ID: 440505
Sample Name: Permission-414467145-06252021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:06:26
Date: 25/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

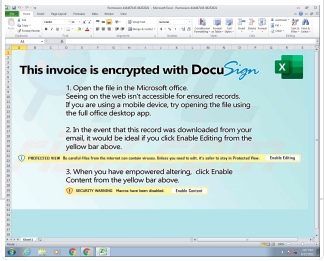
Windows Analysis Report Permission-414467145-06252…

Overview

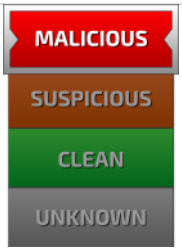
General Information

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

Most interesting Screenshot:



Detection



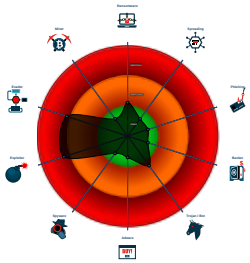
Hidden Macro 4.0

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…
- May sleep (evasive loops) to hinder …
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2492 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 1980 cmdline: regsvr32 ..\Kro.fis MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 3032 cmdline: regsvr32 ..\Kro.fis1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2244 cmdline: regsvr32 ..\Kro.fis2 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **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:

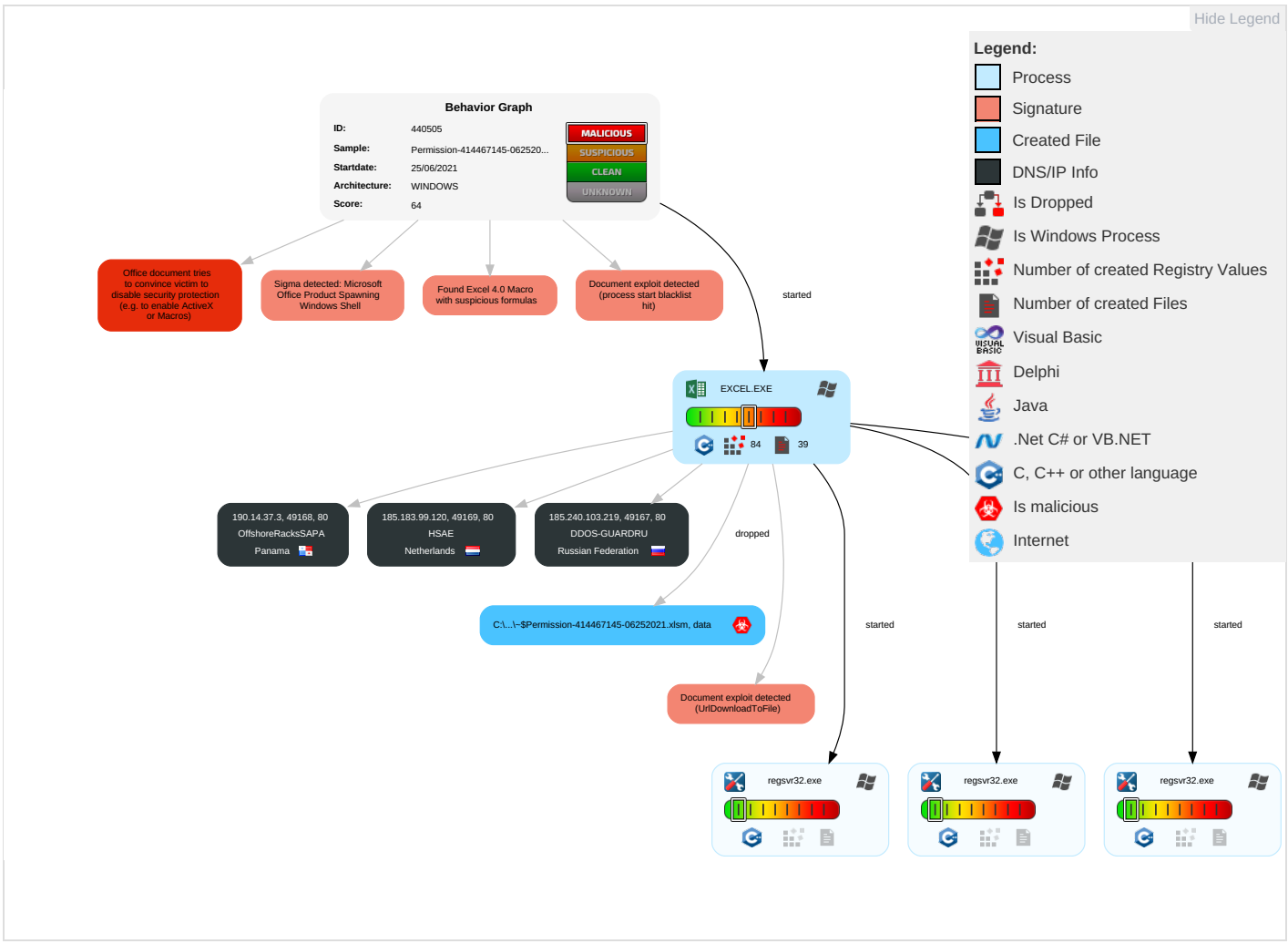
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	Re Se Ef
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

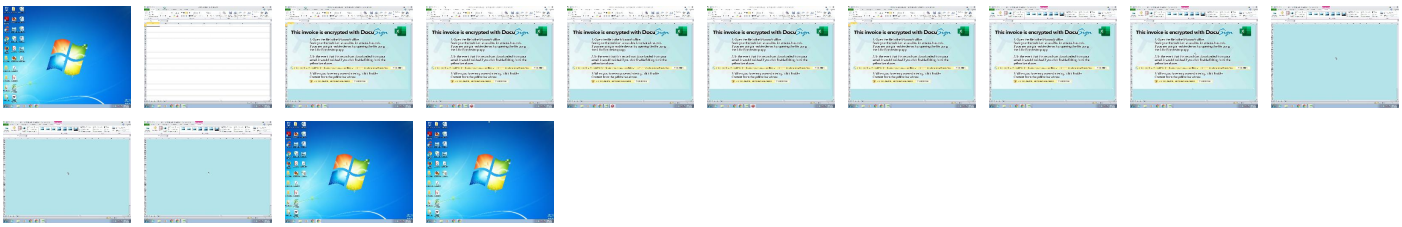
Behavior Graph

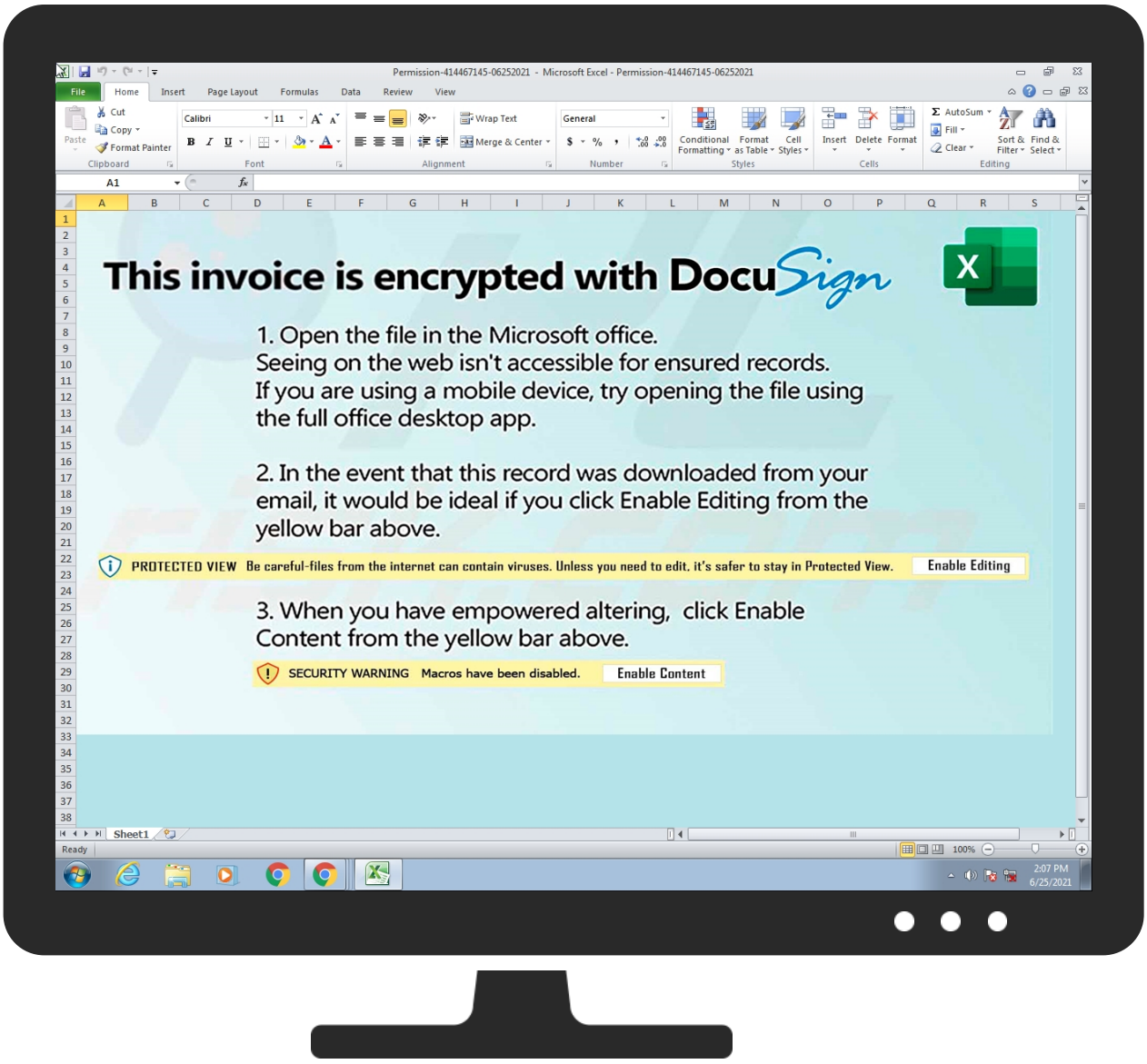


Screenshots

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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://185.183.99.120/44372.5879460648.dat	0%	Avira URL Cloud	safe	
http://190.14.37.3/44372.5879460648.dat	0%	Avira URL Cloud	safe	
http://185.240.103.219/44372.5879460648.dat	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.183.99.120/44372.5879460648.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.3/44372.5879460648.dat	false	• Avira URL Cloud: safe	unknown
http://185.240.103.219/44372.5879460648.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:	14:06:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 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 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
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@7/7@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 • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:06:49	API Interceptor	3x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DDOS-GUARDRU	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	wrHgqtMUGL.exe	Get hash	malicious	Browse	• 45.128.207.237
OffshoreRacksSAPA	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
	Overdue_Debt_829721407_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
HSAE	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
	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
	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\Windows\Temporary Internet Files\Content.MSO\4A07B784.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\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), d atetime=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:	31391EFC3D377EA32A537EF3DDCA41ABAF34C4C83CDFEF9A64D40DE219B88A293BE2BF01D6A5D2B23365513CB880020F37CA8E90506C41FB7FC8E42D4D641 51
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\BECE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	153117
Entropy (8bit):	7.664520146264211
Encrypted:	false
SSDEEP:	3072:cnxmKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZO46M:cng4P4346PgZw9gQad
MD5:	E7FF0DFAC948EB9E3F28829A03D3CF9F
SHA1:	DE0BB99F512724500B07FE16A497934D9B2F3455
SHA-256:	1C614F666606155F93B4EC6462A3FF9196574F1527943EEC11435396B598B0D4
SHA-512:	DD3E1F81FEBF93235D9A6BFCAB0641C0C92FF6B4B234B10DF43B14FFE6C8E99CDB086B7AA142F08CF6FCC786F77474D697CD65EE975B5A1CBEC17E1B54D74 D88
Malicious:	false
Reputation:	low
Preview:	...N.0...+....(q.V...X8.....41.?y..o..dw..i.{i..3....x..+k.7.....E5a.8.vM.~=..Y.I8%.wP.5 ...}.>..`A..k..~p...+.....,|.".mlx.r).....%p.L...M..B..T...F.\;V.l~.Q5.!.-E"....H...-Ay.j.u.!.P.. $k..5....D.....A..*..a.....r.....i..|..d...`...G....._....r...:..iZ,a%.T]d..2.['..hMh.a....D.].N@../9...I.x@G.{.....B...&z..w.....@.....L..4."."..zJt`4_.....:T..Y..~.|..F.\)..i.....tz?F...D.. .>N.\].j.1i...}GWO..2..3s ./.j..w.r.....PK.....!...&n....o.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jun 25 20:06: 38 2021, atime=Fri Jun 25 20:06:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.501022480561873
Encrypted:	false
SSDEEP:	12:85QfLgXg/XAlCPCHaXtB8XzB/twX+WnicvbDS9bDtZ3YilMMEpxRljKHUmn6TdJU:85A/XTd6jkYeihDv3qGnirNru/
MD5:	F1455988FC9FAE5664C5753629ED52BB
SHA1:	6747F36980BE6E1AFF19D8B9F7B7C48997286F85
SHA-256:	2019327C54A56F28B2B0AE5DE5681398F7D8CC190310DD0F6DC6A7D7CEC6824C
SHA-512:	8F4005A91D7D645EA55846348B081CF56F1145650674284AD834626CEC1EDCB7A6B6C2B1BDACC31F9F13668193F81ECEA6527D3DB2F4D844E267AD836E4A827
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G..>w...j..>w...j... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R...Desktop.d.....QK.X.R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\141700\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....141700.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Permission-414467145-06252021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Fri Jun 25 20:06:38 2021, atime=Fri Jun 25 20:06:38 2021, length=153117, window=hide
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	4.555970335453609
Encrypted:	false
SSDEEP:	48:8Hf1W/XT0jFL1SaRS8GiQh2Hf1W/XT0jFL1SaRS8GiQ/:8Hf1W/XojFLnGiQh2Hf1W/XojFLnGiQ/
MD5:	16864E7220CE49809E8CB699A24889CB
SHA1:	15CC58A077446427D87345619805CCAA08ED64A8
SHA-256:	DF8F15797890F5E20498C2E87BA020FACE211A7EF8FE013289C7F7E5D5AEF30C
SHA-512:	B94AC86B7136C833B76D264F21C560C8CE9086440C526EBB5D07B6F6A37CC42A99B1AAED41E956E939F09CF1784F342FB943CE74130493151E9C4AB93B99A49
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{..>w...j..._....j...V.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..X...R. .PERMIS~1.XLS..r.....Q.y.Q.y*...8.....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.....-...8...[.....?J.....C:\Users\..#.....\\141700\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.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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\Desktop\4FCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	153117
Entropy (8bit):	7.664520146264211
Encrypted:	false
SSDEEP:	3072:cnxmKZQmKZ3KNhPQnVbJ2O1gZMys2g4D5JhoD4ZO46M:cng4P4346PgZw9gQad
MD5:	E7FF0DFAC948EB9E3F28829A03D3CF9F
SHA1:	DE0BB99F512724500B07FE16A497934D9B2F3455
SHA-256:	1C614F666606155F93B4EC6462A3FF9196574F1527943EEC11435396B598B0D4
SHA-512:	DD3E1F81FEBF93235D9A6BFCAB0641C0C92FF6B4B234B10DF43B14FFE6C8E99CDB086B7AA142F08CF6FCC786F77474D697CD65EE975B5A1CBEC17E1B54D74D88
Malicious:	false
Reputation:	low
Preview:	...N.0...+....(q.V...X8.....41.?y..o..dw..i.{i..3....x..+k.7.....E5a.8.vM.~=..Y.I8%.wP.5 ...}.>..`A..k..~p...+.....|.".mlx.r).....%p.L...M..B..T...F.\;V.l~.Q5.!.-E"....H...-Ay.j.u.!.P..$k..5....D.....A..*..a.....r.....i..|..d...`...G....._....r...:..iZ,a%.T]d..2.['..hMh.a....D.].N@../9...I.x@G.{.....B...&z..w.....@.....L..4."."..zJt`4_.....:T..Y..~.|..F.\)..i.....tz?F...D..>N.\].j.1i...}GWO..2..3s ./.j..w.r.....PK.....!...&n....o.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Permission-414467145-06252021.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

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:	e4e2aa8aa4bcbcac

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:	

Indicators

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

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	192.168.2.22	49167	185.240.103.219	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:07:18.124540091 CEST	0	OUT	GET /44372.5879460648.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.240.103.219 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:07:18.214699030 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:07:18 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	192.168.2.22	49168	190.14.37.3	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:07:18.454245090 CEST	1	OUT	GET /44372.5879460648.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 190.14.37.3 Connection: Keep-Alive
Jun 25, 2021 14:07:19.251378059 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:07:19 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	192.168.2.22	49169	185.183.99.120	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:07:19.345586061 CEST	3	OUT	GET /44372.5879460648.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.183.99.120 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 14:07:19.648942947 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 12:07:34 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: 2492 Parent PID: 584

General

Start time:	14:06:35
Start date:	25/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fc50000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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 Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 1980 Parent PID: 2492

General

Start time:	14:06:40
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 3032 Parent PID: 2492

General

Start time:	14:06:40
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis1
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 2244 Parent PID: 2492

General

Start time:	14:06:41
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis2
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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