ID: 432818
Sample Name: 3F97s4aQjB.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:28:46
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

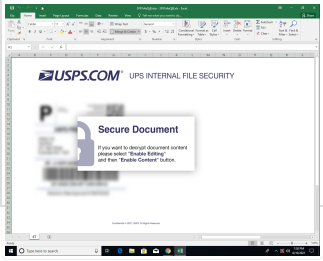
Analysis Report 3F97s4aQjB.xlsx

Overview

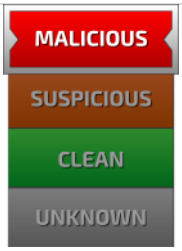
General Information

Sample Name:	3F97s4aQjB.xlsx
Analysis ID:	432818
MD5:	1ac719c744d22f4..
SHA1:	4ddc7358f615987.
SHA256:	d9be275feff4b33…
Infos:	

Most interesting Screenshot:



Detection



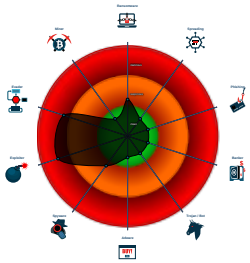
Hidden Macro 4.0

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

Signatures

- Document exploit detected (drops P…
- Multi AV Scanner detection for doma…
- 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…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6564 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 6852 cmdline: wmic process call create 'C:/Users/Public/SettingSyncHost' MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SettingSyncHost (PID: 7044 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

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

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:

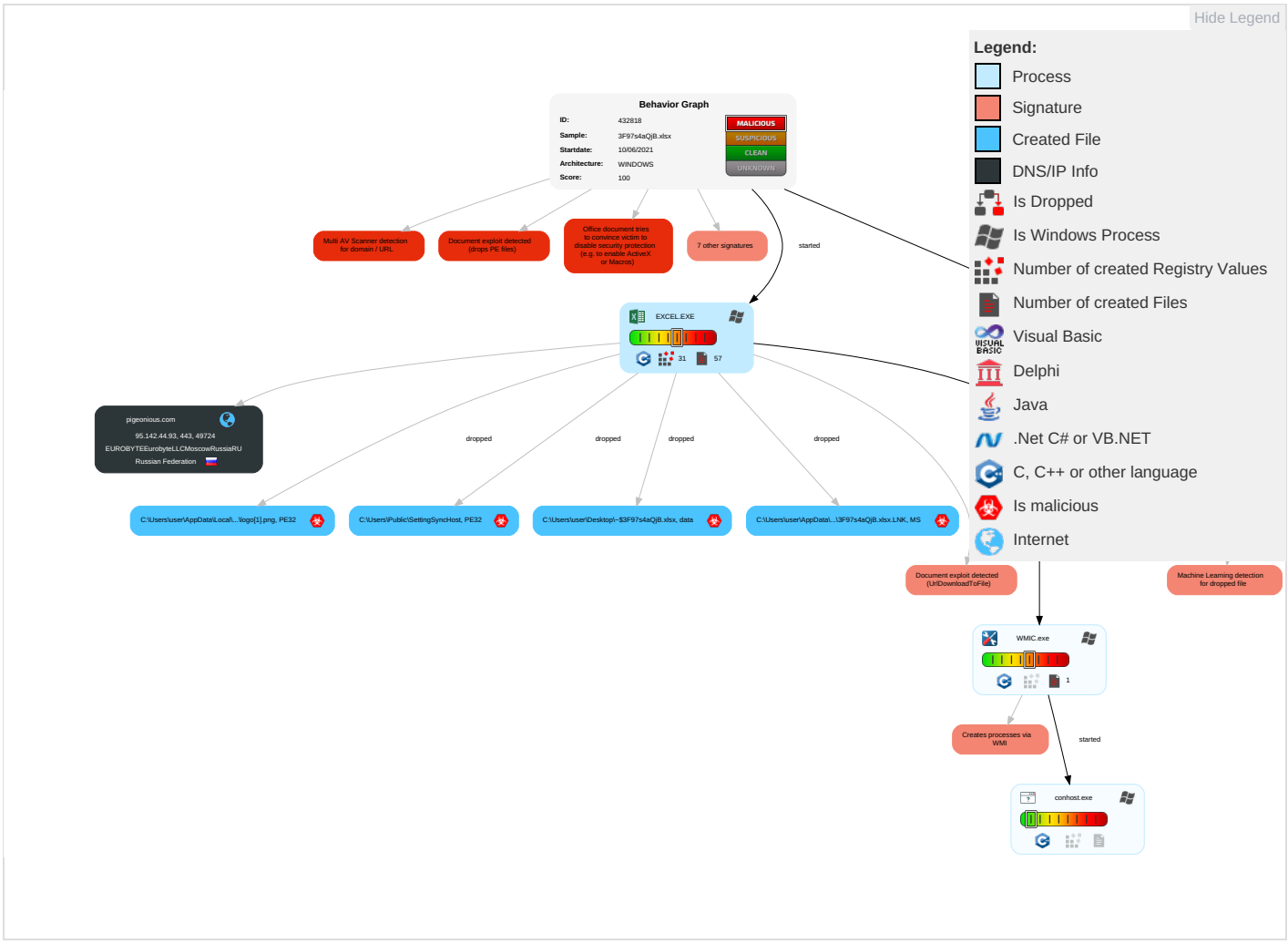
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	Native API 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statior

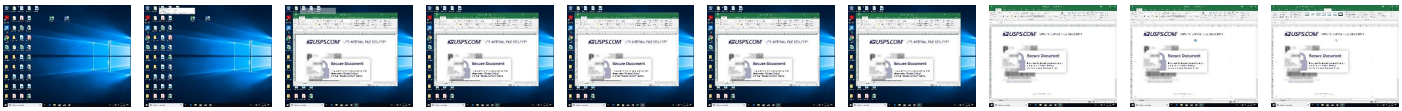
Behavior Graph

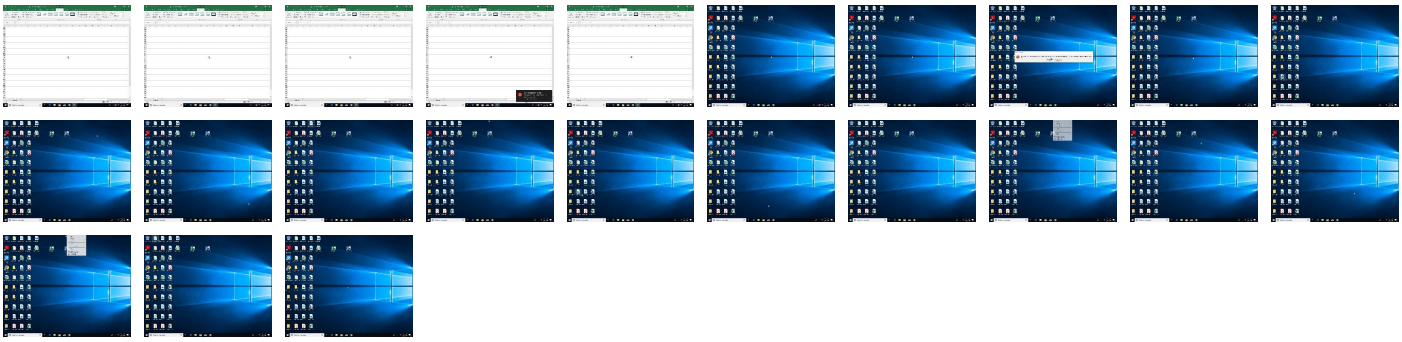


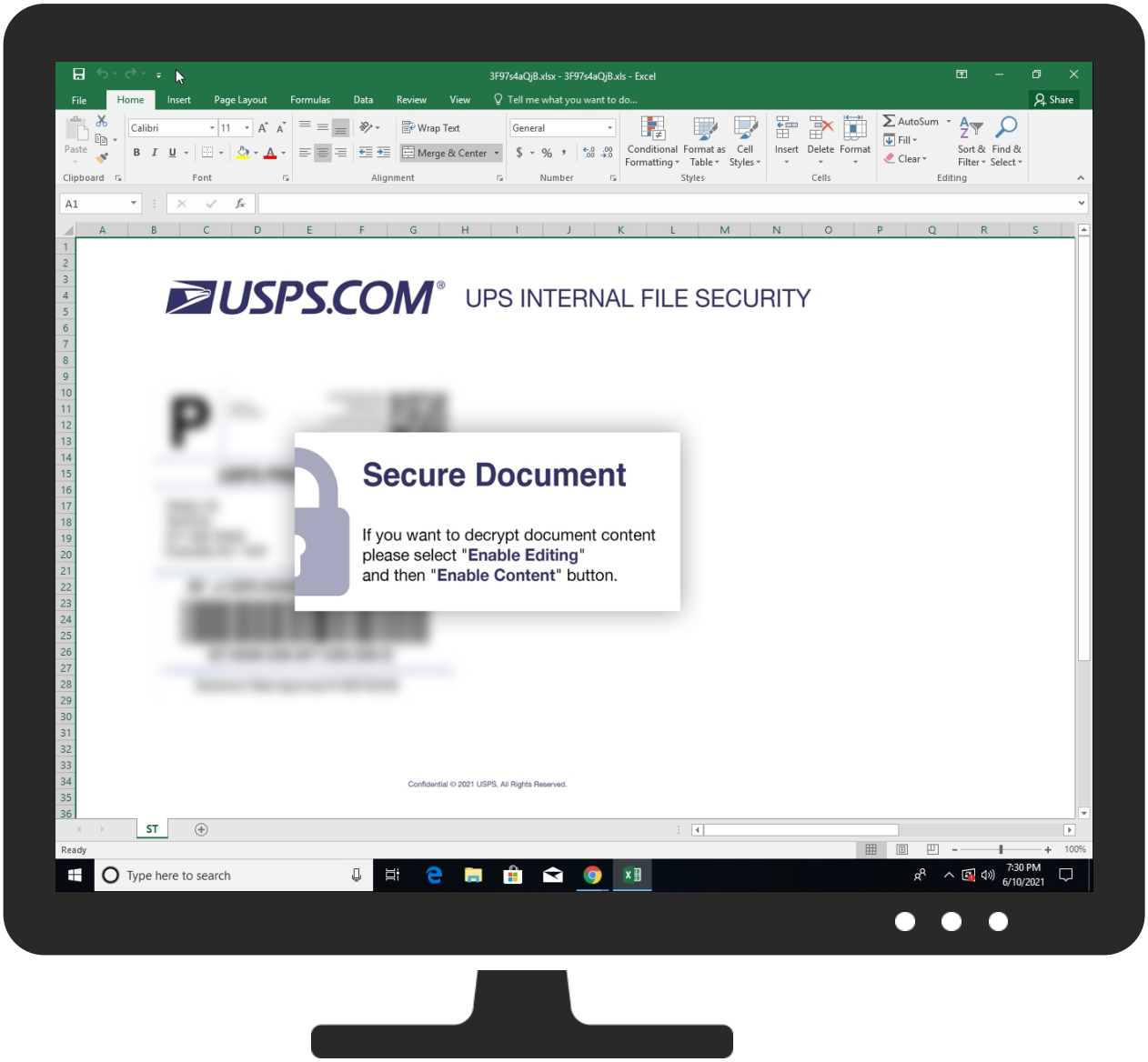
Screenshots

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
3F97s4aQjB.xlsx	7%	Virustotal		Browse
3F97s4aQjB.xlsx	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo[1].png	100%	Joe Sandbox ML		
C:\Users\Public\SettingSyncHost	100%	Joe Sandbox ML		

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://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://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://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
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://https://store.office.cn/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://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://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
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://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	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://ncus.contentsync.	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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	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://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	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
95.142.44.93	pigeonious.com	Russian Federation		210079	EUROBYTEEurobyteLLCMoscowRussiaRU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432818
Start date:	10.06.2021
Start time:	19:28:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3F97s4aQjB.xlsx
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:	38
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.winXLSX@5/12@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 53.5% (good quality ratio 49.2%) • Quality average: 82.5% • Quality standard deviation: 30.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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
19:29:44	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	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
injuryless.com	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	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
	6a867c08_by_Libranalysis.exe	Get hash	malicious	Browse	• 94.103.86.101
	3ef7f0d9_by_Libranalysis.exe	Get hash	malicious	Browse	• 62.113.117.9
EUROBYTEEurobyteLLCMoscowRussia RU	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
	WVaiL4J4cc.exe	Get hash	malicious	Browse	• 185.105.109.19

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	WcCEh3dalE.xls	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.169.243
	ATT00005.htm	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.169.243
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.169.243
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.169.243

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	V2GC02n03l.exe	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243
	research-1315978726.xlsb	Get hash	malicious	Browse	• 95.142.44.93 • 193.178.16 9.243

Dropped Files

No context

Created / dropped Files

C:\Users\Public\SettingSyncHost	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	511488
Entropy (8bit):	7.3404073760047375
Encrypted:	false
SSDEEP:	12288:cyLjvFCsHOFO7t8BmzXiDm/znL2wOhlYuGUoPavYWlJdvrQoDptkYIN:BLDFTHOF0anwGYuGDQ2vQoDk5N
MD5:	526D56017EF5105277FE0D366C95C39D
SHA1:	78A40D523F4B887B2383681FECE447EF911C24EF
SHA-256:	28F2FA4F9AC95C3FC906E201B758D56C6A888B657DCF57C351A4F34FFB3E0FE2
SHA-512:	F2DC53598455B422B6B53108E94229B0F5791AC25188F0ED73FB4BFF1DF018B745F1F73714E97CF4E1C52475473326C1C91DC6070D331080F1FAAF696D58841E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\Public\SettingSyncHost

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\62CC7D8B-1994-4449-80B7-33F7D65A3F46

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):	5.369120137160444
Encrypted:	false
SSDEEP:	1536:6cQIKNEeBXA3gBwlpQ9DQW+z7534ZliKWXboOilX5ENLWME9:qEQ9DQW+ziXOe
MD5:	0A1F23FF748ABC83EE1A72CDC88321CC
SHA1:	4BC44446EB9EFC70B3906CCB9C2027CFB370DC9A
SHA-256:	A05BF9F74150184E3664C14A9B042AF23BB0A75DBA671DB351A1172FF550A47B
SHA-512:	6CE5A0DC7CB9A2749451DE3752DCF2E8A37CFDC6B19C53E79782CC00859C1E4333474641E76EE975EAA169CE136E9A4A7771532866437CDBE49DEA5E8EE704 E
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="2021-06-10T17:29:39">.. 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\96E7ABF8.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\WJ8I2OL4\logo[1].png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
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%
Reputation:	low
IE Cache URL:	http://https://pigeonious.com/img/logo.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\logo[1].png

<table>
<tr><td>Preview:</td><td>MZ......................@..!..L.!This program cannot be run in DOS mode....$.........p....,...,...,..,...,...,...,...,...,...,...,...,.).,...,..,...,...,Rich...,................
........PE..L......`.....................~......#.............@..........................P............@.....................................(.......6................... ...............................................................................<br>.......text...9.......................... ..`.rdata.............................@..@.data...|....p.......X.............@....idata..............r.............@....rsrc...6...........~.............@..@.reloc...#... ...$......
............@..B...
...........................</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\9B810000

<table>
<tr><td>Process:</td><td>C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1041071</td></tr>
<tr><td>Entropy (8bit):</td><td>7.855849071117974</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12288:Ip4WH4vcCRa6p1RtTycQMfTEzs+VfqjROL5bgSj86X/5ARknBqrZsNAde+:G4vdRa6p1Rt/QMfYBVf1xBARkgaNyt</td></tr>
<tr><td>MD5:</td><td>E20BC69C6969DDBF5D19950216EBCC79</td></tr>
<tr><td>SHA1:</td><td>60809A68836DCE9E7B5959B9D975427C3DDE0122</td></tr>
<tr><td>SHA-256:</td><td>FDED8F0DDE8CF5DEACFB80DE6420A3CCD4F30971ACC364FF9DB855DE3D86AA4A</td></tr>
<tr><td>SHA-512:</td><td>C48879E97FC9DBBFA30C8554A1B21BC8D36B080F4AD6D4C0223C5F994C47BE4986ECEEBA038E4617EF4D8D65106E21FEA79042997BF107F2921828B35DCEE1
D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>.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</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\3F97s4aQjB.xlsx.LNK

<table>
<tr><td>Process:</td><td>C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:43 2020, mtime=Fri Jun 11 01:29:42 2021, atime=Fri Jun 11 01:29:42 2021, length=1040132, window=hide</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>2120</td></tr>
<tr><td>Entropy (8bit):</td><td>4.714364232851571</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:8zNDaX/da9OUAJHaD0nKD7aB6myzNDaX/da9OUAJHaD0nKD7aB6m:8zNONJDnKaB6pzNONJDnKaB6</td></tr>
<tr><td>MD5:</td><td>B472516A8AC5D58E2AC16C39CD89EC38</td></tr>
<tr><td>SHA1:</td><td>8ADE9F104953A38DA6917729E309528DD86C2E7C</td></tr>
<tr><td>SHA-256:</td><td>3677EBF291B1C7954ADB892D9D37686C0520C71F33EFF9F8D305985E09D5E0AC</td></tr>
<tr><td>SHA-512:</td><td>4DFC0887B9E26EE12B7D70CD543C2C3105EE9753746005B86D520EBFC52C50E787818F42A05EC120FA1F52FB927AE7A93DAFA1FCD40624E1E8A29439683E5EE
0</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>L..................F.... ....2..:....Bm.i^....j.i^..............................P.O. .:i.....+00../C:\..................x.1......N....Users.d......L...R......................:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1
.8.1.3.....P.1.....>Qwx..user.<.......Ny..R.......S.....................].h.a.r.d.z.....~.1.....>Qxx..Desktop.h.......Ny..R.......Y.............>.........D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.
2.1.7.6.9.....l.2.5&...R.. .3F97S4~1.XLS..P......>Qvx.R......h........................3.F.9.7.s.4.a.Q.j.B...x.l.s.x.......U...............-.......T...........>.S......C:\Users\user\Desktop\
3F97s4aQjB.xlsx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.3.F.9.7.s.4.a.Q.j.B...x.l.s.x.........:..,.LB.)...As...`.......X.......035347...........!a..%.H.VZAj......-.........-..!a..%.H.VZAj......-.......
..-.............1SPS.XF.L8C....&.m.q.........../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9...1</td></tr>
</table>

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Fri Jun 11 01:29:41 2021, atime=Fri Jun 11 01:29:41 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.652208144122537
Encrypted:	false
SSDEEP:	12:8YrXUwcuElPCH2AaSY3ouIk+WrjAZ/2bD/LC5Lu4t2Y+xIBjKZm:8cDatAZiD+87aB6m
MD5:	86C3AEC66964F8B6866416E31E93962D
SHA1:	3C2C30D348DA6A080E03B52ED039E806F29420D2
SHA-256:	BC2C38396F73A0F45177582F64F18992E369E9955EAA89B3DB11823DB19FF1A0
SHA-512:	7F6EB1D91A178E2E39ABBE6560701395E4E9C6F5E1D0F3E4516E33A27D672EF3CB59756004835213BF5935B68946580A7346DD242648B8F61614EC081D103DA2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....N....-..NDN.i^..NDN.i^...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny..R.....S.....].h.a.r.d.z.....~.1.....R....Desktop.h.....Ny..R.....Y.....>.....".D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....035347.....!a..%.H.VZAj...4.4.... .....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	100
Entropy (8bit):	4.721266094754729
Encrypted:	false
SSDEEP:	3:oyBVomxWV2npWrXCMjD2npWrXCmxWV2npWrXCv:djlW3KWvWI
MD5:	4651D7899D0089D49B209C1EEFFC6F66
SHA1:	272A788D9B7814F71C0E53A39A8457512DD43BC2
SHA-256:	7DD3385C0FA67DE6A3477E1E63F4598339456786CC8C0E4B36F667A7D3BAB4FC
SHA-512:	93F4F6602DDC965678EB92C40E9C73174C52A2CBC8D111181744E646380B5E41F0197925086ED935B75D1C5627FBE684C373081B73404FC1CBCEB329959B9BC0
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..3F97s4aQjB.xlsx.LNK=0..3F97s4aQjB.xlsx.LNK=0..[misc]..3F97s4aQjB.xlsx.LNK=0..

C:\Users\user\Desktop\EC810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1040132
Entropy (8bit):	7.8545301896779085
Encrypted:	false
SSDEEP:	24576:lQPPPPPD5rIf8w195QMfYBVf1xBARkgaNyn:BQMQh/m6Nyn
MD5:	90305FD4215DD8A8785DC7F6DD4143A6
SHA1:	A90ED0830BF373E01681C2B491101CD5AF1904A2
SHA-256:	384AC8CE1FF6CF1E8DBDF47CE04898887D669811B982655881FD2FB6F8BCED4D
SHA-512:	50D827E068818BB082EB80487D4CF76C8D835CB6BEAA950F1A4BD6185C61F59F0F34328F3154CBA5274C49F3778878E315B173B5470D46482D674FD3BECB0851
Malicious:	false
Reputation:	low
Preview:	.T.N.0..#....(q..!...G@j...o...my...=kS...P.J\.3...&.....8[..b 2.....x.=."CRV..Y(..PL.....f\m.....:...`yg.B...C-.....9..nd.,...".....`.>Z..W.....X.....T.P..R.B...-.....0c...7.B..... 4]...wW.h.....W.V.1...=.qg.....`0..W..Yu.\....s..0H_3..E....}.?.F.^.g...K.=u..I.....[.`.4..n..=..z..Q.....g.....g. 7.....:..!...G.....X.{..@.~Cb.e.e.<y..SX...-S.....PK.....!...vR....6 .....[Content_Types].xml ...(..... ....MO.0...H.....BKwAH.!T~.I....

C:\Users\user\Desktop\~$3F97s4aQjB.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Desktop\~$3F97s4aQjB.xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330

C:\Users\user\Desktop\~$3F97s4aQjB.xlsx	
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..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:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MglVvlJQAiveyzowv:Yw7gJGWMXJXKSOdYiygKkXe/eg3leAin
MD5:	04F5182CC4DB0183A73CC7E970598ED7
SHA1:	B8E7038F8D7FA64B8FC04EFEBB0100998379C772
SHA-256:	BB316A44410761BABF389A30CA439E952E13C90178E4D3E9C54F45B83998EBE0
SHA-512:	C875CC61B3E6DBDACFD26D6FA0D28F134572D1C8EF955357A2C40BC3B6FF6A6637C325B0237D1DA7E281595A85197E74B54C7FC4FA57B17C9E09F7913A64C1 9
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 7044;...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:	3F97s4aQjB.xlsx
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:	74ecd0d2d6d6d0dc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "3F97s4aQjB.xlsx"

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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-19:29:51.613358	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 19:29:43.196017981 CEST	192.168.2.3	8.8.8.8	0x8251	Standard query (0)	pigeonious.com	A (IP address)	IN (0x0001)
Jun 10, 2021 19:29:46.281454086 CEST	192.168.2.3	8.8.8.8	0x8f87	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 19:29:43.256313086 CEST	8.8.8.8	192.168.2.3	0x8251	No error (0)	pigeonious.com		95.142.44.93	A (IP address)	IN (0x0001)
Jun 10, 2021 19:29:46.346998930 CEST	8.8.8.8	192.168.2.3	0x8f87	No error (0)	injuryless.com		193.178.169.243	A (IP address)	IN (0x0001)
Jun 10, 2021 19:30:56.051986933 CEST	8.8.8.8	192.168.2.3	0x5e57	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 19:34:21.744677067 CEST	8.8.8.8	192.168.2.3	0xdb4b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

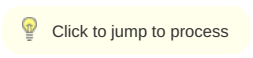
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 19:29:43.417321920 CEST	95.142.44.93	443	192.168.2.3	49724	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 19:29:46.487052917 CEST	193.178.169.243	443	192.168.2.3	49727	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: 6564 Parent PID: 792

General

Start time:	19:29:37
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:	0x12e0000
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: 6852 Parent PID: 6564

General

Start time:	19:29:43
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:	0x13c0000
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: 6860 Parent PID: 6852

General

Start time:	19:29:43
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 7044 Parent PID: 4940

General

Start time:	19:29:44
Start date:	10/06/2021
Path:	C:\Users\Public\SettingSyncHost
Wow64 process (32bit):	true
Commandline:	C:/Users/Public/SettingSyncHost
Imagebase:	0xf90000
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
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis