ID: 452750
Sample Name: K0bg9rZl2L
Cookbook: default.jbs
Time: 19:34:54
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

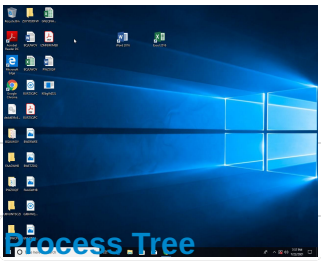
Windows Analysis Report K0bg9rZl2L

Overview

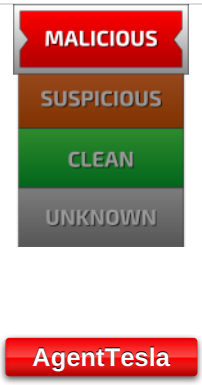
General Information

Sample Name:	K0bg9rZl2L (renamed file extension from none to exe)
Analysis ID:	452750
MD5:	699e56ea4da0b0..
SHA1:	c32dff686616f74…
SHA256:	e5805ba9f911998.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

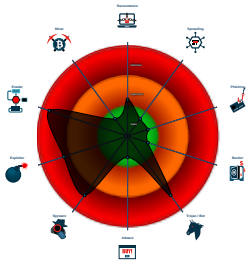


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected UAC Bypass using C…
- Adds a directory exclusion to Windo…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



- **System is w10x64**
- K0bg9rZl2L.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\K0bg9rZl2L.exe' MD5: 699E56EA4DA0B0865FC33308A8B09DF9)
  - powershell.exe (PID: 7060 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\K0bg9rZl2L.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - K0bg9rZl2L.exe (PID: 1316 cmdline: C:\Users\user\Desktop\K0bg9rZl2L.exe MD5: 699E56EA4DA0B0865FC33308A8B09DF9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "bookings@simpleitalian.com.au",
  "Password": "SIpassword101$",
  "Host": "mail.simpleitalian.com.au"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.916660808.00000000029C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000002.914072243.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.914072243.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.K0bg9rZl2L.exe.5a70000.6.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.2.K0bg9rZl2L.exe.3b01478.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.K0bg9rZl2L.exe.3b01478.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.K0bg9rZl2L.exe.3ae1458.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.K0bg9rZl2L.exe.3ae1458.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Exploits:

Yara detected UAC Bypass using CMSTP

System Summary:

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Copyright Joe Security LLC 2021

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

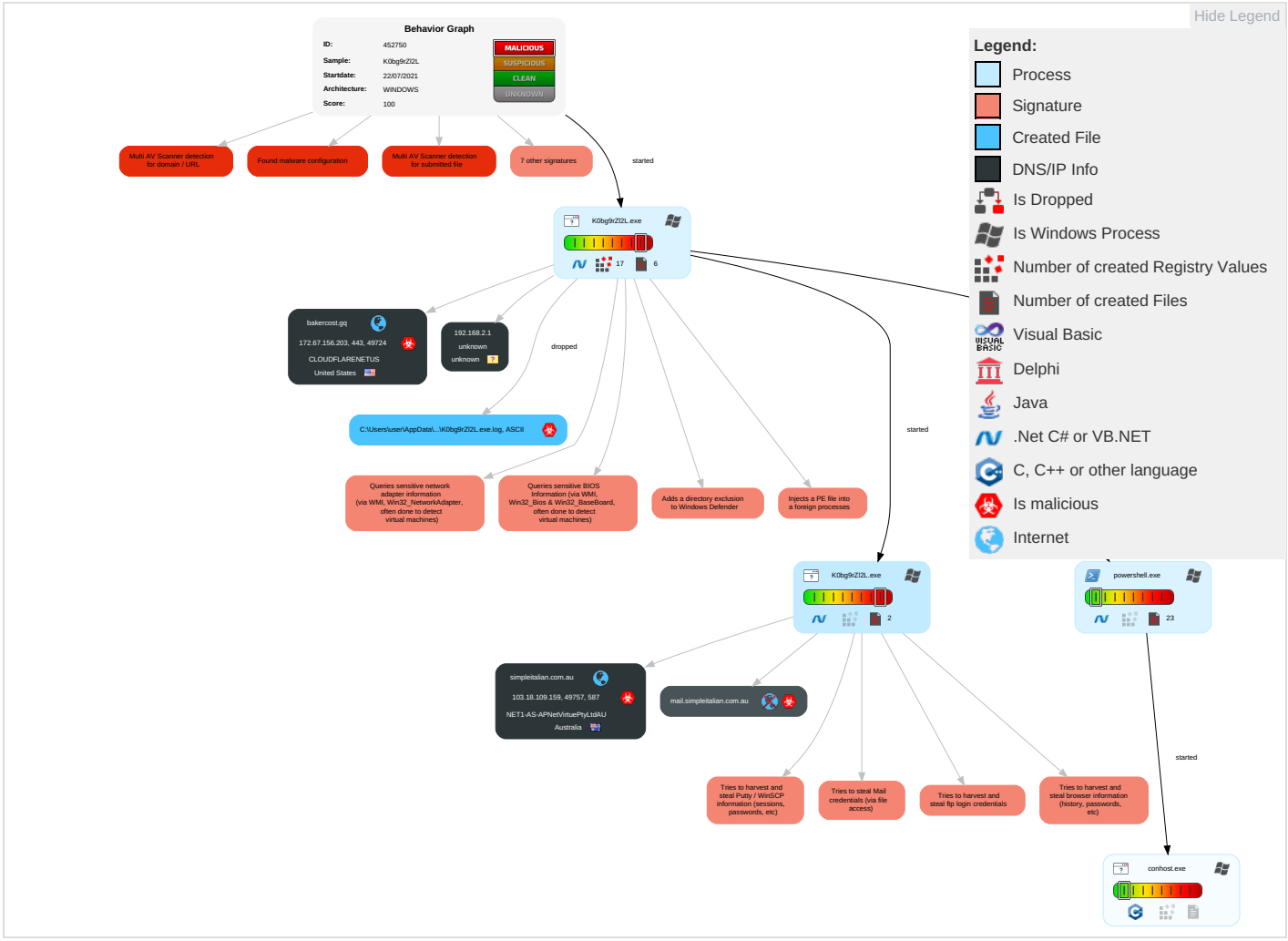
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 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	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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
K0bg9rZI2L.exe	37%	Virustotal		Browse
K0bg9rZI2L.exe	22%	ReversingLabs	Win32.Trojan.Wacatac	
K0bg9rZI2L.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.K0bg9rZI2L.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
simpleitalian.com.au	0%	Virustotal		Browse
bakercost.gq	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://simpleitalian.com.au	0%	Avira URL Cloud	safe	
http://https://mab.data.tm-awx.com/rhs	0%	Avira URL Cloud	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://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	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://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
simpleitalian.com.au	103.18.109.159	true	true	• 0%, Virustotal, Browse	unknown
bakercost.gq	172.67.156.203	true	true	• 13%, Virustotal, Browse	unknown
mail.simpleitalian.com.au	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.156.203	bakercost.gq	United States		13335	CLOUDFLARENETUS	true
103.18.109.159	simpleitalian.com.au	Australia		132680	NET1-AS-APNetVirtuePtyLtdAU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452750
Start date:	22.07.2021
Start time:	19:34:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	K0bg9rZl2L (renamed file extension from none to exe)

Copyright Joe Security LLC 2021

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:	18
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.expl.evad.winEXE@6/8@3/3
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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:36:06	API Interceptor	721x Sleep call for process: K0bg9rZl2L.exe modified
19:36:19	API Interceptor	32x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.156.203	Swift-pdf.exe	Get hash	malicious	Browse	
	aLLEK0YD2O.exe	Get hash	malicious	Browse	
	triage_dropped_file.exe	Get hash	malicious	Browse	
	MPU702734-pdf.exe	Get hash	malicious	Browse	
	o8YvAfzUQl.exe	Get hash	malicious	Browse	
	6x6wq7Dy4t.exe	Get hash	malicious	Browse	
	Itemsreceipt975432907.exe	Get hash	malicious	Browse	
	bank.doc.exe	Get hash	malicious	Browse	
	ANNA-INVOICE-4725434.EXE	Get hash	malicious	Browse	
	Victoria-Invoice-62541323.exe	Get hash	malicious	Browse	
	Aurora-Invoice-9383736.exe	Get hash	malicious	Browse	
	8d9U6fF3H1.exe	Get hash	malicious	Browse	
	purchase order.doc	Get hash	malicious	Browse	
	Madison-Invoice-6220917.exe	Get hash	malicious	Browse	
	OneDrive.exe	Get hash	malicious	Browse	
	jGUR7OQF1a.exe	Get hash	malicious	Browse	
	Product Emm 803030830019971 10082982820091989 1099 38377338393.exe	Get hash	malicious	Browse	
	02_extracted.exe	Get hash	malicious	Browse	
	01_extracted.exe	Get hash	malicious	Browse	
	Company presentation and order specification_IMG.exe	Get hash	malicious	Browse	

Copyright Joe Security LLC 2021

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bakercost.gq	Swift-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 104.21.13.164
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	triage_dropped_file.exe	Get hash	malicious	Browse	• 172.67.156.203
	DOC98374933JULY2021.exe	Get hash	malicious	Browse	• 104.21.13.164
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	o8YvAfzUQl.exe	Get hash	malicious	Browse	• 172.67.156.203
	download.dat.exe	Get hash	malicious	Browse	• 104.21.13.164
	WindowsFormsApp1.exe	Get hash	malicious	Browse	• 104.21.13.164
	6x6wq7Dy4t.exe	Get hash	malicious	Browse	• 172.67.156.203
	Itemsreceipt975432907.exe	Get hash	malicious	Browse	• 104.21.13.164
	bank.doc.exe	Get hash	malicious	Browse	• 172.67.156.203
	ANNA-INVOICE-4725434.EXE	Get hash	malicious	Browse	• 172.67.156.203
	Victoria-Invoice-62541323.exe	Get hash	malicious	Browse	• 172.67.156.203
	Aurora-Invoice-9383736.exe	Get hash	malicious	Browse	• 172.67.156.203
	8d9U6fF3H1.exe	Get hash	malicious	Browse	• 172.67.156.203
	purchase order.doc	Get hash	malicious	Browse	• 172.67.156.203
	3278_pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	Madison-Invoice-6220917.exe	Get hash	malicious	Browse	• 172.67.156.203
	Hazel-Invoice-9002745.exe	Get hash	malicious	Browse	• 104.21.13.164

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NET1-AS-APNetVirtuePtyLtdAU	droxoUY6SU.exe	Get hash	malicious	Browse	• 103.18.109.164
	RfTQP.exe	Get hash	malicious	Browse	• 103.18.109.186
	OUTSTANDING_INVOICE_Statement_077117.xlsm	Get hash	malicious	Browse	• 103.18.108.116
	OUTSTANDING_INVOICE_Statement_112488.xlsm	Get hash	malicious	Browse	• 103.18.108.116
	LYngoHo12f.dll	Get hash	malicious	Browse	• 103.18.108.116
	v2HhnFmaVL.dll	Get hash	malicious	Browse	• 103.18.108.116
	hNWv33c6vO.dll	Get hash	malicious	Browse	• 103.18.108.116
	DT4fKHpvho.dll	Get hash	malicious	Browse	• 103.18.108.116
	F2lEXKEaSG.dll	Get hash	malicious	Browse	• 103.18.108.116
	SRH2EHlixv.dll	Get hash	malicious	Browse	• 103.18.108.116
	XZAKMeSCAh.dll	Get hash	malicious	Browse	• 103.18.108.116
	xA732naDJK.dll	Get hash	malicious	Browse	• 103.18.108.116
	WrJsjSVmIW.dll	Get hash	malicious	Browse	• 103.18.108.116
	Yr8ElL80Bg.dll	Get hash	malicious	Browse	• 103.18.108.116
	xc6uov5QUt.dll	Get hash	malicious	Browse	• 103.18.108.116
	R1Vw5x5Gk7.dll	Get hash	malicious	Browse	• 103.18.108.116
	PVItZxbAhC.dll	Get hash	malicious	Browse	• 103.18.108.116
	YKOVp6Rx9G.dll	Get hash	malicious	Browse	• 103.18.108.116
	4lAXiCvogP.dll	Get hash	malicious	Browse	• 103.18.108.116
	M4WD0oqJPr.dll	Get hash	malicious	Browse	• 103.18.108.116
CLOUDFLARENETUS	lWky5C8Dhwcnso8.exe	Get hash	malicious	Browse	• 172.67.188.154
	q6pnkIaviT.exe	Get hash	malicious	Browse	• 162.159.135.233
	btweb_installer.exe	Get hash	malicious	Browse	• 104.18.88.101
	s2rsXUiUn8.exe	Get hash	malicious	Browse	• 162.159.134.233
	ZzWelCRhns.exe	Get hash	malicious	Browse	• 172.67.130.27
	NqRG532O8h.dll	Get hash	malicious	Browse	• 104.18.7.156
	85vLO1Rpcy.exe	Get hash	malicious	Browse	• 104.21.86.209
	PAYMENT ADVICE.doc	Get hash	malicious	Browse	• 104.21.27.166
	PO20210722.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	New order 11244332.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Z0hOr2pD7k.exe	Get hash	malicious	Browse	• 1.1.1.1
	USD_SLIP.docx	Get hash	malicious	Browse	• 104.21.19.245
	DHL JULY STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 104.21.19.200
	qK3005mdZn.exe	Get hash	malicious	Browse	• 172.67.168.51
	whesilox.exe	Get hash	malicious	Browse	• 172.67.188.154
	Bank contract,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Swift-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	Order _ 08201450.doc	Get hash	malicious	Browse	• 172.67.188.154
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 104.21.13.164

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	IWky5C8Dhwcnso8.exe	Get hash	malicious	Browse	• 172.67.156.203
	ZzWelCRhns.exe	Get hash	malicious	Browse	• 172.67.156.203
	New order 11244332.pdf.exe	Get hash	malicious	Browse	• 172.67.156.203
	DHL JULY STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 172.67.156.203
	whesilox.exe	Get hash	malicious	Browse	• 172.67.156.203
	Bank contract,PDF.exe	Get hash	malicious	Browse	• 172.67.156.203
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 172.67.156.203
	Swift-pdf.exe	Get hash	malicious	Browse	• 172.67.156.203
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 172.67.156.203
	Specifications_Details_20337_FLQ.exe	Get hash	malicious	Browse	• 172.67.156.203
	SgjcpodWpB.exe	Get hash	malicious	Browse	• 172.67.156.203
	10303640_APMC-TRN-C0001-Stability_Calculation_Rev1.exe	Get hash	malicious	Browse	• 172.67.156.203
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 172.67.156.203
	jRPSjUSf.exe	Get hash	malicious	Browse	• 172.67.156.203
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.156.203
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 172.67.156.203
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.156.203
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.156.203
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28334.exe	Get hash	malicious	Browse	• 172.67.156.203
	rrnIEffG4c.exe	Get hash	malicious	Browse	• 172.67.156.203

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\K0bg9rZl2L.exe.log	
Process:	C:\Users\user\Desktop\K0bg9rZl2L.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.35826085534976
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qXKIE4oKFKHKoZAE4Kzr7rE4jE4Ko84G1qE4j:MxHKXwYHKhQnogLHitHoxHhAHKzvrHjz
MD5:	48368BF02895E447540DFBA80D9D9743
SHA1:	D17396B97985D5D390DE4D9A08853F6D944EA3F2
SHA-256:	EC5D2E5B69722E9CF56FF4F1A0D47BE3B11D8B93AB3CF2CAE76E853F4EC794D7
SHA-512:	F3F4A96E9066B64A3750B18FABE5728E886DBDE0F29116BC6A438973A76AD5E1C6775A11E0C565C7643417EA70FDB68A5C1648008A45FE72249215BE8D87CBD
Malicious:	**true**
Reputation:	low
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",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..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKey

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Entropy (8bit):	4.996142136926143
Encrypted:	false
SSDEEP:	384:SEdVoGIpN6KQkj2Zkjh4iUxZvuiOOdBCNXp5nYoJib4J:SYV3IpNBQkj2Yh4iUxZvuiOOdBCNZlYO
MD5:	B7D3A4EB1F0AED131A6E0EDF1D3C0414
SHA1:	A72E0DDE5F3083632B7242D2407658BCA3E54F29
SHA-256:	8E0EB5898DDF86FE9FE0011DD7AC6711BB0639A8707053D831FB348F9658289B
SHA-512:	F9367BBEC9A44E5C08757576C56B9C8637D8A0A9D6220DE925255888E6A0A088C653E207E211A6796F6A7F469736D538EA5B9E094944316CF4E8189DDD3EED9D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.............Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1........Uninstall-Module........inmo..... ...fimo........Install-Module........New-ScriptFileInfo........Publish-Module........Install-Script........Update-Script........Find-Command........Update-ModuleManifest........Find- DscResource........Save-Module........Save-Script........upmo........Uninstall-Script........Get-InstalledScript........Update-Module........Register-PSRepository........Find-Scr ipt........Unregister-PSRepository........pumo........Test-ScriptFileInfo........Update-ScriptFileInfo........Set-PSRepository........Get-PSRepository........Get-InstalledModule... .....Find-Module........Find-RoleCapability........Publish-Script...............T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1* ....Install-Script........Save-Module........Publish-Module........Find-Module........Download-Package........Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22312
Entropy (8bit):	5.601566728872549
Encrypted:	false
SSDEEP:	384:6tCDTkkm1jt/V++SBKnCul6iD7Y9ghSJUeRu1BMrmrZSRV77nMZ7564I+Bg:nUjth4KCulj3hXe1aAnyA
MD5:	1D19BB2AA78F58C5D31B3C2A0DF05B6B
SHA1:	6D18B125CC4ECC1C523116E69DD5A872CBEB40A7
SHA-256:	C61E18E5034EB1018BE94B63F0E9DE35C8E204EC6712143900BC2189AEE42DF3
SHA-512:	6475B28B155A3929AA393956BBA51AA55C1EDA94BA7F6B632CFABEF2C0A0536A807E8F82E4345344D2F60BF56E4047D0F098FA735E13B76FC6D3140B275B0FB E
Malicious:	false
Reputation:	low
Preview:	@...e.......................d.R.2.......1............@..........H...............<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD..............fZve...F.....x.)........System.Managemen t.Automation4...............[...{a.C..%6..h.........System.Core.0..............G-.o...A...4B..........System..4...............Zg5..:O..g..q..........System.Xml..L..............7.....J@......~...... .#.Microsoft.Management.Infrastructure.8...............'....L..}...........System.Numerics.@...............Lo...QN......<Q........System.DirectoryServices<...............H..QN.Y.f....... .....System.Management...4...................].D.E.....#.......System.Data.H................ ....H..m)aUu.........Microsoft.PowerShell.Security...<................~.[L.D.Z.>..m.........Sy stem.Transactions.<...............):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...].......%.Microsoft.PowerShell.Commands.Utility...D.................-.D.F.<;.nt.1 ....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\14906059cf1d40cd99ff18e182ff171d	
Process:	C:\Users\user\Desktop\K0bg9rZl2L.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	622385
Entropy (8bit):	2.8976563455834365
Encrypted:	false
SSDEEP:	6144:YaX4W8j4LrbLhdPAJmpYcgXPCy3poHVcaVxuY6rUi1F+niWgbnkpvbXyGhRlX3J5:XxdP+oHeD9+niWgbnkpj1j/oI
MD5:	451BDA3D085ED031392288F19B600079
SHA1:	58F509AA622F66953E62EE4AACC3C259D57BC573
SHA-256:	EDB98216DC2C2AB2D611928B00D25DC0929953BDF7AD11B91782FF56E1F80724
SHA-512:	80C2683AB5ED7205903ECFE0BE88156B5CC4D5B8928B2194B7D3B8F22D1CE285DA8254276C39BB50C5B8F68A71B7D7FC497326DB3C3982C861B4227857192A4
Malicious:	false
Reputation:	low
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 43 121 246 96 0 0 0 0 0 0 0 0 224 0 2 1 11 1 8 0 0 86 3 0 0 6 0 0 0 0 0 0 206 116 3 0 0 32 0 0 0 0 0 0 0 64 0 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 192 3 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 124 116 3 0 79 0 0 0 0 128 3 0 192 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 160 3 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 212 84 3 0 0 32 0 0 0 86 3 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96 46 114 115 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_liycv4ep.1cw.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_liycv4ep.1cw.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m33dr320.qvb.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\Desktop\dedd659c48564f729136e943657b6aef.dll	
Process:	C:\Users\user\Desktop\K0bg9rZl2L.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	861174
Entropy (8bit):	2.7605214644462466
Encrypted:	false
SSDEEP:	1536:QJ7ZOQz3Kve36nr7bqcbz6XZEn0/EniQ3xt9gO3VLkht2TgHIdD/YJRPRo6549Cb:Lnr/KEnoEnzmALqi/jEX
MD5:	3CE3D10BE646910FD966C60B3E48CA3A
SHA1:	D8B75E0B8F2F34D8471E3F0820410117ADAACBAD
SHA-256:	CC6BD43DA778D5C60B36F23E8890D67D29DFDBEE5744EB69A3AC845297455D39
SHA-512:	1F02B8C7BF07C5B3A6AC11DEE65048282CD0BBC2D951BC508B5BDC4DC9800D0D675982EE7029710D3E3DC5FBEFAFFDA79C98F6B4C1937F1FE5482F1DE3733 0D
Malicious:	false
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 254 142 134 251 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 226 4 0 0 8 0 0 0 0 0 0 254 0 5 0 0 32 0 0 0 32 5 0 0 0 64 0 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 96 5 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 164 0 5 0 87 0 0 0 0 32 5 0 184 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 64 5 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 4 225 4 0 0 32 0 0 0 226 4 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96 46 114 115 11

C:\Users\user\Documents\20210722\PowerShell_transcript.642294.pSUMO4EI.20210722193552.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5785
Entropy (8bit):	5.400381717825487
Encrypted:	false
SSDEEP:	96:BZAjDN+qDo1ZFZkjDN+qDo1ZI6QCjZ+jDN+qDo1ZiHSSfZ8:D
MD5:	5A19C067EE90DB7CFB6448120504E8CA
SHA1:	EED5D09E359C1BB06403423AFCE289874DDAC61D
SHA-256:	586F429CB3926EC5AD029AEF8364122D6E301FCEFBF2EDCC45C0FF73F35982B7
SHA-512:	1EFF6F20DA4244CC2B46258F31EE6D69A207E1890875B4CF737E5C9754F083E1408CBB7C25B3FD4751AAF9163CD2195C0988C279F51EB2237BECF925623C4702
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210722193610..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 642294 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\K0bg9rZl2L.exe -Force..Process ID: 7060..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********************..**********************..Command start time: 20210722193610..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \K0bg9rZl2L.exe -Force..**********************..Windows PowerShell transcript start..Start time: 20210722194035..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.368608644874725
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:	K0bg9rZl2L.exe
File size:	17920
MD5:	699e56ea4da0b0865fc33308a8b09df9
SHA1:	c32dff686616f747f808a5c0bc67484d4755f568
SHA256:	e5805ba9f9119986eb49be00972cb30d5249f8c19c872c4daacb2ad67a157bb5
SHA512:	84586f58c062eb957348ddb548d77b651e6878bddbf4b13f845d7c9021bc6221d4356c8bec8a2ab1b1e3a5a8f4b1ca2871c7c9c2657b1e6dd225f0c738dcb5f0
SSDEEP:	384:r/9hScRkXl+0li1QKYwaCZU6w2mtTAEhVLU6oLUJflQDrbP:rXScRkjl/mv6SNhVPoGfl+bP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...`.,.....".0..:.....Y... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4059ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xAF2CEA60 [Sat Feb 17 16:46:24 2063 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	0x39b4	0x3a00	False	0.489628232759	data	5.5440032904	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x6000	0x6e8	0x800	False	0.35595703125	data	4.6384165532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 19:35:44.346951008 CEST	192.168.2.4	8.8.8.8	0x3df3	Standard query (0)	bakercost.gq	A (IP address)	IN (0x0001)
Jul 22, 2021 19:37:38.028907061 CEST	192.168.2.4	8.8.8.8	0xf8fe	Standard query (0)	mail.simpleitalian.com.au	A (IP address)	IN (0x0001)
Jul 22, 2021 19:37:38.887294054 CEST	192.168.2.4	8.8.8.8	0xea12	Standard query (0)	mail.simpleitalian.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:35:44.414767981 CEST	8.8.8.8	192.168.2.4	0x3df3	No error (0)	bakercost.gq		172.67.156.203	A (IP address)	IN (0x0001)
Jul 22, 2021 19:35:44.414767981 CEST	8.8.8.8	192.168.2.4	0x3df3	No error (0)	bakercost.gq		104.21.13.164	A (IP address)	IN (0x0001)
Jul 22, 2021 19:37:38.439606905 CEST	8.8.8.8	192.168.2.4	0xf8fe	No error (0)	mail.simpleitalian.com.au	simpleitalian.com.au		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:37:38.439606905 CEST	8.8.8.8	192.168.2.4	0xf8fe	No error (0)	simpleitalian.com.au		103.18.109.159	A (IP address)	IN (0x0001)
Jul 22, 2021 19:37:39.098787069 CEST	8.8.8.8	192.168.2.4	0xea12	No error (0)	mail.simpleitalian.com.au	simpleitalian.com.au		CNAME (Canonical name)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:37:39.098787069 CEST	8.8.8.8	192.168.2.4	0xea12	No error (0)	simpleitalian.com.au		103.18.109.159	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 19:35:44.618968964 CEST	172.67.156.203	443	192.168.2.4	49724	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jul 05 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Tue Jul 05 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 19:37:40.488419056 CEST	587	49757	103.18.109.159	192.168.2.4	220-r1.cpcloud.com.au ESMTP Exim 4.94.2 #2 Fri, 23 Jul 2021 03:37:40 +1000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jul 22, 2021 19:37:40.489053965 CEST	49757	587	192.168.2.4	103.18.109.159	EHLO 642294
Jul 22, 2021 19:37:40.777964115 CEST	587	49757	103.18.109.159	192.168.2.4	250-r1.cpcloud.com.au Hello 642294 [84.17.52.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jul 22, 2021 19:37:40.778377056 CEST	49757	587	192.168.2.4	103.18.109.159	STARTTLS
Jul 22, 2021 19:37:41.068491936 CEST	587	49757	103.18.109.159	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: K0bg9rZl2L.exe PID: 6860 Parent PID: 5912

General

Start time:	19:35:43
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\K0bg9rZl2L.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\K0bg9rZl2L.exe'
Imagebase:	0x550000
File size:	17920 bytes
MD5 hash:	699E56EA4DA0B0865FC33308A8B09DF9
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: 00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.690324946.000000000422F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.698060077.0000000005A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.698060077.0000000005A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.681433338.0000000003878000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.681433338.0000000003878000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 7060 Parent PID: 6860

General

Start time:	19:35:49
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\K0bg9rZl2L.exe' -Force
Imagebase:	0x1050000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7100 Parent PID: 7060

General

Start time:	19:35:50
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: K0bg9rZl2L.exe PID: 1316 Parent PID: 6860

General

Start time:	19:35:51
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\K0bg9rZl2L.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\K0bg9rZl2L.exe
Imagebase:	0x5a0000
File size:	17920 bytes
MD5 hash:	699E56EA4DA0B0865FC33308A8B09DF9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.916660808.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.914072243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.914072243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021