ID: 467210
Sample Name: 00620 - 2011 Dept Expense Detail.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 00:48:00
Date: 18/08/2021
Version: 33.0.0 White Diamond

Table of Contents

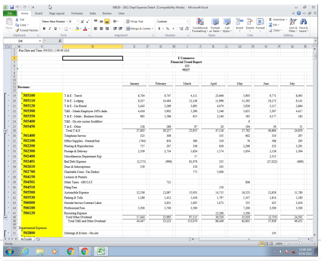
Windows Analysis Report 00620 - 2011 Dept Expense D…

Overview

General Information

Sample Name:	00620 - 2011 Dept Expense Detail.xls
Analysis ID:	467210
MD5:	57bcdf4ddd4c73e..
SHA1:	fb7ee5e7a2ef599..
SHA256:	5c0e2dc5c3e763..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Hidden Macro 4.0

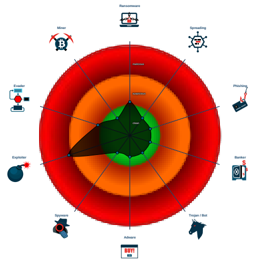
Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Yara detected hidden Macro 4.0 in E…

Document contains embedded VBA …

Classification



Process Tree

- System is w7x64
- EXCEL.EXE (PID: 2652 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

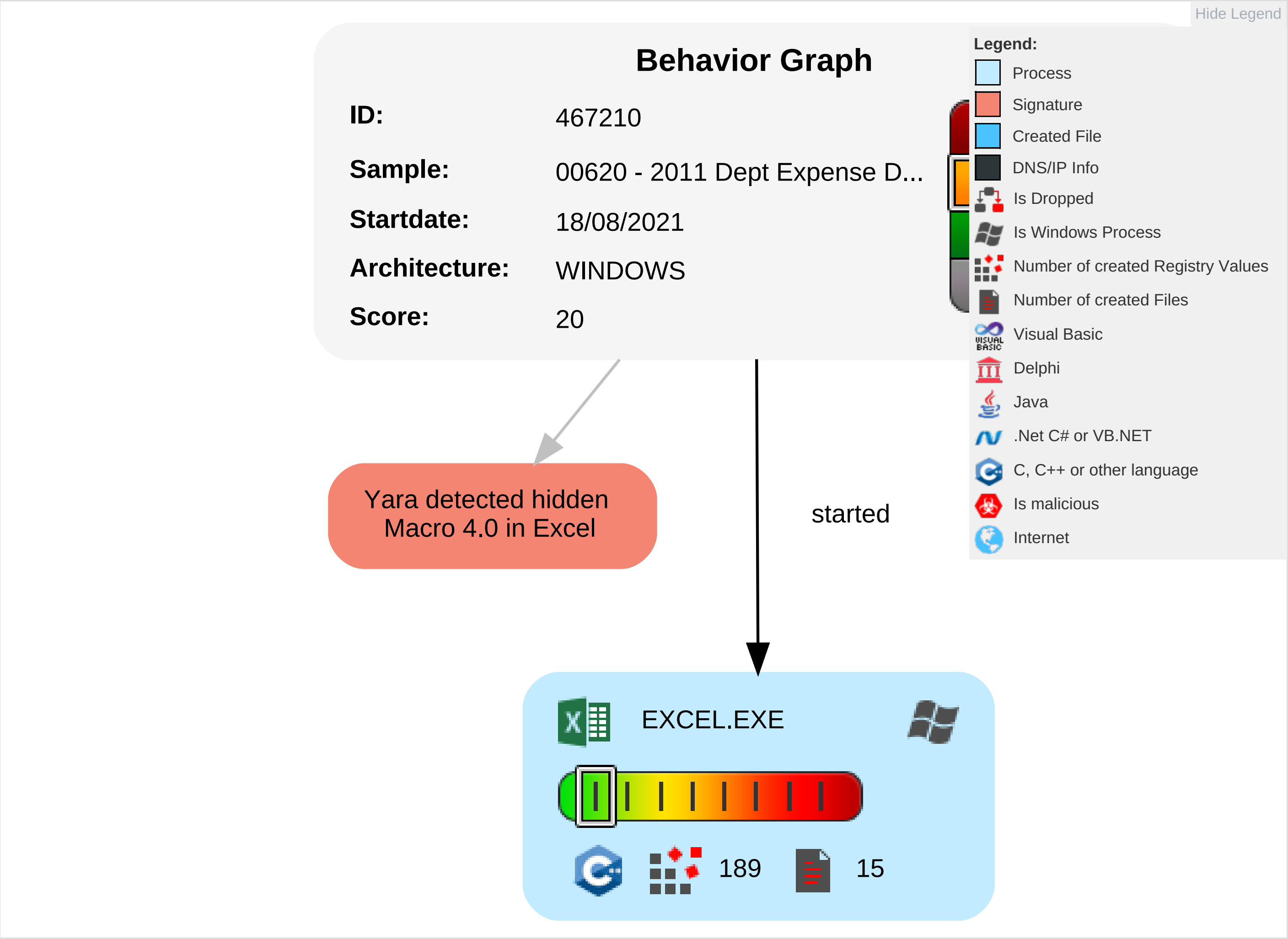
HIPS / PFW / Operating System Protection Evasion:

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

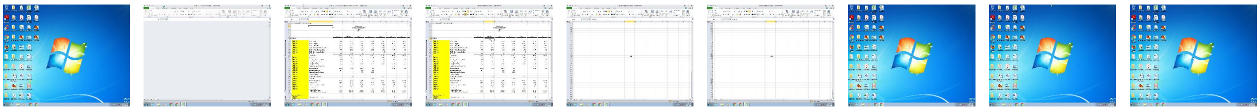
Behavior Graph

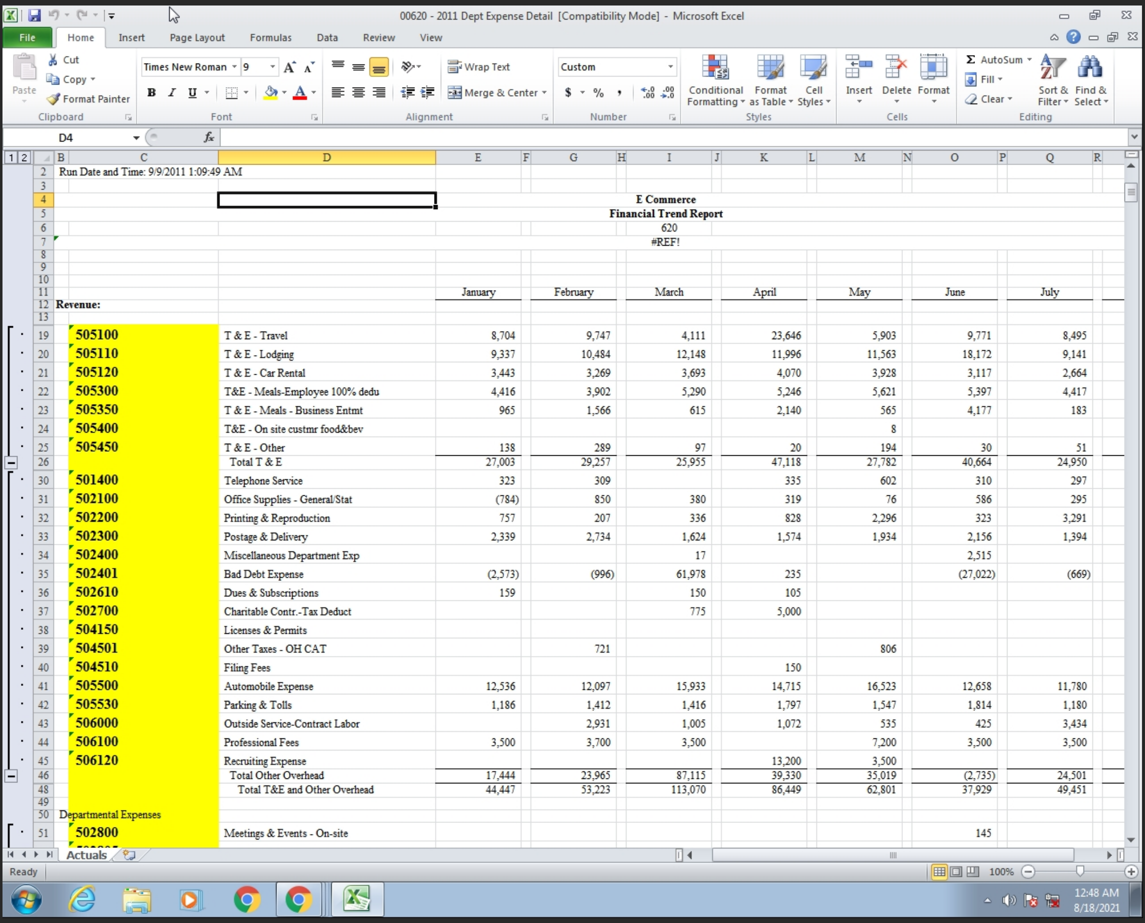


Screenshots

Thumbnails

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





00620 - 2011 Dept Expense Detail [Compatibility Mode] - Microsoft Excel

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
2	Run Date and Time: 9/9/2011 1:09:49 AM																
3																	
4								E Commerce									
5								Financial Trend Report									
6								620									
7								#REF!									
8																	
9																	
10																	
11				January		February		March		April		May		June		July	
12	Revenue:																
13																	
19		505100	T & E - Travel	8,704		9,747		4,111		23,646		5,903		9,771		8,495	
20		505110	T & E - Lodging	9,337		10,484		12,148		11,996		11,563		18,172		9,141	
21		505120	T & E - Car Rental	3,443		3,269		3,693		4,070		3,928		3,117		2,664	
22		505300	T&E - Meals-Employee 100% dedu	4,416		3,902		5,290		5,246		5,621		5,397		4,417	
23		505350	T & E - Meals - Business Entmt	965		1,566		615		2,140		565		4,177		183	
24		505400	T&E - On site custmr food&bev									8					
25		505450	T & E - Other	138		289		97		20		194		30		51	
26			Total T & E	27,003		29,257		25,955		47,118		27,782		40,664		24,950	
30		501400	Telephone Service	323		309				335		602		310		297	
31		502100	Office Supplies - General/Stat	(784)		850		380		319		76		586		295	
32		502200	Printing & Reproduction	757		207		336		828		2,296		323		3,291	
33		502300	Postage & Delivery	2,339		2,734		1,624		1,574		1,934		2,156		1,394	
34		502400	Miscellaneous Department Exp					17						2,515			
35		502401	Bad Debt Expense	(2,573)		(996)		61,978		235				(27,022)		(669)	
36		502610	Dues & Subscriptions	159				150		105							
37		502700	Charitable Contr.-Tax Deduct					775		5,000							
38		504150	Licenses & Permits														
39		504501	Other Taxes - OH CAT			721						806					
40		504510	Filing Fees							150							
41		505500	Automobile Expense	12,536		12,097		15,933		14,715		16,523		12,658		11,780	
42		505530	Parking & Tolls	1,186		1,412		1,416		1,797		1,547		1,814		1,180	
43		506000	Outside Service-Contract Labor			2,931		1,005		1,072		535		425		3,434	
44		506100	Professional Fees	3,500		3,700		3,500				7,200		3,500		3,500	
45		506120	Recruiting Expense							13,200		3,500					
46			Total Other Overhead	17,444		23,965		87,115		39,330		35,019		(2,735)		24,501	
48			Total T&E and Other Overhead	44,447		53,223		113,070		86,449		62,801		37,929		49,451	
49																	
50	Departmental Expenses																
51		502800	Meetings & Events - On-site											145			

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:	00:48:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 51s
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)
Run name:	Without Instrumentation
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 • 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\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254329420014995
Encrypted:	false
SSDEEP:	1536:C6QL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:C5JNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	BA3A5A8B120D0E05EC631751C07686D5
SHA1:	97CC5690EFF6CA2B171FB5FC9C2DE275FF3E1C4F
SHA-256:	6C8F46438F09ED16AF36DF695946F806C5DD8406EBFA9D1930AC7BA6C941F7C8
SHA-512:	85929616D6BB719D5DB8AFDDAF1A12CF61A4E38F6B8C8B2FC78FF05336CDA8A2151514D90AEF46BC9CB182D802D78BD801C77CB9721D1A878A3C2DD5004F8 9
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
Entropy (8bit):	4.043229382190713

General

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:	57bcdf4ddd4c73eb7b1579edf9e10d62
SHA1:	fb7ee5e7a2ef599bcbf982ff6823387792a90335
SHA256:	5c0e2dc5c3e763417c7fb8f02f8d12a64e9aad4f7fa4cf0e7a09e31bfe20e4fd
SHA512:	f0f613246b8fd11cca39102e1aaeea11b3c2228cbee6778245bb34bc96c59bd4ac069e80020ba0bdfb0d90a4b8ccccc6387922b1ec72915fd15c8666bc90643b
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: 2652 Parent PID: 584

General

Start time:	00:48:36
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:	0x13f030000
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