

JOeSandbox Cloud BASIC



**ID:** 417616

**Sample Name:** Claim Covid Tvx  
- Bandoir PBR.docx

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 20:11:35

**Date:** 19/05/2021

**Version:** 32.0.0 Black Diamond


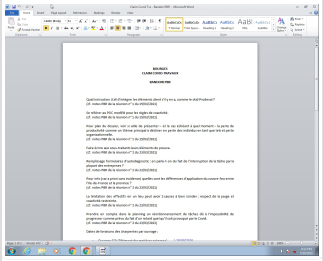
# Table of Contents

Table of Contents	2
Analysis Report Claim Covid Tvx - Bandoir PBR.docx	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Startup	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	10
General	10
File Icon	11
Network Behavior	11
Code Manipulations	11
Statistics	11
System Behavior	11
Analysis Process: WINWORD.EXE PID: 2392 Parent PID: 584	11
General	11
File Activities	11
File Created	11
File Deleted	12
File Read	12
Registry Activities	12
Key Created	12
Key Value Created	12
Key Value Modified	13
Disassembly	15

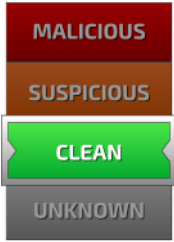
# Analysis Report Claim Covid Tvx - Bandoir PBR.docx

## Overview

### General Information

Sample Name:	Claim Covid Tvx - Bandoir PBR.docx
Analysis ID:	417616
MD5:	405825f6d97456d.
SHA1:	74a879ae98debb..
SHA256:	3d6b6526bbc916..
Infos:	
Most interesting Screenshot:	

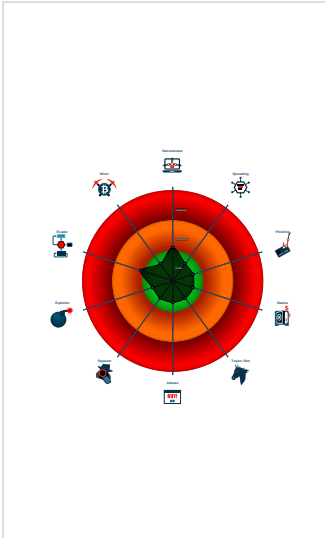
### Detection

	
Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

### Signatures

No high impact signatures.
----------------------------

### Classification



## Startup

- System is w7x64
-  WINWORD.EXE (PID: 2392 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cleanup

## Malware Configuration

No configs have been found

## Yara Overview

No yara matches

## Sigma Overview

No Sigma rule has matched

## Signature Overview



- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section
















There are no malicious signatures, [click here to show all signatures](#).

## 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	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

## Behavior Graph

Legend:

-  Process
-  Signature
-  Created File
-  DNS/IP Info
-  Is Dropped
-  Is Windows Process
-  Number of created Registry Values
-  Number of created Files
-  Visual Basic
-  Delphi
-  Java
-  .Net C# or VB.NET
-  C, C++ or other language
-  Is malicious
-  Internet

**Behavior Graph**

**ID:** 417616

**Sample:** Claim Covid Tvx - Bandoir P...

**Startdate:** 19/05/2021

**Architecture:** WINDOWS

**Score:** 0



MALICIOUS


SUSPICIOUS




CLEAN

UNKNOWN

started


WINWORD.EXE




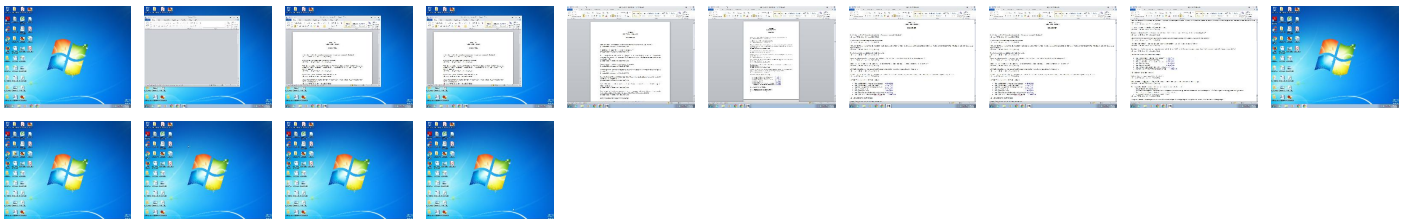

 298
  25

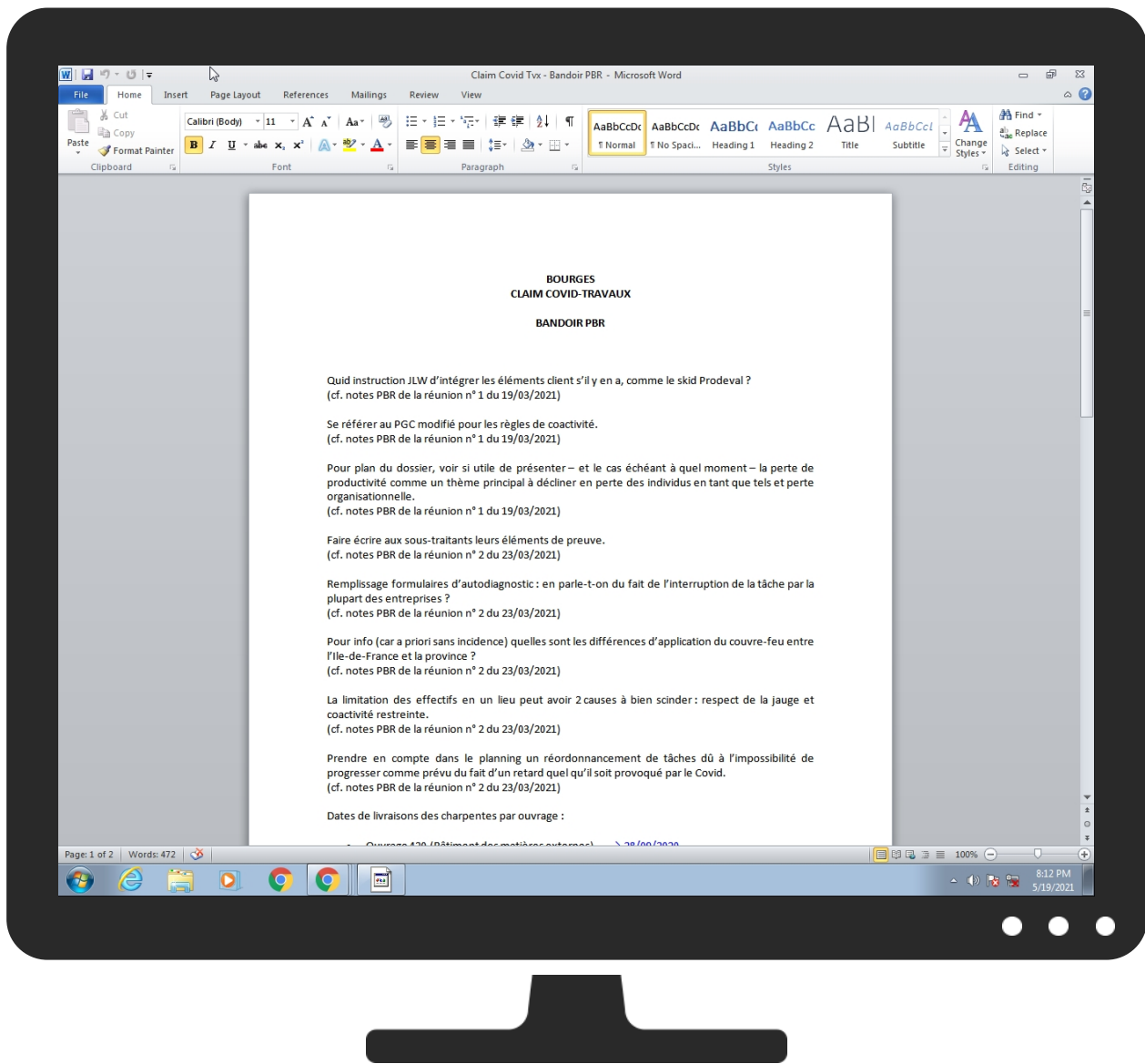
+  
RESET  
-

## 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

No Antivirus matches

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

## Domains and IPs

## Contacted Domains

No contacted domains info

## Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	417616
Start date:	19.05.2021
Start time:	20:11:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Claim Covid Tvx - Bandoir PBR.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	2
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:	<ul style="list-style-type: none"><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winDOCX@1/8@0/0
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .docx</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Scroll down</li><li>• Close Viewer</li></ul>
Warnings:	Show All <ul style="list-style-type: none"><li>• Exclude process from analysis (whitelisted): dllhost.exe</li><li>• Report size getting too big, too many NtQueryAttributesFile calls found.</li></ul>

## Simulations

### Behavior and APIs

No simulations

## Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BCB42A3-025D-4403-9DBE-B492A11253DC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..... ..... ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3A3DB071-4F03-4D2B-8C5C-F1ADB9722678}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8118
Entropy (8bit):	3.5683146808303308
Encrypted:	false
SSDEEP:	192:n0M0kmZMaLqMEDOAuO4ROHZOHV0Oe40no/6Qy6QEAKx6b:0UmZH+TyzRYo2/bngtyFEAc0
MD5:	7BEE0FE6548FC35A5B904CA17B71E4B7
SHA1:	0BF626F096104D23E97110FB101E5ADEAF567657
SHA-256:	A6F64C487CE1D78F1BDF7E7A088530CFF6A734E3E4A885E2794650C028285D2A
SHA-512:	2A2A1ADD516BB88F4390DB371729F3533482EBFDE1FE6555E1D59754BEA410A57C284FF1A4B6C6422FD78C2738A7BBD2ECC41AC5472FC4D49782610C9C65735
Malicious:	false
Reputation:	low
Preview:	..B.O.U.R.G.E.S...C.L.A.I.M..C.O.V.I.D...T.R.A.V.A.U.X.....B.A.N.D.O.I.R..P.B.R.....Q.u.i.d..i.n.s.t.r.u.c.t.i.o.n..J.L.W..d..i.n.t..g.r.e.r..l.e.s...l..m.e.n.t.s..c.l.i.e.n.t..s.. i.l..y..e.n..a..c.o.m.m.e..l.e..s.k.i.d..P.r.o.d.e.v.a.l...?...(c.f.....n.o.t.e.s..P.B.R..d.e..l.a..r...u.n.i.o.n..n.....1..d.u..1.9./0.3./2.0.2.1.).....S.e..r..f..r.e.r..a.u..P.G.C.. .m.o.d.i.f.i...p.o.u.r..l.e.s..r..g.l.e.s..d.e..c.o.a.c.t.i.v.i.t.....(c.f.....n.o.t.e.s..P.B.R.....<...T...V...X...Z.....p..r.....F...H.....V...X.....0..0..... ..... .....gd.....gdX1.....gdic.....

C:\Users\user\AppData\Local\Temp\msocb89.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE



<b>C:\Users\user\AppData\Local\Temp\msocb89.tmp</b>	
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlojAxb4bxdT/CS3wKxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87841
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w...!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....!.....'.....b...RQ.xx.... .....,.....+.....yy...:..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@.....zz.mm.^.....yw.....yx.xw.RR.,*..+..... .....8...>.....4567...=.../0123.....<9:..()*+,-B.@....."#\$%&'..... !.... .....C.?....A;<...HT(;;

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Claim Covid Tvx - Bandoir PBR.LNK</b>	
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=Wed Aug 26 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Thu May 20 02:12:35 2021, length=16919, window=hide
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	4.591819045657863
Encrypted:	false
SSDEEP:	48:8i4/XTFGq2Cb163lQh2i4/XTFGq2Cb163lQ/:8J/XJGq2BIQh2J/XJGq2BIQ/
MD5:	D6B4F97061CF9306EB1B04A1FB2D6F1C
SHA1:	FED733806292E68CCB3740CB2DFEFAB4139857EB
SHA-256:	B399B4D239D80A3D7A1EC9A37C1069BB253CB5D0E32161044E88850F834F50D2
SHA-512:	4FBFB5767DD6016D3FBD0B096B23C3AAF3D25D0407919D60A2853DD74C277D685CC77FB10640C2E41CA333F56187F0A715F47F218AF9D7A1ECB8E1BA3C361F
Malicious:	false
Reputation:	low
Preview:	L.....F.....8.r.{.8.r.{...t%M...B.....P.O. ....+00.../C:\.....t1.....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.....Q.y..user.8.....QK.X.Q.y*...&=...U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._...=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2 .1.7.6.9.....2..B...R.. CLAIMC-1.DOC..r.....Q.y.Q.y*...8.....C.l.a.i.m. .C.o.v.i.d. .T.v.x. -. .B.a.n.d.o.i.r. .P.B.R...d.o.c.x.....-...8..[.....?J..... .C:\Users\.#.....\936905\Users.user\Desktop\Claim Covid Tvx - Bandoir PBR.docx.9.....\.....\.....\.....\D.e.s.k.t.o.p\..C.l.a.i.m. .C.o.v.i.d. .T.v.x. -. .B.a.n.d.o.i.r. .P.B.R...d.o.c.x.....;..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.

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	127
Entropy (8bit):	4.633463401585562
Encrypted:	false
SSDEEP:	3:Hto0lcBHfZul+o0lcBHfZulmxWto0lcBHfZulv:HtoxcB/QhxcB/QzoxcB/Q1
MD5:	26BE34E6054191E5EAA93606038A3C16
SHA1:	671BC0CDD872A1C10DB1A4D4EF884C59040CECEE
SHA-256:	2101CA14A43981BACFB60766DFB9ED0426DA3203C508F6CD4ADD2FC6E5058103
SHA-512:	8EE4E6679401C330A36EC7F295B606EFD060A88B9BB8719236D7279F1CCEAC1390D9774FD60039A75EA80B7BC32EE5256181CEB7780F2BF4DFFC5C7CB877C54
Malicious:	false
Reputation:	low
Preview:	[misc]..Claim Covid Tvx - Bandoir PBR.LNK=0..Claim Covid Tvx - Bandoir PBR.LNK=0..[misc]..Claim Covid Tvx - Bandoir PBR.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOG5Gll3GwSKG/f2+1/l/n:vdsCkWtW2llID9l

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCDBBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....W....Z.....W....X...

<b>C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryFR040c.lex</b>	
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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDFF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..


<b>C:\Users\user\Desktop\~\$aim Covid Tvx - Bandoir PBR.docx</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCDBBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....W....Z.....W....X...

Static File Info

<b>General</b>	
File type:	Microsoft Word 2007+
Entropy (8bit):	7.441952861067262
TrID:	<ul style="list-style-type: none"><li>Word Microsoft Office Open XML Format document (49504/1) 49.01%</li><li>Word Microsoft Office Open XML Format document (43504/1) 43.07%</li><li>ZIP compressed archive (8000/1) 7.92%</li></ul>
File name:	Claim Covid Tvx - Bandoir PBR.docx
File size:	16919
MD5:	405825f6d97456d98d1620db5d1f8314
SHA1:	74a879ae98debb1449692440266e37738d2a7d72
SHA256:	3d6b6526bbc91680db4b6aac33f809bd1758c37be92c6a5193620011c74bcf5e
SHA512:	84d105938a5b92e54cc410f5d25f89d11c0e582492b50cc85d6edb8853bb07f305147b791b755c8e104256eb5d619bb090b922e32b90f647aa76ea3e2a61a9f5

General	
SSDEEP:	192;jh04RPS8YGxTtIsERnKzYpkyAqiCyOA8MS48TuX63DWs9YeYmCAsxGnpX5fx/La:dhVxT2ZNzAqi+AlVmCOndbDCzke
File Content Preview:	PK.....!.2.oWf.....[Content_Types].xml ...(. ..... ..... .....

## File Icon

	
Icon Hash:	e4e6a2a2a4b4b4a4

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## System Behavior

Analysis Process: WINWORD.EXE PID: 2392 Parent PID: 584

### General

Start time:	20:12:36
Start date:	19/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f1c0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### File Activities

#### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VE	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	7FEE93F26B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\-\$aim Covid Vtx - Bandoir PBR.docx	success or wait	1	7FEE9319AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7FR.dub	unknown	16	success or wait	1	7FEE911E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryFR040c.lex	unknown	1	success or wait	1	7FEE9110793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryFR040c.lex	unknown	4096	success or wait	1	7FEE917AD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE9110793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE917AD58	ReadFile
C:\Users\user\Desktop\Claim Covid Tvx - Bandoir PBR.docx	5989	261	success or wait	1	7FEE9319AC0	unknown

## Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3BB9	success or wait	1	7FEE9319AC0	unknown

Key Value Created
<p>                     1. <b>Key Value Created</b>                      2. <b>Key Value Created</b>                      3. <b>Key Value Created</b>                      4. <b>Key Value Created</b>                      5. <b>Key Value Created</b>                      6. <b>Key Value Created</b>                      7. <b>Key Value Created</b>                      8. <b>Key Value Created</b>                      9. <b>Key Value Created</b>                      10. <b>Key Value Created</b>                      11. <b>Key Value Created</b>                      12. <b>Key Value Created</b>                      13. <b>Key Value Created</b>                      14. <b>Key Value Created</b>                      15. <b>Key Value Created</b>                      16. <b>Key Value Created</b>                      17. <b>Key Value Created</b>                      18. <b>Key Value Created</b>                      19. <b>Key Value Created</b>                      20. <b>Key Value Created</b>                      21. <b>Key Value Created</b>                      22. <b>Key Value Created</b>                      23. <b>Key Value Created</b>                      24. <b>Key Value Created</b>                      25. <b>Key Value Created</b>                      26. <b>Key Value Created</b>                      27. <b>Key Value Created</b>                      28. <b>Key Value Created</b>                      29. <b>Key Value Created</b>                      30. <b>Key Value Created</b>                      31. <b>Key Value Created</b>                      32. <b>Key Value Created</b>                      33. <b>Key Value Created</b>                      34. <b>Key Value Created</b>                      35. <b>Key Value Created</b>                      36. <b>Key Value Created</b>                      37. <b>Key Value Created</b>                      38. <b>Key Value Created</b>                      39. <b>Key Value Created</b>                      40. <b>Key Value Created</b>                      41. <b>Key Value Created</b>                      42. <b>Key Value Created</b>                      43. <b>Key Value Created</b>                      44. <b>Key Value Created</b>                      45. <b>Key Value Created</b>                      46. <b>Key Value Created</b>                      47. <b>Key Value Created</b>                      48. <b>Key Value Created</b>                      49. <b>Key Value Created</b>                      50. <b>Key Value Created</b>                      51. <b>Key Value Created</b>                      52. <b>Key Value Created</b>                      53. <b>Key Value Created</b>                      54. <b>Key Value Created</b>                      55. <b>Key Value Created</b>                      56. <b>Key Value Created</b>                      57. <b>Key Value Created</b>                      58. <b>Key Value Created</b>                      59. <b>Key Value Created</b>                      60. <b>Key Value Created</b>                      61. <b>Key Value Created</b>                      62. <b>Key Value Created</b>                      63. <b>Key Value Created</b>                      64. <b>Key Value Created</b>                      65. <b>Key Value Created</b>                      66. <b>Key Value Created</b>                      67. <b>Key Value Created</b>                      68. <b>Key Value Created</b>                      69. <b>Key Value Created</b>                      70. <b>Key Value Created</b>                      71. <b>Key Value Created</b>                      72. <b>Key Value Created</b>                      73. <b>Key Value Created</b>                      74. <b>Key Value Created</b>                      75. <b>Key Value Created</b>                      76. <b>Key Value Created</b>                      77. <b>Key Value Created</b>                      78. <b>Key Value Created</b>                      79. <b>Key Value Created</b>                      80. <b>Key Value Created</b>                      81. <b>Key Value Created</b>                      82. <b>Key Value Created</b>                      83. <b>Key Value Created</b>                      84. <b>Key Value Created</b>                      85. <b>Key Value Created</b>                      86. <b>Key Value Created</b>                      87. <b>Key Value Created</b>                      88. <b>Key Value Created</b>                      89. <b>Key Value Created</b>                      90. <b>Key Value Created</b>                      91. <b>Key Value Created</b>                      92. <b>Key Value Created</b>                      93. <b>Key Value Created</b>                      94. <b>Key Value Created</b>                      95. <b>Key Value Created</b>                      96. <b>Key Value Created</b>                      97. <b>Key Value Created</b>                      98. <b>Key Value Created</b>                      99. <b>Key Value Created</b>                      100. <b>Key Value Created</b> </p>

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings	binary	05 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F3BB9	F3BB9	binary	04 00 00 00 58 09 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 75 89 77 0D 26 4D D7 01 B9 3B 0F 00 B9 3B 0F 00 00 00 00 00 DB 04 00 00 02 00 FF FF FF FF 00	success or wait	1	7FEE9319AC0	unknown

Key Value Modified



