ID: 562530
Sample Name: Contact.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:49:59
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

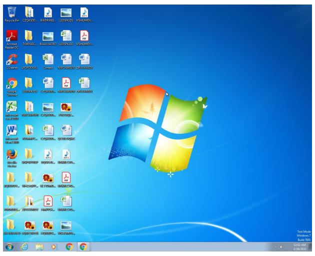
Windows Analysis Report

Contact.xls

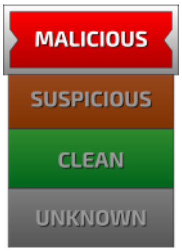
Overview

General Information

Sample Name:	Contact.xls
Analysis ID:	562530
MD5:	fa8570c3fca7bd0..
SHA1:	1e9a8f5de89b43..
SHA256:	0eb209a36a0f42..
Infos:	YARA



Detection

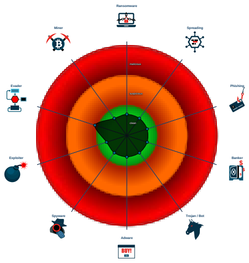


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Yara signature match

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1500 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- **cleanup**

Malware Configuration

⊘ **No configs have been found**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Contact.xls	INDICATOR_OLE_Excel4Macros_DL2	Detects OLE Excel 4 Macros documents acting as downloaders	ditekSHen	• 0x47a3:$e2: 00 4D 61 63 72 6F 31 85 00 • 0x481d:$a1: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A 00 • 0x946:$x1: * #,##0 • 0x952:$x1: * #,##0 • 0x9fb:$x1: * #,##0 • 0xa0a:$x1: * #,##0 • 0xa36:$x1: * #,##0

Sigma Overview

⊘ **No Sigma rule has matched**

Jbx Signature Overview

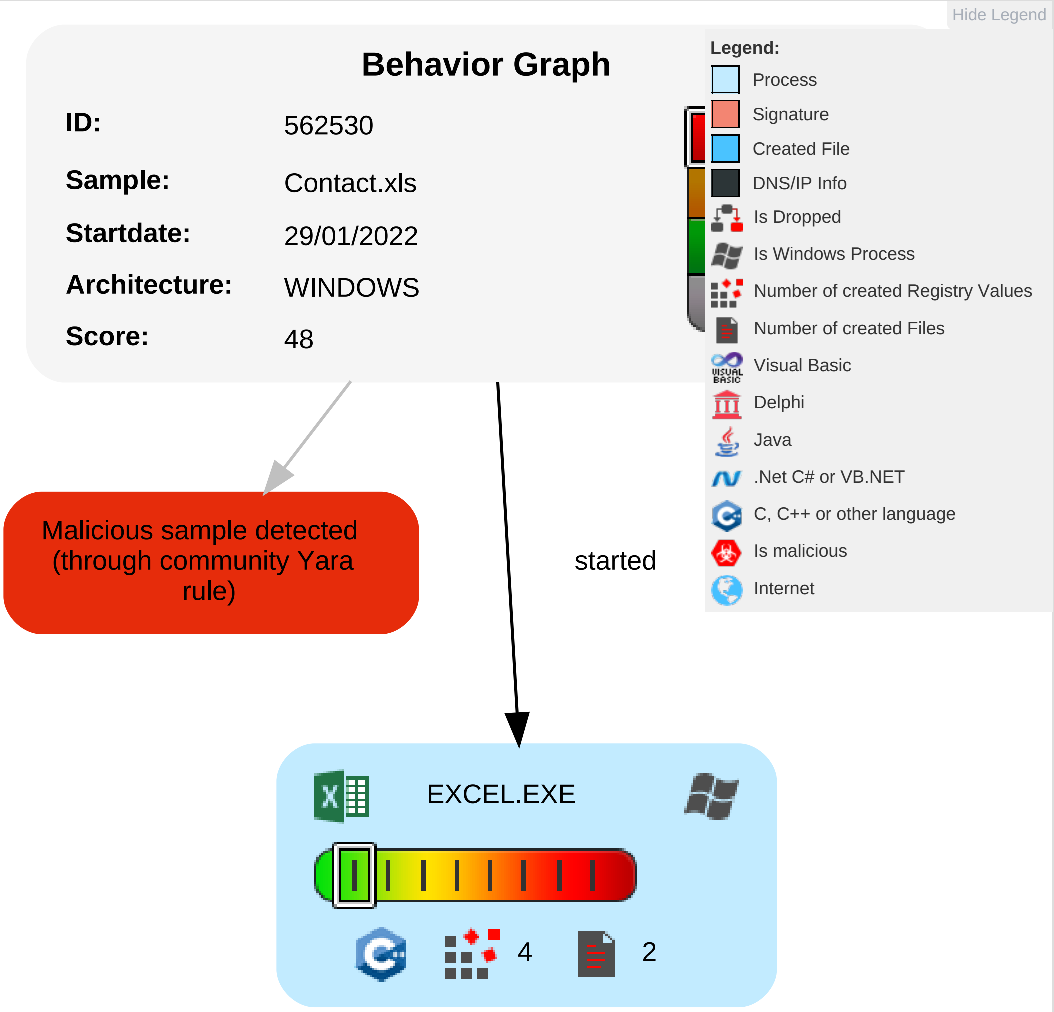
System Summary

Malicious sample detected (through community Yara rule)

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	1 File and Directory Discovery	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	1 System Information Discovery	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



Behavior Graph

ID: 562530

Sample: Contact.xls

Startdate: 29/01/2022

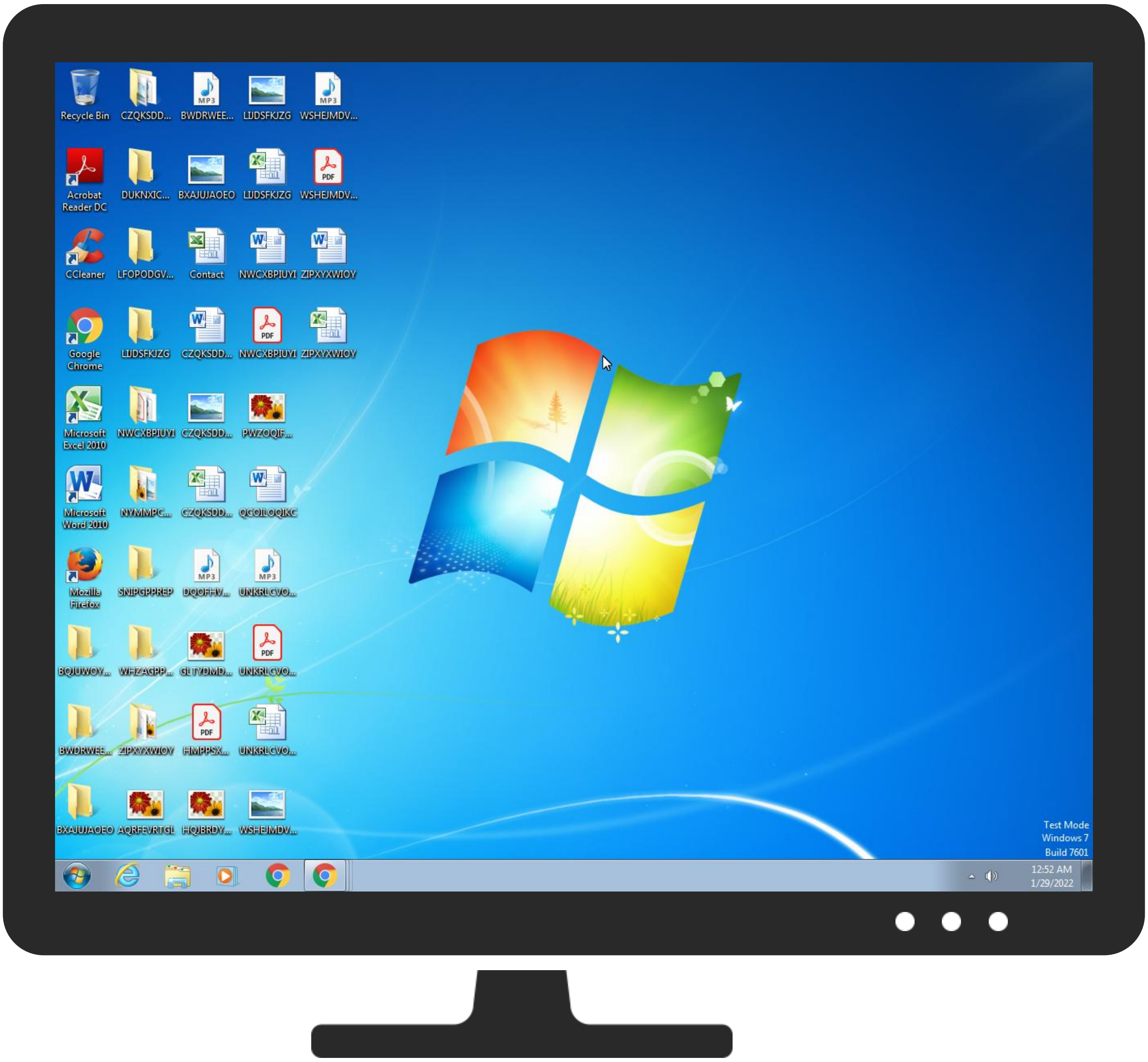
Architecture: WINDOWS

Score: 48

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
Contact.xls	2%	Virustotal		Browse

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**

World Map of Contacted IPs

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562530
Start date:	29.01.2022
Start time:	00:49:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contact.xls
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:	3
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winXLS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 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

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe

Simulations

Behavior and APIs

⊘ **No simulations**

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **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, Can't read SAT
Entropy (8bit):	6.4919219658612315
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Contact.xls
File size:	52470
MD5:	fa8570c3fca7bd0ecc8b2afbc9a2a088
SHA1:	1e9a8f5de89b43a7cb81003f3106cabaaefc4769
SHA256:	0eb209a36a0f427cb97875cc2f0838077e5c3568c84782773a5bf2e101d7dc9a
SHA512:	4b560f493efb55f4496b4f47de8c6aed5e332ea65e78ac9e4944efa92f27e49b9516756b7cf67fae361c7013263126b9fdf1832de058d75714a8caceefdd5d33
SSDEEP:	1536:1I+Hymsbck3hbdlylKsgqopeJBWhZFGkE+cMLxAAISQ5gQ7X:1I+HymsYk3hbdlylKsgqopeJBWhZFGkU
File Content Preview:	........................>..

File Icon

Icon Hash:	e4eea286a4b4bcb4

Network Behavior

⊘ **No network behavior found**

Statistics

⊘ **No statistics**

System Behavior

Analysis Process: EXCEL.EXE PID: **1500**, Parent PID: **596**

General

Target ID:	0
Start time:	00:50:13
Start date:	29/01/2022
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:	0x13f660000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

⊘ **No disassembly**