ID: 440505
Sample Name: Permission-414467145-06252021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:13:06
Date: 25/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

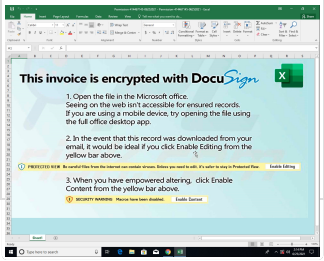
Windows Analysis Report Permission-414467145-06252…

Overview

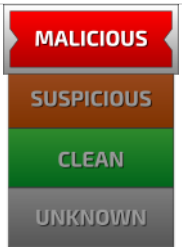
General Information

Sample Name:	Permission-414467145-06252021.xlsm
Analysis ID:	440505
MD5:	590ca0e597487d..
SHA1:	e141e27af930a2c.
SHA256:	20a72dc5350b29..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection



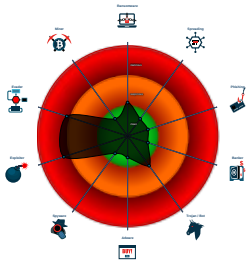
Hidden Macro 4.0

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Tries to load missing DLLs
- Uses a known web browser user age…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6876 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6160 cmdline: regsvr32 ..\Kro.fis MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5008 cmdline: regsvr32 ..\Kro.fis1 MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 3980 cmdline: regsvr32 ..\Kro.fis2 MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

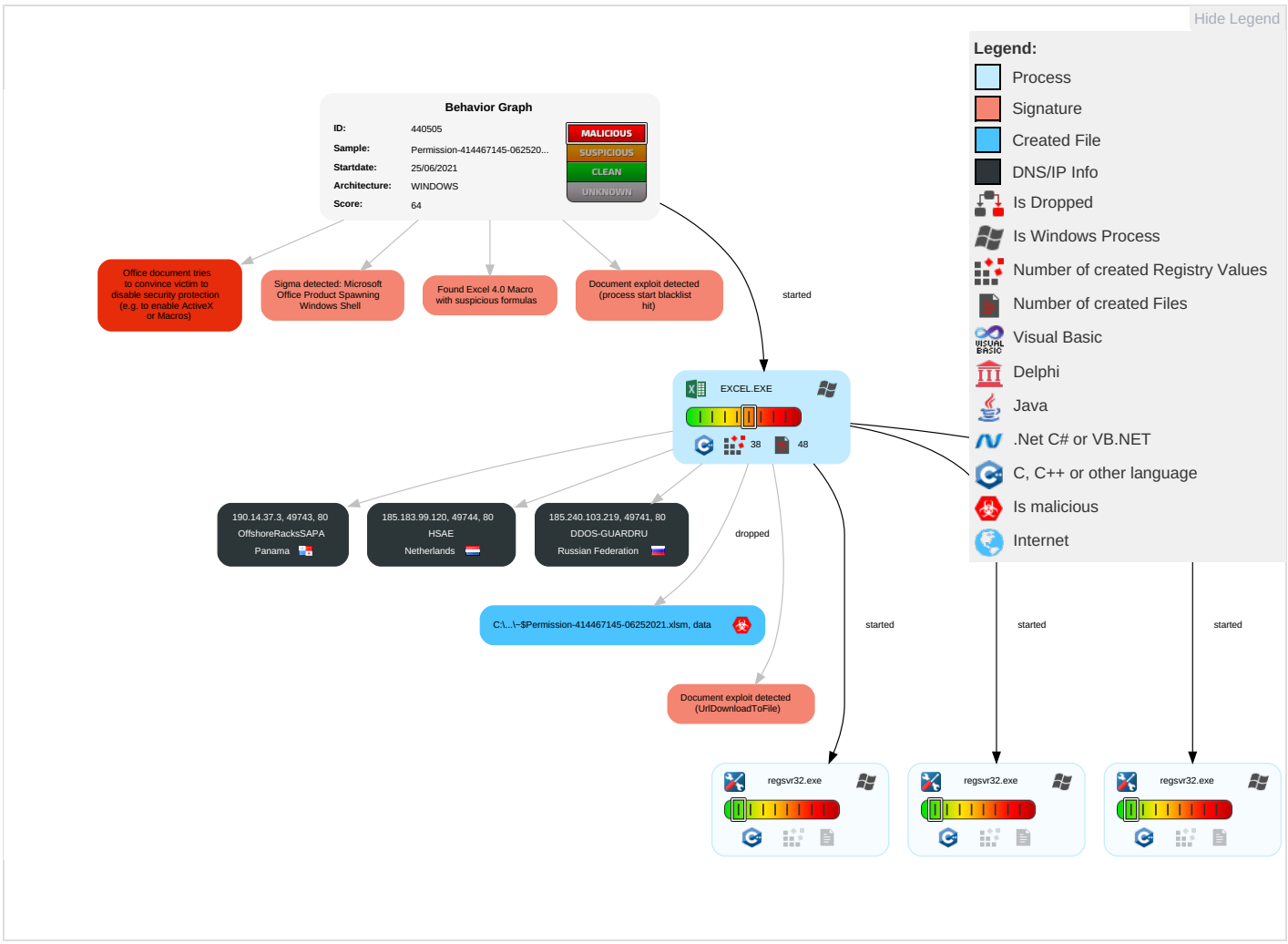
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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	Im
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

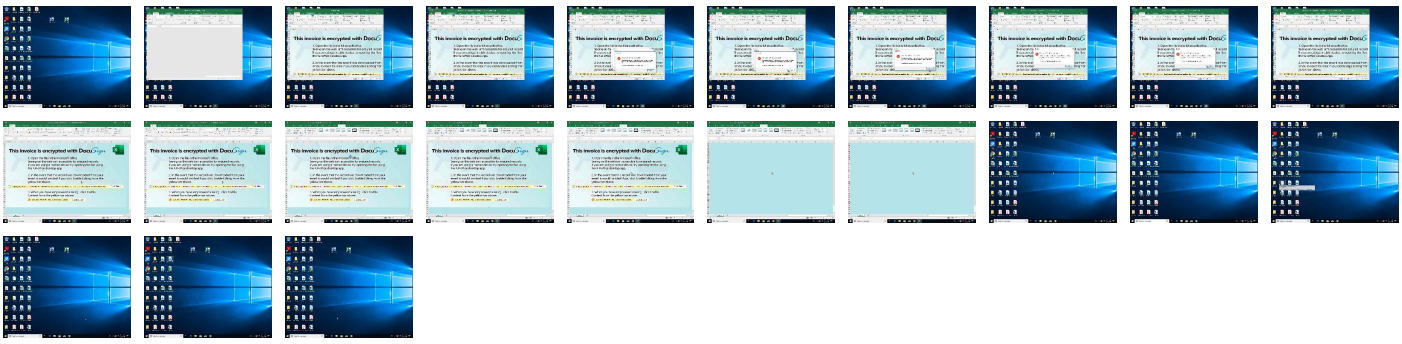
Behavior Graph

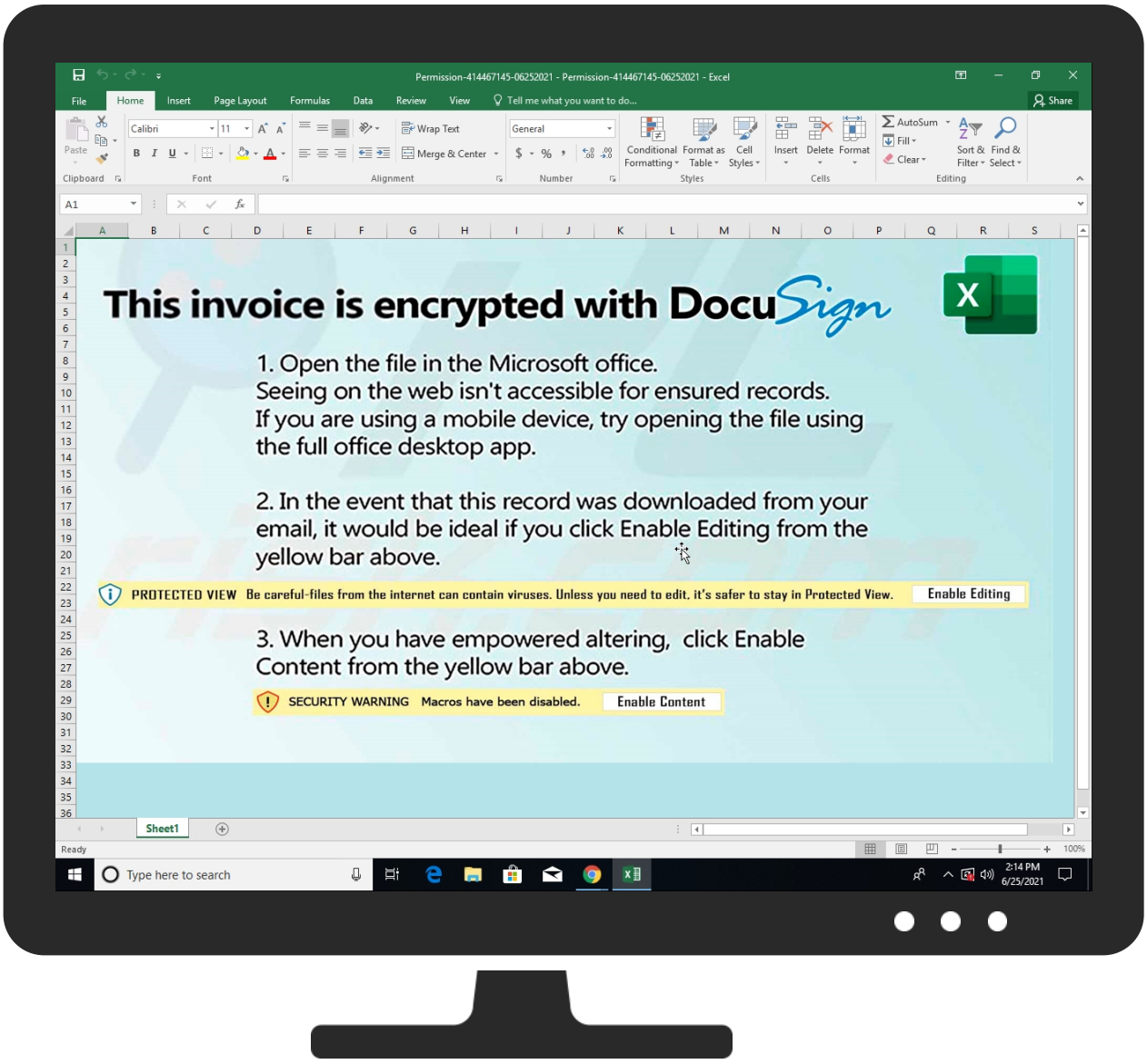


Screenshots

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
Permission-414467145-06252021.xlsm	5%	Virustotal		Browse
Permission-414467145-06252021.xlsm	4%	ReversingLabs	Document-Office.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.240.103.219/44372.593127662.dat	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

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://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://190.14.37.3/44372.593127662.dat	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%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.240.103.219/44372.593127662.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.3/44372.593127662.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.14.37.3	unknown	Panama		52469	OffshoreRacksSAPA	false
185.183.99.120	unknown	Netherlands		60117	HSAE	false
185.240.103.219	unknown	Russian Federation		57724	DDOS-GUARDRU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	440505

Start date:	25.06.2021
Start time:	14:13:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Permission-414467145-06252021.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:	21
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:	mal64.expl.evad.winXLSM@7/9@0/3
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
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
190.14.37.3	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	
185.183.99.120	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 185.183.99.120/44372.5879460648.dat
185.240.103.219	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219/44372.5879460648.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DDOS-GUARDRU	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 185.240.103.219
	Decline-172917164-06242021.xlsm	Get hash	malicious	Browse	• 5.253.62.174
	Decline-172917164-06242021.xlsm	Get hash	malicious	Browse	• 5.253.62.174
	ForceNitro.exe	Get hash	malicious	Browse	• 185.178.208.135
	PO#8076.exe	Get hash	malicious	Browse	• 185.129.100.112
	Cancellation_Letter_2137859823_06112021.xlsm	Get hash	malicious	Browse	• 185.240.103.162
	Cancellation_Letter_2137859823_06112021.xlsm	Get hash	malicious	Browse	• 185.240.103.162
	jebDtHCePK9feGL.exe	Get hash	malicious	Browse	• 185.129.100.112
	EDS03932,pdf.exe	Get hash	malicious	Browse	• 185.178.208.160
	PO_29_00412.exe	Get hash	malicious	Browse	• 185.178.208.160
	PO_29_00412.exe	Get hash	malicious	Browse	• 185.178.208.160
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 185.178.208.160
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 5.253.61.31
	AxR7BY4wzz.exe	Get hash	malicious	Browse	• 185.178.208.189
	SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe	Get hash	malicious	Browse	• 185.178.208.189
	#U041e#U0442#U043a#U0440#U044b#U0442#U044c www.sberbank.ru-0152 .htm	Get hash	malicious	Browse	• 185.129.100.100
	Install.exe	Get hash	malicious	Browse	• 185.219.40.40
	CHEAT.exe	Get hash	malicious	Browse	• 185.178.208.161
	seed.exe	Get hash	malicious	Browse	• 185.219.40.40
	DHL Document. PDF.exe	Get hash	malicious	Browse	• 5.253.61.133
OffshoreRacksSAPA	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	Rebate_247668103_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_247668103_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_1963763550_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_1963763550_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_234359500_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	Rebate_234359500_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
	banUwVSwBY.xlsx	Get hash	malicious	Browse	• 190.14.37.134
	banUwVSwBY.xlsx	Get hash	malicious	Browse	• 190.14.37.134
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 190.14.37.102
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 190.14.37.102
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 190.14.37.121
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 190.14.37.121
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 190.14.37.102
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 190.14.37.102
	Overdue_Debt_829721407_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
HSAE	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 185.183.99.120
	Decline-172917164-06242021.xlsm	Get hash	malicious	Browse	• 185.117.73.74
	Decline-172917164-06242021.xlsm	Get hash	malicious	Browse	• 185.117.73.74
	xa6FEoUw0W.dll	Get hash	malicious	Browse	• 188.116.36.211
	tszs3mwUbe.exe	Get hash	malicious	Browse	• 185.45.193.29
	pZ50mMKSLi.exe	Get hash	malicious	Browse	• 185.45.193.29
	qTnwCotzR9.exe	Get hash	malicious	Browse	• 185.45.193.29
	PwBsqWQ7jJ.exe	Get hash	malicious	Browse	• 185.45.193.29
	aGDehjYIws.exe	Get hash	malicious	Browse	• 185.198.57.204
	Tjhsm8p85Y.exe	Get hash	malicious	Browse	• 185.45.193.29
	T23HJFoN2Y.exe	Get hash	malicious	Browse	• 185.45.193.29
	i7NsO9mhTD.exe	Get hash	malicious	Browse	• 185.45.193.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	o7w2HSi17V.exe	Get hash	malicious	Browse	• 185.141.27.225
	AB1CEF822F66D7B77574A21C8154D4A6E9FCD196A6659.exe	Get hash	malicious	Browse	• 185.198.57.204
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 194.36.189.154
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 194.36.189.154
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 194.36.189.154
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 194.36.189.154
	xax2K3BWhm.exe	Get hash	malicious	Browse	• 185.45.192.246
	Cancellation_480942562_06082021.xlsm	Get hash	malicious	Browse	• 185.45.192.236

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\15D09FEF-C541-4421-B5FD-A7FAC873EAA7	
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):	135189
Entropy (8bit):	5.363278820688444
Encrypted:	false
SSDEEP:	1536:qcQIKNgeBTA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:MEQ9DQW+zvXO1
MD5:	F38B40054738BD6073A9C534507A6805
SHA1:	0C9A6C5AACF1AB3CF4508EB8D144A28FF790773A
SHA-256:	47A4A43F857AF1950F2F34C4839065A9CABCA5945870725E9492DD3A45830561
SHA-512:	8409A69838F0BAD4AFCD3DC65980550D57057170C81B3F64FDFECF2FAE94F59C8B6724D614F032AD8A5D9083205830C718021C03566C184C1337AB33B05181F8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-25T12:14:02">.. Build: 16.0.14223.30528-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\66A06DB.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS6 (Windows), datetime=2021:02:11 21:11:18], baseline, precision 8, 1860x1000, frames 3
Category:	dropped
Size (bytes):	139381
Entropy (8bit):	7.677272725029824
Encrypted:	false
SSDEEP:	3072:CmKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZOy:54P4346PgZw9gQat
MD5:	53918FB868F1540920FC189C6783FC7C
SHA1:	135CB103C5B5125C80285A83AE728B559313BADC
SHA-256:	7F6AD5212338A6586251AEF92D2543AA8E70C815FE0BF7ADDCE2C0A83D20A0B3
SHA-512:	31391EFC3D377EA32A537EF3DDCA41ABAF34C4C83CDFEF9A64D40DE219B88A293BE2BF01D6A5D2B23365513CB880020F37CA8E90506C41FB7FC8E42D4D641F51
Malicious:	false
Reputation:	low
Preview:	....!jExif..MM.*.....b.....j.(.....1.....r.2.....i.....-....'..-....'.Adobe Photoshop CS6 (Windows).2021:02:11 21:11:18.....D.....&.(..... 4.....H.....H.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ.....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch....

C:\Users\user\AppData\Local\Temp\F2C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	153180
Entropy (8bit):	7.664758560737542
Encrypted:	false
SSDEEP:	3072:4mKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZO0:34P4346PgZw9gQaV
MD5:	B3C9DCAE5BA602A016E3A0B990B3ACB0
SHA1:	7B5C10C9996DDF867EB67FB7BB144B0A924C3639
SHA-256:	7BB381BFFE20BF95226DC719D26D3795F77D76D764075DE7BC3677504BA025FB
SHA-512:	A6793F065DD6366A7BFBE679D2D7710797F079375882BA2A2CB70F8D593777A6450460950CD2819298BD37BC4632CB88A1242FE7042F32AB6F6CAF5C45BB2BB3
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...B..EP...H.e. ....Xb.?.Lb.C.Q....,..X..y.Gi8.Y.].a...]T.V..N*.....g...1.....1..../...XP..5kS..G..X9..V...H.34.XB..r2....6.)k.....U..nE.o..e.....x...DF.... .[,.@..!.*.. c....|PD ....5.....8..*;c.U>~.....S.29...MF....%.x..~....J.w..s..anN...W.u.EV....Y.k.5P.....2..rq.....N:.....F...T..\...hL..6.c(.#.D.5.....d..i.1.....[.(.....!..g.|....B.\.Z...9.^.....Cp>... p...i..KOB...~...]=.N..;.||I.;;.g.....PK.....!...&n....o.....[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=Fri Jun 25 11:14:06 2021, atime=Fri Jun 25 11:14:06 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.672487375948491
Encrypted:	false
SSDEEP:	12:8c3b3MXUILhduCH2BvOPa4RLwtlX+WrjAZ/DYbDtTSeuSeL44t2Y+xIBjKZm:8c3b3yLPqm/sxAZbcDP7aB6m
MD5:	15F9B05AA76E721A8112D5ACB6973F9E
SHA1:	B41D5E6F983E668338A8B9553F3BDA940144F6DA
SHA-256:	DB623572223367F01DBE4C55FD34A956CCCB93574B942937BFE403E219A2CA3A
SHA-512:	0FEAFCD317C7A4ABE803F357B589EDE7B041CCF0AB218B14A9EAF0C44B94DDF11E3F2D55BCB5576CFAD66DF4C9B7656A35F7657F5D74670901A5175810008F1
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..'....i..'....i...@.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.a.....:.....;..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.a....#J.....j.o.n.e.s.....~.1.....R.a..Desktop.h.....N...R.a.....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.....715575.....!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..m D..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Permission-414467145-06252021.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 06:35:55 2020, mtime=Fri Jun 25 11:14:06 2021, atime=Fri Jun 25 11:14:06 2021, length=153171, window=hide
Category:	dropped
Size (bytes):	2310
Entropy (8bit):	4.7033086268941915
Encrypted:	false
SSDEEP:	48:8Kr6zqmt94SlyKSBqBB6pKr6zqmt94SlyKSBqBB6:8rzZtMKrzZtM
MD5:	9611BB32458DE0DFF867587A7A0CA3D6
SHA1:	09FB3A21BA6DA2A6345FFB30CFC97623469361D8
SHA-256:	8CA23CB6310B56C4C6B58E60848F37688DB2B534B4EE68D5637912E2E3CFE9FB
SHA-512:	502D18E03681726D9DB8C1A576F03F9E610AC15AF61A1ACC1CBB0D13F9A491A11D70709CFC074CE7D92A09ABF57BED9A2DBEAEC87ED07D7E2354D5497D56AD4B
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...r..U...'....i..'....i..SV.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.a.....:.....;..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.a....#J.....j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N...R.a.....Y.....>.....(...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9. .....2..X...R.a .PERMIS~1.XLS..v.....>Q|<.R.a.....V.....n<E.P.e.r.m.i.s.s.i.o.n.-.4.1.4.4.6.7.1.4.5.-.0.6.2.5.2.0.2.1...x.l.s.m.....h.....-.....g.....>.S.....C:\Users\user\Desktop\Permission-414467145-06252021.xlsm..9.....\....\....\....\....\.D.e.s.k.t.o.p.\.P.e.r.m.i.s.s.i.o.n.-.4.1.4.4.6.7.1.4.5.-.0.6.2.5.2.0.2.1...x.l.s.m.....:..,.LB.)... As...`.....X.....715575.....!a..%.H.VZAj...{.....!a..%.H.VZAj...{.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.

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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	142
Entropy (8bit):	4.642670559637109
Encrypted:	false
SSDEEP:	3:oyBVomxW+LxCRTnv5NUltLxCRTnv5NUlmxW+LxCRTnv5NUlv:djHC5vI/FC5vIaC5vI1
MD5:	DAC8913182CCB2EAEA86304F342799F4
SHA1:	394074391582ABC7A7F67CB563FC01E438712E12
SHA-256:	F287F47508BBBDFC7A95F43C0F435981E1EEDADBBF48926265E42EA173C07199
SHA-512:	EF9B7E2A51367E553A3116022DBE8FE56E7845FE79B05902048FF6C3C409BECFAA9C7C59AA64E8BB8BF3A7AEE0A63A6E93A47A3681381578FE181A43728810D5
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Permission-414467145-06252021.LNK=0..Permission-414467145-06252021.LNK=0..[misc]..Permission-414467145-06252021.LNK=0..

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
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\C3C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	153171
Entropy (8bit):	7.664923963279183
Encrypted:	false
SSDEEP:	3072:EQUmKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZOO:d4P4346PgZw9gQaX
MD5:	12C91792452047527412E56EA989C4F2
SHA1:	08CA222837655C41E730B939C5994AD13F4CC315
SHA-256:	79DCDDF89882885164D1EDDBA371B8AA88FC0E43538F3DB0B5DB8AD899CA9D98
SHA-512:	0078147D19E4C1F9492FA728D72FAB9B682DB3431E482CFCBA9F707E4AB52CD43BAC2DE25E57437555B86B77F6F165ED7C62950477DE44F9030DEF2FCB9FE09
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...B..EP...H.e. ....Xb.?.Lb.C.Q....X..y.Gi8.Y.].a...]T.V..N*.....g...1.....1..../...XP..5kS..G..X9..V...H.34.XB..r2....6.)k.....U..nE.o..e.....x...DF.... .[,.@..!.*.. c....|PD ....5.....8..*;c.U>~.....S.29...MF....%.x..~....J.w..s..anN...W.u.EV....Y.k.5P.....2..rq.....N:.....F...T..\...hL..6.c(.#.D.5.....d..i.1.....[.(.....!..g.|....B.\.Z...9.^.....Cp>... p...i..KOB...~...]=.N..;.||.:,:.g.....PK.....!...&n....o.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Permission-414467145-06252021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD067
Malicious:	**true**

C:\Users\user\Desktop\~$Permission-414467145-06252021.xlsm	
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.666395274852154
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Permission-414467145-06252021.xlsm
File size:	153750
MD5:	590ca0e597487dd5ad6c2f1fb64184dd
SHA1:	e141e27af930a2cdeafab2eb20727000de893629
SHA256:	20a72dc5350b296f2857911444fa065f5b0bb437be8d1bc61819cf29828a2955
SHA512:	fceb07823442eccaed6727b3c780fc7fbed475c15ac7131c7921505060b475d511e928c312d22980e40ebf12506d05308b55cc9fc0bc1509b244b435920fdc2e
SSDEEP:	3072:SmKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZOYJ:p4P4346PgZw9gQaVJ
File Content Preview:	PK.....!.....o.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Permission-414467145-06252021.xlsm"

Indicators

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

Macro 4.0 Code

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/25/21-14:07:18.214699	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	185.240.103.219	192.168.2.22
06/25/21-14:07:19.251378	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	190.14.37.3	192.168.2.22
06/25/21-14:07:19.648943	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	185.183.99.120	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

HTTP Request Dependency Graph

- 185.240.103.219
- 190.14.37.3
- 185.183.99.120

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49741	185.240.103.219	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:14:06.418955088 CEST	1071	OUT	GET /44372.593127662.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 185.240.103.219 Connection: Keep-Alive
Jun 25, 2021 14:14:06.508730888 CEST	1072	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:14:06 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49743	190.14.37.3	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:14:06.722661972 CEST	1073	OUT	GET /44372.593127662.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 190.14.37.3 Connection: Keep-Alive
Jun 25, 2021 14:14:07.517127991 CEST	1085	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:14:07 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49744	185.183.99.120	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:14:07.592284918 CEST	1086	OUT	GET /44372.593127662.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 185.183.99.120 Connection: Keep-Alive
Jun 25, 2021 14:14:07.876260042 CEST	1086	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:14:22 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6876 Parent PID: 800

General

Start time:	14:14:01
Start date:	25/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x810000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6160 Parent PID: 6876

General

Start time:	14:14:07
Start date:	25/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\Kro.fis
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: regsvr32.exe PID: 5008 Parent PID: 6876

General

Start time:	14:14:08
Start date:	25/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\Kro.fis1
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: regsvr32.exe PID: 3980 Parent PID: 6876

General

Start time:	14:14:09
Start date:	25/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\Kro.fis2
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Disassembly

Code Analysis