ID: 549967
Sample Name: Quote.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:36:08
Date: 10/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

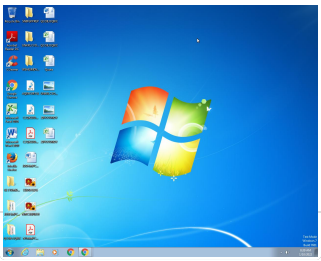
Windows Analysis Report Quote.xlsx

Overview

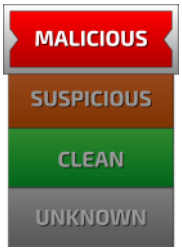
General Information

Sample Name:	Quote.xlsx
Analysis ID:	549967
MD5:	936274be0d0b8b..
SHA1:	5d0c5244908621..
SHA256:	8542bae8ca5e29..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection

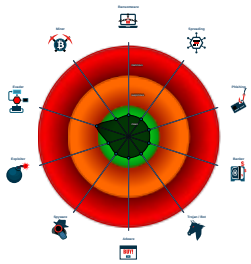


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2952 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

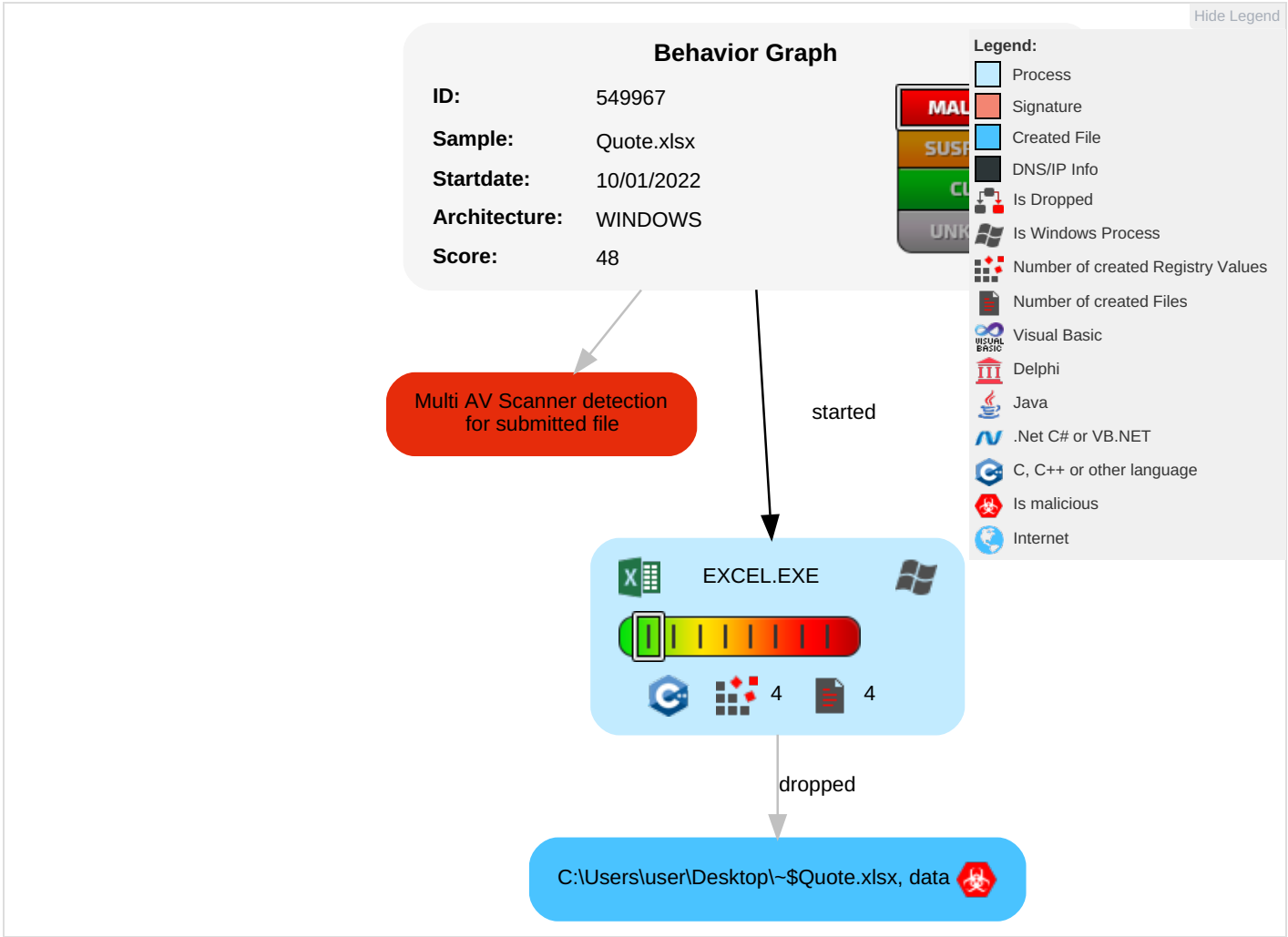
Click to jump to signature section

AV Detection:

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	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
Quote.xlsx	10%	Virustotal		Browse
Quote.xlsx	9%	ReversingLabs		

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:	34.0.0 Boulder Opal
Analysis ID:	549967
Start date:	10.01.2022
Start time:	08:36:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quote.xlsx
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.winXLSX@1/1@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: .xlsx • 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\Desktop\~$Quote.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58[
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.820937256475767
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Quote.xlsx
File size:	12899
MD5:	936274be0d0b8b9e2679898d54409b31
SHA1:	5d0c52449086210ed600a5d4d05aa63260a00c19
SHA256:	8542bae8ca5e29462fc1c127103b38d084005e18e843a5ef075c7e331a75bae3
SHA512:	0f2d901fa451e27ba1ad976701910b9d6acd45ad3b2effc43afcd5a8c0915cc9164e786e0166a11ec1bf0b52d78c3a93ff05c9048aadfc3eeac63e582e2d811c
SSDEEP:	192:RddlSLVxbAi8HaxsC7sCAlxNpwMU7mF3gSOX9vtmfGQTYYLfC:R0LbAgOCICAlDpmaQxXb6XrC

General

File Content Preview:	PK.....)T...r.....[Content_Types].xmlUT....#.a.#.a.#.a.U.N.0..#..U.h...Bh..?G@.<@.xkX.D.....vcB..L....m..8....r.....1.."....~Z.....7....X.....2.f..X..(^J...Ja."x...T)..4.Q....<.....S.j.q5...zs..-.....z....j.B.....xZ...&.....`.~...cL

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2952 Parent PID: 596

General

Start time:	08:37:12
Start date:	10/01/2022
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:	0x13fd60000
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

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Disassembly

Code Analysis