

ID: 432839
Sample Name: Current-Status-062021-81197.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:29:54
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Current-Status-062021-81197.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Persistence and Installation Behavior: 5
Boot Survival: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 15
General 15
File Icon 15
Static OLE Info 16
General 16
OLE File "Current-Status-062021-81197.xlsb" 16
Indicators 16
Macro 4.0 Code 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTPS Packets 16
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: EXCEL.EXE PID: 7076 Parent PID: 800 17
General 17
File Activities 18
File Created 18
File Deleted 18
File Written 18
Registry Activities 18
Key Created 18
Key Value Created 18
Analysis Process: WMIC.exe PID: 2460 Parent PID: 7076 18
General 18
File Activities 18

File Written 18
Analysis Process: conhost.exe PID: 352 Parent PID: 2460 18
General 18
Analysis Process: SettingSyncHost PID: 1808 Parent PID: 5060 19
General 19
File Activities 19
File Created 19
File Read 19
Disassembly 19
Code Analysis 19

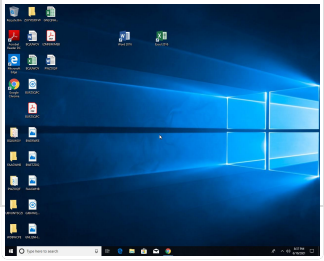
Analysis Report Current-Status-062021-81197.xlsb

Overview

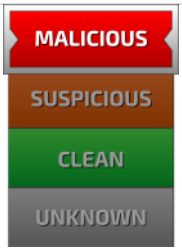
General Information

Sample Name:	Current-Status-062021-81197.xlsb
Analysis ID:	432839
MD5:	1ac719c744d22f4..
SHA1:	4ddc7358f615987.
SHA256:	d9be275feff4b33…
Infos:	

Most interesting Screenshot:



Detection



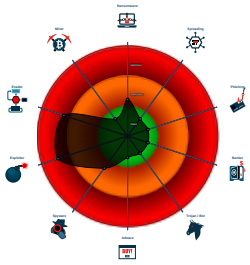
Hidden Macro 4.0

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

Signatures

- Document exploit detected (drops P…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Contains functionality to create proc…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found abnormal large hidden Excel …
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7076 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 2460 cmdline: wmic process call create 'C:/Users/Public/SettingSyncHost' MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SettingSyncHost (PID: 1808 cmdline: C:/Users/Public/SettingSyncHost MD5: 526D56017EF5105277FE0D366C95C39D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Copyright Joe Security LLC 2021

Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:



Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Contains functionality to create processes via WMI

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Persistence and Installation Behavior:



Creates processes via WMI

Boot Survival:



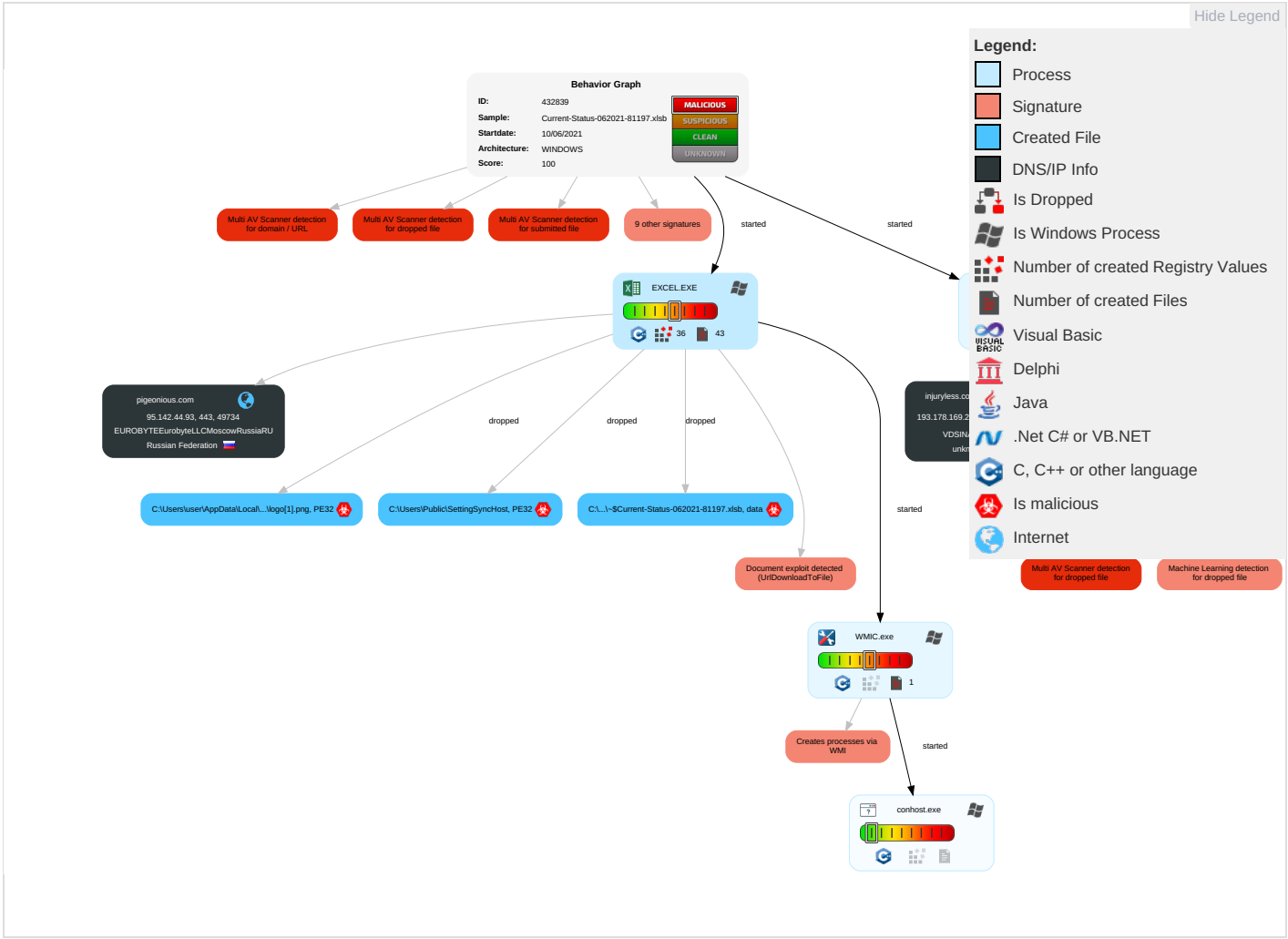
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 2 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Process Injection 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Command and Scripting Interpreter 2	Network Logon Script	Network Logon Script	Masquerading 1 2 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 2	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 2	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 Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols

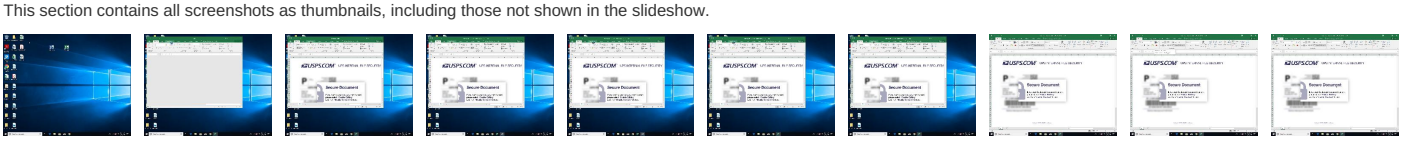
Behavior Graph

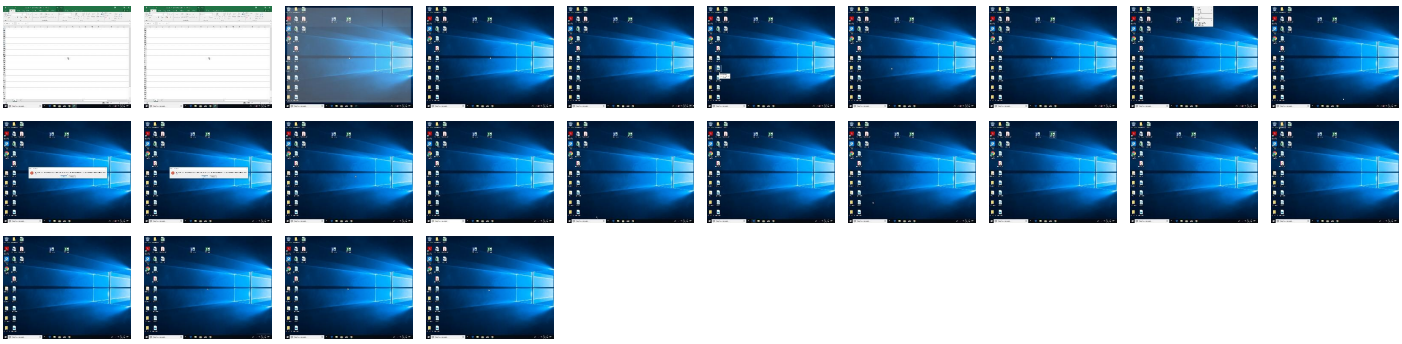


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Current-Status-062021-81197.xlsb	8%	Virustotal		Browse
Current-Status-062021-81197.xlsb	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png	100%	Joe Sandbox ML		
C:\Users\Public\SettingSyncHost	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\Public\SettingSyncHost	17%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png	17%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
injuryless.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588/3	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588z2	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://injuryless.com/rosoft	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588I3	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588.	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA15881	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA15887	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://injuryless.com/	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588G	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://injuryless.com/icies	0%	Avira URL Cloud	safe	
http://https://injuryless.com/11.10.3.41.3.6.1.4.1.311.10.3.12	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588Z	0%	Avira URL Cloud	safe	
http://https://injuryless.com/id=124406_ECF4BBEA1588p	0%	Avira URL Cloud	safe	
http://https://injuryless.com/X	0%	Avira URL Cloud	safe	
http://https://injuryless.com/id=124406_ECF4BBEA1588	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588m	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://injuryless.com/?id=124406_ECF4BBEA1588m2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
injuryless.com	193.178.169.243	true	true	• 8%, Virustotal, Browse	unknown
pigeonious.com	95.142.44.93	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.178.169.243	injuryless.com	unknown	?	48282	VDSINA-ASRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.142.44.93	pigeonious.com	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432839
Start date:	10.06.2021
Start time:	20:29:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Current-Status-062021-81197.xlsb
Cookbook file name:	defaultwindowsofficecookbook.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:	22
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.expl.evad.winXLSB@5/8@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 35.3% (good quality ratio 32.5%) • Quality average: 82.1% • Quality standard deviation: 30.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:30:52	API Interceptor	1x Sleep call for process: WMIC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.178.169.243	logo.png.exe	Get hash	malicious	Browse	
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	
	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	
95.142.44.93	3F97s4aQjB.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pigeonious.com	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 95.142.44.93
injuryless.com	logo.png.exe	Get hash	malicious	Browse	• 193.178.169.243
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 193.178.169.243
	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	• 193.178.169.243

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VDSINA-ASRU	logo.png.exe	Get hash	malicious	Browse	• 193.178.169.243
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 193.178.169.243
	uew5jAHqCT.exe	Get hash	malicious	Browse	• 109.234.38.213
	APPkj4zf3F.exe	Get hash	malicious	Browse	• 94.103.93.224
	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	• 193.178.169.243
	N1LUjx76rV.exe	Get hash	malicious	Browse	• 109.234.35.229
	0izHwHXyfm.exe	Get hash	malicious	Browse	• 109.234.35.229
	gtJl8IPauk.exe	Get hash	malicious	Browse	• 109.234.35.229
	tAL6n3gs6p.exe	Get hash	malicious	Browse	• 109.234.35.229
	f1GoI1S7Qi.exe	Get hash	malicious	Browse	• 94.103.93.224
	SecuriteInfo.com.Troj.Kryptik-TR.10844.exe	Get hash	malicious	Browse	• 193.178.170.41
	SecuriteInfo.com.Troj.Kryptik-TR.30930.exe	Get hash	malicious	Browse	• 193.178.170.41
	S5.exe	Get hash	malicious	Browse	• 62.113.114.79
	A5A2471193648C16E45C9C053C8672A3F71F21862388C.exe	Get hash	malicious	Browse	• 94.103.85.106
	PZ33n8HQNu.exe	Get hash	malicious	Browse	• 62.113.119.33
	VofcOsB5QO.exe	Get hash	malicious	Browse	• 94.103.86.101
	8vH1bonSn8.exe	Get hash	malicious	Browse	• 94.103.86.101
	87PLLTuhpG.exe	Get hash	malicious	Browse	• 178.208.83.27
	AC09B75D9728CEA73319605AEE734B0B776E2D1677914.exe	Get hash	malicious	Browse	• 195.2.78.227
	file3.exe	Get hash	malicious	Browse	• 62.113.117.9
EUROBYTEEurobyteLLCMoscowRussia RU	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 95.142.44.93
	template-jn02b3.dot	Get hash	malicious	Browse	• 95.142.40.220
	PREMIUM FINANCE AGREEMENT.docx	Get hash	malicious	Browse	• 95.142.40.241
	PREMIUM FINANCE AGREEMENT.docx	Get hash	malicious	Browse	• 95.142.40.220
	l8Cu5Vky6C.xls	Get hash	malicious	Browse	• 185.154.52.100
	l8Cu5Vky6C.xls	Get hash	malicious	Browse	• 185.154.52.100
	PooYhdlQZY.xls	Get hash	malicious	Browse	• 185.154.52.100
	PooYhdlQZY.xls	Get hash	malicious	Browse	• 185.154.52.100
	sUeyYgEiCb.xls	Get hash	malicious	Browse	• 185.154.52.100
	794c5aa1_by_Libranalysis.exe	Get hash	malicious	Browse	• 185.105.109.19
	njAzoIkDJu.exe	Get hash	malicious	Browse	• 185.105.109.19
	U92T8qzIbi.exe	Get hash	malicious	Browse	• 185.105.109.19
	rUUR0qQI22.exe	Get hash	malicious	Browse	• 185.105.109.19
	scan_DHL39382493.exe	Get hash	malicious	Browse	• 185.105.109.34
	3UiiwuZ4YR.exe	Get hash	malicious	Browse	• 95.142.44.135
	5WIxZYV73V.exe	Get hash	malicious	Browse	• 185.105.109.19
	0anROWjIhR.exe	Get hash	malicious	Browse	• 185.105.109.19
	fast.exe	Get hash	malicious	Browse	• 185.105.109.19
	kinsing2	Get hash	malicious	Browse	• 185.154.53.140
	kinsing	Get hash	malicious	Browse	• 185.154.53.140

JA3 Fingerprints

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	logo.png.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	ATT00005.htm	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	iX22xMeXIc.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	QWkt5w3cO2.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	vTtOheCXBQ.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	Check 57549.Html	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	audit-78958169.xlsb	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	Docc.html	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	askinstall39.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	Lista e porosive.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	askinstall39.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	SecuriteInfo.com.Trojan.GenericKD.46459351.411.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	YI6482CO6U.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	ZmZvKByoew.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\SettingSyncHost	3F97s4aQjB.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png	3F97s4aQjB.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\SettingSyncHost

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Copyright Joe Security LLC 2021

C:\Users\Public\SettingSyncHost

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	511488
Entropy (8bit):	7.3404073760047375
Encrypted:	false
SSDEEP:	12288:cyLjvFCsHOFO7t8BmzXiDm/znL2wOhlYuGUoPavYWIJdvrQoDptkYIN:BLDFTHOF0anwGYuGDQ2vQoDk5N
MD5:	526D56017EF5105277FE0D366C95C39D
SHA1:	78A40D523F4B887B2383681FECE447EF911C24EF
SHA-256:	28F2FA4F9AC95C3FC906E201B758D56C6A888B657DCF57C351A4F34FFB3E0FE2
SHA-512:	F2DC53598455B422B6B53108E94229B0F5791AC25188F0ED73FB4BFF1DF018B745F1F73714E97CF4E1C52475473326C1C91DC6070D331080F1FAAF696D58841E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: 3F97s4aQjB.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.........p...,...,...,...,...,...,...,...,...,...,...,...,...,...).,...,...,...,...,...,Rich...,................ ........PE..L......`....................~......#............@.........................P............@.....................................(.......6................... ............................................................................ .......text...9.......................... ..`.rdata.............................@..@.data...\|....p.......X.............@....idata..............r.............@....rsrc...6...........~.............@..@.reloc...#... ...$...... ....@..B.. ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\091AD497-E671-4FDF-8396-74EDF92EBBCF

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134922
Entropy (8bit):	5.369119258003808
Encrypted:	false
SSDEEP:	1536:4cQIKNEeBXA3gBwlpQ9DQW+z7534ZliKWXboOilX5ENLWME9:gEQ9DQW+ziXOe
MD5:	042D3F746892226A7BE71431B6635EBD
SHA1:	A171A408788DD9EE855D4C87E960E98CF4C43ED0
SHA-256:	F0FF8798D6B5E8D85FADFF08F7A9974F0843DF23BE340F28B886C9E84F0BB6FC
SHA-512:	9AAF01336D99A1754C9C1B5AB6AEA9402CC2FB9B821656FBF4FBDF8DD9912BB805526D6974AB4F650D293A2D33779B9C16BEAB621E404CE8EF2A29E7AD9F8E 40
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-10T18:30:47">.. Build: 16.0.14209.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\49018F97.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 2186 x 1539, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	462772
Entropy (8bit):	7.968569347884841
Encrypted:	false
SSDEEP:	12288:yycQMfTEzs+VfqjROL5bgSj86X/5ARknBqrZsNAdee:yQMfYBVf1xBARkgaNyr
MD5:	5D1C907B7A28ED91D8A704A7CE928FAF
SHA1:	FA56635F0C2A6D93DABE3E0636DADEAECDFCE804
SHA-256:	AD72EF87E54764A13E87BBD446029F48D70114B120E6DA7025947B1D51554486
SHA-512:	52A22A801395A467AABC02B4C24236FCAC4197407FC0F5C4B0D9C79C8DFB9A5DD0D935C67A7730B7EBFCD80013967F392D48D6E697A09E684BCDC62F7DBB6 6
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR..............I.\....sRGB.........gAMA......a.....pHYs..!...!..........IDATx^...W.Y.7~...o=.33..&+..9.q.H..1..1.b..9+.P0G.E...T..$%.wk.......i..Y{.r.S....s..................!=......... ....UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z..... ....V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH............. h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=.............UH.............h..3............Z...............V!=...... ....UH.............h..3............Z...............V!=.............UH.............h..3............Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo[1].png

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	511488
Entropy (8bit):	7.3404073760047375
Encrypted:	false
SSDEEP:	12288:cyLjvFCsHOFO7t8BmzXiDm/znL2wOhlYuGUoPavYWIJdvrQoDptkYIN:BLDFTHOF0anwGYuGDQ2vQoDk5N
MD5:	526D56017EF5105277FE0D366C95C39D
SHA1:	78A40D523F4B887B2383681FECE447EF911C24EF
SHA-256:	28F2FA4F9AC95C3FC906E201B758D56C6A888B657DCF57C351A4F34FFB3E0FE2
SHA-512:	F2DC53598455B422B6B53108E94229B0F5791AC25188F0ED73FB4BFF1DF018B745F1F73714E97CF4E1C52475473326C1C91DC6070D331080F1FAAF696D58841E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: 3F97s4aQjB.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://pigeonious.com/img/logo.png
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.........p....,...,...,..,...,...,...,...,...,...,...,...,.).,...,..,...,...,...,Rich...,................ ........PE..L......`.....................~......#.............@..........................P............@......................................(.......6................... ................................................................................ .......text...9........................... ..`.rdata.............................@..@.data...\|....p.......X.............@....idata..............r.............@....rsrc...6...........~.............@..@.reloc...#... ...$...... ....@..B.. ....

C:\Users\user\AppData\Local\Temp\A6B40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1041070
Entropy (8bit):	7.855884638864563
Encrypted:	false
SSDEEP:	12288:Qp4WH4vcCRa6p1RtTycQMfTEzs+VfqjROL5bgSj86X/5ARknBqrZsNAde5:O4vdRa6p1Rt/QMfYBVf1xBARkgaNys
MD5:	A6832F006ECA34E5E7495F7A3B5ADC6B
SHA1:	801FE0D57B16BFF66056840CD47BEED33B4ABB5C
SHA-256:	8DE78336A3BD486ABFE0B3DF88EFC9AD8BF2A64BF309C7107565F16BF838F757
SHA-512:	F7CC6E711DB08682BF125388C1395696A9073A236BB8196647DA27A4B53F450373D3BC52A1EAFCDB017108845450A469FFA14E1859DA419FE18135E3C7FD0EBF
Malicious:	false
Reputation:	low
Preview:	.T.n.0....?..........C....I?`M.%.|..$..w);n..V.....;3;...f.l...L.jf.B..6.k.....QQ.......".......6"U...}...zt@M..9...A.....j......T.g....C,..q.O6W..^.)Y./.o.}.....5.2...^.!..je...C7.....1;..d.1=`.\..y.3 ....qEsY?....4.{....J..D.d.N0..i..y?....X.C.w..-...%..2.us.....B...5.T.....9..*<.4..RI...)...GhJASY.......DG.k.rx........B.[...O.T...c.!.~..@....7.....H.......:....>.H<..Nw...Kv...S6x..c.t`. i....2N5.#.r..........PK..........!..j0.............[Content_Types].xml ...(.. ....M

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$Current-Status-062021-81197.xlsb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165

Copyright Joe Security LLC 2021

C:\Users\user\Desktop\~$Current-Status-062021-81197.xlsb	
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.083203110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1Mgjd330qJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/eg1deAin
MD5:	C62814DB19512E50685CCD10C45F4557
SHA1:	91CB5A204B91F9F81D791B07AACBE4CB2A79CC85
SHA-256:	FBDC5DD1D2DA5FEACF83F4FF1781A49DEDA141E18E33326B92B66D8D49C6725F
SHA-512:	7608BF46F85343150B8B4BD37FD994EEE0CE3D61BF5613A8D1DD3C93DD2B11E63190D419140DFE5A7AFED08E88C8B3C592E5241E4C048E6D670747A522B1D4D
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 1808;...ReturnValue = 0;..};....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.994144310692157
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.73% • Excel Microsoft Office Open XML Format document (40004/1) 41.88% • ZIP compressed archive (8000/1) 8.38% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Current-Status-062021-81197.xlsb
File size:	468533
MD5:	1ac719c744d22f42e4978e7b55828435
SHA1:	4ddc7358f615987bf92ed9192430693db65b097c
SHA256:	d9be275feff4b3383821b1483ba93424fb27aa40e138da41a91511193d9538cb
SHA512:	736bcf96ca99c893c535c555133a092400e1dbc5f5143500d152c537bccc9d3faf7d541b3b11be82b68bbf4c7a1528c5fa3b45394d5b2b958c4d1d4d024e7d22
SSDEEP:	12288:ag+iWCVTHlJFnI6TDEeTSH/NJDjXcXdeanuxZ2:4iVVTHxNcoSJDK1nuxA
File Content Preview:	PK.....R.....docProps/PK.....!.,.....docProps/app.xml.S.N.0.....`.N...Zu.#T.XQ.....u&.EbG.....m.ZNp{3o....."-8....x.Q.F.\.ML.....x.&..5...xz-...Kg.p... a|LK.f..W%....m.SXWK...0[.Z..U.5.d.Qt.`.`r./.^..)N[..hn.....vM...

File Icon



Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Current-Status-062021-81197.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 20:30:50.593030930 CEST	192.168.2.4	8.8.8.8	0xf09c	Standard query (0)	pigeonious.com	A (IP address)	IN (0x0001)
Jun 10, 2021 20:30:54.151655912 CEST	192.168.2.4	8.8.8.8	0xc717	Standard query (0)	injuryless.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 20:30:50.654596090 CEST	8.8.8.8	192.168.2.4	0xf09c	No error (0)	pigeonious.com		95.142.44.93	A (IP address)	IN (0x0001)
Jun 10, 2021 20:30:54.212208986 CEST	8.8.8.8	192.168.2.4	0xc717	No error (0)	injuryless.com		193.178.169.243	A (IP address)	IN (0x0001)
Jun 10, 2021 20:35:24.996901989 CEST	8.8.8.8	192.168.2.4	0x725c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

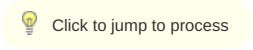
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 20:30:50.816432953 CEST	95.142.44.93	443	192.168.2.4	49734	CN=pigeonious.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jun 08 15:19:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 06 15:19:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 10, 2021 20:30:54.346164942 CEST	193.178.169.243	443	192.168.2.4	49739	CN=injuryless.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 27 15:42:29 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 25 15:42:29 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 7076 Parent PID: 800

General

Start time:	20:30:45
Start date:	10/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1150000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 2460 Parent PID: 7076

General

Start time:	20:30:51
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create 'C:/Users/Public/SettingSyncHost'
Imagebase:	0x60000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 352 Parent PID: 2460

General

Start time:	20:30:51
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000

Copyright Joe Security LLC 2021

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: SettingSyncHost PID: 1808 Parent PID: 5060

General

Start time:	20:30:52
Start date:	10/06/2021
Path:	C:\Users\Public\SettingSyncHost
Wow64 process (32bit):	true
Commandline:	C:/Users/Public/SettingSyncHost
Imagebase:	0x390000
File size:	511488 bytes
MD5 hash:	526D56017EF5105277FE0D366C95C39D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021