ID: 344974
Sample Name: lWAGihypmY0YXgh.exe
Cookbook: default.jbs
Time: 15:15:14
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

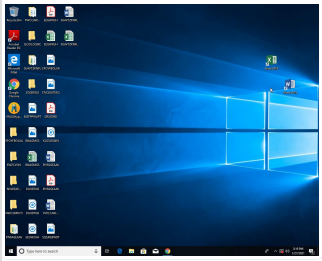
Analysis Report lWAGihypmY0YXgh.exe

Overview

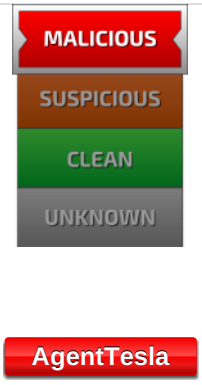
General Information

Sample Name:	lWAGihypmY0YXgh.exe
Analysis ID:	344974
MD5:	4c0f12aff663820…
SHA1:	4742ebd00f82dcc..
SHA256:	c935dd6128830f5.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



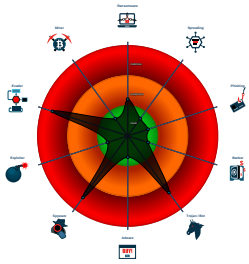
AgentTesla

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…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- lWAGihypmY0YXgh.exe (PID: 988 cmdline: 'C:\Users\user\Desktop\lWAGihypmY0YXgh.exe' MD5: 4C0F12AFF6638202B87A156B8BCABB8A)
  - schtasks.exe (PID: 4588 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HQNbDThyljJh' /XML 'C:\Users\user\AppData\Local\Temp\tmp38D3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - lWAGihypmY0YXgh.exe (PID: 6068 cmdline: {path} MD5: 4C0F12AFF6638202B87A156B8BCABB8A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "eS6gY1q65emm",
  "URL: ": "http://Lh0EfnfAinQ8pAa5.net",
  "To: ": "",
  "ByHost: ": "mail.sardaplywood.com:5878",
  "Password: ": "wyujHc",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.247243531.000000000457 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.245486243.000000000338 E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.632866048.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.246672076.00000000043F4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

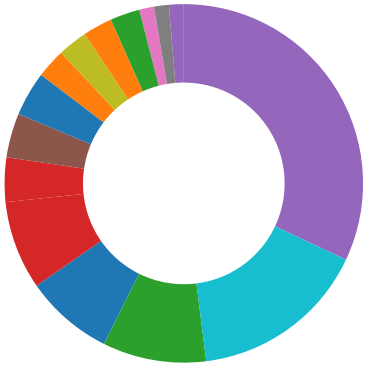
Source	Rule	Description	Author	Strings
4.2.IWAGihypmY0YXgh.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

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

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

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

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 AntiVM_3

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)

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

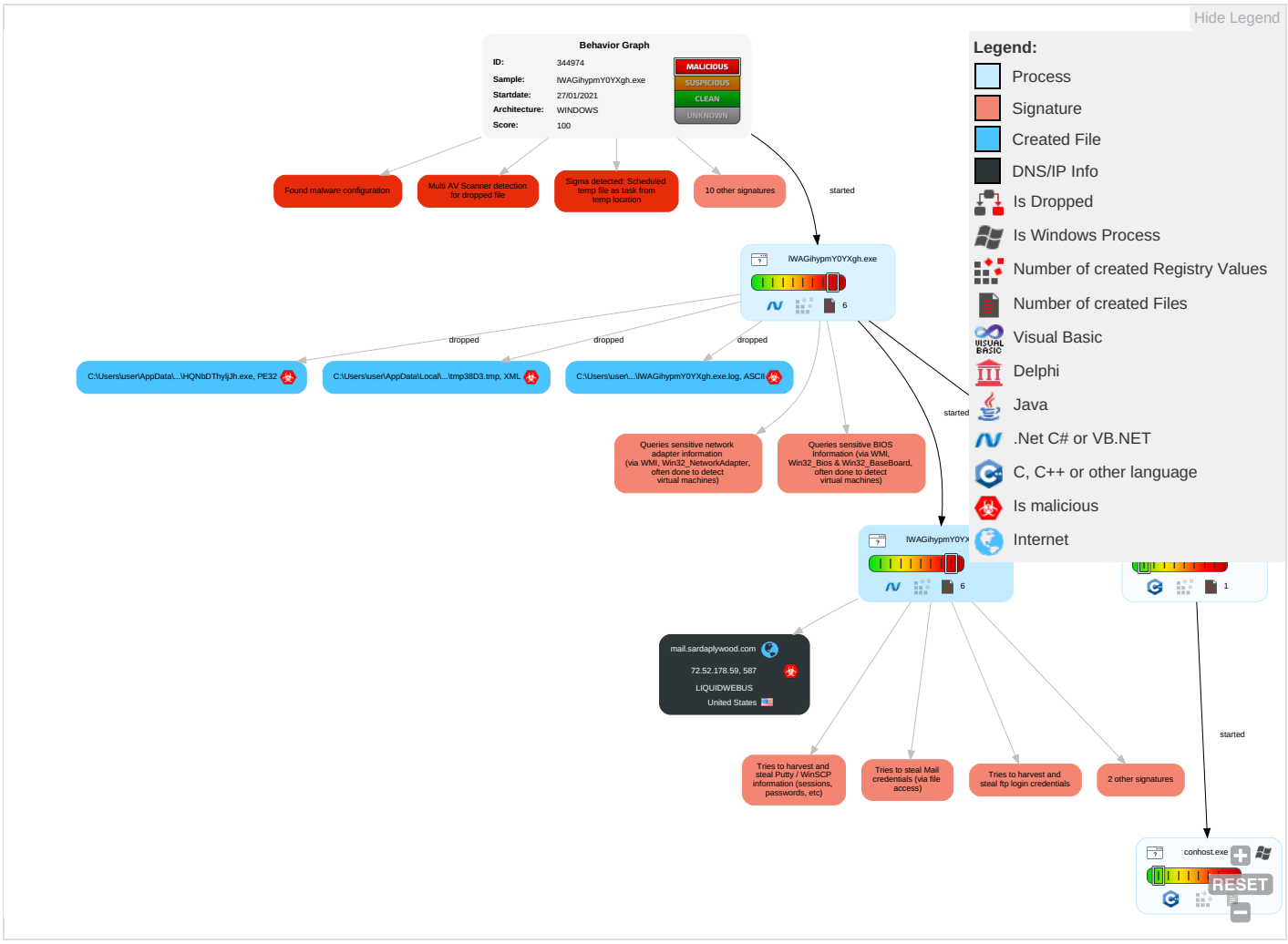
Yara detected AgentTesla

Mitre Att&ck Matrix

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

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

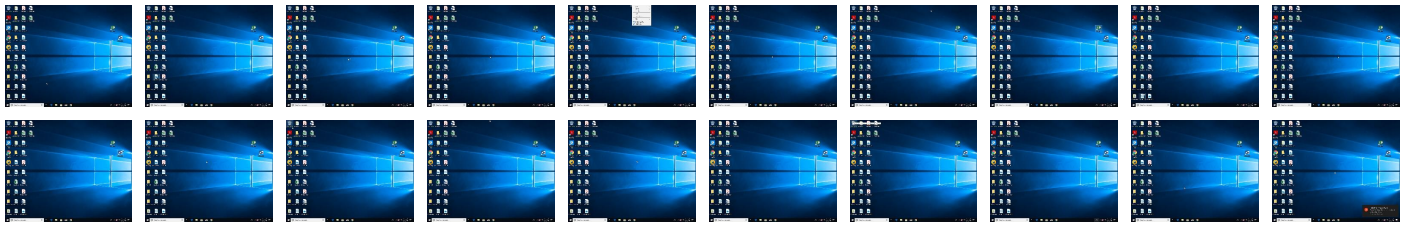
Behavior Graph



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
IWAGihypmY0YXgh.exe	33%	Virustotal		Browse
IWAGihypmY0YXgh.exe	33%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
IWAGihypmY0YXgh.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HQNbDThyljJh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\HQNbDThyljJh.exe	33%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.IWAGihypmY0YXgh.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.sajatypeworks.comiv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.sajatypeworks.com2	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.jiyu-kobo.co.jp/://wInI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/dn	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	0%	Avira URL Cloud	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.founder.com.cn/cnFROM	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	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.sakkal.comva	0%	Avira URL Cloud	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/cnm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/%n	0%	Avira URL Cloud	safe	
http://RwbTYu.com	0%	Avira URL Cloud	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.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.sajatypeworks.comtu	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.jiyu-kobo.co.jp/.n	0%	Avira URL Cloud	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	

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://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://mail.sardaplywood.com	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://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	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.fontbureau.comessedVnl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://Lh0EfnfAinQ8pAa5.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	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.fontbureau.comicno	0%	Avira URL Cloud	safe	
http://www.fontbureau.comW.TTFInl	0%	Avira URL Cloud	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/cncn4g	0%	Avira URL Cloud	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.sardaplywood.com	72.52.178.59	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://Lh0EfnfAinQ8pAa5.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	IWAGihypmY0YXgh.exe, 00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comiv	IWAGihypmY0YXgh.exe, 00000001.00000003.224219916.0000000006 32B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com2	IWAGihypmY0YXgh.exe, 00000001.00000003.224219916.0000000006 32B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html0	IWAGihypmY0YXgh.exe, 00000001.00000003.228943788.0000000006 31D000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/://wInI	IWAGihypmY0YXgh.exe, 00000001.00000003.225782389.0000000006 31B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/dn	IWAGihypmY0YXgh.exe, 00000001.00000003.225782389.0000000006 31B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/a-d	IWAGihypmY0YXgh.exe, 00000001.00000003.226307399.0000000006 31D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnU	IWAGihypmY0YXgh.exe, 00000001.00000003.224935169.0000000006 317000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnFROM	IWAGihypmY0YXgh.exe, 00000001.00000003.225020310.0000000006 317000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp, IWAGihypmY0YXgh.exe, 00000001.00000003.232456297.0000000006317000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comessed	IWAGihypmY0YXgh.exe, 00000001.00000003.229367097.0000000006 31C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comva	IWAGihypmY0YXgh.exe, 00000001.00000003.226385091.0000000006 344000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	IWAGihypmY0YXgh.exe, 00000001.00000003.224219916.0000000006 32B000.00000004.00000001.sdmp, IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnm	IWAGihypmY0YXgh.exe, 00000001.00000003.224935169.0000000006 317000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/%n	IWAGihypmY0YXgh.exe, 00000001.00000003.226307399.000000006631D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://RwbTYu.com	IWAGihypmY0YXgh.exe, 00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comtu	IWAGihypmY0YXgh.exe, 00000001.00000003.224219916.000000006632B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	IWAGihypmY0YXgh.exe, 00000001.00000002.245252670.0000000033311000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/.n	IWAGihypmY0YXgh.exe, 00000001.00000003.226307399.000000006631D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	IWAGihypmY0YXgh.exe, 00000001.00000002.247243531.0000000004573000.00000004.00000001.sdmp, IWAGihypmY0YXgh.exe, 00000004.00000002.632866048.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.sardaplywood.com	IWAGihypmY0YXgh.exe, 00000004.00000002.637537848.0000000003205000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	IWAGihypmY0YXgh.exe, 00000001.00000003.225380050.0000000006317000.00000004.00000001.sdmp, IWAGihypmY0YXgh.exe, 00000001.00000003.225415215.0000000006317000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.0000000007522000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	IWAGihypmY0YXgh.exe, 00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	IWAGihypmY0YXgh.exe, 00000001.00000003.229468329.000000006631E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlu	IWAGihypmY0YXgh.exe, 00000001.00000003.228943788.000000006631D000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	IWAGihypmY0YXgh.exe, 00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comessedVnl	IWAGihypmY0YXgh.exe, 00000001.00000003.228853121.000000006631C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	IWAGihypmY0YXgh.exe, 00000001.00000003.226307399.000000006631D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	IWAGihypmY0YXgh.exe, 00000001.00000003.228943788.000000006631D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	IWAGihypmY0YXgh.exe, 00000001.00000003.229367097.000000006631C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	IWAGihypmY0YXgh.exe, 00000001.00000003.224018588.0000000006316000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.00000000007522000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.00000000007522000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comicno	IWAGihypmY0YXgh.exe, 00000001.00000003.232456297.0000000006317000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comW.TTFInl	IWAGihypmY0YXgh.exe, 00000001.00000003.229367097.0000000006361C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	IWAGihypmY0YXgh.exe, 00000001.00000003.224977850.0000000006318000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.00000000007522000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cncn4g	IWAGihypmY0YXgh.exe, 00000001.00000003.224977850.0000000006318000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comt	IWAGihypmY0YXgh.exe, 00000001.00000003.229367097.0000000006361C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	IWAGihypmY0YXgh.exe, 00000001.00000003.232733352.0000000006317000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	IWAGihypmY0YXgh.exe, 00000001.00000003.225782389.0000000006361B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	IWAGihypmY0YXgh.exe, 00000001.00000003.232456297.0000000006317000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	IWAGihypmY0YXgh.exe, 00000001.00000002.250251822.00000000007522000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn5k	IWAGihypmY0YXgh.exe, 00000001.00000003.224977850.0000000006318000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsief	IWAGihypmY0YXgh.exe, 00000001.00000003.229468329.0000000006361E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.52.178.59	unknown	United States		32244	LIQUIDWEBUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344974
Start date:	27.01.2021
Start time:	15:15:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lWAGihypmY0YXgh.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:	33
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@6/4@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 23.210.248.85, 51.104.144.132, 95.101.22.224, 95.101.22.216, 20.54.26.129, 51.103.5.159, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus17.cloudapp.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:16:06	API Interceptor	1149x Sleep call for process: lWAGihypmY0YXgh.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
72.52.178.59	Shipping Documents.doc	Get hash	malicious	Browse	
	8Aobnx1VRi.exe	Get hash	malicious	Browse	
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	
	QImd3Q4VM0mNPFC.exe	Get hash	malicious	Browse	
	yarobelo.exe	Get hash	malicious	Browse	
	New order.doc	Get hash	malicious	Browse	
	Purchase order.doc	Get hash	malicious	Browse	
	PO-A2031150 AVI41916.exe	Get hash	malicious	Browse	
	uQQ6orCz0I.exe	Get hash	malicious	Browse	
	tM0AaInQN843GBX.exe	Get hash	malicious	Browse	
	GMo4SZUHaO.exe	Get hash	malicious	Browse	
	6IvaO5k09S.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	y4EDfjLJfDnggGQ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.4ddf98cd8e5a012c.exe	Get hash	malicious	Browse	
	hBpR9WytClXymyi.exe	Get hash	malicious	Browse	
	qu89NOv44s.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	part1.rtf	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.sardaplywood.com	Shipping Documents.doc	Get hash	malicious	Browse	• 72.52.178.59
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 72.52.178.59
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 72.52.178.59
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 72.52.178.59
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 72.52.178.59
	Order 21-21.doc	Get hash	malicious	Browse	• 67.225.218.11
	SecuriteInfo.com.BehavesLike.Win32.Generic.qm.exe	Get hash	malicious	Browse	• 67.225.218.11
	QImd3Q4VM0mNPFC.exe	Get hash	malicious	Browse	• 72.52.178.59
	yarobelo.exe	Get hash	malicious	Browse	• 72.52.178.59
	New order.doc	Get hash	malicious	Browse	• 72.52.178.59
	Purchase order.doc	Get hash	malicious	Browse	• 72.52.178.59
	PO-A2031150 AVI41916.exe	Get hash	malicious	Browse	• 72.52.178.59
	uQQ6orCz0I.exe	Get hash	malicious	Browse	• 72.52.178.59
	tM0AaInQN843GBX.exe	Get hash	malicious	Browse	• 72.52.178.59
	GMo4SZUHaO.exe	Get hash	malicious	Browse	• 72.52.178.59
	6IvaO5k09S.exe	Get hash	malicious	Browse	• 72.52.178.59
	y4EDfjLJfDnggGQ.exe	Get hash	malicious	Browse	• 72.52.178.59
	SecuriteInfo.com.Generic.mg.4ddf98cd8e5a012c.exe	Get hash	malicious	Browse	• 72.52.178.59
	hBpR9WytClXymyi.exe	Get hash	malicious	Browse	• 72.52.178.59
	qu89NOv44s.exe	Get hash	malicious	Browse	• 72.52.178.59

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LIQUIDWEBUS	ARCH 05 2_80074.doc	Get hash	malicious	Browse	• 209.59.139.39
	Shipping Documents.doc	Get hash	malicious	Browse	• 72.52.178.59
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 72.52.178.59
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 72.52.178.59
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 72.52.178.59
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 72.52.178.59
	433.doc	Get hash	malicious	Browse	• 67.227.152.97
	Order 21-21.doc	Get hash	malicious	Browse	• 67.225.218.11
	SecuriteInfo.com.BehavesLike.Win32.Generic.qm.exe	Get hash	malicious	Browse	• 67.225.218.11
	Adjunto-30.doc	Get hash	malicious	Browse	• 67.227.195.169
	935 2021 7-1529257.doc	Get hash	malicious	Browse	• 209.59.139.39
	Purchase Order_pdf.exe	Get hash	malicious	Browse	• 69.16.211.30
	937 2912 2020 2_90961070.doc	Get hash	malicious	Browse	• 67.227.152.97
	Archivo_2020.doc	Get hash	malicious	Browse	• 67.227.152.97
	81msxxUisn.exe	Get hash	malicious	Browse	• 72.52.178.23
	Archivo.doc	Get hash	malicious	Browse	• 67.227.152.97
	Q38V8rfI5H.js	Get hash	malicious	Browse	• 72.52.178.23
	Q38V8rfI5H.js	Get hash	malicious	Browse	• 72.52.178.23
	Doc.doc	Get hash	malicious	Browse	• 67.225.191.31
	ARCH_2021.doc	Get hash	malicious	Browse	• 209.59.139.39

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lWAGihypmY0YXgh.exe.log	
Process:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	
Process:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.183233044081882
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBMAPtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3SAF
MD5:	4FFF7ED5E1697C90C08C0405B1ADB58B
SHA1:	5560656702998474BF8DBA257CA9CA870F4D6660
SHA-256:	72ACEA1E93A7C1666866037903EDF735A225B732DE2392792FD332F572E8D1DD
SHA-512:	8A7CBD44EA0327DFBE311CFA3014D6D89A7E7961245783D071D6EF8B536ED1513EECC74C68C1E8BC9664B603217832784B97C4B2B5D0929F79967F41D594441
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\HQNbDThyIjJh.exe	
Process:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	832000
Entropy (8bit):	7.376167485974427
Encrypted:	false
SSDEEP:	12288:Rqfu196mwIFAW3WgWpMj/HtxVTfid5rBtqKuCwaBbaBx:z5wIue3Wqj/txVTU5rBtq9ZaRa
MD5:	4C0F12AFF6638202B87A156B8BCABB8A
SHA1:	4742EBD00F82DCC2A520E2165D5C941E6CBA4936
SHA-256:	C935DD6128830F5506AF13B5E46043D4F8B2781E345936F069647228 65AB0C6E
SHA-512:	D77B8B4F17A840897ADD306E358A97A19F1BE2E7605741EFA8386F7E8FB23C1664228A47F9DF8A3B4CF8CD0B311C1EE58E82F18BC4615273103E3FD080473322
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low

C:\Users\user\AppData\Roaming\HQNbDThyljJh.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j..`.....0..... .....@.. ..... ..@.....h...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....d...._.....y....<..p.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*"".....*.0 ..!.....(....r1..p~....o.....t.....+..*".(.....*Vr?..p.....rK..p.....*^..}.....(.....(.....*.0..J.....rY..pr...p(....&.(....t!...o.....#..r...p.o....(....r...p...(....&...*.....%&.# ....0..+.....,.{.....+.. ..,...{....o .....(!....*..0.....s"...}.....s"...}.

C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.376167485974427
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:	lWAGihypmY0YXgh.exe
File size:	832000
MD5:	4c0f12aff6638202b87a156b8bcabb8a
SHA1:	4742ebd00f82dcc2a520e2165d5c941e6cba4936
SHA256:	c935dd6128830f5506af13b5e46043d4f8b2781e345936f06964722865ab0c6e
SHA512:	d77b8b4f17a840897add306e358a97a19f1be2e7605741fa8386f7e8fb23c1664228a47f9df8a3b4cf8cd0b311c1ee58e82f18bc4615273103e3fd080473322
SSDEEP:	12288:Rqfu196mwIFAW3WgWpMj/HtxVTfid5rBtqKuCwaBbaBx:z5wIue3Wqj/txVTU5rBtq9ZaRa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j..`.....0..... .....@.. ..... @.....

File Icon

Icon Hash:	e0dc9e0e1e9296e8

Static PE Info

General

Entrypoint:	0x4bbdba

General

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:	0x6010C76A [Wed Jan 27 01:52:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbbd68	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x10e98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	0xc	.reloc

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb9dc0	0xb9e00	False	0.66132260844	data	7.53579555496	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x10e98	0x11000	False	0.132999195772	data	4.50647829778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc100	0x10828	data		
RT_GROUP_ICON	0xcc938	0x14	data		
RT_VERSION	0xcc95c	0x33c	data		
RT_MANIFEST	0xccca8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

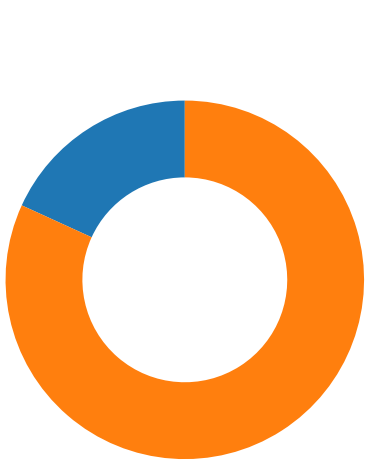
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	i7hDxntRTQ.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HotelMgmtSystem
ProductVersion	1.0.0.0
FileDescription	HotelMgmtSystem
OriginalFilename	i7hDxntRTQ.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:17:52.778460979 CET	49737	587	192.168.2.5	72.52.178.59
Jan 27, 2021 15:17:55.763927937 CET	49737	587	192.168.2.5	72.52.178.59
Jan 27, 2021 15:18:01.764501095 CET	49737	587	192.168.2.5	72.52.178.59
Jan 27, 2021 15:18:15.942601919 CET	49738	587	192.168.2.5	72.52.178.59
Jan 27, 2021 15:18:18.953504086 CET	49738	587	192.168.2.5	72.52.178.59
Jan 27, 2021 15:18:24.953892946 CET	49738	587	192.168.2.5	72.52.178.59

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:15:56.917489052 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:15:56.974052906 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 15:15:57.998327971 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:15:58.046441078 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:15:58.912138939 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:15:58.960170984 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:00.000684977 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:00.051584005 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:00.873547077 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:00.923321962 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:22.828087091 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:22.890472889 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:26.554241896 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:26.605107069 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:29.726089954 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:29.783792019 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:42.237662077 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:42.294150114 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:45.877793074 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:45.925832033 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:47.475452900 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:47.523392916 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 15:16:50.426089048 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:16:50.486789942 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 15:17:26.807775021 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:17:26.858573914 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 15:17:51.258930922 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:17:51.309784889 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 15:17:51.775666952 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:17:51.826503992 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 15:17:52.484864950 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:17:52.632637024 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:15.879472017 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:15.940701008 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:38.646527052 CET	54450	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:18:38.708085060 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:39.348392010 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:39.399883032 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:40.190232992 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:40.239104033 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:40.912715912 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:40.969495058 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:41.610985041 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:41.672333002 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:42.297666073 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:42.359169960 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:43.215058088 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:43.263248920 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:44.532676935 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:44.591362000 CET	53	56432	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:46.108494043 CET	52929	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:46.165102005 CET	53	52929	8.8.8.8	192.168.2.5
Jan 27, 2021 15:18:46.677643061 CET	64317	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:18:46.728189945 CET	53	64317	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:17:52.484864950 CET	192.168.2.5	8.8.8.8	0x9441	Standard query (0)	mail.sardaplywood.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:18:15.879472017 CET	192.168.2.5	8.8.8.8	0x25ff	Standard query (0)	mail.sardaplywood.com	A (IP address)	IN (0x0001)

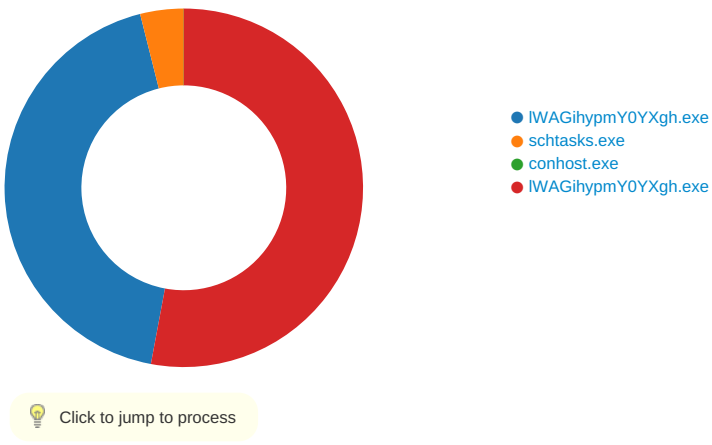
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:17:52.632637024 CET	8.8.8.8	192.168.2.5	0x9441	No error (0)	mail.sardaplywood.com		72.52.178.59	A (IP address)	IN (0x0001)
Jan 27, 2021 15:18:15.940701008 CET	8.8.8.8	192.168.2.5	0x25ff	No error (0)	mail.sardaplywood.com		72.52.178.59	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: lWAGihypmY0YXgh.exe PID: 988 Parent PID: 5632

General

Start time:	15:16:01
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lWAGihypmY0YXgh.exe'
Imagebase:	0xf70000
File size:	832000 bytes
MD5 hash:	4C0F12AFF6638202B87A156B8BCABB8A
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: 00000001.00000002.247243531.0000000004573000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.245486243.000000000338E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.246672076.00000000043F4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC9CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC9CF06	unknown
C:\Users\user\AppData\Roaming\HQNbDThyljJh.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CAE7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lWAGihypmY0YXgh.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFAC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	success or wait	1	6CAE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\HQNbDThyljJh.exe	unknown	832000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6a c7 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 9e 0b 00 00 12 01 00 00 00 00 00 ba bd 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...j..`.......... ....0................. ....@.. ....@................	success or wait	1	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	unknown	1649	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6CAE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lWAGihypmY0YXgh.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6DFAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Users\user\Desktop\lWAGihypmY0YXgh.exe	unknown	832000	success or wait	1	6CAE1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4588 Parent PID: 988

General

Start time:	15:16:10
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\HQNbDThyljJh' /XML 'C:\Users\user\AppData\Local\Temp\tmp38D3.tmp'
Imagebase:	0x3f0000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	unknown	2	success or wait	1	3FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp38D3.tmp	unknown	1650	success or wait	1	3FABD9	ReadFile

Analysis Process: conhost.exe PID: 5440 Parent PID: 4588

General

Start time:	15:16:10
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: lWAGihypmY0YXgh.exe PID: 6068 Parent PID: 988

General

Start time:	15:16:11
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\lWAGihypmY0YXgh.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaf0000
File size:	832000 bytes
MD5 hash:	4C0F12AFF6638202B87A156B8BCABB8A
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: 00000004.00000002.632866048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.635904351.0000000002EF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC9CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC9CF06	unknown
C:\Users\user\AppData\Roaming\j04yismf.sjk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CAEDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default\Cookies	success or wait	1	6CAE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CAEDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\694b85b1-6f05-4c33-b0b3-45a2ee446545	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Users\user\AppData\Roaming\j04yismf.sjk\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CAE1B4F	ReadFile

Disassembly

Code Analysis