

JoeSandbox Cloud BASIC



ID: 438536

Sample Name: CRE Cash Flow

- ETBF - Becker.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 18:13:40

Date: 22/06/2021

Version: 32.0.0 Black Diamond


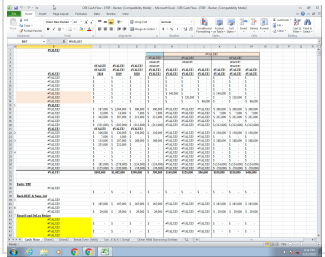
Table of Contents

Table of Contents	2
Windows Analysis Report CRE Cash Flow - ETBF - Becker.xls	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	6
Contacted IPs	6
General Information	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	7
Static OLE Info	7
General	7
OLE File "CRE Cash Flow - ETBF - Becker.xls"	7
Indicators	8
Summary	8
Document Summary	8
Streams	8
Network Behavior	8
Code Manipulations	8
Statistics	8
System Behavior	8
Analysis Process: EXCEL.EXE PID: 1924 Parent PID: 584	8
General	8
File Activities	9
File Created	9
File Deleted	9
File Moved	9
Registry Activities	9
Key Created	9
Key Value Created	9
Disassembly	9

Windows Analysis Report CRE Cash Flow - ETBF - Beck...

Overview

General Information

Sample Name:	CRE Cash Flow - ETBF - Becker.xls
Analysis ID:	438536
MD5:	0d701f8c3fd87eb..
SHA1:	4f25bbee69dd003.
SHA256:	bbb844c0d0874e..
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

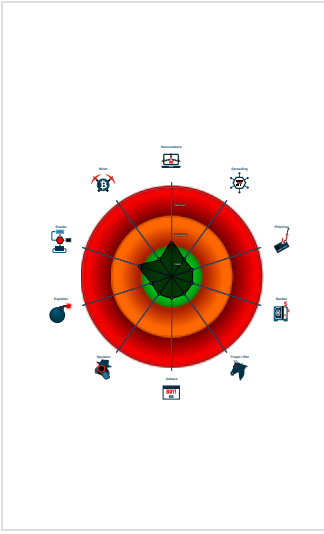
UNKNOWN

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

Signatures

No high impact signatures.

Classification



Process Tree

- System is w7x64
-  EXCEL.EXE (PID: 1924 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- cleanup

Malware Configuration

No configs have been found


Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

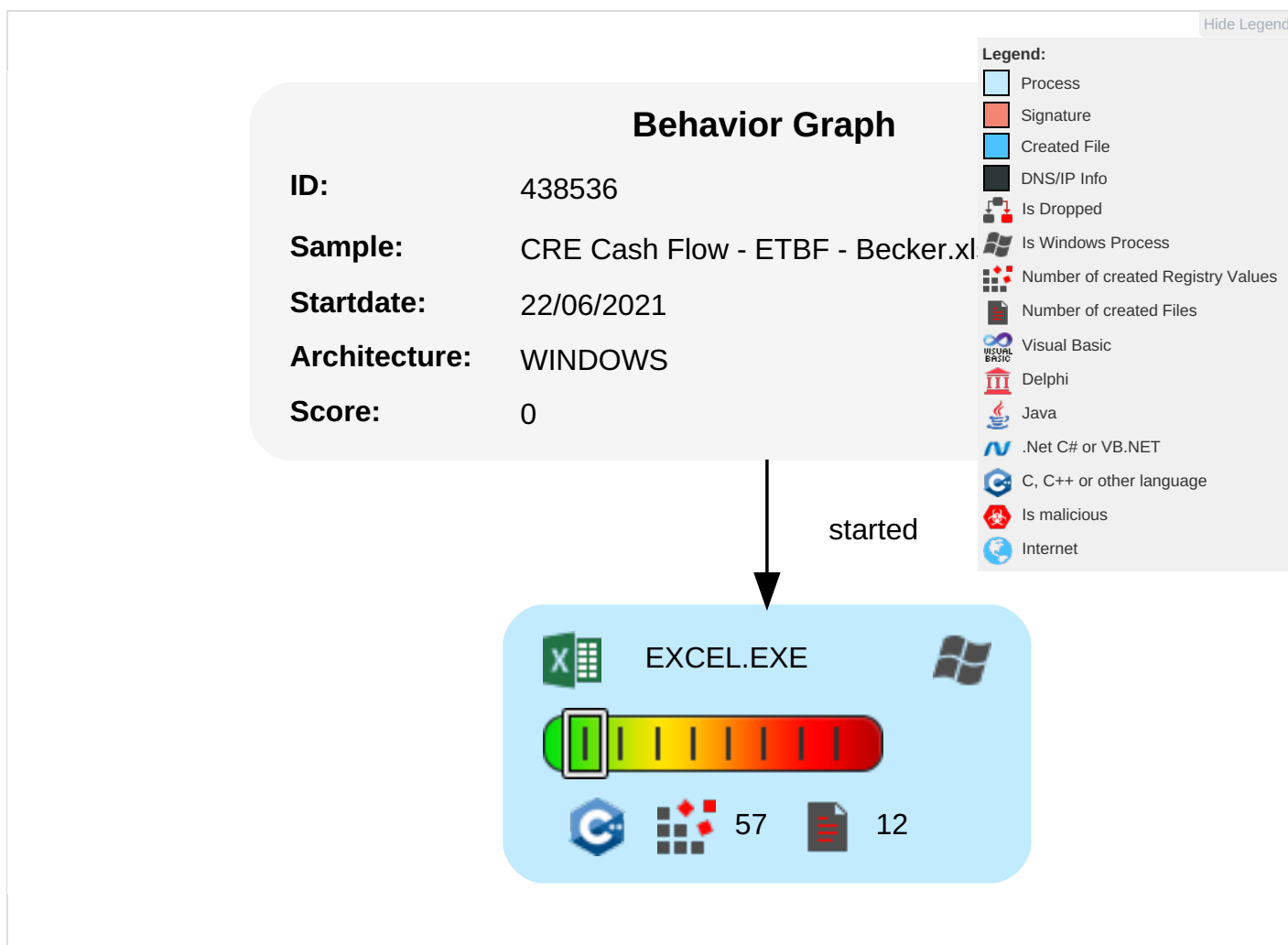
 Click to jump to signature section

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	Direct Volume Access	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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

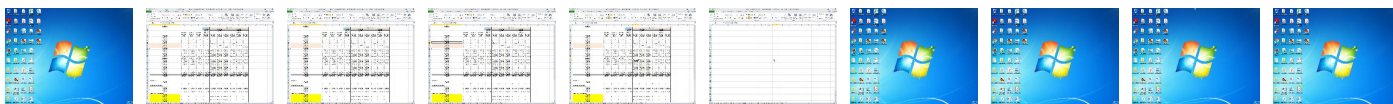
Behavior Graph



Screenshots

Thumbnails

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



Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438536
Start date:	22.06.2021
Start time:	18:13:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CRE Cash Flow - ETBF - Becker.xls
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">• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winXLS@1/0@0/0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .xls• Found Word or Excel or PowerPoint or XPS Viewer• Attach to Office via COM• Scroll down• Close Viewer
Warnings:	Show All

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

No created / dropped files found

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Employee, Last Saved By: David G. Schreiber, Name of Creating Application: Microsoft Excel, Last Printed: Wed Mar 10 17:03:02 2021, Create Time/Date: Thu Nov 8 15:24:39 2001, Last Saved Time/Date: Tue Jun 22 16:39:09 2021, Security: 0
Entropy (8bit):	2.9256624131355142
TrID:	<ul style="list-style-type: none">Microsoft Excel sheet (30009/1) 78.94%Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	CRE Cash Flow - ETBF - Becker.xls
File size:	303616
MD5:	0d701f8c3fd87eb9f1ff112dd917831e
SHA1:	4f25bbe69dd003073220de14e3d1c4bb2d20c11
SHA256:	bbb844c0d0874ef8c925e61ba1bb094f29fca834d534357208541c866292182a
SHA512:	3772be278535ad0ac434d9153ef0a279ce29c0d4eb812173493823d8be73bb047c380787f33e91863e6ce964454cb255979c68d690b29744c72bcbf4eb55d86c
SSDEEP:	6144:3KxEtjPOtioVjDGUU1qfDlavx+W/IeyDV7peO:KDZpeO
File Content Preview:>.....O.....J...K... L...M...N.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "CRE Cash Flow - ETBF - Becker.xls"

Indicators		
Has Summary Info:		True
Application Name:		Microsoft Excel
Encrypted Document:		False
Contains Word Document Stream:		False
Contains Workbook/Book Stream:		True
Contains PowerPoint Document Stream:		False
Contains Visio Document Stream:		False
Contains ObjectPool Stream:		
Flash Objects Count:		
Contains VBA Macros:		False

Summary		
Code Page:		1252
Author:		Employee
Last Saved By:		David G. Schreiber
Last Printed:		2021-03-10 17:03:02
Create Time:		2001-11-08 15:24:39
Last Saved Time:		2021-06-22 15:39:09
Creating Application:		Microsoft Excel
Security:		0

Document Summary		
Document Code Page:		1252
Thumbnail Scaling Desired:		False
Company:		Moody National Bank
Contains Dirty Links:		False
Shared Document:		False
Changed Hyperlinks:		False
Application Version:		1048576

Streams		
----------------	--	--

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1924 Parent PID: 584

General

Start time:	18:14:34
Start date:	22/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13ffb0000

File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly