ID: 682599
Sample Name: cnewton doc 08.11.2022.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:56:49
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

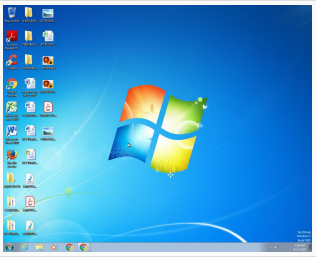
Windows Analysis Report

cnewton doc 08.11.2022.doc

Overview

General Information

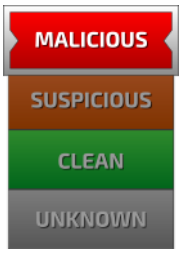
Sample Name:	cnewton doc 08.11.2022.doc
Analysis ID:	682599
MD5:	ee1d6eb5b07b99.
SHA1:	9d4dbf701c8ede..
SHA256:	23b9a20a59041f..
Tags:	doc IcedID
Infos:	



Errors

⚠ Corrupt sample or wrongly selected analyzer.

Detection

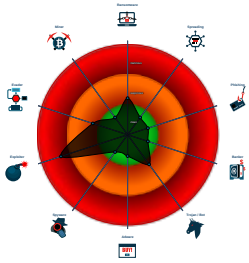


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Document contains an embedded V…
- Machine Learning detection for sam…
- Potential document exploit detected…
- Uses a known web browser user age…
- Detected potential crypto function
- Document contains an embedded V…
- Document contains embedded VBA…
- Potential document exploit detected…
- IP address seen in connection with …

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2476 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (creates forbidden files)

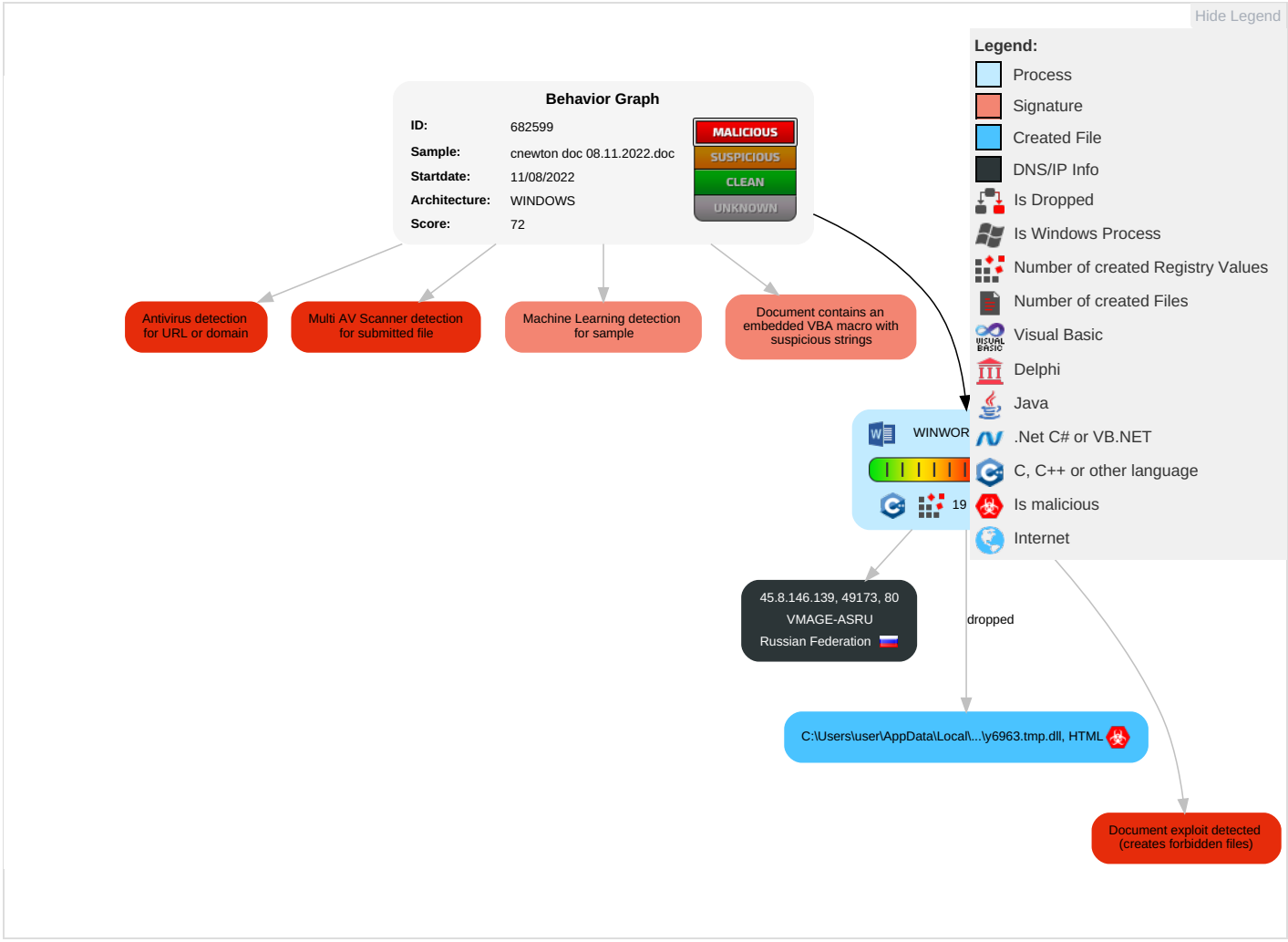
System Summary

Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Scripting	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

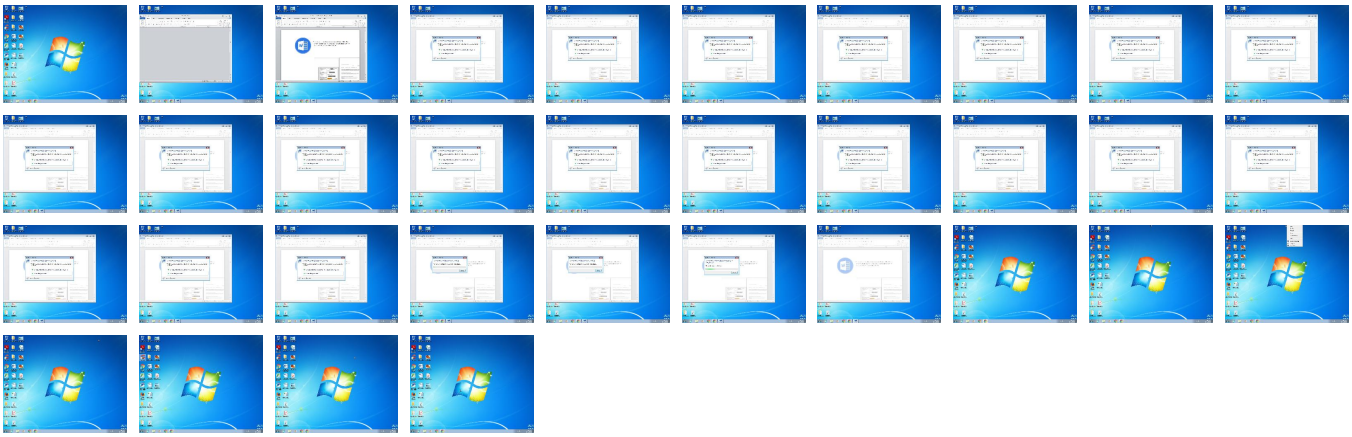
Behavior Graph



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
cnewton doc 08.11.2022.doc	22%	Virustotal		Browse
cnewton doc 08.11.2022.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
cnewton doc 08.11.2022.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://www.%s.comPA	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fC:	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fggC:	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-ftem32	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	WINWORD.EXE, 00000000.00000002.1033598751.0000000004170000.00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	WINWORD.EXE, 00000000.00000002.1033598751.0000000004170000.00000002.00000001.00040000.00000000.sdmp	false		high
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fC:	WINWORD.EXE, 00000000.00000002.1038045478.0000000006877000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.1014226864.0000000006877000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/NH1-X8NL7CO4_	WINWORD.EXE, 00000000.00000000.1014370074.00000000068EF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fggC:	WINWORD.EXE, 00000000.00000000.1008798885.0000000000450000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-ftem32	WINWORD.EXE, 00000000.00000000.1013985218.00000000067CF000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000002.1037858643.00000000067CF000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682599
Start date and time:	2022-08-11 18:56:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cnewton doc 08.11.2022.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:	6
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@1/7@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Unable to detect Microsoft Word • Close Viewer

Errors

- Corrupt sample or wrongly selected analyzer.

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.89.179.12, 104.208.16.93
- Excluded domains from analysis (whitelisted): onedsblobprdcus07.centralus.cloudapp.azure.com, watson.microsoft.com, legacywatson.trafficmanager.net, onedsblobprdcus17.centralus.cloudapp.azure.com

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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\-f[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	201
Entropy (8bit):	5.120826232488609

Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
Malicious:	false
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "-f" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\CVR5475.tmp.cvr

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	modified
Size (bytes):	1216
Entropy (8bit):	3.0679960309839154
Encrypted:	false
SSDEEP:	24:uZp1Q/svtl/aXiFuWFZsyb/douhISPdddBBlmWmwgVrZrpkQXVhlnlNAq6:40cvutmouhIodddBB8hPPfhHeq6
MD5:	EB17AABF5AEABA10C903E128A8A42ABF
SHA1:	5065A7F1BDBDE9D271C88C2B07BF0CF98EC88A7F
SHA-256:	A2220FFE6B9EF21235D26E997213FABD2F38116D7A31BE35F7A0935D148D9433
SHA-512:	FF025028E03A078BC93E05B9A1CA6267DE6E1CEC3847F64D964F0B99F19218C1271AE9887F7DA53A006D478B9A7C0B865EC9B91616E4C5372EE25A6C6FCB4D(A
Malicious:	false
Reputation:	low
Preview:	MSQMx.....H.....{*.....~..<.....X.....WINW.....N.....5.....;.....<.....A..... ....I.....f.....f...N.....Q.....`.....f.....X...b.....f...S.....f...N.....<.....B.....C.....F..... .....I.....f...H.....f.....+.....0...../...:...../...;...../.....z.....z.....n".....7#...../...?.....f...I.....f.....$.....rr l7.....rrl7....X...rrl7....X...rrl7....X...rrl7....X...rrl7.....rrl7.....rrl7....z...rrl7....z...rrl7....z...rrl7.....rrl7.....rrl7.....rrl7.....rrl7.....rrl7.....rrl7.....rrl7.....\..... ....cw1p.....

C:\Users\user\AppData\Local\Temp\y6963.tmp.dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.120826232488609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
Malicious:	**true**
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 "-f" was not found on this server. .</body></html>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cnewton doc 08.11.2022.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=Tue Mar 8 15:45:54 2022, mtime=Tue Mar 8 15:45:54 2022, atime=Fri Aug 12 01:06:11 2022, length=2343230, window=hide
Category:	dropped
Size (bytes):	1074
Entropy (8bit):	4.554552292941248
Encrypted:	false
SSDEEP:	12:8SqpUXs9gXg/XAlCPCHaXBKBnB/eLX+WAyXfcfaiFGnicvbNV7p9lAG9DtZ3YilJ:8SqeQ/XTRKJMey+tneRhp9bDv3qVu7D
MD5:	EFFF0D3E50A0D012C05106D066F8ECE9

SHA1:	1CBB4D4ED8A8205BCC101074A39D94F14E851BCC
SHA-256:	685293DAAEDEE9AE46AC93A6EDF6CDF03F2DC0D0805810D2A68DDCFFAA832CAE
SHA-512:	2872E36E61C0D66025B36EA58EDA26C64EDBE8BE82B9F3C67920B8A2C3806695D34FEA7CF4F281B89C33E6AB9E9D1CD5B4A647BA51BBCFB4CB992AB9E3E3471F
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....nI..3...nI..3.....>.#.....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.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....~.2.>.#..U.. .CNEWTO~1.DOC..b.....hT..hT..*...r....'.....c.n.e.w.t.o.n. .d.o.c. .0.8...1.1...2.0.2.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\390120\Users.user\Desktop\cnewton doc 08.11.2022.doc.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.n.e.w.t.o.n. .d.o.c. .0.8...1.1...2.0.2.2...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.....390120....

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):	95
Entropy (8bit):	4.627376468057002
Encrypted:	false
SSDEEP:	3:bDuMJle+FXF7Uk9omX1c6FXF7Uk9ov:bCMXF7p9kuXF7p9y
MD5:	92FF1982FE0A0AF246E8E293141DD9D0
SHA1:	2B3D182D219D3178040B9F2F41B196A4742FE18B
SHA-256:	23ED12834D5AB9375C9AA71150EFFA53645FD337190A76B86AEA3381372D8EC0
SHA-512:	4F9D1DAFADD29B0826B11BEE4AA9F87637B8BD82540FD57C66FC9073442399DB3BA6C0FE4FAAACDC282DFA932E440CA1EBE1D385FE82E690FA37F0BB00664519
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..cnewton doc 08.11.2022.LNK=0..[doc]..cnewton doc 08.11.2022.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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\Desktop\~$ewton doc 08.11.2022.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993716519832146
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	cnewton doc 08.11.2022.doc
File size:	2343230
MD5:	ee1d6eb5b07b99e65fc0cb477193c35c
SHA1:	9d4dbf701c8ede93a79036dd5a0316da988a2eeb
SHA256:	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab
SHA512:	869cdd01eb85cd12a1a27dc0099250e4fb33b3ed72a7e0375e80206b07b01aaff108ede1626de99f29c9a7cbc7524a4e4947b976be2e392b2d777c8df1fc54fc
SSDEEP:	49152:xyG/bJ98ozhp4kBA4Y0bRfqmlYOxtKW72swkql:QS8otukBbRfqUjRy7T
TLSH:	C4B5333D16FB0348D87D3A125E1F1EC212BDCD45E01BC82F684B657AB5377846A68EE8
File Content Preview:	PK.....!..U~...._rels/.rels...J.@.....4.E..D.....$....T..w-..j.....|.zs..z..z.*X.%(v.....6O.{PI.....`S__._x .C..CR...:....t..R.....hI.3..H.Q..*.;..=..y... n.....yo..... [vrf..A..6..3[.>_...-K....\NH!....<..r...E.B..P...<_.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682599/sample/cnewton doc 08.11.2022.doc"

Indicators

Has Summary Info:	
Application Name:	
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:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 2836

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2836
Data ASCII:	.J.Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl. .Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Funct.ion . Li. b "user3.2" Alias. "SetTim.er" (ByV8al ..... As Long*, ...5.....
Data Raw:	01 4a b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.302596554682153
Base64 Encoded:	True
Data ASCII:	I D = " { 1 4 9 A B 1 3 B - 1 5 A A - 4 3 8 2 - 8 9 7 7 - F C 2 5 F 7 E D D 7 B A } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 3 A 3 8 C 5 0 D F B 1 1 F B 1 1 F B 1 1 F B 1 1 " . . D P B = " 7 4 7 6 8 B 4 F F F 8 8 0 0 8 8 0 0 8 8 " . . G C = " A E A C 5 1 9 1 B 1 F 1 E A F 2 E A F 2 1 5 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 31 34 39 41 42 31 33 42 2d 31 35 41 41 2d 34 33 38 32 2d 38 39 37 37 2d 46 43 32 35 46 37 45 44 44 37 42 41 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5108

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5108
Entropy:	1.9370407590218233
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) > . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6897674029679903
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . ! . . . . . . . . Q . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . P . 1 . . . . . . . . . . . , . . p . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . a . . . . X . . p . . . . a . . . .

General	
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 b1 08 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.304387507848704
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . l d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . . \ \ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \ \ W i n . d o w s \ \ s y s @ t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A - .
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 c5 49 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 19:05:34.165986061 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:05:34.269232035 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 19:05:34.269417048 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:05:34.270216942 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:05:34.373137951 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 19:05:34.389308929 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 19:05:34.389625072 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:05:39.394372940 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 19:05:39.394573927 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 19:06:39.472704887 CEST	49173	80	192.168.2.22	45.8.146.139

HTTP Request Dependency Graph

- 45.8.146.139

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	45.8.146.139	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 19:05:34.270216942 CEST	0	OUT	GET /fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 45.8.146.139 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 19:05:34.389308929 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 17:05:34 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: 201 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 2d 66 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 "-f" was not found on this server. </body></html>

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2476, Parent PID: 576

General

Target ID:	0
Start time:	19:06:12
Start date:	11/08/2022
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:	0x13fb60000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E132B14	CreateDirectoryA

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E4AA0EB	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E18A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E18A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E18A5E3	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly