ID: 573118
Sample Name: _FM_BUSAN_HOCHIMINH_.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:18:10
Date: 16/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

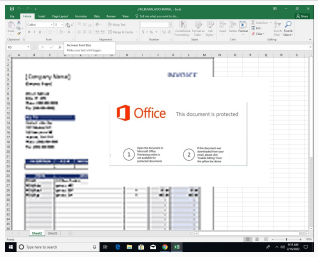
Windows Analysis Report

_FM_BUSAN_HOCHIMINH_.xlsx

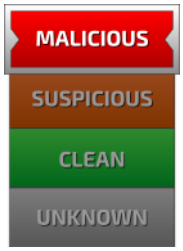
Overview

General Information

Sample Name:	_FM_BUSAN_HOCHIMINH_.xlsx
Analysis ID:	573118
MD5:	9d7bf0f2fbb8166..
SHA1:	7adf1d60fd08b3a.
SHA256:	d60188bc3e17e3..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection

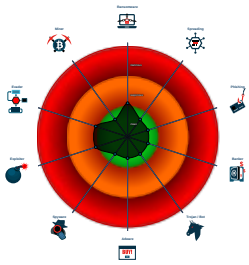


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince v…
- Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6700 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

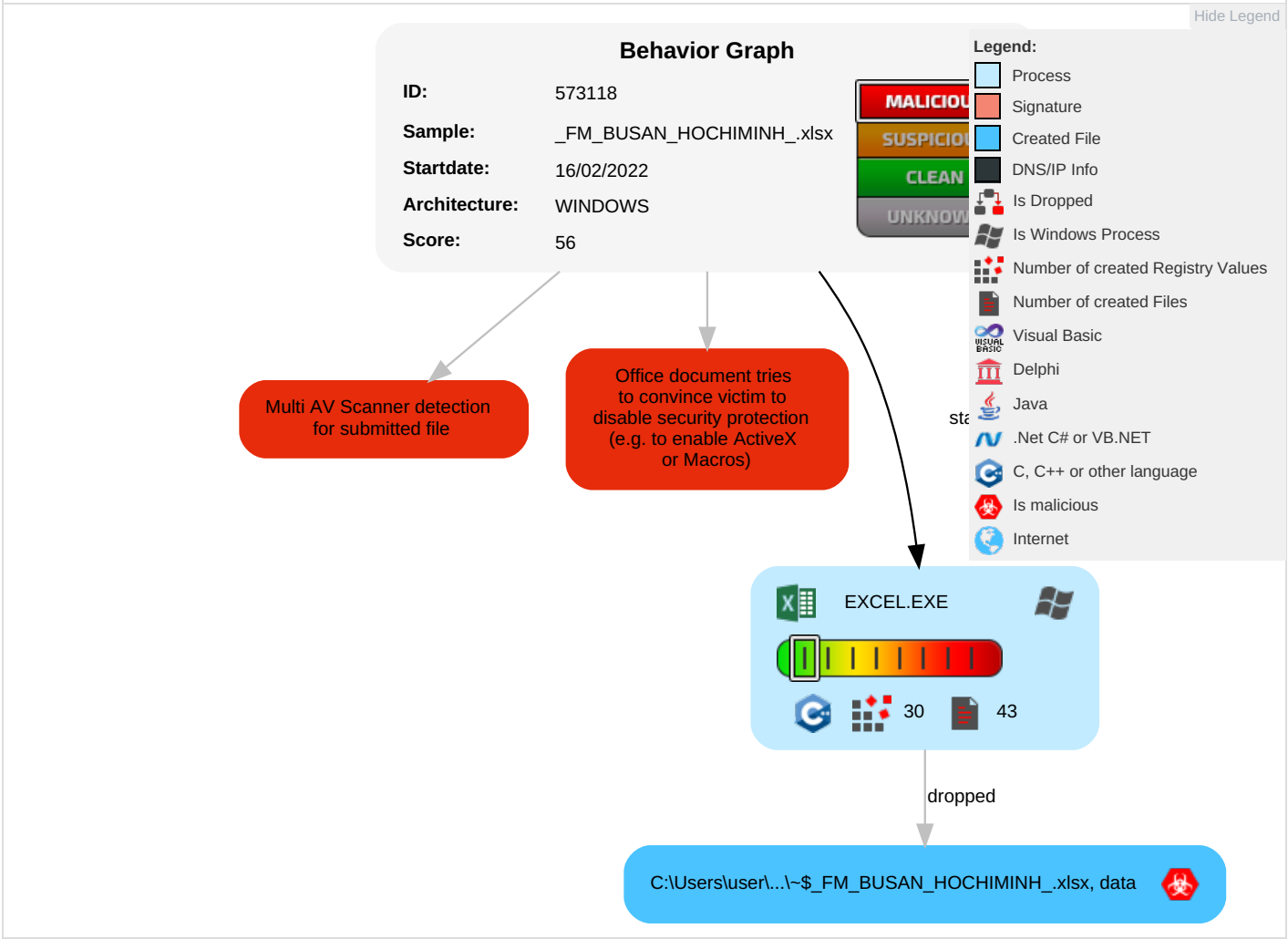
System Summary

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

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Extra Window Memory Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

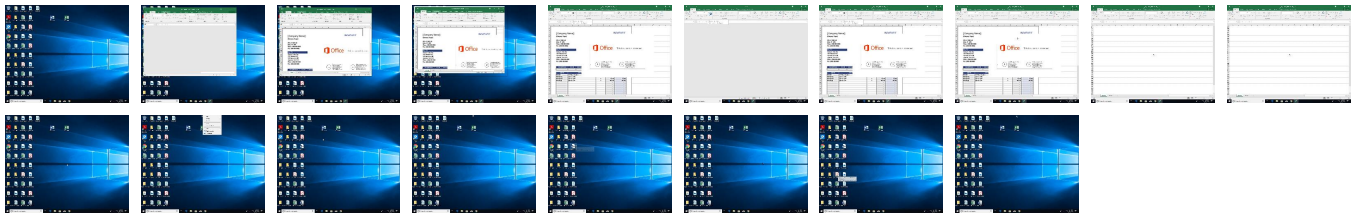
Behavior Graph

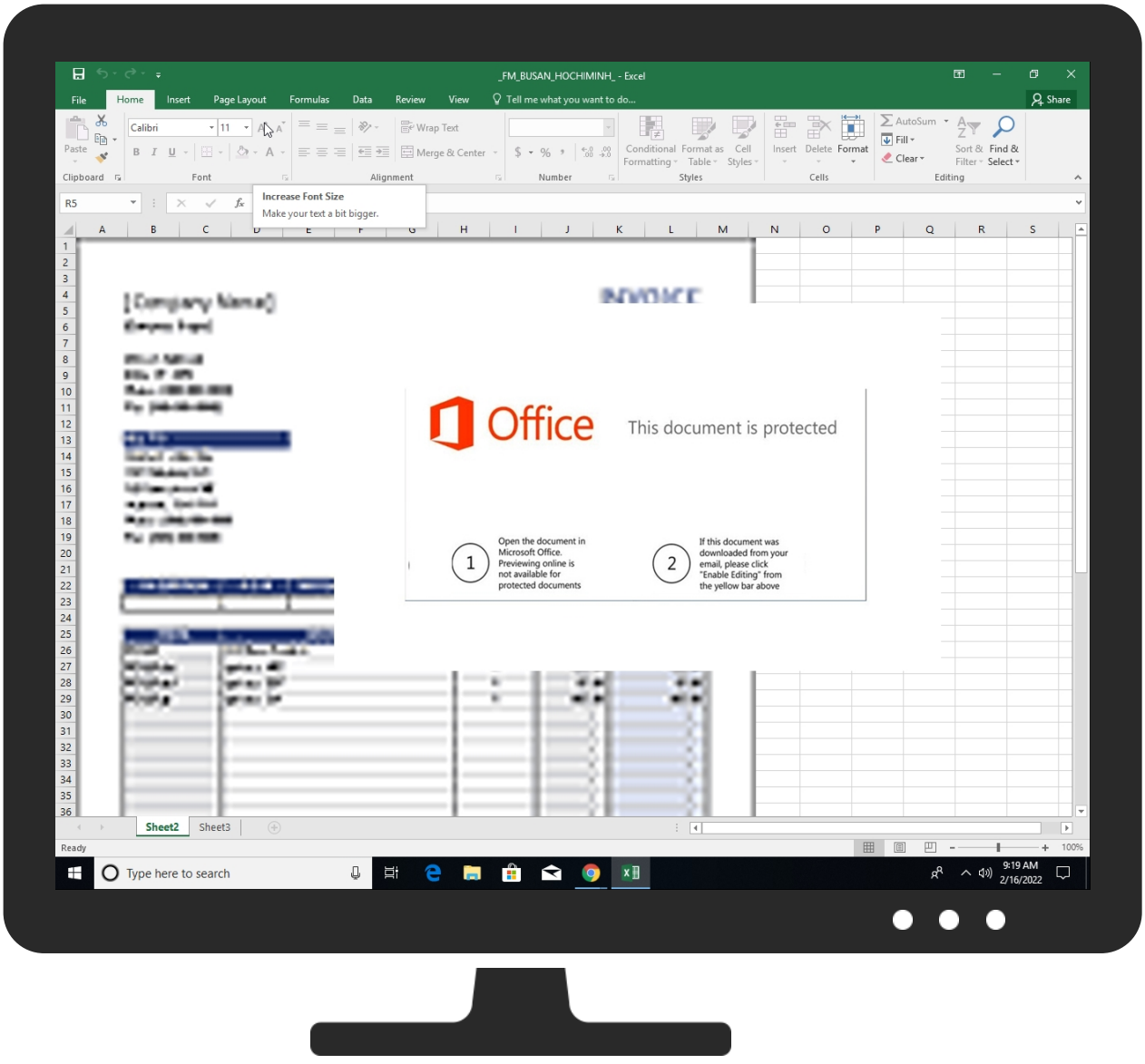


Screenshots

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
_FM_BUSAN_HOCHIMINH_.xlsx	38%	Virustotal		Browse
_FM_BUSAN_HOCHIMINH_.xlsx	36%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://ncus.contentsync.	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://asgsmsproxyapi.azurewebsites.net/	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://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://login.microsoftonline.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://shell.suite.office.com:1443	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://roaming.edog.	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://cdn.entity.	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://powerlift.acompli.net	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://cortana.ai	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://api.aadrm.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://api.microsoftstream.com/api/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://cr.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://graph.ppe.windows.net	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://store.office.cn/addinstemplate	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://web.microsoftstream.com/video/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.addins.store.officeppe.com/addinstemplate	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dataservice.o365filtering.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://ncus.contentsync.	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://weather.service.msn.com/data.aspx	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://apis.live.net/v5.0/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://management.azure.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://outlook.office365.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://wus2.contentsync.	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://api.office.net	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://entitlement.diagnostics.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://outlook.office.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://outlook.office365.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://webshell.suite.office.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://management.azure.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://devnull.onenote.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://ncus.pagecontentsync.	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://messaging.office.com/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://augloop.office.com/v2	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://skyapi.live.net/Activity/	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high
http://https://dataservice.o365filtering.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://api.cortana.ai	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com	7D1365BD-572E-4B01-B81C-338095DDB517.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	573118
Start date:	16.02.2022
Start time:	09:18:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	_FM_BUSAN_HOCHIMINH_.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	15
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:	mal56.winXLSX@1/19@0/0
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: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.32.63, 52.109.12.21, 52.109.8.23
- Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, config.officeapps.live.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7D1365BD-572E-4B01-B81C-338095DDB517

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):	143624
Entropy (8bit):	5.358424207530797
Encrypted:	false

SSDEEP:	1536:lcQIfgxrBdA3guwu/Q9DQW+zUk4F77nXmvidZXtE5LWm69:PaQ9DQW+zwXCe
MD5:	7BC9701D8DFD41989D9A51BC07EF6819
SHA1:	E4F74D848331B6B190CEF779DE93396718F6341E
SHA-256:	07018A0F9CA369FD8281C627981E95F33A6A68D13C8543625DD7C272470EADED
SHA-512:	590F30A4B3F6E2A0BED03346D94D24725CA5873BC375E3493BBAD752208573225B7F244E6BC4ADA54287888A134178C6627BE9810BB83191725B7E27FA43FC58
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="2022-02-16T08:19:10">.. Build: 16.0.15004.30525-->.. <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\243BBE31.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF... ....+!.$...2"3*7%"0...................".........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2EA1469F.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.............../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE............&f||}\\]..........5G}..._l....778...IDATx..]...<.nh........../)....;..~; .U..>.i.$..0*..QF@.)."..,.../._,.y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.......*......v;.R.a..i.B.......A.T`.....v....N..u.........NG......e....}.4=."{.+.."..7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t............G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR......b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4...........*.f..&X..V......#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.......5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t......m+....OI...........+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).......F.,m.......6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\37992E7E.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo

MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....|>...?299I&.!...:....nW.4...?.....|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3E7E5F3C.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,..<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5379E248.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!...:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\659B9067.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C

SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR.............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8....Y..............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.......O.....$2.=\|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7559DAF0.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG........IHDR............../....EPLTE......................o...ttu`aaLML.s;.../-,...............~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y.".\|.2A@y.../...X.X..X..2X.........o.Xz}go.*m..UT.DK...ukX.....t.%..iB......w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v......*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x.,....t.1..6.....}K).$.I.%n$b..G.g.w.....M..w..B.......tF".YtI..C.s.~)..<@"......-..._.(x...b..C.........;5.=.......c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8......HuYw.~X.+&Q.a.H.C..ly..X..a.?O.yS,C.r..........Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.......2.;..gNqH`...X..\...AS...@4...#.....!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N........@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC..........x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\92B388A3.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0..................."........................."..............#............"..!1."AQa..q.#2R....BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}},....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&...c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj.........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JLj]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D338BE0D.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false

Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~; .U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wu!{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E0A1A796.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y...<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E487A1EB.emf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015387492153731
Encrypted:	false
SSDEEP:	3072:w0Xtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cT:xahIFdyiaT2qtXl
MD5:	BE871EA2D026762E96E3DDBDB386F589
SHA1:	66FA5F1942CA698B189EA90C885C5A468B99A312
SHA-256:	EA25DD3B6161C5D8C8D4FE64B3D2105F158391DF08991A28ACD0D8B0A0D176C6
SHA-512:	8F54B12A5D00773223F3EE01132C1DF7F76FCFF3A4C53CAB121B9D619F1677F7A399E4687B0ED08E95F798F7746A8EE57B5F59D68A3483DBADCF7983E7CE1CF 2
Malicious:	false
Preview:	....l.....C.....m>..?$.. EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....y$...../..f.y.@.. %...../.(./...../.../.RQUQ../.../...../.p./.$QUQ../.../. ...Id.y../.../. .....,.6..d.y.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i...../.X...../.../..8.y.. ...,.6.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+* @..$.....?.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E4DFD4AA.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.l..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E6612DA9.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31lAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... (..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Temp\~DF41E48DC5999769CD.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191784
Entropy (8bit):	7.958202975592025
Encrypted:	false
SSDEEP:	3072:dnK3hkFr084G2tQX/WdCcsE7i9y6T9BSRIjDALPOWEW7eDy/wLyjjBvRhNasgKVT:c3K108GtC/uCcsjk6TWODA7heDvwa5y
MD5:	9D7BF0F2FBB81660C8B91C2A323FDE4E
SHA1:	7ADF1D60FD08B3ACCD3A8E58FBDCC674BD1B02EE
SHA-256:	D60188BC3E17E3FE9A8353A5EB4B791316968F3C1CEA1E4E88138718EFEC0611
SHA-512:	39842639F118D709102B7E8440CF569D542CA950F77DCA21615B74639AC3E1F50BF9901E4DEF0DF93D4ADDFE3F8DBC2A4E46E84CF56C85EC33C6F8D43E19F42
Malicious:	false
Preview:	.....>..... ....!...".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF46678429D5C1163F.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFCD447DFDBA0B9D87.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD9862BF895814717.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.958202975592025
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	_FM_BUSAN_HOCHIMINH_.xlsx
File size:	191784
MD5:	9d7bf0f2fbb81660c8b91c2a323fde4e
SHA1:	7adf1d60fd08b3accd3a8e58fbdcc674bd1b02ee
SHA256:	d60188bc3e17e3fe9a8353a5eb4b791316968f3c1cea1e4e88138718efec0611
SHA512:	39842639f118d709102b7e8440cf569d542ca950f77dca21615b74639ac3e1f50bf9901e4def0df93d4addfe3f8dbc2a4e46e84cf56c85ec33c6f8d43e19f462
SSDEEP:	3072:dnK3hkFr084G2tQX/WdCcsE7i9y6T9BSRIjDALPOWEW7eDy/wLyjjBvRhNasgKVT:c3K108GtC/uCcsjk6TWODA7heDvwa5y

File Content Preview:	.......................>...

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: EXCEL.EXE PID: **6700**, Parent PID: **800**

General

Target ID:	0
Start time:	09:19:08
Start date:	16/02/2022
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:	0x90000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx	0	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	1F51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx	55	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	pratesh	success or wait	1	1F5241	WriteFile
C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx	0	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	1F51E4	WriteFile
C:\Users\user\Desktop\~$_FM_BUSAN_HOCHIMINH_.xlsx	55	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	pratesh	success or wait	1	1F5241	WriteFile

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	1020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	10211C	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	10213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	10213B	RegSetValueExW

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

Disassembly

No disassembly