

JoeSandbox Cloud BASIC



ID: 433197

Sample Name:

SOA_31052021.exe

Cookbook: default.jbs

Time: 12:42:21

Date: 11/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report SOA_31052021.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Compliance:	5
Networking:	5
Spam, unwanted Advertisements and Ransom Demands:	5
System Summary:	5
Data Obfuscation:	5
Boot Survival:	6
Hooking and other Techniques for Hiding and Protection:	6
Malware Analysis System Evasion:	6
HIPS / PFW / Operating System Protection Evasion:	6
Lowering of HIPS / PFW / Operating System Security Settings:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	14
General	14
File Icon	15
Static PE Info	15
General	15
Entrypoint Preview	15
Data Directories	15
Sections	15
Resources	15
Imports	15
Version Infos	15
Network Behavior	16
Code Manipulations	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: SOA_31052021.exe PID: 6648 Parent PID: 6020	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Written	16
File Read	16

Analysis Process: schtasks.exe PID: 6584 Parent PID: 6648	16
General	16
File Activities	17
File Read	17
Analysis Process: conhost.exe PID: 6596 Parent PID: 6584	17
General	17
Analysis Process: SOA_31052021.exe PID: 6616 Parent PID: 6648	17
General	17
File Activities	18
File Created	18
File Deleted	18
File Written	18
File Read	18
Registry Activities	18
Key Value Created	18
Analysis Process: kprUEGC.exe PID: 1320 Parent PID: 3440	18
General	18
File Activities	18
File Created	18
File Written	18
File Read	19
Analysis Process: kprUEGC.exe PID: 2924 Parent PID: 3440	19
General	19
File Activities	19
File Created	19
File Written	19
File Read	19
Disassembly	19
Code Analysis	19

Analysis Report SOA_31052021.exe

Overview

General Information

Sample Name:

SOA_31052021.exe

Analysis ID:

433197

MD5:

9a7deb4c1dc1dff..

SHA1:

29752ad3e3e436..

SHA256:

53f410cfcb4ba20..

Tags:

AgentTesla

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

Score:

100

Range:

0 - 100

Whitelisted:

false

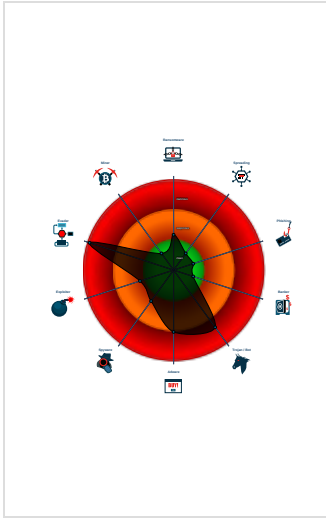
Confidence:

100%

Signatures

- Detected unpacking (changes PE se...
- Detected unpacking (overwrites its o...
- 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...
- Hides that the sample has been dow...
- Injects a PE file into a foreign proce...

Classification



Process Tree

System is w10x64

SOA_31052021.exe

(PID: 6648 cmdline: 'C:\Users\user\Desktop\SOA_31052021.exe' MD5: 9A7DEB4C1DC1DFF1BB42585200668BAE)

schtasks.exe

(PID: 6584 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lakYFibIJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp8347.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe

(PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

SOA_31052021.exe

(PID: 6616 cmdline: {path} MD5: 9A7DEB4C1DC1DFF1BB42585200668BAE)

kprUEGC.exe

(PID: 1320 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 9A7DEB4C1DC1DFF1BB42585200668BAE)

kprUEGC.exe

(PID: 2924 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 9A7DEB4C1DC1DFF1BB42585200668BAE)

cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "importdox_jberedo@afcihil.com.phr35eCaRt4mail.afcihil.com.ph"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.593685889.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.593685889.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000012.00000002.602545420.000000000445 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.602545420.000000000445 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Page 4 of 19

Source	Rule	Description	Author	Strings
00000000.00000002.425655543.000000000379 7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.SOA_31052021.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.SOA_31052021.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
12.0.SOA_31052021.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.0.SOA_31052021.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
19.2.kprUEGC.exe.4131f68.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

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

Compliance:



Detected unpacking (overwrites its own PE header)

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

Data Obfuscation:



Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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

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

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 delay execution (extensive OutputDebugStringW loop)

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

Injects a PE file into a foreign processes

Modifies the hosts file

Modifies the hosts file

Yara detected AgentTesla

Yara detected AgentTesla

Yara detected AgentTesla

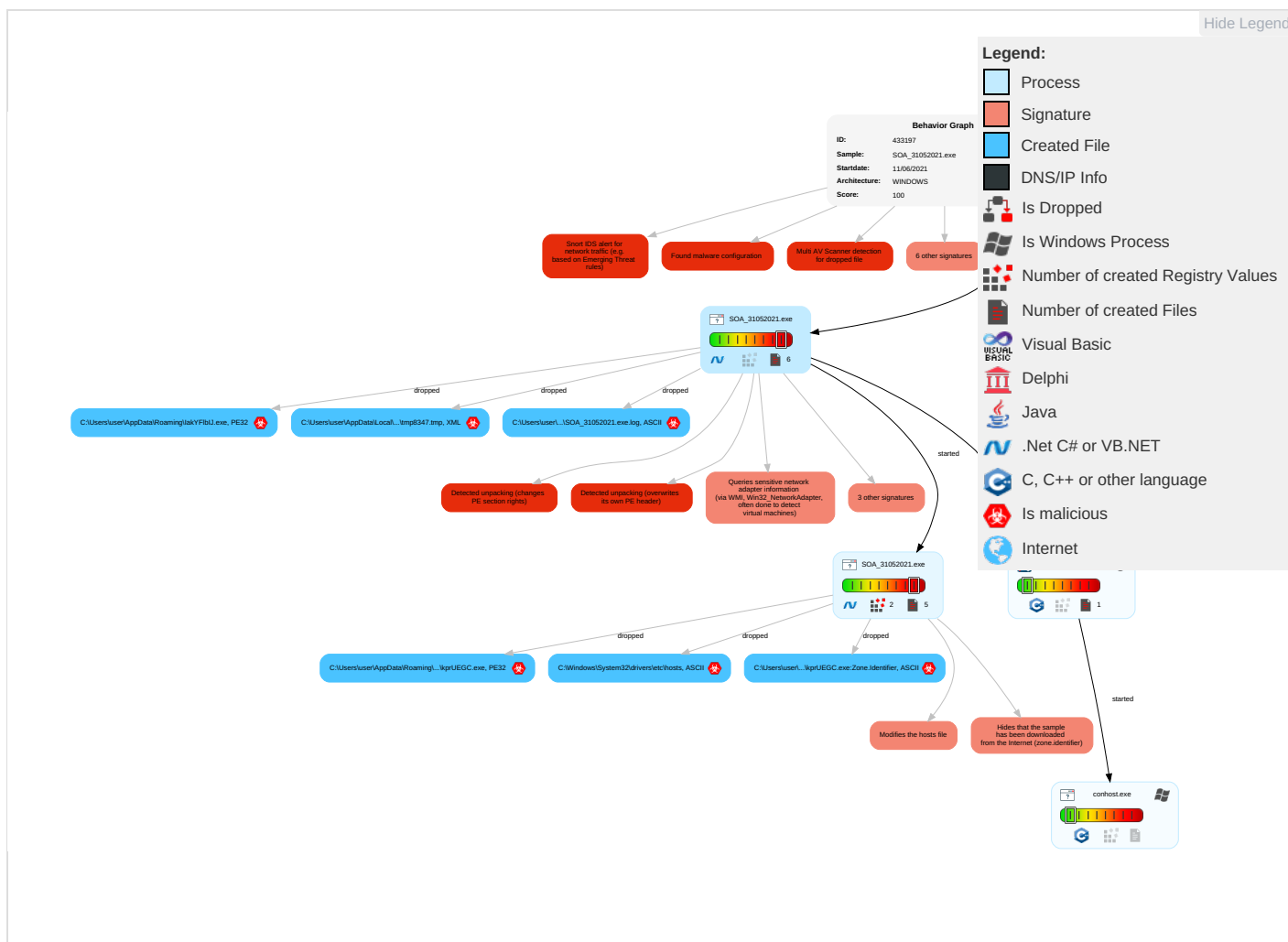
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 3 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	File and Directory Permissions Modification 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2 5 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Account Discovery 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	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory 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	Obfuscated Files or Information 3	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

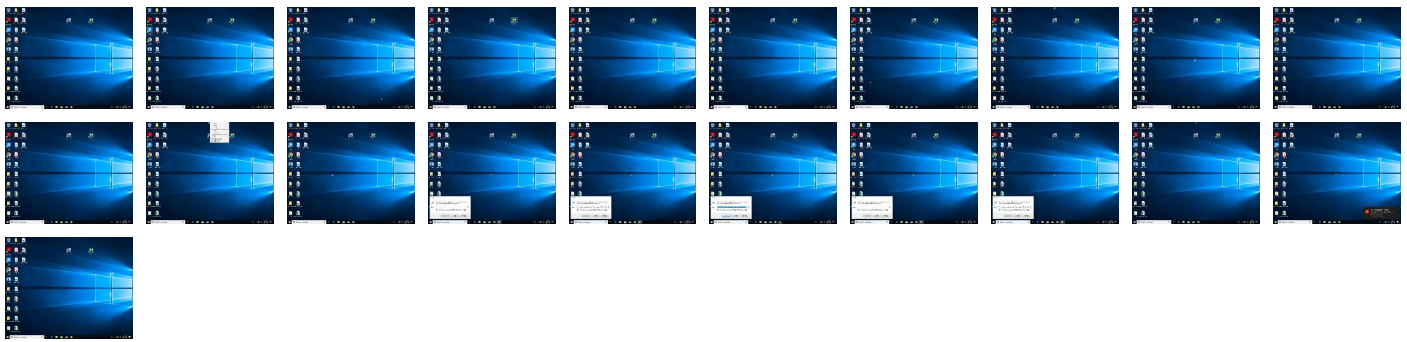
Behavior Graph



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_31052021.exe	36%	Virustotal		Browse
SOA_31052021.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NakyFIbIJ.exe	36%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\IakYFblJ.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	36%	Virustotal		Browse
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.SOA_31052021.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.2.SOA_31052021.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.SOA_31052021.exe.310000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
18.2.kprUEGC.exe.f00000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
19.2.kprUEGC.exe.b80000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		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://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://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://HqokBq.com	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatpeworks.com	0%	URL Reputation	safe	
http://www.sajatpeworks.com	0%	URL Reputation	safe	
http://www.sajatpeworks.com	0%	URL Reputation	safe	
http://www.sajatpeworks.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.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.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	

Source	Detection	Scanner	Label	Link
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://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.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.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://www.galapagosdesign.com/DPlease	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://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://www.sandoll.co.kr	0%	URL Reputation	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.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.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://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	
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

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433197
Start date:	11.06.2021
Start time:	12:42:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOA_31052021.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:	24
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@8/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 1%) • Quality average: 39% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 94% • 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
12:44:09	API Interceptor	440x Sleep call for process: SOA_31052021.exe modified
12:44:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
12:44:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

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\luser\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SOA_31052021.exe.log	
Process:	C:\Users\luser\Desktop\SOA_31052021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\1d8480152e0da9a60ad49c6d16a3b6d\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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

C:\Users\luser\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	
Process:	C:\Users\luser\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\1d8480152e0da9a60ad49c6d16a3b6d\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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

C:\Users\luser\AppData\Local\Temp\1tmp8347.tmp	
Process:	C:\Users\luser\Desktop\SOA_31052021.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1654
Entropy (8bit):	5.161713715862094
Encrypted:	false

C:\Users\user1\AppData\Local\Temp\tmp8347.tmp	
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rIMhEMjNpGwjplgUYODOLD9RJh7h8gKB3ytn:cbha7JINQV/rydbz9I3YODOLNdq3+
MD5:	B52B45472DE92600D506F57A2681D00E
SHA1:	BFF32A7554139796A962ADFFEEAEB07A7E36B73D
SHA-256:	4FD5097F42F74FF6FCC01416504976F7B36626791A134A7ED0EDC327C451C642
SHA-512:	FD396E3EECF5D75481B316BA2BE3EAB2EF6BE8A6F9DF066EA4C50F316AA2125B38E27CC7B14AD81B619C1712B1E6F0B993FF32E0A43F08B1C61A89C9FB54F0DF
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\user1\AppData\Local\Temp\tmpA2E0.tmp	
Process:	C:\Users\user1\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1654
Entropy (8bit):	5.161713715862094
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rIMhEMjNpGwjplgUYODOLD9RJh7h8gKB3ytn:cbha7JINQV/rydbz9I3YODOLNdq3+
MD5:	B52B45472DE92600D506F57A2681D00E
SHA1:	BFF32A7554139796A962ADFFEEAEB07A7E36B73D
SHA-256:	4FD5097F42F74FF6FCC01416504976F7B36626791A134A7ED0EDC327C451C642
SHA-512:	FD396E3EECF5D75481B316BA2BE3EAB2EF6BE8A6F9DF066EA4C50F316AA2125B38E27CC7B14AD81B619C1712B1E6F0B993FF32E0A43F08B1C61A89C9FB54F0DF
Malicious:	false
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\user1\AppData\Roaming\lakYFlibJ.exe	
Process:	C:\Users\user1\Desktop\SOA_31052021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	939520
Entropy (8bit):	7.084415206568188
Encrypted:	false
SSDEEP:	12288:IZbocnFWNlaY8ziWDM3xYiL/gF/5zB3/pohoLhH3qxMOS7AKCgPK3AJfZCbXG/0g:ibosaD3M3xYFF/r/pvV3qxMHL
MD5:	9A7DEB4C1DC1DFF1BB42585200668BAE
SHA1:	29752AD3E3E4369A93A11F15855B9BC06B6CA6D1
SHA-256:	53F410CFEB4BA2090CBB4D494E2752E5DB040DD66060562917B4EC5198B6BD28
SHA-512:	9C4BDA4BCD44BFF492CA4CF6AF1EAD5AA249C11BF2B0FD95D98C77666B18D3FA18D9234FBC4D4E1A0F1180D02DE04F8148D79270105D260494DE6228B166FC8
Malicious:	true
Antivirus:	- Antivirus: Virustotal, Detection: 36%, Browse - Antivirus: ReversingLabs, Detection: 69%
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....PE..L...o.`.....0..@.....N_...`...@.. ..@.....^..S_.....H.....text..T?.....@......rsrc.....B.....@..@.rel oc.....T.....@..B.....0_.....H.....8.....r.....8.....0.....(.....(*..0..2.....r...p...r...p(.....-K ... W./a%...^E.....f...8.....8..... q.q.+..... 0.y.+r...p(..... }5.Z i..Va+..r...p(..... ^..%+. .C2.%&. ...Za8f.....(.....rC..p(..... %9 %+. .U%&. ..AVZa83.....s.....(.....%.....(..... 4...8..... 1..y%+. W.5P%&. ..Za8...*.0.....(0..*.0..0.....u..... .[. ..gba%...

C:\Users\user1\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user1\Desktop\SOA_31052021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	939520
Entropy (8bit):	7.084415206568188
Encrypted:	false

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe		 
SSDEEP:	12288:iZboenfWNlaY8ziWDM3xYiL/gF/5zB3/pohoLhH3qxMOS7AKCgPK3AJfZCbXG/0g:ibosaD3M3xYFF/r/pvV3qxMHL	
MD5:	9A7DEB4C1DC1DFF1BB42585200668BAE	
SHA1:	29752AD3E3E4369A93A11F15855B9BC06B6CA6D1	
SHA-256:	53F410CFEB4BA2090CBB4D494E2752E5DB040DD66060562917B4EC5198B6BD28	
SHA-512:	9C4BDA4BCD44BFF492CA4CF6AF1EAD5AA249C11BF2B0FD95D98C77666B18D3FA18D9234FBC4D4E1A0F1180D02DE04F8148D79270105D260494DE6228B166F08	
Malicious:	true	
Antivirus:	- Antivirus: Virustotal, Detection: 36%, Browse - Antivirus: ReversingLabs, Detection: 69%	
Reputation:	low	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......PE..L...o.`.....0..@.....N_...`....@.. ..@.....^..S...`.....H.....text..T?... ..@.....`..rsrc.....B.....@..@.rel oc.....T.....@..B.....0_.....H.....8.....f.....8.....0.....(.....*.0..2.....f...p.....p.....-K ... W./a%...^E.....f...8.....8....{.... q.q.+..{.... 0.y.+..r...p.....}5.Z i..Va+..f...p.....{..... ^..%+. .C2.%&...Za8f.....{.....rC..p....., .9 %+. .U%&...AVZa83.....S.....{....{.... 4..8....., 1..y%+. W.5P%&...Za8*...0.....(0..*.0..0.....u..... [. .gba%...	

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier		
Process:	C:\Users\user\Desktop\SOA_31052021.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]....Zoneld=0	

C:\Windows\System32\drivers\etc\hosts		
Process:	C:\Users\user\Desktop\SOA_31052021.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	modified	
Size (bytes):	11	
Entropy (8bit):	2.663532754804255	
Encrypted:	false	
SSDEEP:	3:iLE:iLE	
MD5:	B24D295C1F84ECBFB566103374FB91C5	
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A	
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4	
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA	
Malicious:	true	
Reputation:	high, very likely benign file	
Preview:	..127.0.0.1	

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.084415206568188
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_31052021.exe

General	
File size:	939520
MD5:	9a7deb4c1dc1dff1bb42585200668bae
SHA1:	29752ad3e3e4369a93a11f15855b9bc06b6ca6d1
SHA256:	53f410cfcb4ba2090cbb4d494e2752e5db040dd66060562917b4ec5198b6bd28
SHA512:	9c4bda4bcd44bff492ca4cf6af1ead5aa249c11bf2b0fd95d98c77666b18d3fa18d9234fbc4d4e1a0f1180d02de04f8148d79270105d260494de6228b166f0c8
SSDEEP:	12288:lZbocnfWNlaY8ziWDM3xYiL/gF/5zB3/pohoLhH3qxMOs7AKCgPK3AJfZCbXG/Qg:ibosaD3M3xYFF/r/pvV3qxMHL
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE..L.... o`.....0..@.....N_...`.....@.....@.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x4e5f4e
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:	0x60C16FBA [Thu Jun 10 01:49:46 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	0xe3f54	0xe4000	False	0.665448105126	data	7.0883461968	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x10f8	0x1200	False	0.377170138889	data	4.90664012555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: SOA_31052021.exe PID: 6648 Parent PID: 6020

General

Start time:	12:43:11
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SOA_31052021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SOA_31052021.exe'
Imagebase:	0x310000
File size:	939520 bytes
MD5 hash:	9A7DEB4C1DC1DFF1BB42585200668BAE
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: 00000000.00000002.425655543.0000000003797000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.425655543.0000000003797000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6584 Parent PID: 6648

General

Start time:	12:43:53
-------------	----------

Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lakYFibIJ' /XML 'C:\User\suser\AppData\Local\Temp\tmp8347.tmp'
Imagebase:	0x980000
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: 6596 Parent PID: 6584

General

Start time:	12:43:53
Start date:	11/06/2021
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: SOA_31052021.exe PID: 6616 Parent PID: 6648

General

Start time:	12:43:54
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SOA_31052021.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa30000
File size:	939520 bytes
MD5 hash:	9A7DEB4C1DC1DFF1BB42585200668BAE
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: 0000000C.00000002.593685889.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.593685889.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.597745767.0000000002D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.597745767.0000000002D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.419979399.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.419979399.0000000000402000.00000040.00000001.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: kprUEGC.exe PID: 1320 Parent PID: 3440

General	
Start time:	12:44:30
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xf00000
File size:	939520 bytes
MD5 hash:	9A7DEB4C1DC1DFF1BB42585200668BAE
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: 00000012.00000002.602545420.0000000004453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.602545420.0000000004453000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.599007756.0000000003454000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 36%, Virustotal, Browse • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: kprUEGC.exe PID: 2924 Parent PID: 3440

General

Start time:	12:44:39
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xb80000
File size:	939520 bytes
MD5 hash:	9A7DEB4C1DC1DFF1BB42585200668BAE
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: 00000013.00000002.602521914.0000000004063000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.602521914.0000000004063000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.599139134.0000000003065000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis