ID: 440340
Sample Name: Decline-172917164-06242021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:23:46
Date: 25/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

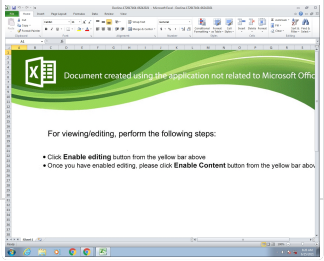
Windows Analysis Report Decline-172917164-06242021....

Overview

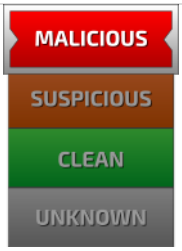
General Information

Sample Name:	Decline-172917164-06242021.xlsm
Analysis ID:	440340
MD5:	f022a2159442cd4.
SHA1:	cd4a698d830594..
SHA256:	4bd593279e649fa.
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection



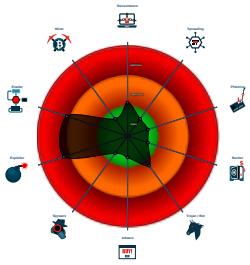
Hidden Macro 4.0

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- 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: 1780 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2972 cmdline: regsvr32 ..\Kro.fis MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2884 cmdline: regsvr32 ..\Kro.fis1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2996 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

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

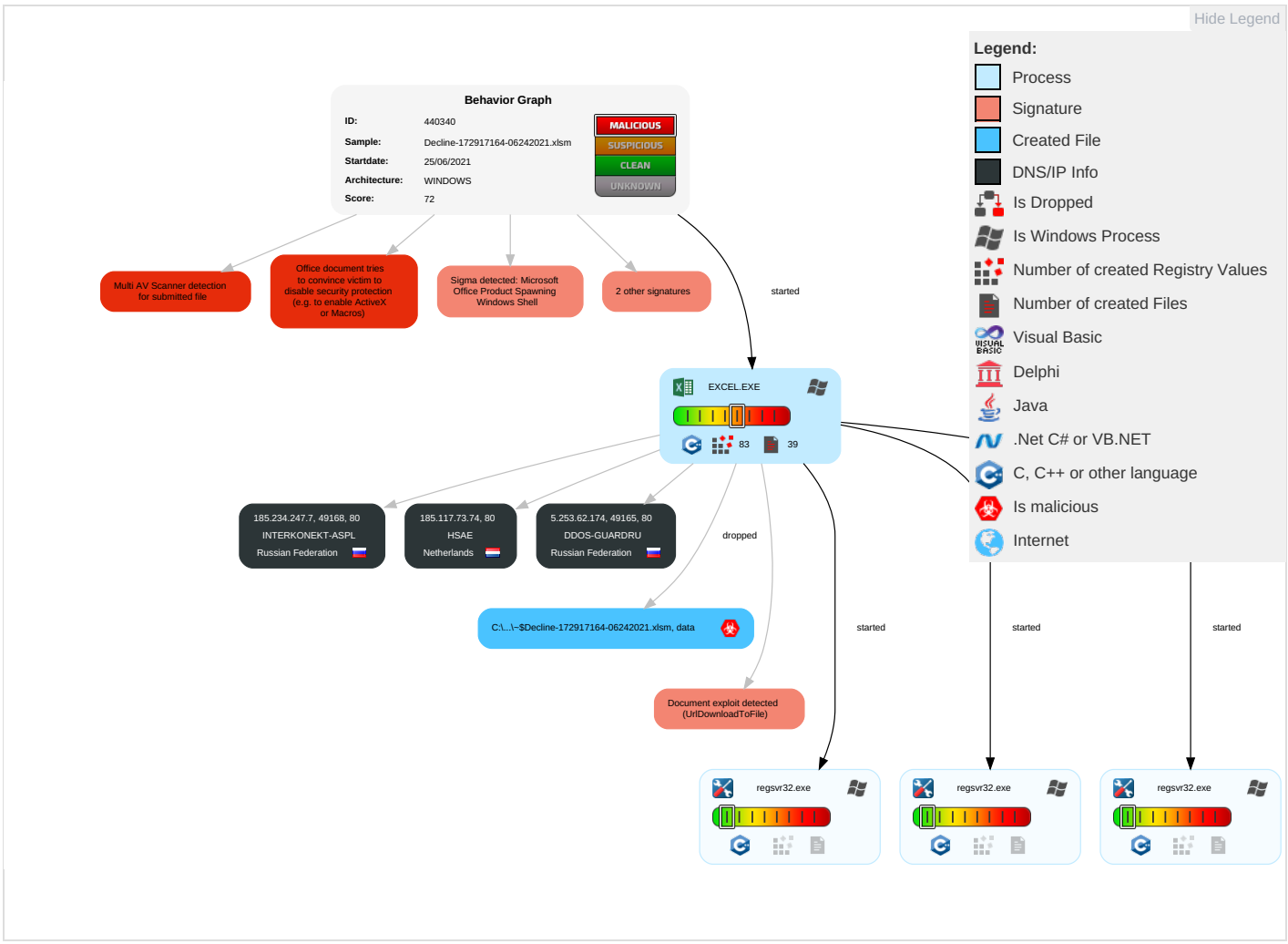
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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 El
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	

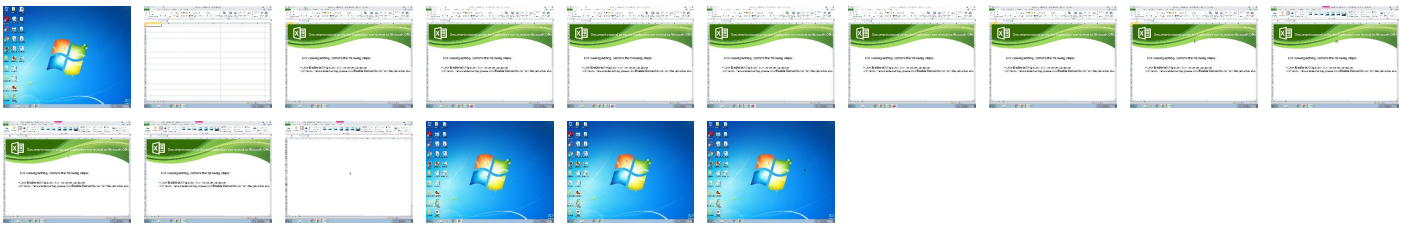
Behavior Graph

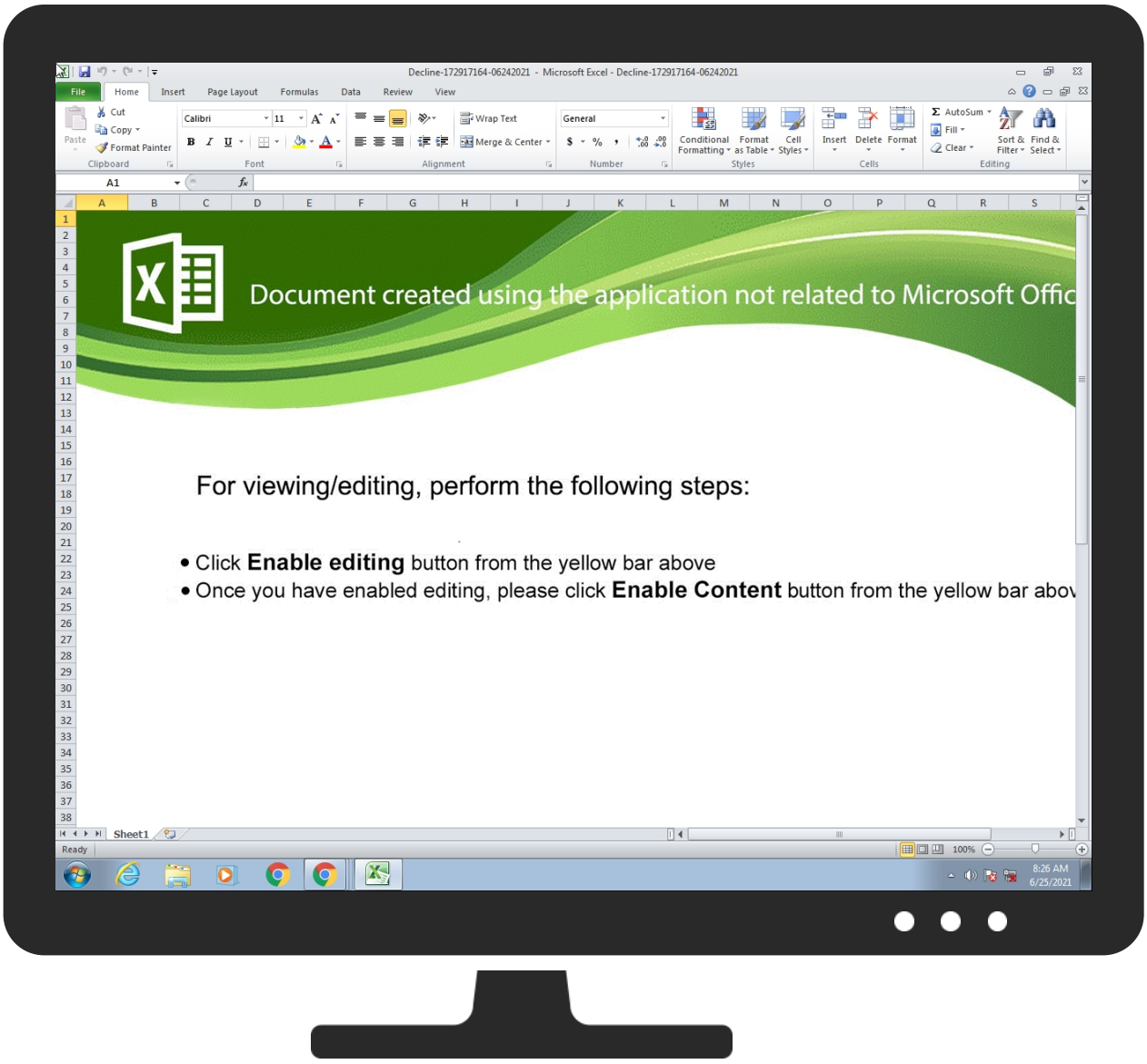


Screenshots

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
Decline-172917164-06242021.xlsm	18%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.234.247.7/44372.3504680556.dat	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
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.%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://5.253.62.174/44372.3504680556.dat	0%	Avira URL Cloud	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://185.234.247.7/44372.3504680556.dat	false	• Avira URL Cloud: safe	unknown
http://5.253.62.174/44372.3504680556.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.234.247.7	unknown	Russian Federation		198004	INTERKONEKT-ASPL	false
5.253.62.174	unknown	Russian Federation		57724	DDOS-GUARDRU	false
185.117.73.74	unknown	Netherlands		60117	HSAE	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	440340
Start date:	25.06.2021
Start time:	08:23:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Decline-172917164-06242021.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:	mal72.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
08:25:31	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
INTERKONEKT-ASPL	inquiry.06.21.doc	Get hash	malicious	Browse	• 185.234.247.9
	inquiry.06.21.doc	Get hash	malicious	Browse	• 185.234.247.9
	inquiry.06.21.doc	Get hash	malicious	Browse	• 185.234.247.9
	trustScr.hta	Get hash	malicious	Browse	• 185.234.247.14
	aXgdOUvL9L.exe	Get hash	malicious	Browse	• 185.234.247.183
	qH8pUgpOeA.exe	Get hash	malicious	Browse	• 185.234.247.244
	UqdoQQIqio.exe	Get hash	malicious	Browse	• 185.234.247.244
	29B9058449C81CF5AAA57316C620D80A48E2161D583C6.exe	Get hash	malicious	Browse	• 185.234.247.183
	2fr18s8lrd.exe	Get hash	malicious	Browse	• 185.234.247.219
	SecuriteInfo.com.W32.AIDetect.malware1.509.exe	Get hash	malicious	Browse	• 185.234.247.219
	a1wnP3RcrY.exe	Get hash	malicious	Browse	• 185.234.247.219
	Hs52qascx.dll	Get hash	malicious	Browse	• 185.234.247.193

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E2ucBaWqpe.exe	Get hash	malicious	Browse	• 185.234.247.233
	malware.doc	Get hash	malicious	Browse	• 185.234.247.180
	malware.doc	Get hash	malicious	Browse	• 185.234.247.180
	yqwit.exe	Get hash	malicious	Browse	• 185.234.247.233
	require,02.21.doc	Get hash	malicious	Browse	• 185.234.247.180
	adjure.02.21.doc	Get hash	malicious	Browse	• 185.234.247.179
	adjure.02.21.doc	Get hash	malicious	Browse	• 185.234.247.179
	adjure.02.21.doc	Get hash	malicious	Browse	• 185.234.247.179
DDOS-GUARDRU	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
	wrHgqtMUGL.exe	Get hash	malicious	Browse	• 45.128.207.237
	1jjYj8IYOD.exe	Get hash	malicious	Browse	• 45.128.207.237
	SecuriteInfo.com.Generic.mg.d4927d53f24b7662.exe	Get hash	malicious	Browse	• 45.128.204.36

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD7B9C26.tif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	TIFF image data, little-endian, direntries=19, height=1600, bps=53710, compression=LZW, PhotometricIntepretation=RGB, width=1600
Category:	dropped
Size (bytes):	315878
Entropy (8bit):	7.988901270632308
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD7B9C26.tif	
SSDEEP:	6144:hRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZN3:hRMmEv2Bc/nvm8IKABfsYOmauFD
MD5:	BB737290D394078D8A16D5509C5BC970
SHA1:	C8A63B0AB1EB7745A0027E0A17A6CB4C6F79487E
SHA-256:	E11121ECA3FAD55F66EA240EADD4F5B4C978828C94C34736F7673540529B17A5
SHA-512:	3D8A6025171D283FA08D8A5BA4EAAD1EABAD55D7D34629F17F4C6601DD4438FB536B29D7B8CA71E540EDB782433118628EBD3A56CE8FFA453C6A45792425CBA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	II*.....h*.....t2#...1..Z)....).~9&.H.r.,.C+.I....e-.M.Si..}0.K.SJ...3.Ng.ZL..G.S..:m..N.Tk5..Z.Z...+.~.f.X.v.-..k.Y.....m.].Wk...p.[.WL...s.^o.\M....c..<n/!..ds9..{)...-..9. .h.z...C..i....e..m.[m..}..k.[N.....nw.^N....s..>o/.r.....C4U.kw{.....f..~.W....y.....y...'...;.R..<.[..;....o...T.....+.....?p....N.....#.....ht'...Q..E....CQ.^.\m.E.....o.Ba[.#Dp...>.<c .1$.*.Q.E....Ir..+.....Y.(H..*K..{..Q...I.....R.Y(Fr|m<$.I...RL.&.3..GP0..D....=.s.5CT,.FN.==7Sq...Iu.3JQ.%GUKS..X...5V.Hu.Z..9T..O4...KC.5.N.Q..aD...g.V.Mh.m.c.M.eMSe.?V..UoR...j....<]...G.v.B$v\Iv[.].f...N\...y_...M....p`w..b.6%.a.....T3.c..S.WQ...S.....tHk[7.[4;..k.#....~e...f.m.&...-.iz6....V5.jzN....:.3.k.....M..[.....m[N...~.nz~.o...k....;.....y..{`.....u..|?-.q.f...|...m6...b..#..]'5..<...g.7_.....q.u..].....$[.....~...+..I.p.zt.Y.N.}.....FS5.....k..H...#....~.w.....:..?.....".... 4..PB.A....l...j..... .p..BX1..D..0..Bx

C:\Users\user\AppData\Local\Temp\95DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328749
Entropy (8bit):	7.982562663364122
Encrypted:	false
SSDEEP:	6144:bnlXRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZNe:blXRMmEv2Bc/nvm8IKABfsYOmauFjW
MD5:	1DDE60AF4802D997D564DCC19FCF8924
SHA1:	01040AF635B254E2387CBDA2379A02C1ADD7B27B
SHA-256:	59B39E1F85E3318A929558831AB2D65DAAA38292B613F65BDB8DBFD28ACE14A3
SHA-512:	64FBD728A651D17147655F1EF88F6EE6F8EF64ECC693A426E0A15F8E54294BF4D28D24B7C0649CBF5D020F66EB39D1C613EEB2C3576796B1F29CAD48D0BB864C
Malicious:	false
Reputation:	low
Preview:	..n.0...+.;D.....C.=n+.....<...~.fw..."..$f...'.xz..\...m..&.....~Q..O?..@R.(.<.b.(.g_.L.....j..h...)Q..).B..+MH.".L...^.....J...<..5.lz..zvT.....zQ.l..Q.P1:...Q.....Mc5...;..0&P.[..\..ebz."..B.e&px.t.....6.7.~..W..:\G...].&.o2.`.....]r..kH.y...87w...V.\...N....^S..:B.+Q._..@.....9l/<..}..!.....`g.....7~...;...GZ;.3....[..<.....=..$..-...}+4....w.?....X}H!"O....x.....,.,..r.L..< .O.....f.[.....PK.....!...Wm.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Decline-172917164-06242021.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 14:24:40 2021, atime=Fri Jun 25 14:24:40 2021, length=328749, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.50661144098561
Encrypted:	false
SSDEEP:	48:81/XT0jFDt262TB+Qh21/XT0jFDt262TB+Q/:81/XojFDyd+Qh21/XojFDyd+Q/
MD5:	2D3FA1E5457926B56AE6600BA3D476FA
SHA1:	2F3FA829061E0BD5BF8F24F2EF63DDABB39E478D
SHA-256:	FE15AAA8305867D305D2944ED0BB890D09964D52FE972D0B169E3281204520F6
SHA-512:	33D321AC668DB01BEAF3D3E1831917FD85591D6A26D23AC3C20246736CAC7DFE271676CDBC0EBBA1CC18D2FB10B9671EF829F3F4AC88AAE82F6E6D3191AE6E2
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...K2.{...\C7.i..K.L7.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.....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.R....R.{ .DECLIN~1.XLS..l.....Q.y.Q.y*...8.....D.e.c.l.i.n.e.-.1.7.2.9.1.7.1.6.4.-.0.6.2.4.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\035347\Users.user\Desktop\Decline-172917164-06242021.xlsm.6.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.e.c.l.i.n.e.-.1.7.2.9.1.7.1.6.4.-.0.6.2.4.2.0.2.1...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.-.1.0.0.6.....`

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 14:24:40 2021, atime=Fri Jun 25 14:24:40 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.47495889914137
Encrypted:	false
SSDEEP:	12:85QJF4FcLgXg/XAlCPCHaXtB8XzB/RwxX+WnicvbbbDtZ3YilMMEpxRljKzTdJP8:852D/XTd6jUxYejDv3q+rNru/
MD5:	2580406BFAE06A1C59616E3B17B9C490

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA1:	7330C14D2F37BB8B2DBB21665DBE1F38C5342D06
SHA-256:	4CA54148064EFC7BF7E77972F5F24F437F80F671C8DC0C6C1668737F5B6F5D61
SHA-512:	C2827E176CED0EC998DFFEEB8122DA69BECA81DDACDAB3277A85E4A15F0A920F9B040FB1F80640B36F977E401BB10B8F6F12512A4F4B05F4723B33B8B811ABF4
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...\C7.i...\C7.i... .....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\..#.....\\035347\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.....035347.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

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):	133
Entropy (8bit):	4.587558026448006
Encrypted:	false
SSDEEP:	3:oyBVomxWqGLtgLZbRFK6l51MLtgLZbRFK6lmxWqGLtgLZbRFK6lv:djnLlPrJLlPoLlP1
MD5:	C583482E01AB0E15D757BF76E7C5D737
SHA1:	FAD60796DF25EA9F73455FEF5ACB980371425D1C
SHA-256:	39089D648F6A966B83E19AC3FEC4BF268C7574340248FE1700B47B497210812F
SHA-512:	E8D50E7882FF9D6F3BAD87B167D4AD7BB4484966059E97D38FFF4F04E57318C3ABF21A02AD5B7E749694205077D174234C09D8469ADB04B7BB058253728061AD
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Decline-172917164-06242021.LNK=0..Decline-172917164-06242021.LNK=0..[misc]..Decline-172917164-06242021.LNK=0..

C:\Users\user\Desktop\66DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328749
Entropy (8bit):	7.982577224576017
Encrypted:	false
SSDEEP:	6144:bnlXRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZNa:blXRMmEv2Bc/nvm8IKABfsYOmauFjC
MD5:	4D63C3DCB6D2C3F5839B7FE96E34939D
SHA1:	8DAF3CA9BE70E9FE8BE12F12124F10E1AD077DDA
SHA-256:	744118B0D611EED117C6907221549EAE6D477206EDD837F30EE55FABC2D8E328
SHA-512:	7278D22DD1495189808B45774FBC3E5CFCEDFDF012C2B0134569CD9A90CAC2EC34EF94DD0B9C190D58712925AAC5371ECEBBAAFFA411D0F1B432604CEEEE04B
Malicious:	false
Reputation:	low
Preview:	..n.0...+.;D.....C.=n+.....<...~.fw..."..$f...'.xz..\...m..&.....~Q..O?..@R.(.<.b.(.g_.L.....j..h...)Q..).B..+MH.".L...^.....J...<..5.lz..zvT.....zQ.l..Q.P1:...Q.....Mc5...;..0&P.[..\..ebz."..B.e&px.t.....6.7.~..W..:\G...].&.o2.`.....]r..kH.y...87w...V.\...N....^S..:B.+Q._..@.....9I/<..}..!.....`g.....7~....;...GZ;.3....[..<.....=..$..-...}+4....w.?....X}H!"O....x.....,..,..r.L..<.O.....f.[.....PK.....!...Wm.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Decline-172917164-06242021.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**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.982649799738301
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Decline-172917164-06242021.xlsm
File size:	329298
MD5:	f022a2159442cd4e16d7fe3dee1d634b
SHA1:	cd4a698d83059462498e48b8dec47662bd2a0ec4
SHA256:	4bd593279e649fae847a2b702655c571d7ca9e1949a422a8d289250aeaa3305
SHA512:	ba433280caf91d3ee2b17848d398566e69802e1346573cbe16b4bb77045aa0a8739affcaa27e216018bb6b051dba2b6bf83503a88492b4aa470147c0c716a891
SSDEEP:	6144:97u1GRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZw:97sGRMmEv2Bc/nvm8IKABfsYOmauFq
File Content Preview:	PK.....!.^.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Decline-172917164-06242021.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
06/25/21-08:24:40.521992	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	5.253.62.174	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/25/21-08:24:41.376990	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22
06/25/21-08:24:45.028969	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22
06/25/21-08:24:51.240465	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22
06/25/21-08:25:04.623723	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22
06/25/21-08:25:07.631782	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22
06/25/21-08:25:10.979362	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22
06/25/21-08:25:22.914129	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	185.234.247.7	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 5.253.62.174
- 185.234.247.7

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	5.253.62.174	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 08:24:40.426493883 CEST	0	OUT	GET /44372.3504680556.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: 5.253.62.174 Connection: Keep-Alive
Jun 25, 2021 08:24:40.521991968 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 06:24:40 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	185.234.247.7	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 25, 2021 08:25:22.717233896 CEST	2	OUT	GET /44372.3504680556.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: 185.234.247.7 Connection: Keep-Alive
Jun 25, 2021 08:25:22.914129019 CEST	3	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 25 Jun 2021 06:25:22 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: 1780 Parent PID: 584

General

Start time:	08:24:37
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:	0x13f1c0000
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: 2972 Parent PID: 1780

General

Start time:	08:25:23
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis
Imagebase:	0xff790000
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: 2884 Parent PID: 1780

General

Start time:	08:25:23
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis1
Imagebase:	0xff790000
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: 2996 Parent PID: 1780

General

Start time:	08:25:23
Start date:	25/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\Kro.fis2
Imagebase:	0xff790000
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