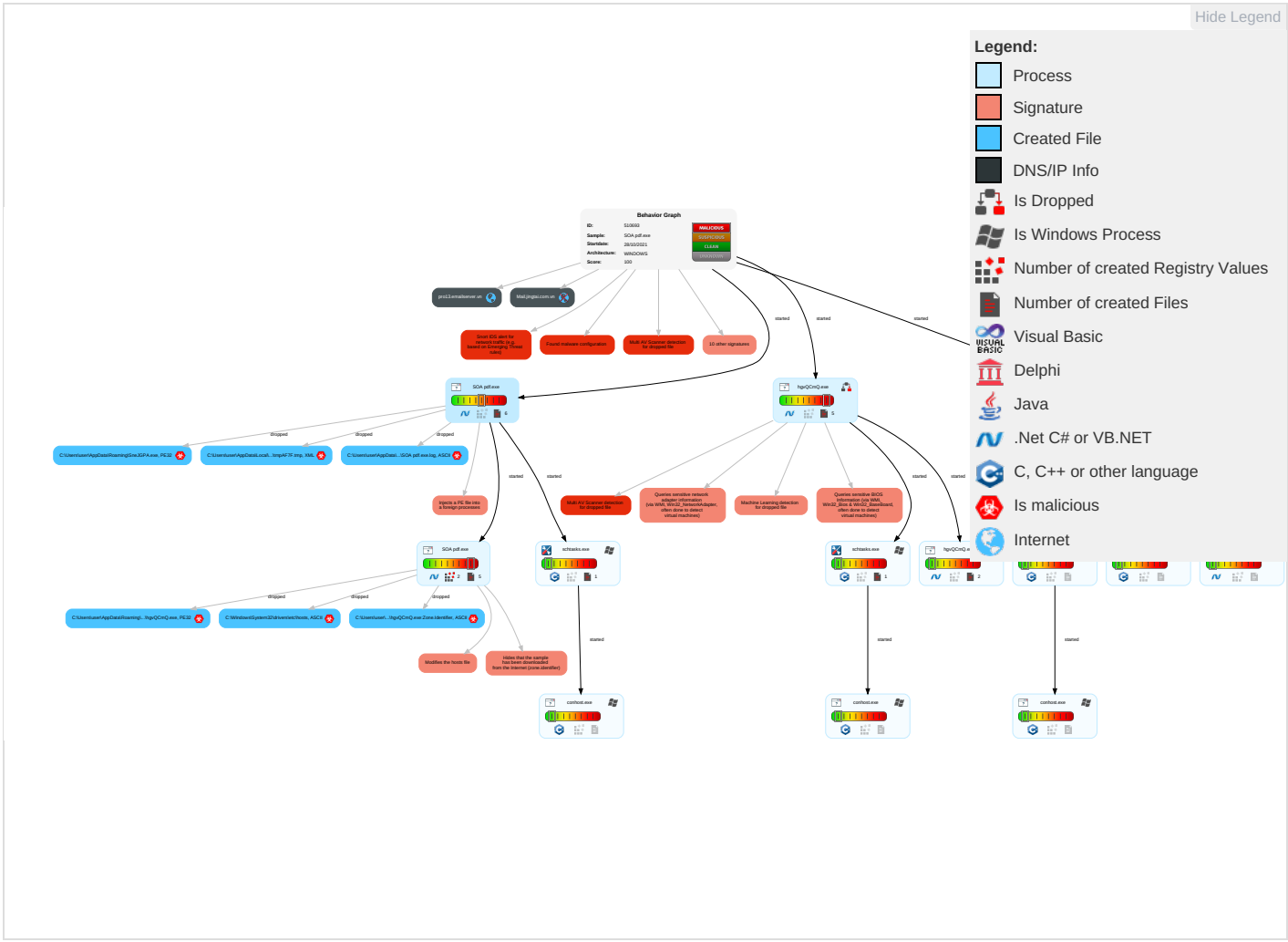
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	File and Directory Permissions Modification 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Security Account Manager	System Information Discovery 1 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Security Software Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Virtualization/Sandbox Evasion 1 3 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	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

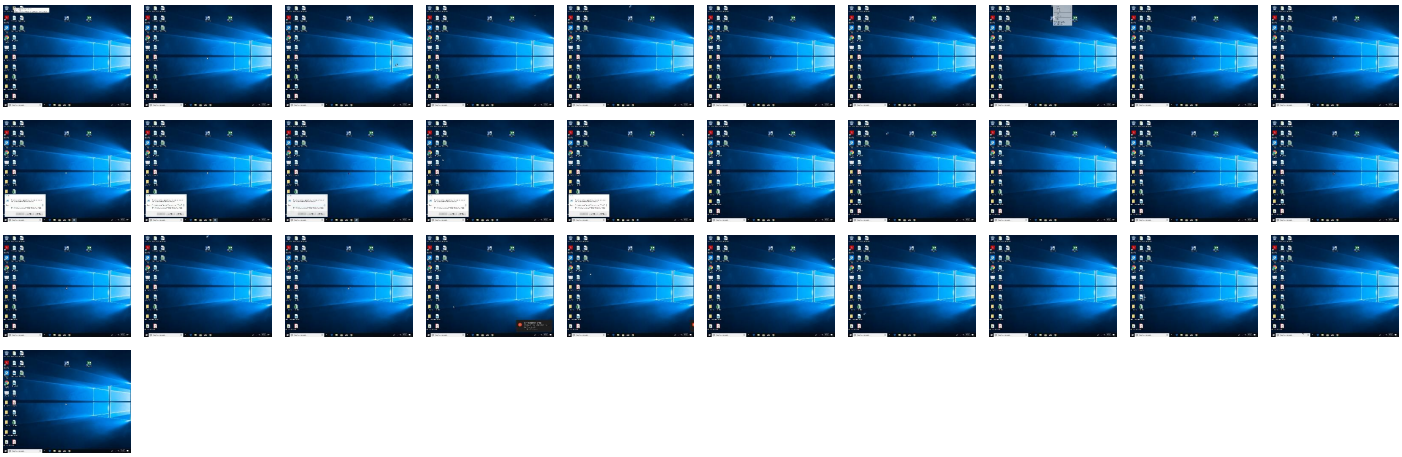
Behavior Graph



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
SOA pdf.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SOA pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\SneJGPA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\SneJGPA.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.0.hgvQCmQ.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.hgvQCmQ.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SOA pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SOA pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.0.hgvQCmQ.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SOA pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.hgvQCmQ.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.hgvQCmQ.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SOA pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.hgvQCmQ.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.0.hgvQCmQ.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.SOA pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.hgvQCmQ.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.0.hgvQCmQ.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.2.hgvQCmQ.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.0.hgvQCmQ.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.0.hgvQCmQ.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.SOA pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.urwpp.deFy	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/~P	0%	Avira URL Cloud	safe	
http://www.urwpp.deras	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/soft	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comI	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comsiva=P	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://bWFhc41K6WqcMA6O.net	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comlicd	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s/r	0%	Avira URL Cloud	safe	
http://www.urwpp.de3	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/uP	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com4P	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fonts.comy	0%	Avira URL Cloud	safe	
http://bWFhc41K6WqcMA6O.nett	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comn	0%	Avira URL Cloud	safe	
http://www.fontbureau.com~P	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsZP)	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.tiro.comslnt	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://Mail.jingtai.com.vn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/=P	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv4	0%	Avira URL Cloud	safe	
http://rlhupJ.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/=P	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://tempuri.org/DatabaseDataSet.xsd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/QP	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/~P	0%	Avira URL Cloud	safe	
http://www.fonts.com9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitud	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pro13.emailserver.vn	103.15.48.233	true	false		high
Mail.jingtai.com.vn	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510693
Start date:	28.10.2021
Start time:	05:02:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOA pdf.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:	30
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.adwa.evad.winEXE@20/9@2/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.8%) • Quality average: 41.7% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 93% • 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
05:03:12	API Interceptor	604x Sleep call for process: SOA pdf.exe modified
05:04:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run hgvQCmQ C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
05:04:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run hgvQCmQ C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
05:04:13	API Interceptor	91x Sleep call for process: hgvQCmQ.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SOA pdf.exe.log	
Process:	C:\Users\user\Desktop\SOA pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hgvQCmQ.exe.log	
Process:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp9A6B.tmp	
Process:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1652
Entropy (8bit):	5.15524173262602
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Btn:cbha7JlNQV/rydbz9I3YODOLNdq39
MD5:	547A57D0C6F33FFF8CEE44D3E39D8DA7
SHA1:	ABFF0A1195CC7990001D97F2D1FE8CC61FE76103
SHA-256:	7D3194E43F24ECB3ACD7178BCE03DC6950DADB21C354880E482BD5CADBAD4EF4
SHA-512:	DE3E452A0CC228F3685A305BF71F0F0BB4792CB07F5EA1B3905994BB9EB23C57B7E83966751668C273FEC57799BBA98929B21256EFEF442C94EAFACAFB90DC90
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp9A6B.tmp	
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\Local\Temp\tmpAF7F.tmp	
Process:	C:\Users\user\Desktop\SOA pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1652
Entropy (8bit):	5.15524173262602
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Btn:cbha7JlNQV/rydbz9I3YODOLNdq39
MD5:	547A57D0C6F33FFF8CEE44D3E39D8DA7
SHA1:	ABFF0A1195CC7990001D97F2D1FE8CC61FE76103
SHA-256:	7D3194E43F24ECB3ACD7178BCE03DC6950DADB21C354880E482BD5CADBAD4EF4
SHA-512:	DE3E452A0CC228F3685A305BF71F0F0BB4792CB07F5EA1B3905994BB9EB23C57B7E83966751668C273FEC57799BBA98929B21256EFEF442C94EAFACAFB90DC90
Malicious:	**true**
Reputation:	unknown
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\Local\Temp\tmpBCF7.tmp	
Process:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1652
Entropy (8bit):	5.15524173262602
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Btn:cbha7JlNQV/rydbz9I3YODOLNdq39
MD5:	547A57D0C6F33FFF8CEE44D3E39D8DA7
SHA1:	ABFF0A1195CC7990001D97F2D1FE8CC61FE76103
SHA-256:	7D3194E43F24ECB3ACD7178BCE03DC6950DADB21C354880E482BD5CADBAD4EF4
SHA-512:	DE3E452A0CC228F3685A305BF71F0F0BB4792CB07F5EA1B3905994BB9EB23C57B7E83966751668C273FEC57799BBA98929B21256EFEF442C94EAFACAFB90DC90
Malicious:	false
Reputation:	unknown
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\SneJGPA.exe	
Process:	C:\Users\user\Desktop\SOA pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1221632
Entropy (8bit):	7.168491804997157
Encrypted:	false
SSDEEP:	24576:WPiYAeqKpRlMSN1Kq1I2LewqJptTV01LXh2VYJUEKlCW:WjjtewGp2LeYJUEKlCW
MD5:	A4777DD931C6B16901478A2C1888DC27
SHA1:	BAC3170333A0C8DA9E5E1827D065D78B683FBB53
SHA-256:	59BB800D65D8C2670FE30E036B9D9D7E81AB3A863DF72E1F00E27C709DDCF1E8
SHA-512:	616FC84120CDAAC5D78087CE4DF25EF6CCB6AF693F74FD194242BECE4DE53D87ECD25B0E6281495D3683AE646190C8FC5BBFF60FFE9B2F6E3466FDF156636D0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%

C:\Users\user\AppData\Roaming\SneJGPA.exe

Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ya.....P..Z...H.....y... .....@.. ....@.....x..O.....E..... ....H.....text...4Y... ...Z..... ..`.rsrc....E.....F...\.....@..@.rel oc.....@..B.....y.....H.....`..$.....[.....0.....*....0..P.....(,...(.... ^>.* 1'q.a%..^E.....+... /J|.Z S...a+.....(.....(.....* .....?@.....0..*.....(-.....(.....(/.....(.....(0....*...0..W..... .*.. .K@.a%..^E....!...1.....+/.(....o....(1.... >.$.Z ....a+... f.>QZ ...a+.*..0.....(2...*..0.....o3...*.0..... (4...*.0.....(5....*....0..3.....s6.....s7.....s8.....s9

C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe

Process:	C:\Users\user\Desktop\SOA pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1221632
Entropy (8bit):	7.168491804997157
Encrypted:	false
SSDEEP:	24576:WPiYAeqKpRlMSN1Kq1I2LewqJptTV01LXh2VYJUEKlCW:WjjtewGp2LeYJUEKlCW
MD5:	A4777DD931C6B16901478A2C1888DC27
SHA1:	BAC3170333A0C8DA9E5E1827D065D78B683FBB53
SHA-256:	59BB800D65D8C2670FE30E036B9D9D7E81AB3A863DF72E1F00E27C709DDCF1E8
SHA-512:	616FC84120CDAAC5D78087CE4DF25EF6CCB6AF693F74FD194242BECE4DE53D87ECD25B0E6281495D3683AE646190C8FC5BBFF60FFE9B2F6E3466FDF156636D 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ya.....P..Z...H.....y... .....@.. ....@.....x..O.....E..... ....H.....text...4Y... ...Z..... ..`.rsrc....E.....F...\.....@..@.rel oc.....@..B.....y.....H.....`..$.....[.....0.....*....0..P.....(,...(.... ^>.* 1'q.a%..^E.....+... /J|.Z S...a+.....(.....(.....* .....?@.....0..*.....(-.....(.....(/.....(.....(0....*...0..W..... .*.. .K@.a%..^E....!...1.....+/.(....o....(1.... >.$.Z ....a+... f.>QZ ...a+.*..0.....(2...*..0.....o3...*.0..... (4...*.0.....(5....*....0..3.....s6.....s7.....s8.....s9

C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SOA pdf.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:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\SOA pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	unknown
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.168491804997157
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SOA pdf.exe
File size:	1221632
MD5:	a4777dd931c6b16901478a2c1888dc27
SHA1:	bac3170333a0c8da9e5e1827d065d78b683fbb53
SHA256:	59bb800d65d8c2670fe30e036b9d9d7e81ab3a863df72e1f00e27c709ddcf1e8
SHA512:	616fc84120cdaac5d78087ce4df25ef6ccb6af693f74fd194242bece4de53d87ecd25b0e6281495d3683ae646190c8fc5bbff60ffe9b2f6e3466fdf156636d40
SSDEEP:	24576:WPiYAeqKpRlMSN1Kq1I2LewqJptTV01LXh2VYJUEKlCW:WjjtewGp2LeYJUEKlCW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ya.....P..Z...H.....y... .....@.. .....@.....

File Icon

Icon Hash:	04fcf0b0d4a6e46c

Static PE Info

General

Entrypoint:	0x4f792e
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:	0x6179E8D5 [Thu Oct 28 00:03:33 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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf5934	0xf5a00	False	0.630883229962	data	7.20610912902	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf8000	0x345c8	0x34600	False	0.444990863663	data	6.26279856475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-05:05:14.576080	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49770	587	192.168.2.6	103.15.48.233

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 05:05:11.860570908 CEST	192.168.2.6	8.8.8.8	0x9b41	Standard query (0)	Mail.jingtai.com.vn	A (IP address)	IN (0x0001)
Oct 28, 2021 05:05:12.196542025 CEST	192.168.2.6	8.8.8.8	0x5f60	Standard query (0)	Mail.jingtai.com.vn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 05:05:12.192008018 CEST	8.8.8.8	192.168.2.6	0x9b41	No error (0)	Mail.jingtai.com.vn	pro13.emailserver.vn		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 05:05:12.192008018 CEST	8.8.8.8	192.168.2.6	0x9b41	No error (0)	pro13.emailserver.vn		103.15.48.233	A (IP address)	IN (0x0001)
Oct 28, 2021 05:05:12.535784006 CEST	8.8.8.8	192.168.2.6	0x5f60	No error (0)	Mail.jingtai.com.vn	pro13.emailserver.vn		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 05:05:12.535784006 CEST	8.8.8.8	192.168.2.6	0x5f60	No error (0)	pro13.emailserver.vn		103.15.48.233	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SOA pdf.exe PID: 5552 Parent PID: 340

General

Start time:	05:03:02
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\SOA pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SOA pdf.exe'
Imagebase:	0x890000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
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: 00000001.00000002.401458000.00000000040A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.401458000.00000000040A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.400803068.0000000003E00000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.400803068.0000000003E00000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6392 Parent PID: 5552

General

Start time:	05:03:18
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF7F.tmp'
Imagebase:	0x1030000
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: 6448 Parent PID: 6392

General

Start time:	05:03:20
Start date:	28/10/2021
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: SOA pdf.exe PID: 6484 Parent PID: 5552

General

Start time:	05:03:21
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\SOA pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x490000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
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: 00000004.00000002.622548824.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.622548824.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.392455880.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.392455880.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.394004490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.394004490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.393041501.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.393041501.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.630306300.0000000002871000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.630306300.0000000002871000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.393509699.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.393509699.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: hgvQCmQ.exe PID: 240 Parent PID: 3440

General

Start time:	05:04:08
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe'
Imagebase:	0x250000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.531462689.0000000002A6E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.532515883.0000000003850000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.532515883.0000000003850000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: hgvQCmQ.exe PID: 396 Parent PID: 3440

General

Start time:	05:04:17
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe'
Imagebase:	0x8a0000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
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: 0000000E.00000002.574319167.0000000003EA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.574319167.0000000003EA0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6344 Parent PID: 240

General

Start time:	05:04:18
Start date:	28/10/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmp9A6B.tmp'
Imagebase:	0x1030000
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: 1636 Parent PID: 6344

General

Start time:	05:04:19
Start date:	28/10/2021
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: hgvQCmQ.exe PID: 5344 Parent PID: 240

General

Start time:	05:04:20
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4a0000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
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: 00000012.00000000.523738351.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.523738351.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.521046677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.521046677.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.522087904.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.522087904.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.570961957.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.570961957.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.574206873.0000000002941000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.574206873.0000000002941000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000000.519772323.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000000.519772323.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: schtasks.exe PID: 400 Parent PID: 396

General

Start time:	05:04:28
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SneJGPA' /XML 'C:\Users\user\AppData\Local\Temp\tmpBCF7.tmp'
Imagebase:	0x1030000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5648 Parent PID: 400

General

Start time:	05:04:29
Start date:	28/10/2021
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: hgvQCmQ.exe PID: 5868 Parent PID: 396

General

Start time:	05:04:30
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x180000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: hgvQCmQ.exe PID: 6620 Parent PID: 396

General

Start time:	05:04:34
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\hgvQCmQ\hgvQCmQ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6d0000
File size:	1221632 bytes
MD5 hash:	A4777DD931C6B16901478A2C1888DC27
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: 0000001A.00000000.553026976.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.553026976.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.629021312.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.629021312.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.559051654.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.559051654.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.622610702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000002.622610702.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.556463107.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.556463107.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000000.554521283.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000000.554521283.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis