

JoeSandbox Cloud BASIC



ID: 467210

Sample Name: 00620 - 2011

Dept Expense Detail.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 00:39:02

Date: 18/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report 00620 - 2011 Dept Expense Detail.xls	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Initial Sample	3
Sigma Overview	3
Jbx Signature Overview	3
HIPS / PFW / Operating System Protection Evasion:	4
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	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
General Information	6
Simulations	6
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
File Icon	8
Static OLE Info	8
General	8
OLE File "00620 - 2011 Dept Expense Detail.xls"	8
Indicators	8
Summary	8
Document Summary	8
Streams with VBA	8
Streams	8
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: EXCEL.EXE PID: 2672 Parent PID: 584	9
General	9
File Activities	9
File Created	9
File Deleted	9
File Moved	9
File Written	9
Registry Activities	9
Key Created	9
Key Value Created	9
Disassembly	9

Windows Analysis Report 00620 - 2011 Dept Expense D...

Overview

General Information

Sample Name:

00620 - 2011 Dept Expense Detail.xls

Analysis ID:

467210

MD5:

57bcd4f4ddd4c73e..

SHA1:

fb7ee5e7a2ef599..

SHA256:

5c0e2dc5c3e763...

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Hidden Macro 4.0

Score:

20

Range:

0 - 100

Whitelisted:

false

Confidence:

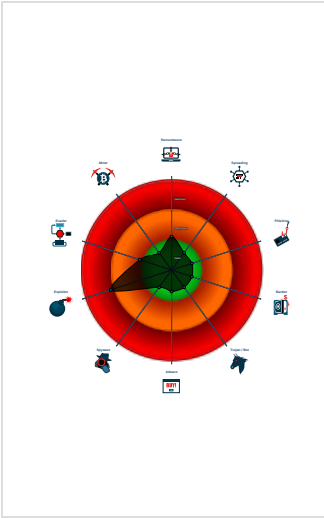
80%

Signatures

Yara detected hidden Macro 4.0 in E...

Document contains embedded VBA ...

Classification



Process Tree

- System is w7x64
- EXCEL.EXE (PID: 2672 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
00620 - 2011 Dept Expense Detail.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

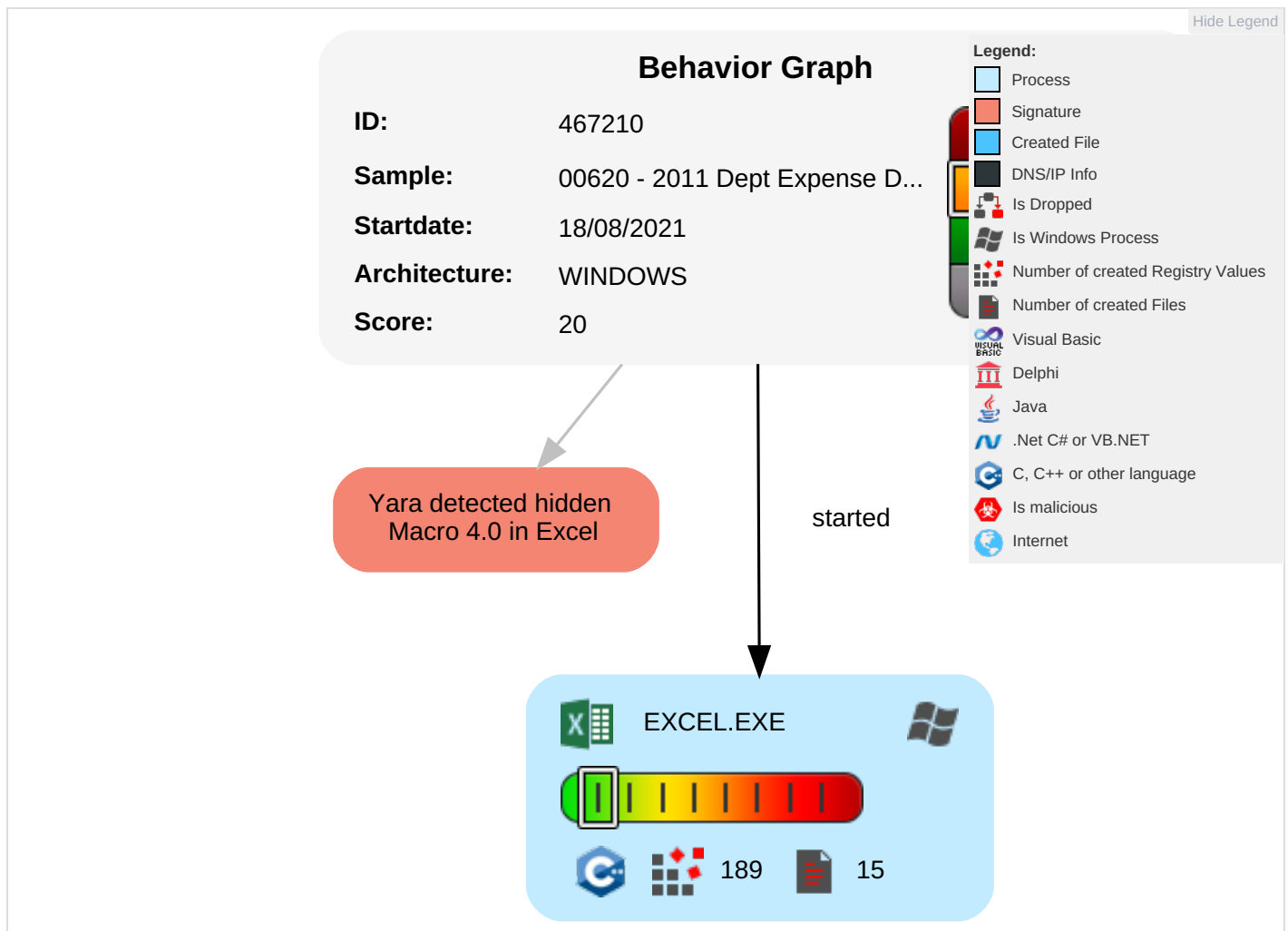


Yara detected hidden Macro 4.0 in Excel

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	Scripting 1	Path Interception	Path Interception	Scripting 1	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

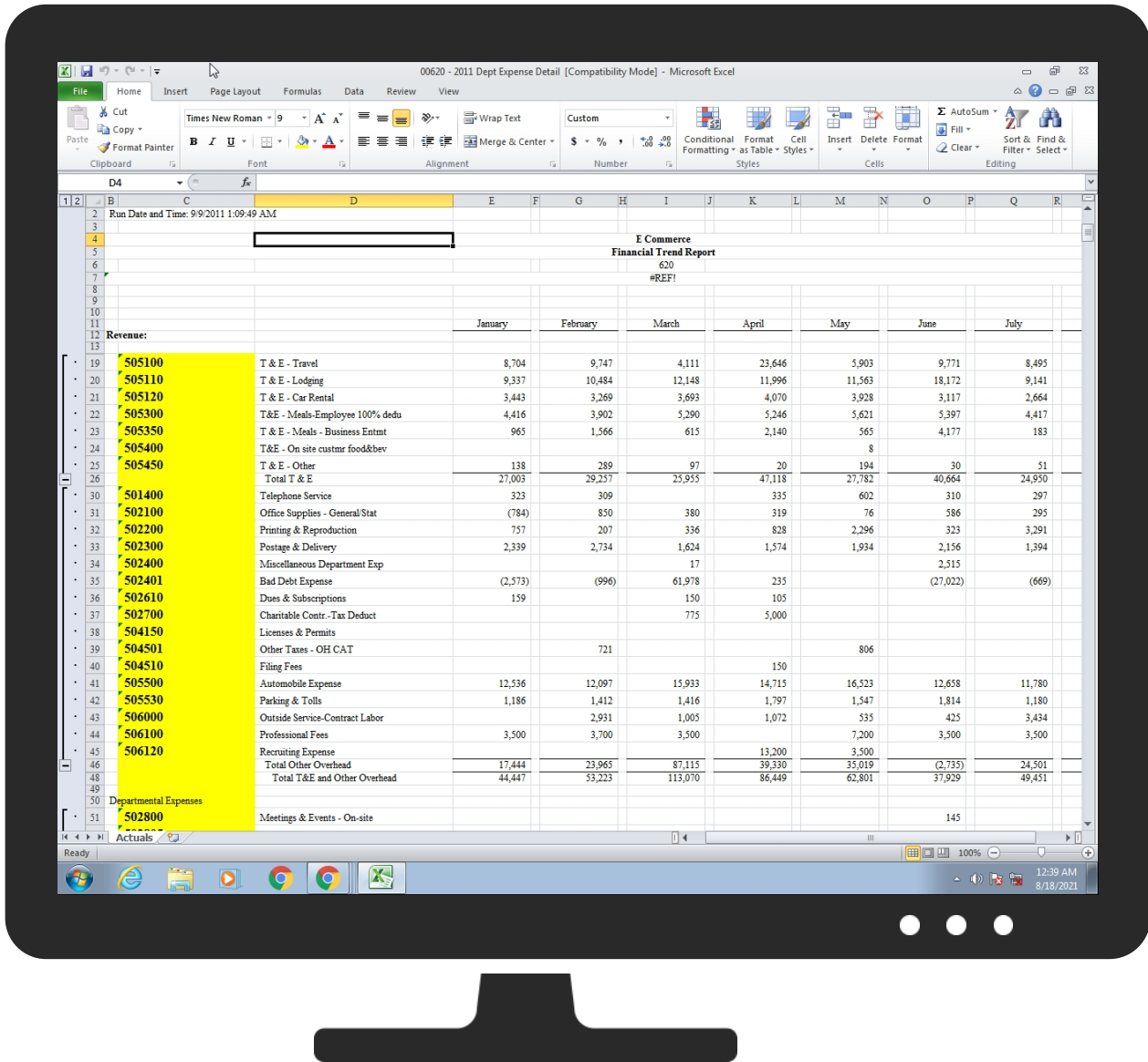
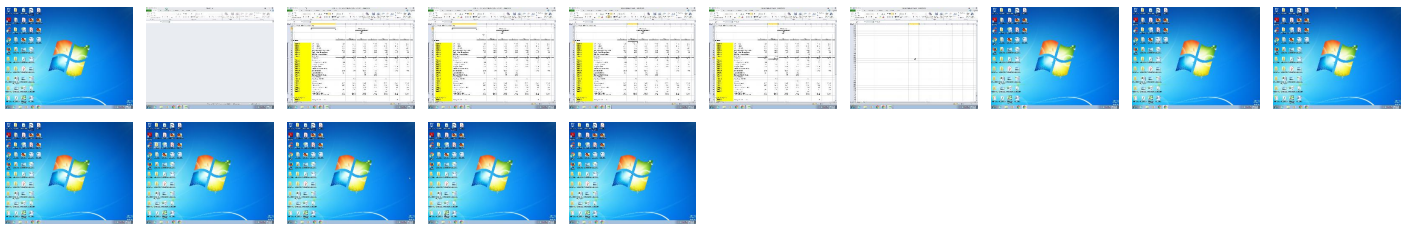
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
00620 - 2011 Dept Expense Detail.xls	2%	Virustotal		Browse
00620 - 2011 Dept Expense Detail.xls	2%	ReversingLabs	Document.Trojan.CutwailOLE	

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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	467210
Start date:	18.08.2021
Start time:	00:39:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	00620 - 2011 Dept Expense Detail.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:	• EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus20.expl.winXLS@1/1@0/0
Cookbook Comments:	• 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

C:\Users\user1\AppData\Local\Temp\VBEMISForms.exe	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254475228883147
Encrypted:	false
SSDEEP:	1536:C6vL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CWJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	CCD3611D3446F144D1CA56FBC509280F
SHA1:	633BE892B522D00D8F03C98634B311B63C2396C3
SHA-256:	D353C4B1F4F3800EE210702E80E0BAF6D73069BBD18675122993661A5B46A54B
SHA-512:	4D0DE72EF3E04F5B7205866B7C051BD7B8A3F8CA31E5089C71FA56D959B918D834BB7D11BFD2467962ED7F5248B768BE60E3A41205222F624DB6449F6FE2FA06
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....#.....\$.....d.....X.....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....\$.....P.....D.....p.....8.....d.....X.....L.....x.....@......l......4!...!...!...™...".(##...#.T\$..\$..%..%..%..H&.. &... 't'...'<((...(..)h)...)..0*...*.. \+...+..\$. , , , , , P- - - - D/./...0..p0...0.81..1...2..d2...2...3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... \$.x..xG.....T.....&!.....

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.2, Code page: 1252, Author: AutoNation USA, Last Saved By: DupreeP, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Feb 4 16:48:36 1999, Last Saved Time/Date: Tue Sep 20 15:04:38 2011, Security: 0

General	
Entropy (8bit):	4.043229382190713
TrID:	- Microsoft Excel sheet (30009/1) 47.99% - Microsoft Excel sheet (alternate) (24509/1) 39.20% - Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	00620 - 2011 Dept Expense Detail.xls
File size:	53760
MD5:	57bcd4f4ddd4c73eb7b1579edf9e10d62
SHA1:	fb7ee5e7a2ef599bcbf982ff6823387792a90335
SHA256:	5c0e2dc5c3e763417c7fb8f02f8d12a64e9aad4f7fa4cf0e7a09e31bfe20e4fd
SHA512:	f0f613246b8fd11cca39102e1aaeea11b3c2228cbee6778245bb34bc96c59bd4ac069e80020ba0bdfb0d90a4b8ccc6387922b1ec72915fd15c8666bc90643b
SSDEEP:	768:g9RUbndMNMu2jm1xW5aUgAVZx5mXMr2q3rLrLn+zghx0QQDI:iKndMwfjSW5SAVZdygP8
File Content Preview:	>.....M.....

File Icon	
	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "00620 - 2011 Dept Expense Detail.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:	True

Summary	
Code Page:	1252
Author:	AutoNation USA
Last Saved By:	DupreeP
Create Time:	1999-02-04 16:48:36
Last Saved Time:	2011-09-20 14:04:38
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	730895

Streams with VBA

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2672 Parent PID: 584

General

Start time:	00:39:35
Start date:	18/08/2021
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:	0x13fe80000
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

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

