ID: 353581
Sample Name:
COVID19open_closedPodsVACCINE_LETTER2B.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:20:44
Date: 16/02/2021
Version: 31.0.0 Emerald

Table of Contents

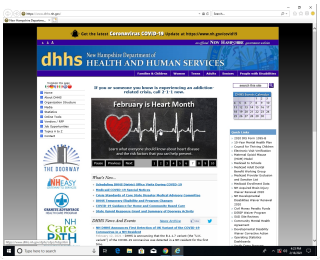
Analysis Report COVID19open_closedPodsVACCINE_L…

Overview

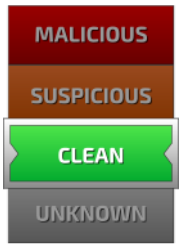
General Information

Sample Name:	COVID19open_closedPodsVACCINE_LETTER2B.docx
Analysis ID:	353581
MD5:	e65769cca6ce82…
SHA1:	d3800da27e0aa6..
SHA256:	b0ecb837f4df662..

Most interesting Screenshot:



Detection

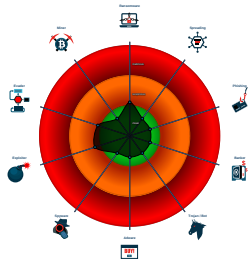


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Allocates a big amount of memory (p…
- JA3 SSL client fingerprint seen in co…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6304 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- iexplore.exe (PID: 5696 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4368 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

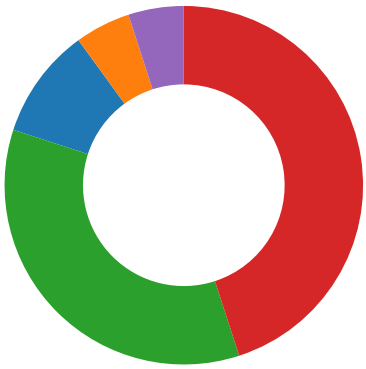
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Compliance:

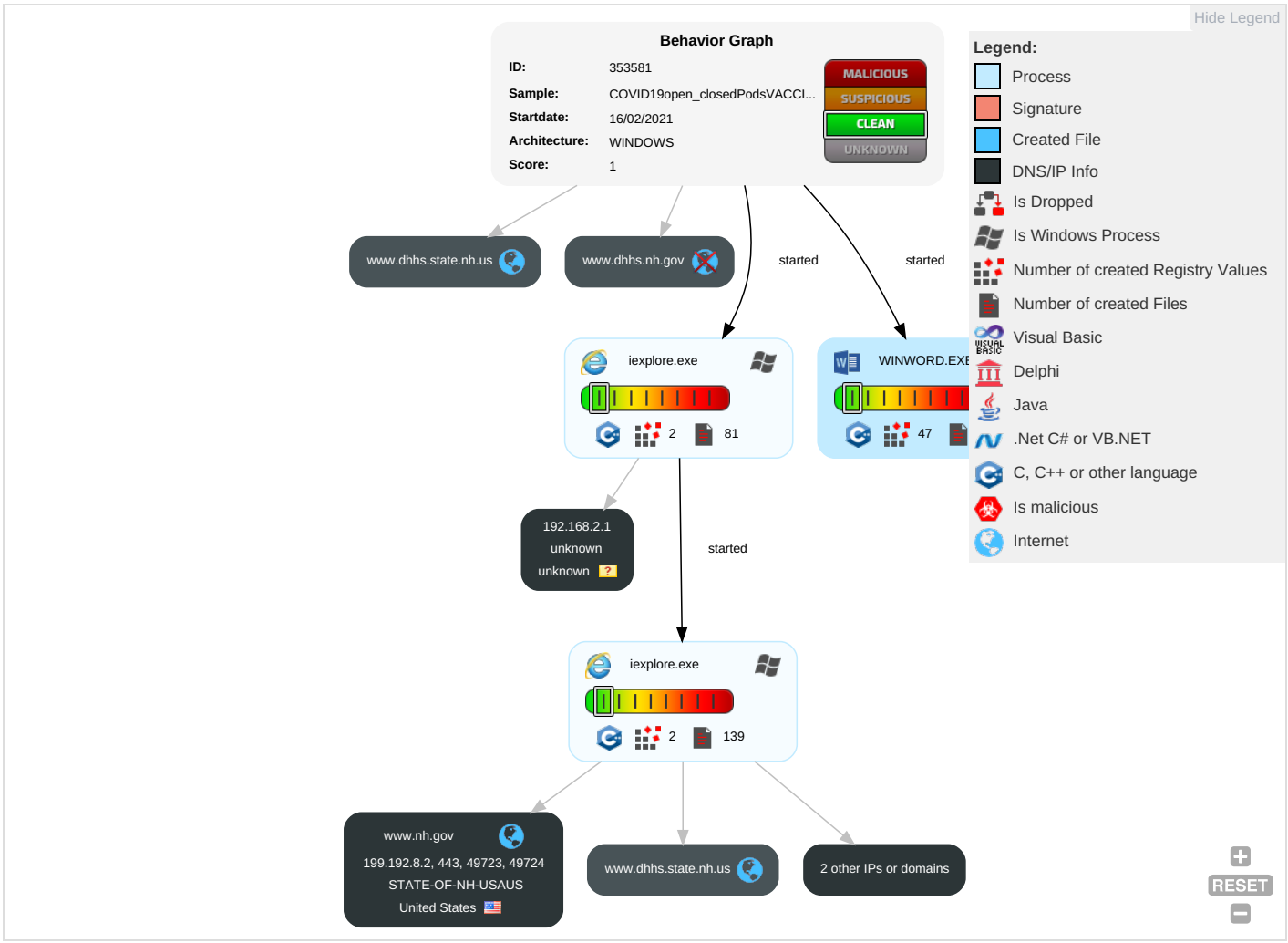
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Process Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carrie Billing Fraud

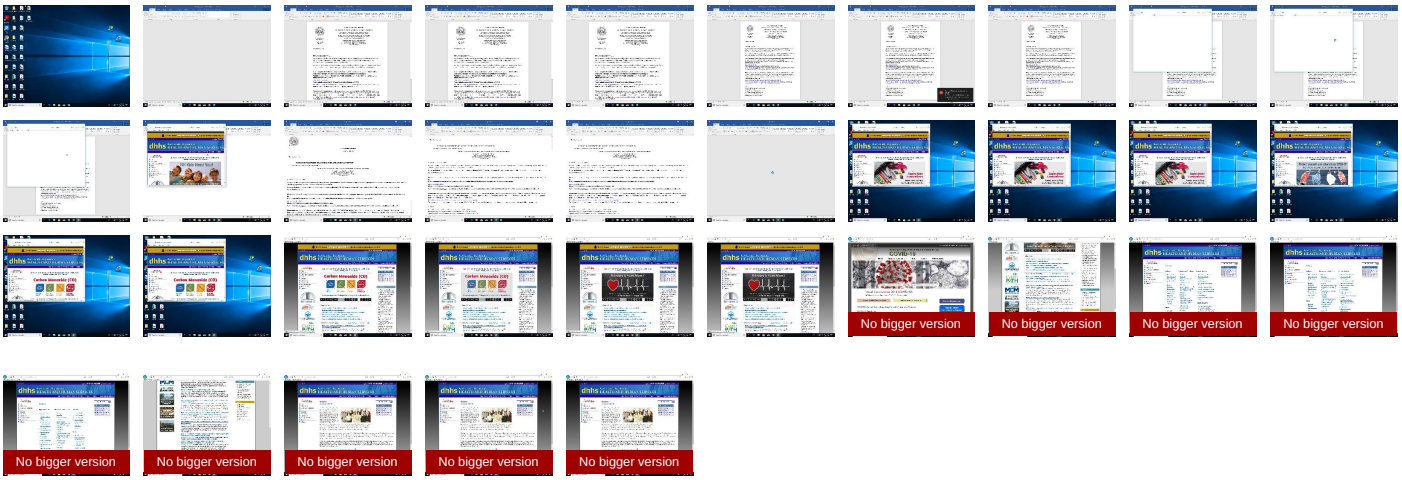
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
COVID19open_closedPodsVACCINE_LETTER2B.docx	0%	Virustotal		Browse
COVID19open_closedPodsVACCINE_LETTER2B.docx	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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://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://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%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://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.dhhs.nh.go	0%	Avira URL Cloud	safe	
http://www.dynamicdrive.com)	0%	Avira URL Cloud	safe	
http://coveringnewhampshire.org/	0%	Avira URL Cloud	safe	
http://txkang.com	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://ekallevig.com/jshowoff	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.dhhs.state.nh.us	199.192.8.2	true	false		unknown
www.app-support.nh.gov	199.192.8.2	true	false		high
www.nh.gov	199.192.8.2	true	false		high
www.dhhs.nh.gov	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.dhhs.nh.gov/foryou/teens.htm	false		high
http://https://www.dhhs.nh.gov/foryou/women.htm	false		high
http://https://www.dhhs.nh.gov/foryou/disabilities.htm	false		high
http://https://www.dhhs.nh.gov/foryou/seniors.htm	false		high
http://https://www.dhhs.nh.gov/index.htm	false		high

URLs from Memory and Binaries

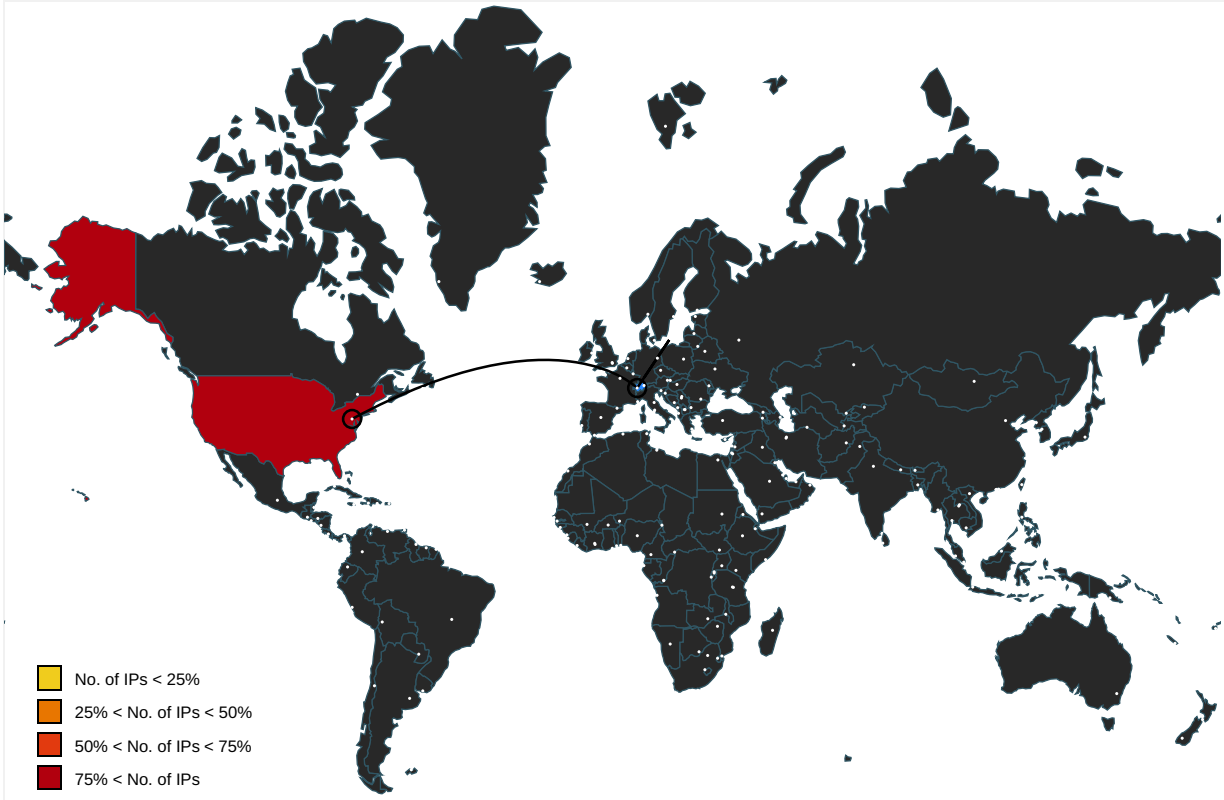
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://twitter.com/NHPubHealth	covid19[1].htm0.14.dr	false		high
http://https://autodiscover-s.outlook.com/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://cdn.entity.	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://api.aadrm.com/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.dhhs.nh.gov/foryou/seniors.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://api.microsoftstream.com/api/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://cr.office.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.nh.gov/policy/accessibility.htm	covid19[1].htm0.14.dr	false		high
http://https://www.dhhs.nh.gov/#translateilities.htmt	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.dhhs.nh.gov/favicon.ico~	imagestore.dat.14.dr	false		high
http://www.reddit.com/	msapplication.xml4.13.dr	false		high
http://https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-medium.woff)	lg-screen[1].css.14.dr	false		high
http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-regular.woff)	lg-screen[1].css.14.dr	false		high
http://https://www.dhhs.nh.gov/foryou/adults.htmm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.nh.gov/covid19	index[1].htm.14.dr	false		high
http://https://officeci.azurewebsites.net/api/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dhhs.nh.gov/about/index.htmies.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.dhhs.nh.gov/foryou/adults.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://dashboard.nh.gov/#/site/DHHS/views/COVID-19LrgMaps/MAPCumulativeLrg.pdf	covid19[1].htm0.14.dr	false		high
http://https://store.office.cn/addinstemplate	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.servicelink.nh.gov/	adults[1].htm.14.dr, disabilities[1].htm.14.dr	false		high
http://https://wus2-000.pagecontentsync.	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-bold-italic.woff)	lg-screen[1].css.14.dr	false		high
http://https://www.dhhs.nh.gov	covid19[1].htm0.14.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/foryou/women.htmmr	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.odwebp.svc.ms	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://web.microsoftstream.com/video/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/foryou/women.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.doj.nh.gov/covid-19-scams/	covid19[1].htm0.14.dr	false		high
http://https://graph.windows.net	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.nh.gov	adults[1].htm.14.dr, index[1].htm.14.dr	false		high
http://https://dashboard.nh.gov/#/site/DHHS/views/COVID19InteractiveMapDashboard/Town-ActiveCases-Data.csv?	covid19[1].htm0.14.dr	false		high
http://https://www.dhhs.nh.gov/index.htmjNew	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/foryou/families.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.hhs.gov/sites/default/files/ocr-bulletin-3-28-20.pdf	covid19[1].htm0.14.dr	false		high
http://https://www.dhhs.nh.gov/dphs/cdcs/covid19/crisis-soc-medical-ad-comm.htm	covid19[1].htm0.14.dr	false		high
http://https://www.dhhs.nh.gov/index.htmilities.htmd	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://weather.service.msn.com/data.aspx	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-bold.woff)	lg-screen[1].css.14.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/#skip/www.dhhs.nh.gov/favicon.ico	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/foryou/families.htmx	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://www.amazon.com/	msapplication.xml.13.dr	false		high
http://https://entitlement.diagnostics.office.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.who.int/health-topics/coronavirus	covid19[1].htm0.14.dr	false		high
http://www.twitter.com/	msapplication.xml5.13.dr	false		high
http://https://outlook.office.com/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.nh.gov/file-format/pdf.htm	covid19[1].htm0.14.dr	false		high
http://https://www.dhhs.nh.gov/index.htmilities.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://www.nh.gov/index.htm	covid19[1].htm0.14.dr	false		high
http://https://www.nh.gov/covid19/resources-guidance/vaccination-planning.htm	~WRS{B268D7D1-175E-4774-8B62-5FC8DD9A2BB9}.tmp.0.dr, document.xml	false		high
http://https://www.dhhs.nh.go	{2B1065E6-70B6-11EB-90E5-ECF4BB570DC9}.dat.13.dr	false	• Avira URL Cloud: safe	unknown
http://www.dynamicdrive.com)	textsizer[1].js.14.dr	false	• Avira URL Cloud: safe	low
http://https://graph.windows.net/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://devnull.onenote.com	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://coveringnewhampshire.org/	index[1].htm.14.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dhhs.nh.gov/about/index.htm	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://https://messaging.office.com/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://txkang.com	textsizer[1].js.14.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dhhs.nh.gov/foryou/women.htmm	~DFE0551548F1A31EE1.TMP.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://skyapi.live.net/Activity/	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.nh.gov/covid19/X	~DFE0551548F1A31EE1.TMP.13.dr	false		high
http://ekallevig.com/jshowoff	jquery.jshowoff.min[1].js.14.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.13.dr	false		high
http://https://api.cortana.ai	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.nh.gov/covid19/index.htm	index[1].htm.14.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://staging.cortana.ai	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.nhcarepath.dhhs.nh.gov/	index[1].htm.14.dr	false		high
http://https://onedrive.live.com/embed?	ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D.0.dr	false		high
http://https://www.dhhs.nh.gov/favicon.ico	imagestore.dat.14.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.192.8.2	unknown	United States		19713	STATE-OF-NH-USAUS	false

Private

IP
192.168.2.1

General Information

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	353581
Start date:	16.02.2021
Start time:	16:20:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID19open_closedPodsVACCINE_LETTER2B.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@4/132@4/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: http://www.dhhs.nh.gov/ • Scroll down • Close Viewer • Browsing link: https://www.nh.gov/covid19 • Browsing link: https://www.dhhs.nh.gov/#skip • Browsing link: https://www.dhhs.nh.gov/foryou/families.htm • Browsing link: https://www.dhhs.nh.gov/foryou/women.htm • Browsing link: https://www.dhhs.nh.gov/foryou/teens.htm • Browsing link: https://www.dhhs.nh.gov/foryou/adults.htm • Browsing link: https://www.dhhs.nh.gov/foryou/seniors.htm • Browsing link: https://www.dhhs.nh.gov/foryou/disabilities.htm • Browsing link: https://www.dhhs.nh.gov/#translate • Browsing link: https://www.dhhs.nh.gov/index.htm • Browsing link: https://www.dhhs.nh.gov/about/index.htm

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.104.139.180, 204.79.197.200, 13.107.21.200, 93.184.220.29, 168.61.161.212, 104.43.193.48, 23.211.6.115, 104.43.139.144, 13.88.21.125, 52.109.32.63, 52.109.76.35, 52.109.88.40, 184.30.20.56, 51.104.144.132, 88.221.62.148, 142.250.180.142, 216.58.209.42, 142.250.180.163, 2.20.142.210, 2.20.142.209, 51.103.5.186, 92.122.213.194, 92.122.213.247, 152.199.19.161, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, www3.l.google.com, store-images.s-microsoft.com, translate.googleapis.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, go.microsoft.com.edgekey.net, translate.google.com, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 199.192.8.2
	CHT International.exe	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Generic.mg.44669e0ff064dfc9.dll	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 199.192.8.2
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 199.192.8.2
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 199.192.8.2
	13xakh1PtD.dll	Get hash	malicious	Browse	• 199.192.8.2
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 199.192.8.2
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 199.192.8.2
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 199.192.8.2
	L257MJZ0TP.htm	Get hash	malicious	Browse	• 199.192.8.2
	brewin-02-02-21 Statement_763108amFtZXMubXV0aW1lcg==.htm	Get hash	malicious	Browse	• 199.192.8.2
	658908343Bel.html	Get hash	malicious	Browse	• 199.192.8.2
	P178979.htm	Get hash	malicious	Browse	• 199.192.8.2
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 199.192.8.2
	PO 20191003.exe	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Trojan.GenericKD.36134277.347.exe	Get hash	malicious	Browse	• 199.192.8.2
	SecuriteInfo.com.Trojan.PWS.Siggen2.61222.12968.exe	Get hash	malicious	Browse	• 199.192.8.2
37f463bf4616ecd445d4a1937da06e19	MV CHEN GLORY 1 Q88.DOC.exe	Get hash	malicious	Browse	• 199.192.8.2
	quotation professional pricelist for 2021 - 1009 232356 0000 565.exe	Get hash	malicious	Browse	• 199.192.8.2
	quotation professional pricelist for 2021 - 1009 232356 0000 565.exe	Get hash	malicious	Browse	• 199.192.8.2
	Kreuzmayr_PO_22656_65564345565643ETD,pdf.exe	Get hash	malicious	Browse	• 199.192.8.2
	DHL_Shipment_Notofication#554334.exe	Get hash	malicious	Browse	• 199.192.8.2
	jYHhaKx7OH.exe	Get hash	malicious	Browse	• 199.192.8.2
	DHL_6368638172 receipt document,pdf.exe	Get hash	malicious	Browse	• 199.192.8.2
	Facturas de datos bancarios FA00001120.pdf.exe	Get hash	malicious	Browse	• 199.192.8.2
	TR8IqBxed5.exe	Get hash	malicious	Browse	• 199.192.8.2
	CorporateProspal.exe	Get hash	malicious	Browse	• 199.192.8.2
	EmployeeComplaintReport.exe	Get hash	malicious	Browse	• 199.192.8.2
	necessary (47).xls	Get hash	malicious	Browse	• 199.192.8.2
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 199.192.8.2
	D200821ROB.ppt	Get hash	malicious	Browse	• 199.192.8.2
	significant (92).xls	Get hash	malicious	Browse	• 199.192.8.2
	necessary (47).xls	Get hash	malicious	Browse	• 199.192.8.2
	obligations (84).xls	Get hash	malicious	Browse	• 199.192.8.2
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 199.192.8.2
	HyperLinkDemo.exe	Get hash	malicious	Browse	• 199.192.8.2
	DOCUMENT (63).xls	Get hash	malicious	Browse	• 199.192.8.2

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2B1065E4-70B6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.868265279767621
Encrypted:	false
SSDEEP:	96:rCZ1Zp2+WCGdtCCbfC7/oKMChgqCVmQCHgqCJLtC1/363:rCZ1Zp2+WCCtCSfC7VMC9CtCjCFtC1y3
MD5:	42A0AB8DE54E258342487B9218ADE23E
SHA1:	5984C2CD478753F749287760ADED00EAF91D8E9E
SHA-256:	BFB6FF9519CA36127D57DD9D01E43CD8BD1BE7FECE6B4C347CD6C2984FC05E85
SHA-512:	ADEE2D130E84EE061D85E42643B169C723BB0C5F04F599155EFA8FDCAD223965F5B6A8D66EE5C1FF6A38AB216A8ED98B5342FC0A99C082DC0FE8C3FCD79D0BE
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2B1065E6-70B6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	159906
Entropy (8bit):	2.3997698519945723
Encrypted:	false
SSDEEP:	384:rdxPX+eeiWRdZkDTjA302AG2o0vAPW92iul9GpAt1rFLo2AM2cKsu41KGlIpoPMH:UukEdduo
MD5:	329087A4C531477131744CEBE0328D8F
SHA1:	62547710FE4E15C1DA6421066ABE3BF2B0B3F915
SHA-256:	EDACB9F3D6A803566D4229DFA709321AE6F3037E8FFF1C514BDD5A2BE491AC08
SHA-512:	53124A2D9740CFE86052760F76538350F49F5814EAE390F8C56EA10CCD0969AD3CAF923F07E7F1A5FA4A7B397BAE30FD36EED1D040DFD622D181BB07851B33B
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{43C50248-70B6-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5632254934354755
Encrypted:	false
SSDEEP:	48:IwjGcpr2GwpayG4pQOGrapbS/GQpKqG7HpROTGIpG:rZZuQC6ABSpAFTqA
MD5:	6921D435197A19C623F97E1B0001CCCC
SHA1:	19516D3DE53FC4098F6964480AA828CA5D9FF8BD
SHA-256:	4A6BACF4C66F52429392F06989BAE695CEE45A6DFF4CC293C3C21BDADB882302
SHA-512:	4218F15C68896CB49153C643BD4C43B2706E28B48EA7444F88D5602A9804AE9768B3F1FF6C750702A1976E8619F7421A2B7CD9D1618DF57C9CA5DB8FF546DE26
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Size (bytes):	657
Entropy (8bit):	5.04756477364833
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEu+g+JnWimI002EtM3MHdNMNxOEu+g+JnWimI00ONVbkEtMb:2d6NxO5+g+JSZHKd6NxO5+g+JSZ7Qb
MD5:	E34B5BD82676E71C134828C22A67B1C5
SHA1:	C6150EFDDE584BF3B6F4DA4F1E140B73E44B445E
SHA-256:	157619DC8B11D67F57CF6B7022709273EEC61B96F1D422B605CE935644EB13AC
SHA-512:	1B87CCA74026B7F344DEAE3721A68F111298B7781A99C0713873743C178ABD6BAC320227E339862354DC6E253AEAA40B50CE553E567141C31ED41506624E8CDE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x056a6aad,0x01d704c3</date><accdate>0x056a6aad,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x056a6aad,0x01d704c3</date><accdate>0x056a6aad,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.100875853335666
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kk+y+JnWimI002EtM3MHdNMNxe2kk+O0nWimI00ONkak6EtMb:2d6NxrSdJSZHKd6NxrSO0SZ72a7b
MD5:	4A6660DCFB060AC3733117D0DC240B1C
SHA1:	33F89FEB0CEE025D3B8F787D1169A84A33A43271
SHA-256:	3F09E5FD3B9EF3F99FC508AB2E70DEB052014960CBE67322A135E230EF729EC2
SHA-512:	BA9EAEC4149C08B1175C0A60D660291C462519AC668749E539571E0A6EA4D7D75D6DC92E92A71AA3A758489C24F3AC2CF11DA432709A84A5F802B00A6DE2E25
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x054909cd,0x01d704c3</date><accdate>0x054909cd,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x054909cd,0x01d704c3</date><accdate>0x054b6c37,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.077923439738975
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLbnWimI002EtM3MHdNMNxvLbnWimI00ONmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7Ub
MD5:	605D31B35D0B2A3466232CA81A01B2AA
SHA1:	3470F7586C02C8EC4A5D77A0694A7BBC7BFDB495
SHA-256:	22389A004CD7639C25973D018C1D7659E4A55BF2BCD8A7BD522560B7B6DF9623
SHA-512:	A6E40C2016B7390ADA7A1895BA5F03037371B096AA92DC84D2604C52619A65EA1F75228B829C841F79C6BD4DF55FE2F4A044064D1AFA2770AA6F1126815EA8F4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x056ccd2a,0x01d704c3</date><accdate>0x056ccd2a,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x056ccd2a,0x01d704c3</date><accdate>0x056ccd2a,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.05344037103215
Encrypted:	false
SSDEEP:	12:TMHdNMNxiIcRc0nWimI002EtM3MHdNMNxiIcRc0nWimI00ONd5EtMb:2d6NxhOVSZHKd6NxhOVSZ7njb
MD5:	0DFA09664BD868B28A94D6A188BA8774
SHA1:	EAABE783B4724D93AD60B4900F34C77741D5EE51

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-256:	2CFBA8BD6DA410E72A97685D6EB6F1D97D8CBE2F981B804FEB74A182CD46B181
SHA-512:	D2FC7A8E8027CBCC8980E52995E17CCA518B3798AAD021844820932ADAE61A95627D03C5E99A1D6C2D76264E1229E55CBDBD949B813A82FA4066A7123213672
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0560e13e,0x01d704c3</date><acc date>0x0560e13e,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x0560e13e,0x01d704c3</date><accdate>0x0560e 13e,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.115787784840534
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwpnWimI002EtM3MHdNMNxhGwpnWimI00ON8K075EtMb:2d6NxQgSZHKd6NxQgSZ7uKajb
MD5:	CFB25D44F764B3F971411044DD884F63
SHA1:	DD3CF0D65A13D61E195FC23902A3E75F884E2846
SHA-256:	CE9AE1851BB182A0B9794D4B0D0344041E07743630BBB164F515790468EB3EF1
SHA-512:	D6576E879FD002CB19226F986B687CDD23AF3896FA6EE0D6AA8DD86E226DDC03B7265473541D730083ABEA29FEC81DDBD7FE6CD550021E131705439A46C4C2 7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x056f2f60,0x01d704c3</date>< accdate>0x056f2f60,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x056f2f60,0x01d704c3</date><accdate>0 x056f2f60,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.04855201827873
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nu+g+JnWimI002EtM3MHdNMNx0nu+g+JnWimI00ONxEtMb:2d6Nx0u+g+JSZHKd6Nx0u+g+JSZ7Vb
MD5:	511996E48300E7E2B9B45DDCF6FFF08F
SHA1:	977A1C3022756BC5CF26F8BB467DB41DCD0799CC
SHA-256:	70C98F121061784D2918820FFFA82601AB9588C7CCE766FE2340C66E4EA1A69F
SHA-512:	3EBB4E4743BC06429E6CA8532F2EE9DFEDA933AE5720F360B20310684D035569FC39DD8A54D2D8EDE2F80ABD6586C4DA5BE5D96055FB0CA5483AC6FC80E501 01
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x056a6aad,0x01d704c3</date><a ccdate>0x056a6aad,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x056a6aad,0x01d704c3</date><accdate>0x0 56a6aad,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.133466678209735
Encrypted:	false
SSDEEP:	12:TMHdNMNxx5V8VknWimI002EtM3MHdNMNxx5V8VknWimI00ON6Kq5EtMb:2d6NxjSZHKd6NxjSZ7ub
MD5:	C33903FF0BF413B9EE18E3B3B6F57ECA
SHA1:	9CB1370452503A7DCAC02BD06AE2F3E1BB12EB67
SHA-256:	C4EF70ACBB336326E99005488F49200B1DB38D5A2EF1D109D7ED0D737544EE49
SHA-512:	F966AB14C9482922459CD5C30F257BB8EF042E841F0D84C19595F497B51511DCF91A2E391D178EA9E9502B36A98F175B021ECA648F698AC85912B56EE04E5284
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x05680893,0x01d704c3</date><accdate>0x05680893,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x05680893,0x01d704c3</date><accdate>0x05680893,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.063953523101619
Encrypted:	false
SSDEEP:	12:TMHdNMNxchnWimI002EtM3MHdNMNxchnWimI00ONVEtMb:2d6NxoSZHKd6NxoSZ71b
MD5:	4A4B08B27CA317B7FF04E4EFD694D224
SHA1:	B8918B5C097552775663EEBD84E8EF3369E23782
SHA-256:	7C33DE9B7ED2F4EE76A453FB5D9C5F3839A6DE1392900B5B617DF0BA14A4378B
SHA-512:	43C5F7F7747C48746FAF81CB22B0E0C595CD3626197A52A95B666C38462C4CE0CBEEC99018AE986FFE50D79FA664FC50A15A36B3156D62AE535C854234F913F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x055030f8,0x01d704c3</date><accdate>0x055030f8,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x055030f8,0x01d704c3</date><accdate>0x055030f8,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.042926777601526
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnhnWimI002EtM3MHdNMNxfnLnWimI00ONe5EtMb:2d6NxJSZHKd6NxDSZ7Ejb
MD5:	90CF02B24D3EFB9F40B38DA560B2C4B0
SHA1:	40B94BE4BAB87740ECF573F2F80263674DFB3807
SHA-256:	06ACC1E729FF06353F6D48415543BE8C33235E4DC828C5420A32B02146B57AC9
SHA-512:	9BB3FB2CCA65694FA9BA414CAEE350C7B138C14D9CB694422EC5BA29119484B873029E08A1FFD0F119BE62D9A78E66C3CEA2068BA9F629BD14E94BA219F9E549
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x055030f8,0x01d704c3</date><accdate>0x055030f8,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x055030f8,0x01d704c3</date><accdate>0x055e7f0c,0x01d704c3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3860
Entropy (8bit):	5.934351382476207
Encrypted:	false
SSDEEP:	48:4vla4sBnR9IO65JbMY715WtkSavlaZp0whXeBkCoW5nUbcmZvpy24ZZuk78+zAnp:bt6bYY7X9O0wVjcyvpx4GW8oAnUyu5od
MD5:	997FD32E31F6C6D35B962DE5F07771E7
SHA1:	FD6D04AB5DA7986EE49EC53D3FAA7B3D8B9877DD
SHA-256:	A4A748973F701AB3472497F7F4DB7C641217BB6E727A2E01A78A939023002D30
SHA-512:	6A5F0B5F615F6890731B8F1BF85F1A5B79B3BAD1931850F5B4FA0FFBDB7187BF8028A0220B0B7134584A8C1123CA78A41707856569164F7AFA20E3852DA7D8B3
Malicious:	false
Reputation:	low
Preview:	#.h.t.t.p.s.:././.w.w.w...d.h.h.s...n.h...g.o.v./.f.a.v.i.c.o.n...i.c.o.~.....h.....(..... .....@.....R...{....Is.B(B.....B}R.....{.s.s...kUc.)m...41.....1Ec.Ru{.....e..J.....)..AR.)}k.Z.k.J]R.....!}...U..c...Z...B]s.....B...),J.....9}..)01.JIc.)as..as.s.....9q{.R....u..k.s.Z....m{.!8Z.!Ms..<c.....!.{..Y..Rik.cq..9uc.{.....Ak.c...k.{.k.....u...e..Z.c.94J.....().)ec.....!y.....R.s.....s....M{.c...J...Juk.9}s..]..s...{....i..1u.....)AZ.....Us.!]..k...c.c.R...Z....$1..M...Mk..]{.c.....{...c.s.Zys.J.{.....U{.!Ek.!U{.k...!ek.1Ys..u..)e.....J]{.Jms.c...!,).....!<c..a...}..c.k.By..Zu.....10J..Q{.)Ic..a...Y...Y{.)Qs.R...k...!.s.!i..s.s.)u..Ba{.R.k.....Y...e...i..JQc.)a{.)}s.....)u..1m..Z.k.s...s.....lk..Q{..]..!Qs.JEc..]{..q...e.....c...Jqs.Z.k.cu..c.....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\ADCB58F4-D1C1-44B4-8E35-2D0947F07A2D	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132453
Entropy (8bit):	5.3757764325974575
Encrypted:	false
SSDEEP:	1536:OcQceNquBXA3gBw+pQ9DQW+zA9H34ZldpKWXboOilXNErLKzEh:8DQ9DQW+z0XiT
MD5:	203CCAB7FA4B3C142E948D7BFCB56DC5
SHA1:	0C657B6B569BE54CC5F28AA1941B48376006C146
SHA-256:	78CAEC1ABD673D53059FFD502352BF7003B61D9BCD7163312C74EA97CAD8A9C5
SHA-512:	4DF1CDD0A2823C88FBD6242F78731C91DF6FA588E8DF6E98795DC305D46608FC06DF557E4E4CE4CE7A1462BACEB153D39AFA6DC6F1FFA6F64470E19BD0506E18
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-16T15:21:38">.. Build: 16.0.13810.30527-->.. <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\698A8F31.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 293 x 295, 1-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	6897
Entropy (8bit):	7.961710048383538
Encrypted:	false
SSDEEP:	192:C/va+mFRJNG78dpYUIMa3LXA53yBndb4h8HuyHAcD:C0FRJNtdpzUbXA530bw0uBE
MD5:	DA0E31545E3B38505B7318C64BDEC26B
SHA1:	48C54C0AA75AAB40686252301EA47FAB74B1190A
SHA-256:	EBC4D461F08B5EFAF6A44B314B4DDBA9025D6D6FB6614FED17A5A03010C68330
SHA-512:	A6257BD4DCAA72AC63DF003A2E1FBB2048DBB0EE7A894D93D238BFC7CF545757D8D0B96C840B9F7D3DA49F73408938843AF172E73CC103E117B81EAE244B15F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...%...'.....a.?....PLTE.....bKGD....H....pHYs.....+.....IDATh.}.}t..u...,].P.IM7.G..{.T...$K.....{v.....#..4l.u .>.a~<.E{...q.l....v...R.lH.....>.9.:k.....cW...H...w...._.3G..0.y..}..w.}O.-.....l.V.V..J._N....$..b...M.....w.7.q..r..S.=....J..."..y..(.2..oS..x;.... -D`...8*.0..RE...0.$..lG*..nOa..r..o?6v..T.0R.g.)@.:..].&M....P...8T...v..Y.....L..oG.l..`.....=...@M.:...~k.. "....j..dw....?..1 r+.DZ...*..D.$..[)[23.H.....*<..hn..F.G.e!.\e...5.....xE...Bg....T..j...NY...,Ch...k.....V!.&.k.....t.$Lsy[..).)ii+e.".$...Fox).....Z...d8..vF.....kT....B....\...v3q..rU.v".eYy..M...d.b....7.9.?n.n...$...."i^m....F..?.....(.hM.*.p..f....^..w.a...M.d....>D...n.<....M.+..jR....%.0..*....%.*.T...!>.y..NR.)&...V...G?A.yY0..F..qxU].....sq.6.6R6..V...F|.\`..F..t...$c..N.#..h.TQ..... ..3..@..g...QYs.1.r.>....7....TQ.R.Q....b....{$...5U.('...2.....).:*...SL...,I...p.Q.....8..NQ.....6.(....bC..1..N.}..O,.`+.R..`Q...4W6P.2..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{684EC546-5172-4E4C-A638-EBF4CDF1FB1E}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9766F8FA-474A-4D26-9B90-1E4FEFAFF644}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9766F8FA-474A-4D26-9B90-1E4FEFAFF644}.tmp	
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07D C
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{B268D7D1-175E-4774-8B62-5FC8DD9A2BB9}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8648
Entropy (8bit):	3.9088978163461343
Encrypted:	false
SSDEEP:	96:v8DY16W2/Zx7P5154V1lGcAxW5aGpphPqWoFIA0y9Y4UnPwl/lBEM8m/+:QRv7e7lG/vGpp34UnYFHzm
MD5:	90D64E86C16A1DE41068701C702A394A
SHA1:	294170381818D2CE67FB86B25F0AE1BD3D237A78
SHA-256:	541B4E4DE318973D77F071E3869B4A3FE52993B06CB911EF1A7DE2ABE9E1782E
SHA-512:	28551CF3DFFB31FEA858D99F224897FF93E6D071F633B0529596C1598E9321D49A673C25F71EDA40FEE51F02DCFF0BAF0F3C65C4ECDFEF65CCF08910F24D98E
Malicious:	false
Preview:	../.....L.o.r.i. .A... .S.h.i.b.i.n.e.t.t.e. .C.o.m.m.i.s.s.i.o.n.e.r.....L.i.s.a. .M... .M.o.r.r.i.s. .D.i.r.e.c.t.o.r.....F.e.b.r.u.a.r.y. .1.5.,. .2.0.2.1.....S.T.A.T.E. .O.F. .N.E.W. .H.A.M.P.S.H.I.R.E. .D.E.P.A.R.T.M.E.N.T. .O.F. .H.E.A.L.T.H. .A.N.D. .H.U.M.A.N. .S.E.R.V.I.C.E.S...D.I.V.I.S.I.O.N. .O.F. .P.U.B.L.I.C. .H.E.A.L.T.H. .S.E.R.V.I.C.E.S...B.U.R.E.A.U. .O.F. .I.N.F.E.C.T.I.O.U.S. .D.I.S.E.A.S.E. .C.O.N.T.R.O.L. .I.M.M.U.N.I.Z.A.T.I.O.N. .P.R.O.G.R.A.M...2.9. .H.A.Z.E.N. .D.R.I.V.E.,. .....H...J...z...|...~..... .....$...j.....$.....]...^...a$. .....$.....dc.....]...^...a$.....^.....d.....dx.....]...^.d.`.....d.]...^.d.gd@.....$.....d....]...^...a$.....$.....d....]...^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\400x25officialsite[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 400 x 25
Category:	downloaded
Size (bytes):	3455
Entropy (8bit):	7.723531087767753
Encrypted:	false
SSDEEP:	48:5nlnNANz4PIt65pH87mCYGZG9LFLBxYkjshyV7t0A28qK4JldlQPueht:5n1Yr4pH8KCYGqFLQkjTJrxehPzj
MD5:	C242FCDA1B5DAA99D53BAD09E619D169
SHA1:	36C3FA7B2EFDD718550348B7E3E445782C912341
SHA-256:	90E1AE9F18C3A094D16CC4ED11AC93E3561ABB41308B0FEB0B30C166DC15D130
SHA-512:	995BD2A3B5DB4B2FF05D6796BBF1ED9014ED501E58BD118E8F4886F2EC5FF827B174E365D7D36CEE5A82120693C69B8DF1D709D93EDE78B8D3F0341AE31CD6 A3
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/400x25officialsite.gif
Preview:	GIF89a.....?Ts.....;Pp.....^p.BWu{.....bs.w.....iz.....hy....;Qpu.....~..k{....:PoPc.L`|Ob.I]{M`}\n....G[yH\y=Rq.....ZI.iy....Uh.....[m....Wi....y..... .....gx.K_|.....[m.....Xk....>SrMa}Sf.....m}.J^{I]z.....r..Wj.....z..{..`r.....Pd.....<Rq.....@Uts.....q..du....AVt.....v.....j{.....ct..... Qd.Vi.t.....Tg.n~.Yk._p.F[xo.....CXvfw.EYw.....}.....p..bt....fv.ar.Tf.]o.I|.t.....p..x.....Nb~.....|.....m}.....9Oo.....DYw.....ev..... .....Re.....FZx....._q.....|.....H.....*\....#J.H....3j.... C..I...(S.\...0c.I...8s.L. .....xT.....x..i..;.j.....`+..pA$....j...C.p..e..... ...Ao.....-A.D`.'H.@.....)..@Hb`.+....X....[\...@....].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a-large[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 13, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1105
Entropy (8bit):	6.192290130492558
Encrypted:	false
SSDEEP:	24:UKr1he91WwylZ82lYSqMHYPNV+W2T3byJCpkrsGn8UdY:dqQinNuI0KJpQnZ
MD5:	664946890B46D3F72816050F1600FAD0
SHA1:	21D7E29B5B89E50FA6AE15FF2A903F947FEC4DEF
SHA-256:	A631A85CACBB5FA0C7F80F957EF2B327AE912324915B4D2B8CDE3A3F903760E0
SHA-512:	13CA53EEA65B3290F7C513DA5FF92D5168887F1092AA0BFABE951C772CDE72C34E38E07B5E1312D5866D58CA9EFEE6D1C2653B2B0FCDBADE62CAD8B043C5C 1B7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a-large[1].png	
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/a-large.png
Preview:	.PNG.....IHDR.....$....tEXtSoftware.Adobe ImageReadyq.e<...iiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:438258F0C81811E4AEFFBD7DB352EAB2" xmpMM:InstanceID="xmp.iid:438258EFC81811E4AEFFBD7DB352EAB2" xmp:CreatorTool="Adobe Photoshop CS3 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:7392920C0151DE118F1C842F631D718C" stRef:documentID="uuid:156814919CEBDC11A2CFD38C7E53D8A9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...6...~IDATx.b...?.%.....f.....b .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\arrow_ltblue[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 11 x 11
Category:	downloaded
Size (bytes):	57
Entropy (8bit):	4.359205803638424
Encrypted:	false
SSDEEP:	3:Cd/lfl02fLt+En:OO24En
MD5:	481110EE043514D98BD1293AF5C9AB25
SHA1:	3E578D2A402635332D857D4A5C3FD007A4A9AEEB
SHA-256:	5A25D796794B161D9F544F007A2BF016CF724D9EA39E3DF0EA704CCC3768843E
SHA-512:	270EC8E231006A3BC1AECD0BDB9AACD290D5F84198899FAB75E99E40F550EF67D525B8911ABC22BD66FDB76225162D4CE2C2D1CBFF7C12F5AC6F14A1F1404A3
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/arrow_ltblue.gif
Preview:	GIF89a.....3f.!.....,.....@.....0.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\background-hi-lite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 34 x 400, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	384
Entropy (8bit):	6.006467429758594
Encrypted:	false
SSDEEP:	6:6v/lhPKRxWnDsin14xbG6Qt39OdUMfLNilody3m9n3c8/N/bp:6v/7SRxRi1ki6QF1Mhin29n3c8/N/1
MD5:	719E71300729BDA463838DA2B60552D5
SHA1:	7636C163A0D1EE130E07ABD02CAD0918BBC3E1C4
SHA-256:	A24D2929B0151300C46BCF87D1AF44B08166DDCA0F5BAE7AF0B818B4684245F7
SHA-512:	B4E62CF1AEDBD591558B8059966167DD097D794F97F9657D614AED2AC3D7561FD1D6306B969EAA425DE44A69D176B453F432E7139EEE00AFBBF880E6E0E75AA
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/background-hi-lite.png
Preview:	.PNG.....IHDR..."".....2.....tEXtSoftware.Adobe ImageReadyq.e<..."IDATx...A.D!.DA#....H.>.H3.+.....9.W.....# ...."h .f.....4.....DG@@@..4 .f....eu.....7.....3.4 ...q.....x....H.i@@@..E@@@..4 .f....1.....D.@@@t.4 :b....A3.....D.L..."h .....x...._....!W.....m.:fT....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\contribute[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	8648
Entropy (8bit):	5.113242529210202
Encrypted:	false
SSDEEP:	96:vR4ayh44eZhS2NlGEN2qRh8L7aaPpI+n/3z9Ge048XhFJy85tB/P/JBQvOPtS50b:vRpyhT8Si/2FLq48XlyUFgn6BFaRxUIa
MD5:	F4AA7DC965F75669BA81E2FCADB6C90C
SHA1:	ED92B90179E71ED3FB69524E04E4CB4F3C0BE012
SHA-256:	D618BD7BB0D1C11CAC61D9C0B4EA612A48489373A6438E22605B084B15CFEDD1
SHA-512:	8B3208282A6AA989C4A9023D1D4D7E079A90E671FFBF666D0A35504CE1482F59FAECAB6A0F1115A1502A24770CC3185046029B8F1F356C13D8916DC6B6F83716
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/contribute.css
Preview:	@charset "utf-8";../* CSS Document */.....SubTitle {...font-size: 125%;...font-weight: bold;...display: block;...margin-top: 25px;..}.....Bold {...font-weight: bold;..}.....BoldCenter {...text-align: center;...font-weight:bold;..}.....grayText {...color:#777575;...font-size: 10px;...font-weight: normal;...text-align: left;...vertical-align:middle;...padding: 0px;..}...caption {...text-align: center;...font-style: italic;...font-family: "Times New Roman", Times, serif;...font-size: 1em;...padding: 0 0 3px 3px;...margin: 0px;...}.....rfp-caption {...line-height: 1.5em;...background: #ccc;...text-align: left;...font-weight: bold;...font-style: normal;...font-size:1em;...padding: 0 0 3px 3px;...}.....Italic {...font-style: italic;..}.....BoldItalic {...font-weight: bold;...font-style: italic;..}.....indented {...padding-left: 42px;..}.....indentedBold {...padding-left: 42px;...font-weight:bold;..}.....indented2 {...padding-left: 62px;..}.....indentedBold2 {...padding-left: 62px;...font-w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\element_main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	249009
Entropy (8bit):	5.477400514029805
Encrypted:	false
SSDEEP:	3072:uXpL1f/XaqZ4pmoNGUkaUeH/ktyU2cfRwv+9g5LydY4SeJ/5Hn:u5n/KUef8yU2cfSvCQydBJ/5H
MD5:	92DFFCE3439552F9ACEC893F2868D717
SHA1:	5C9896BAC2ECE31D9AC9EB06F987868305BBC294
SHA-256:	86207A548361E9FCDC830F7CCA9540C7C93FF4132DDE2A72FB38D23151BD46A4
SHA-512:	ED64C2CEC4BB25119747F97370E9ACF905647820F64C80F590C52694975BAD507D1085D4460E53EE26514AA32B24B8CC187A13BD9897BC23034A34D69150ABA6
Malicious:	false
IE Cache URL:	http://https://translate.googleapis.com/element/TE_20201130_00/e/js/element/element_main.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa="' style="background-image:url(',ba="-disabled",ca="-document.getElementById('",da="/translate_a/t",ea="/translate_suggestion?client=",fa='</button> </td></tr><tr id="',ha='</td><td class="goog-te-banner-margin"></td><td nowrap> <button id="',ia='<head><meta http-equiv="Content-Type" content="text/html; charset=UTF8"><link rel="stylesheet" type="text/css" href="',ja="Component already rendered",g="DIV",ka="Edge",la="Google Website Translator",.ma="IFRAME",na="INPUT",oa="INTERNAL_SERVER_ERROR",pa="Opera",qa="POST",ra="SPAN",sa="TEXTAREA",ta="Unable to set parent component",ua="[goog.net.IframeIo] Unable to send, already active.",va="about:invalid#zClosurez",wa="about:invalid#zSoyz",xa="absolute",ya="action",za="activedescendant",Aa="activity-form-container",Ba="alt-edited",Ca="array",Da="auto",Ea="backgroundImage",Fa="backgroundPosition

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\emergency[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 515x250, frames 3
Category:	downloaded
Size (bytes):	45170
Entropy (8bit):	7.975705424400901
Encrypted:	false
SSDEEP:	768:2JkGcmrkzxN4vhummv4CZgIz91xUUeFSFLBHN7/VWaJj+jB3Z6+JZJ:Z0Dhnmv4Ctz5OFSLHN/VbjYp6+t
MD5:	C60B197F794D1EB6EF8D8A73033E969D
SHA1:	4AF6B6DAA296BC4CDC72EDB6A268EF335A5CD8CC
SHA-256:	BFD7FE7E41D9E55BD6BF4B0D9914AC28A93260F09F6D932ED2177BA2178F8956
SHA-512:	EB6584956A6BC9F796502A3BE0C848A02FF9D71271520A2944AB1A130167D2227B7EEFDF8ED97CC9A7C7F894F1F4A1FC3047D92C16EFD18EB7FEE6A76C809C85
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/emergency.jpg
Preview:	......Exif..II*.................Ducky.....<.....qhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:3BF68D6069DFE7118708B7A8E415CF04" xmpMM:DocumentID="xmp.did:B72AC8C146B411EA8712CF657FF392F3" xmpMM:InstanceID="xmp.iid:B72AC8C046B411EA8712CF657FF392F3" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:e0d1c088-7095-954f-aab6-b0177551b83b" stRef:documentID="xmp.did:3BF68D6069DFE7118708B7A8E415CF04"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>…Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\flags[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 133 x 27
Category:	downloaded
Size (bytes):	2907
Entropy (8bit):	7.775139824223661
Encrypted:	false
SSDEEP:	48:OiQfywiU9qoIZgTtchHBui2qZE2JXeAV1s4exJKzo70BAcophyU:LQgoc+cTuyE2JXeAVe1yzTBAcWyU
MD5:	CEFACB60C7B755E1A53603D7CEAB1BB3
SHA1:	435E52E63BEC97DCC13C2B42A25D5AE761B346A4
SHA-256:	258CC7FC6046B5AB054B2072DE33F2911711C33F49E69651E6012BE6AE33C27C
SHA-512:	535F4720AD534264EAF62DFB619B0EE190D978A8096D1C43CA2A7113F943CBEE25ECF79D532434DF3C9E3C88A497402D071A45419B67ADE444EDA1A0D673EBE1
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/flags.gif
Preview:	GIF89a.....Q\..lm...St..HH....LX.....***.....:;....m/V.ir..TT.fU.....qrr.....yy.ww.....i....dd....%$...PPP.....z.11.....AAA.....<C.....L.z.n..0.....[[.ii....st.....GG...y.V..~.....gE...o.....+.....I$.....'.....l.F...Yc.h.....t.....vW.....\.1.....z....d.=...]h....._.....n..O.....)....yo)5.=I.aaa.kynllvw.\.....-9.....7.m..... $.}c.$.....++q.M.....11x.....&.....=Cz....#-.....Pqoo.....GR.H...._...Hj.*1v7\.....k.....Za.`d....a.....i..3.....5D.....8.....?c.....Z]....|..~.\.kU.....iff.....>.....tt.....v..q..}.....!.....,.....H.....T...@.,.J.H.bB..3Z$(. ...?...p..(SZ..O C.,p.....@....#..9..ZTRf.C..6..?.(v.).*..8...9..@.*..c)P./.(p(...V..I.p.#.k.....RFW.....k".9.....5.&I*P.....(..X,J.uM...14b...E.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\flu-fighters[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\flu-fighters[1].jpg	
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 515x250, frames 3
Category:	downloaded
Size (bytes):	50879
Entropy (8bit):	7.969332347625548
Encrypted:	false
SSDEEP:	768:78l+pJaYV+EgGXseX0Dw4uG8uq6UgI4MTaFk9kO2oT3mP+t1KkBTz//clJuWioYJ:ILaggGXpXCw4u3LEQsqmoX//PtYk9w
MD5:	C6E205CAA1F6106D3F67425E4C6E8E70
SHA1:	4FA3F989BE28B335B08F71A84F9B9DC13172A76E
SHA-256:	4D07033D5B68191D651197A33C485FE6C650B1B01F8D1588F7B82BD8B12AB432
SHA-512:	320FCADF1A76D42EA443A80B900F4050F779ED9CA69F2E3BB66C1FDB0EE872B89C8CD8B7A6E8EEE47F4EF2A5B08A6A63BDC165C4329D4B22C5DFC03552AF869A
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/flu-fighters.jpg
Preview:	......Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164360, 2020/02/13-01:07:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmpMM:OriginalDocumentID="xmp.did:06ab1a7f-dd40-3c4f-bddc-1b0ba2abf848" xmpMM:DocumentID="xmp.did:69AB87A8649A11EBAF02BFF896AA0070" xmpMM:InstanceID="xmp.iid:69AB87A7649A11EBAF02BFF896AA0070" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:03a6aa20-2557-2d42-8fb0-f01a7fa3285a" stRef:documentID="adobe:docid:photoshop:c0f84c4e-74b8-11e8-bb6e-dc81c73ad40f"/> <dc:title> <rdf:Alt> <rdf:li xml:lang="x-default">Promo</rdf:li> <

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\googlelogo_color_42x16dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 42 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	910
Entropy (8bit):	7.7455040862049085
Encrypted:	false
SSDEEP:	24:do/cXeTrHaRodw+UWNhsGzRSIhAugV7unmH4ifkx08v5:K/cXeqadLUWNhNzRSMXgV7unbisx08B
MD5:	EFA6BB2BFE459BC6F4BDAFA3DB0383F6
SHA1:	52D15CE52FE50643E542C17812DE43F4ED1B6EE0
SHA-256:	6318394F737C66F0E2CCFCD88E3935C6667633A1B95FA29FBA2B75431D55EEF2
SHA-512:	E23C04D8997F5C2F92070E09261B7EE50D9DF8753F45CF66F604F0874FFA8D99E947C97C528EC02A2C3FBE8E43D840B343A7D0225532980D5DA95031216415B7
Malicious:	false
IE Cache URL:	http://https://www.gstatic.com/images/branding/googlelogo/1x/googlelogo_color_42x16dp.png
Preview:	.PNG.....IHDR...*.....`"....UIDATx..T...=.Mm.....&[....Sl..m.m....U....;.uf..frrr...v...U)...).....2Q..`.y.*...U.9..;..0.^.....B.....].h.^..... . L3....jQw..vB.D....<..P.4..|.B....d..?...Qv.....Dv..$...._|.*.@.....k....`..JG...$..T.y|T.....v.iH...yc6'...%..&.w.oI.ZS{..!6A@.Y.....a....U]..:....g-.....01F.....Q...k#..G\....~.+....z.>....F...}1[..~.9..r[.?..9.....2~....e."1.).}[.WW.{.r...|D..<7..t.M.`..S...8.ab..F ....n..S.:n.>1(g.p$.:k1..6...Y..@.5.8.0y.....R...;.K\. 0p...g.,r.E.....=....!.^..Y!..D.Z.....aV.....;F.4...!.`^.L.VQ.....&...d....O.\...I).!1....{...K.f*.e ....L.....~.%lY(..Y.....NeA...?.^..2.C..^.....P....)T.&?.zm.Sl.b..l.D...%.{.B>X{.9Y..M..:.).....EK..b.....}....|.o..].....GH?..3F.B(.:.....AdA.....Z... .L....)..@?...f.F....6.....u..oQfMC.....OC.1[3..j..j.G...&..D`.....@>...g....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\granite-advantage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 150x95, frames 3
Category:	downloaded
Size (bytes):	9409
Entropy (8bit):	7.917091441614061
Encrypted:	false
SSDEEP:	192:d7F8bw8x4bUUmPrdRlYTKJDt/+FXS+8jUNe4rd9KvzxqBYJNmWHYMtT9jv:dK084UUQrtVRUS+e4rdsv8BYJNpHHtJ
MD5:	6C3A8F80884C06933EAFB4EC5FA06097
SHA1:	E76940F48B89C65B91384FB2F13BBBDE7897C419
SHA-256:	6494DEFEDB24BDCFA6D32AD4DEBC58BB064ADB5A55F03E3A6DE2DE7CEF24D04A
SHA-512:	40C3DE8DA0D3757FB76239838DBB25484C64B87EFF3BFAF3202D57921373483A3017F7EB623CB6F1460D97CF727306B4A36D1D14CE30FB5A5404CFAF9B52FFE
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/granite-advantage.jpg
Preview:	......Exif..II*.....Ducky.....P.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:cfc4720c-3b55-0f4d-b462-f237ad27231e" xmpMM:DocumentID="xmp.did:9901221A0EC611E9A5EF8686F5A610D2" xmpMM:InstanceID="xmp.iid:990122190EC611E9A5EF8686F5A610D2" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:cfc4720c-3b55-0f4d-b462-f237ad27231e" stRef:documentID="xmp.did:cfc4720c-3b55-0f4d-b462-f237ad27231e"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\icon-twitter-bird[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 21 x 20
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\icon-twitter-bird[1].gif	
Size (bytes):	604
Entropy (8bit):	6.242982454000789
Encrypted:	false
SSDEEP:	6:6LlShNn2Hveq2Qu79OzUV8e+gToqyj1D00UsR1HjBewOi27SPksum0frmmYxx5W1:2HUQg9x8e+g8j1ZzHtewOdsutrcxhOPN
MD5:	E102D568E8974BB0951E4196BA687BFF
SHA1:	4D019064F21C2322E537DE510F1649418FF573CA
SHA-256:	67DC276FFF422D3FD9A118EC00E8375CBD3BC036BB31507CFD5DF3D4B479D4C6
SHA-512:	5D5AEC096F090DBE608BC1381772FDBACABBC029FC95249EB359FFE91651B1A9B414CBF0395BEB2278CDADDFBB0A30EFFB6D5FB5B82E49E8FC6B85E021B1EC17
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/icon-twitter-bird.gif
Preview:	GIF89a.....W.....c.....R.....(.....p.....o.....l.....&.....+.....N..L.....t..(..-.....(..U.....l..e.....U.....*..Z.....#... .....!.....W.,.....W.....;...G..@.TUT.SK..B>..1&UV.....H.....E../5<...VT-N..L ..".....(..U.0.VU*..C+..:..I...T...3..=...$7.T...OMT.V.,.....(.P.....2B.7kT.DAd...`...bQ..'..P !.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\mediumA[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 13
Category:	downloaded
Size (bytes):	299
Entropy (8bit):	5.303426088371302
Encrypted:	false
SSDEEP:	6:6liaaRbZtZNf2jOWxlrt+F5d/bsF2Wt0n/n:6vaRbZf8OWPcxQF2//n
MD5:	5A98EE12BAD5586737424F8F3F58EDB6
SHA1:	1CC67DA5C621209969D0EE01EDAEDBC505187B0D
SHA-256:	43707815C4248E0946B2DB9117290955CB5EB684F8C8D3D45EA467C88EECB197
SHA-512:	2D43F687EB11C6DAA47E465CB746641C05EDAE9292E146A283F313016C71C9D19A5876F5546797D4DBB5BF092A50193CE7F3DC9ADD70DB6AC2AD386A94D4C0A
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/mediumA.gif
Preview:	GIF89a.....%.fff...DDD.....;;;.....iiiIII.....eeeYYY.....sss.....===...555SSS.....!.....%.,.....H..pH,...!H....Sh ...RB. 0..G...*'%..I!TJ...B..1.f..(:H...C. H!"#C$"DA.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nheasy-sm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 150x57, frames 3
Category:	downloaded
Size (bytes):	5072
Entropy (8bit):	7.8154030612201995
Encrypted:	false
SSDEEP:	96:l236UtdSb7k5nQMataaEtDfpYB/+TAj+ZrNmDIWgNS:yxA/qQ/twrqBmTA6ZrEss
MD5:	62503F5C9E724CE0B0FD8DAE92EEDE35
SHA1:	05C0EC56843E278D8D58907922D5BBC08DE8F7B7
SHA-256:	3945CF14451E5306AD82AE641F105BD4EBDEBBD65F1CB0FD6F865D1F39BE7571
SHA-512:	C0E5EADE4CCCF69415D2AB1D0CCDEF85982F41B7C4F2D58F254F87F9C2AF187C6321C8040C40C0707E4C2068B332AA2166FA21A31253BC83E88368CB8CCC23F
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/nheasy-sm.jpg
Preview:	......Exif..II*.....Ducky.....<.....)http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:FE9DC7AFFA6311E59447A65323C12060" xmpMM:DocumentID="xmp.did:FE9DC7B0FA6311E59447A65323C12060"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:FE9DC7ADFA6311E59447A65323C12060" stRef:documentID="xmp.did:FE9DC7AEFA6311E59447A65323C12060"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-bold-italic[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 65060, version 1.10
Category:	downloaded
Size (bytes):	65060
Entropy (8bit):	**7.992093389930961**
Encrypted:	**true**
SSDEEP:	1536:Vl4UBHdlaBzNVuEusOn6twV8qiKdsoK2Ua5FtvYgWC7YEf/N9zCcg:Vl9HdwBzNVuZLndV8fKl+alkEfVUr
MD5:	64CF197914FC96C7B92E54BFB7379EE9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-bold-italic[1].woff	
SHA1:	255689E40B8AB1C03264425D5F5C8959E9561929
SHA-256:	259B8272F9578583660384E665AE905BAA908E6D076BBFE9D1CDCABE1E3DD15A
SHA-512:	02015DD5D42E1CF9D5EE4A82B702F4498FD83E062776648C5CEC9593132640BAC49746A7803E923A1AD6EE08E7A01B005F5DFA2345FE540633651BEB339B0037
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-bold-italic.woff
Preview:	wOFF.....$.....FFTM....._.6.GDEF..... ....GPOS.....>\..MGSUB.....{#._OS/2..!...._...`.q..cmap.."........nZ&..cvt ..%(...b.....g.ifpgm..%.....s .ugasp..*@.....glyf..*L...4..".\.W.head.....4...6...Rhhea.....#...$....hmtx..... .....loca.....X....maxp..... ... .=..name...8.....~^.k.post...8....."..prep...0.....=.. .....cl.....J.x.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=.k.NT.U]8GU.J. .o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j.9.. AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 70188, version 1.10
Category:	downloaded
Size (bytes):	70188
Entropy (8bit):	**7.992855179836391**
Encrypted:	**true**
SSDEEP:	1536:BlFGuO/z18Niu+LxlinBDCBbPdk+A4wt5ORBjSmAaYL:BlUucz1PwnIBrmd5yBlM
MD5:	2DCB93D58BA4D53D72CD2B63D3681A08
SHA1:	981CD70798F1E7DB1C764BBACCCEED57FE3FA938
SHA-256:	7C556BCEB86172609B85B74001EEC2D961DA6D8D9D6CEF9F6AF67184D9DA2300
SHA-512:	258439CD092A49B4CC40F0C8A31C59CB6E61181D4BD3A6D77875FF06BE5BD69D3129D5811536525F0384644F024C217824029D0D1568C69ECAF39D7C8E2272CI
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-bold.woff
Preview:	wOFF.....,.....FFTM....._h..GDEF..... ....GPOS.....>\..MGSUB.....{#._OS/2..!....`...`.m.)cmap.."........nZ&..cvt ..%(...].....-..fpgm..%.....s .ugasp..*<.....glyf..*H...]..O4?.s.head.....4...6.%.Phhea.....!...$.).Vhmtx....."x..loca.....3...X.z..maxp...D... ... .6..name...d.....-.*..post...L....."..prep...@..... k.....=.....B.....J.x.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=. k.NT.U]8GU.J..o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j.9..AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-italic[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 65184, version 1.10
Category:	downloaded
Size (bytes):	65184
Entropy (8bit):	**7.992075893557577**
Encrypted:	**true**
SSDEEP:	1536:Cl9CBqDrD0fq12v0nMkFlQfoMSbbj2zZpoYR9zCi:ClQUDrD0S1nMKeRqbKoqUi
MD5:	7629C4119ABAE5C1279C38F4F332173D
SHA1:	910B6E1DDFD18DF34F93B88C3D3704C718F2851E
SHA-256:	A58FA6273D7383BEFF16D521694E65A5CA67A4D1D0A7617A387740848DD52411
SHA-512:	CD0C61D70A52DDAF82A4BEAB2E3B96EFEA3429FAFB040774BF9221A5F9DF8F36EC90352769E663CE1C7774FF0CE6043875DB1193CE7F8CC064488827A251F5A B
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-italic.woff
Preview:	wOFF.....FFTM....._.7^GDEF..... ....GPOS.....>\..MGSUB.....{#._OS/2..!....^...`.E.Lcmap.."........nZ&..cvt ..%(...W.....fpgm..%.....~ a..gasp..*,.....#glyf..*<.....!...<.head.....3...6.j.Xhhea.....#...$...Hhmtx...8...A.....loca...|...$...X.'..maxp..... ... .D..name.....Ej...post.....".prep.....T.....= .....cH.....K.x.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=.k.NT.U]8GU. J..o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j.9 ..AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-semibold-italic[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 65888, version 1.10
Category:	downloaded
Size (bytes):	65888
Entropy (8bit):	**7.99154426632837**
Encrypted:	**true**
SSDEEP:	1536:YlNP3dgTYjSOjOzkRjFdktmP3qf1nLcZDhU9zCj:YlhqgjOWlP3qdLcZDSUj
MD5:	CC9039BD213ED3300C8D067F6B70F162
SHA1:	F15AB088A7FCED99FEE5ED257250534B170653E3
SHA-256:	248D23B4B49EB98435BAD3D34DF8872165E16654C2A79472DCFD28B08B06B78A
SHA-512:	8409B4FD4E38BC9E46A9452F3F2372A87395A36DFD66181F623B9160024FEAFE6160E3C7E533CF833E12A3859BC420453C76CD0B7AA388BFF25595D0CDFBB038
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-semibold-italic[1].woff	
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-semibold-italic.woff
Preview:	wOFF.....`.....FFTM.....\_.8.GDEF..... ....GPOS.....>\..MGSUB.....{#.\_OS/2..!....^...`....cmap.."........nZ&..cvt ..%(...^.....fpgm..%.....~ a..gasp..*4.....glyf..*@..... .1..head...L...4...6...@hhea.....#...$...ihmtx.....@....p...loca.....'...XAE.*maxp..... ... .P..name...,...1...,....post...`.....".prep...X.....x..% .....=.....cH.....L.x.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=.k .NT.U]8GU.J..o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j.9..AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans-semibold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69884, version 1.10
Category:	downloaded
Size (bytes):	69884
Entropy (8bit):	**7.991788037606492**
Encrypted:	**true**
SSDEEP:	1536:+llniJWBUUrv4ZNp5+gmeOAWg0OZSr6WFVvGg/1KFhYG:+lyWmUrv4fpAteeOAvFVN1Ex
MD5:	39534C858FE20A3FC1AAFB039B83352F
SHA1:	7ED8ECCB0B2105E1A9329B233D70EEAB879E8926
SHA-256:	1210A816BFF3871F1F998C24A681256C0965253D3309979C6A38AA18C33D13F5
SHA-512:	ACF65CF393959B9C5CD123D30368AF0A44F7A60DAD478CDF48B2751026838AFDED35F8F99E9C380335FD91216056266168528879BB1F45528C9589E5054F5CDE3
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-semibold.woff
Preview:	wOFF.....FFTM....._.r..GDEF..... ....GPOS.....>\..MGSUB.....{#._OS/2..!....`...`....cmap.."........nZ&..cvt ..%(...[.....4fpgm..%.....~ a..gasp..*0.....glyf..*<.....A.e...head.....4...6...=hhea...$...!...$....hmtx...H...O.....!.loca...../...X..g.maxp..... ... .9..name.....post....."..prep.....x..n..... .=.....L.}.....Lxx.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=.k.NT.U]8G U.J..o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j .9..AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\opensans[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67524, version 1.10
Category:	downloaded
Size (bytes):	67524
Entropy (8bit):	**7.992783189415623**
Encrypted:	**true**
SSDEEP:	1536:pJl+Wp+Zxz8HN2jBMgUQ9xTOL/l4YN0cUADypY7:pJl/p+ZxQHYBQQ9C4YNoADypw
MD5:	81B753A6C202063E3BBE940D13562737
SHA1:	F60C0A7A5795B8DB8FB8B9045C63239BA61D24E3
SHA-256:	163D36DD2444B0D0EAC30D110DDB2E18BE4741EB6BAEC32FFBD3A4C479E74DDC
SHA-512:	E53DAD1D7E5673CC98E3D0EE37703E7ADA29628C2847D6570E6B7CE758351D445C51CCCEECAA66B3A8226059E16E229E38889C3DCBF03CEBF660CB9A3F645C5
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans.woff
Preview:	wOFF.....X.....FFTM....._[.GDEF..... ....GPOS.....>\..MGSUB.....{#._OS/2..!...._...`.6..cmap.."........nZ&..cvt ..%(...Y.....M..fpgm..%.....~ a..gasp..*0.....#glyf..*@.....3.....head... ...3...6...Rhhea...T...!...$...whmtx...x...0.....=.loca.....)...X...|maxp..... ... .D..name.....r.post.....".prep.....C.....= .....51.....LLx.c`d``..b...`b..W.I.0.....x.....Q`.D!.3l:,3,."(B...B.AE../h.N..g8F\..FM.KE..CG..(..Q....+....Sf3.s.....7o. .;...._...w..QZ)..RG....{.....O9^...)...v=.k.NT.U]8GU. J..o..q.r..&{.].....3...d].ov=...`].....sr..=.mX....O.k..m.....~u.o..;.....K.<.h..u...7..k.zN.Z..am....[.....)..;n....t.~.z,.....e..N..r.#\..^.....s.{..0p.l..%G1....h...l.Z...c..h g7.l:...A.6.j.9 ..AW4..<.....>h.A.6=9...C..t..<d2{..`.b>.g.x.....G.w..'..5l.N....%[....7.X>..aSF67...a..G..i.).+F-.S..p..#'...rE.5b..1-W..i]....M.1rt...3.X...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\print[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	28522
Entropy (8bit):	5.17542403704878
Encrypted:	false
SSDEEP:	768:Hx6uVUQyb/S8MtU2xjJ0aJj48DqWp5hQV6rJnJAJIOadL05pbknJ9dZ5lJX0zw4e:/o
MD5:	AF5C8F644AC17AC040DBA5348C6F1551
SHA1:	277C9549B4CC6D7D8A1FF99B02BBAD1D2A560F42
SHA-256:	07BFC685C04932BF25EF8506BE79F3B0539B46E55741C90129F3CFB66F87EACA
SHA-512:	C7F46CAA4FB5B923422F0C9C7CBE729C0B1FD3B674D77016BF483CC4AF302DAC999D636CEF289A99F197344C8735C014D16E685E83513474AB3E3FD99532159
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/print.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\print[1].css	
Preview:	@charset "utf-8";....* {..margin: 0pt;..padding: 0pt;..}....@font-face {...font-family: 'encode-cond';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-medium.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-bold';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-bold.woff) format('woff');...font-weight: bold;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-black';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-black.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url(https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url(https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-bold.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\search-btn[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 36 x 30, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	910
Entropy (8bit):	7.633264256069046
Encrypted:	false
SSDEEP:	24:D2egDtS1EkJikc4dccRmREbM5tHjx7Lf1BvAaEKc:CeUQ1EVXQWRtDxHzAa+
MD5:	A1A1172B6955F3F06DCB37F463A2761F
SHA1:	52E918EDA5F91F36A686D2D28D57E85EDBBCF7CA
SHA-256:	BB5C7B2B21EB3601FE8E001E6454A33C959C9C7187BA1D864A0BA466D90D8DA0
SHA-512:	C5EF377A97127DCAEF1A6057AF03CDB457F327A76ACA08C02CDEB45955DC533477535CA8D4D263CC70A02AEA30EA0DA949979BCD78FD627CF37C8E2F692CE CC
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/search-btn.png
Preview:	.PNG.....IHDR...$.....D.S...UIDATX...?H+I...o..QP.F.....)DI.y ..p.p.Y...P,.....B,.kN...B-..F...(..TL...h$.\...{.....~..v.....fxx.w.....~.+p.hVVVb..0.x....~.....~....J.@.k.@.(..N*2CF.VU..!.|..NY..B`6.)++#..pyy..]. .^O__.V...^.$..r#..;;;x<....%{.H..222..b.&v``.....H&....h4...f0.`.....t.L&.....YXX....c@.....pvv...:777.vEQp..LLL`.....(.,.$...n. b..333.....2....477..h....t..F.....v.....^_x.,.'...ov.(J.Sl.....:+--.@..V.-<.....6.-..B.....p8...t..q8....a..@.A.GGG@j.....o..hdrr...*.vww.^..\..n7...455Q__...,...\]]..F....j.ff...9 ..'/.@.D...y.N'v....Jzzz.Y/I.%%%y.>...B.....!H&..B!|>..X.....P.....B..^/^....@MM....D.Q....x.....a677s..A...(.....P.x<.@ .`uu.UU.....8.l.(..... ...=....$....d.\.....>....r... e.sAB.\.....L[[[..h:.y..K$.I.....d+U.....H....l./..:5.\dD..g....u../.22...B....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\the-doorway[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 150x112, frames 3
Category:	downloaded
Size (bytes):	10721
Entropy (8bit):	7.9222857327358
Encrypted:	false
SSDEEP:	192:n7FuknE1nfULiWFwwlfoy5jtVA/wAkZ1tsMW+kLbY0sspgKtZuKchTKr2aaJdJBN:nfn08LBfRjA49psTLbY0xgiuwr3aJo7y
MD5:	C258A4DB13A03F1076CBD63293759F48
SHA1:	D710F07E70044D66A5021F9FC5A1D72DD7856670
SHA-256:	1482933B0E678AAB9D19132EE458E09FCB16A01712D9755BBA31A74B4A76FEE7
SHA-512:	9308FE2CB30AF1A309E7CDE9562A698D3D7BC67A7415318A0F2A88405B9B036A54420E86DE99521B48BCE2BA69DF4A00109DF95A9F1E772119C6E9CE7C3BAE 5
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/the-doorway.jpg
Preview:	......Exif..II*.....Ducky.....K.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmpMM:OriginalDocumentID="uuid:5D20892493BFDB11914A8590D31508C8" xmpMM:DocumentID="xmp.did:E561AC3D144511E9ADD486A11D2B4417" xmpMM:InstanceID="xmp.iid:E561AC3C144511E9ADD486A11D2B4417" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:56075E5F4414E911AF80F736676497D0" stRef:documentID="xmp.did:066f07fb-c2ec-6a41-98c4-ecf3f60ffcec"/> <dc:title> <rdf:Alt> <rdf:li xml:lang="x-default">Print</rdf:li> </rdf:Alt> </dc:title> </r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\trans[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.292508224289396
Encrypted:	false
SSDEEP:	3:CUkw0Bl/Hh/:G/
MD5:	BF7D3E1972B3FE5BFE8C119FEE05E89D
SHA1:	081AF0BCFECBA29D5C4AC9025A3AEBADF79032A5
SHA-256:	5B4B97B224D9827C01D7A887A722F4C2A680195C4A66108559BAA0C65220DF90
SHA-512:	69B7926725CC19180618609A92BD27CEEC465BAF3DCE01CB6AA05C6A0EBB057DCA62AD2E5DC57FCE75F5B8B2C3B67E456EC880D6DE2B3F3C2581DB78FD6E D7F
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/trans.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\translate_24dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1847
Entropy (8bit):	7.840750948954508
Encrypted:	false
SSDEEP:	48:0BUfsw9mAtN6tl4XZACwezLhPa0V7dHy+1pqWv33z:0iT8+6QJcmLddquz
MD5:	BFA09D19AEA98592C45CE0A814F0EB2C
SHA1:	5DB965A451D9B6B3A5156836182ABE8240D4A0DE
SHA-256:	5FE03BFD95A2D4E640ED7D04DCB08EF991C327A5AB6F6FDB9EB06E1EFC76AF30
SHA-512:	65FCB486B6E1120FE47897BCFE75E310AC72D23213A72754729EFE89E019A431E700202A879A94407F46277ADFAF3B03B5248775645555EB5F8698AA0FE4913B
Malicious:	false
IE Cache URL:	http://https://www.gstatic.com/images/branding/product/2x/translate_24dp.png
Preview:	.PNG.....IHDR...0...0.....W.....IDATx...s#I..{....Yf.C.L..h.0.;...f....0$..s^.I.V.JVT\....5./..'h.....G....5F'..z.%?.8...o4..zC.....v..#...5w.).Y...$.'..&x.b....m.....K.....M.#.....?..J .....\Ha.|...W.x...#...]......F.B%._..k.....P...3.g....\"0...H/...w..A.....{100..)LMMazz.W...I.....M...&..F.0.B...w_. G.....Ocff.!$. V.z{..,0.!.jq.y..K...D{..}..B.....1..*....4...1x.''. s7.....6.*w.....;.v/F.&(..@.A...O.T.~.....a%.w.(;. E..:..QW..^o@ty\;.b..b..%UH..I....Nw.X.C.F.(.'..B..F.m.8]^..!.,L..F.<+.p6f.=.u.c.]?.v._..5.....A.Dzy.....':Oy...zh.....y.....`0..\|i ..2.eUp`)?<.a8}ylr.....B!...1Dv.P..6.p..M.O7..Q.<.....-^.`0^...j..5h.G. ....R<S...h....y.Y.@`.@Aq.OB!.O....+4"+.T..31....f.xG,m.....~Q..o*..}..~ .D.....x..Q\.(*o...R*.6....@.<.. ...../.^^1... ..!^L.*.....e..a.'R^;._..o...U..Jd.V...L..F.R^r....]...>.F..Mj...3Q..W.)N4.(vx.q..Y.h.goEq.;.....y.....P3...hi.....$..I.!...W..J.CL.OB.mq..gbR:.<..;..v;r...]..jd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\translate_24dp[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	825
Entropy (8bit):	7.704648162446466
Encrypted:	false
SSDEEP:	24:ssHKYGXsIPtbm+dBUWkhweNeFb6wfO2GNzj/4vs:ssq/rldTDNd6wfoJ/5
MD5:	55FF382A8B09329E3230A1797EB8F5FD
SHA1:	026AE089006A674DA7DCC9BF6B986C5D59E75478
SHA-256:	1BB2279AED6BC1438D2B17A5FFCBAC9D37864582AEDEEEC8D301EAB162B2C213
SHA-512:	E787C75CD8F6796DE116FDBE0D7B8A3707BB09E02FE3D9F3FA15E5D783931023DBD62344D5178F547E401DBA160F0382A1204DB09EFB322273C7525E592EDD7
Malicious:	false
IE Cache URL:	http://https://www.gstatic.com/images/branding/product/1x/translate_24dp.png
Preview:	.PNG.....IHDR.....w=.....IDATx.....cY.Fk.c..a.m.|e.m..c.6.3.....k.b...9IU..!...7....GOF.Nc.....>..[.H.9.W.:..t{.....c..*../.=.....o.._...s9Qs.....?.P(.`0(...D.~?....Y.h.(..@....< .....8.....|..@.x.,...b.$....YQNt....U.t:3.._. .wQ..T..d...g..h...1.P..E..pA&..l.....G.L...t....CZ.x.D.....a#..F$.H...9...;od.L&E.....P..0.....C...2..o.a....S..Kq9:2z...!s..[..#.....cV4 `.....8.P....i,?..!...}....A.ql.....K7H..|.....$.....59.g..`A.v..~.3....N...N..J..U...W..#.....p...E.....%9Q.C..(F/l.....1X.V1.p8.H..HK..r...a.-<}....,r...).6.G.7..m..V.1....5z,n..w.. n.....>.....^....i....fM....(.Z..&...1U..2..w?.<..z....9...%..d2.b..o..3|..O...XQw.r6....&.<.....;.....*.....1.....y.ZQs.... .).Vk..j...E.....r.i...8...[..~[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\YEY3408P.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	25487
Entropy (8bit):	5.083554954745144
Encrypted:	false
SSDEEP:	384:SGunySC4SJLM/Ex1v2xiJgDc0hAtgn5uB+ec2zgrjeAhiN:SGuFyLMMx1ux/Zh6gn5uB+deAhe
MD5:	5E7BD12E328C4AE593734E1AE2AB3317
SHA1:	5E1CF57202212E5A99323A7728FD8D2B5489C244
SHA-256:	D0E97980D5E7C8609F31EDD59D321A0F9A22E44464929387251959EAEFF56069
SHA-512:	962C34614EBC31A9680FAB8DF4CCFF71B9C5B57E9D012B84CA7FBFA1BE466958B2DD3083CD6171DE1D45886269DD07AD9B52FC3B326565BB99738F32CD074C 8
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml"> InstanceBegin template="/Templates/home.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> .. InstanceBeginEditable name="doctitle" -->..<title>New Hampshire Department of Health and Human Services</title>..<meta name="Description" content="Welcome to the New Hampshire Department of Health and Human Services" />..<meta name="Keywords" content="health, human, services, dhhs, new, hampshire, nh, nh medicaid , tanf, child care, substance abuse, wic, child support" />.. InstanceEndEditable --> InstanceBeginEditable name="head" -->.. InstanceEndEditable -->..<link href="c ss/base.css" rel="stylesheet" type="text/css" />..<link href="css/contribute.css" rel="stylesheet" type="text/css" />..<link href="css/print.css" rel="stylesheet" type="text/css" m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\arrow_blue0[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 11 x 11
Category:	downloaded
Size (bytes):	56

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\arrow_blue0[1].gif	
Entropy (8bit):	4.564221148126157
Encrypted:	false
SSDEEP:	3:CEaiQEllIpbjuE:zaiQElyb
MD5:	8B3611F88D6E07154DFE8D4A742873E1
SHA1:	614D6285952ECF50A5F0F1440E9D21BBAFD1CB2E
SHA-256:	A3933D871CF7DAD771954B3BF4FB984C0212903943C88873F0E3439E85285F06
SHA-512:	5905DA1FB768EA3B2C5AFC29601BD6A78A68C94E79373AF8B826795839F6E986D85459209D3C96713E29FABA92C4C041A450F47FA61A89138077C311C458B165
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/arrow_blue0.gif
Preview:	GIF89a.....R.....!.....,.....ta2...4..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\arrow_gold0[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 11 x 11
Category:	downloaded
Size (bytes):	48
Entropy (8bit):	4.381328385912461
Encrypted:	false
SSDEEP:	3:Ct/00llh3uJT+H:Ac0ydUTm
MD5:	D7A4D95354A5FFDF666AFFE4F7516A0E
SHA1:	E65484EB06115E888D29C35C3864981BE8EC9D42
SHA-256:	3F4D9CC02EB84C4BC1BF181F3452386B2FFC1D64E62FDA21E03F3B6D94CF0866
SHA-512:	EEE1B4350B08CAB3FEF1ADD3DB67F90F527F289BF64C3EA8D22804A297EA2A830A8426F17348B123E39EA9D6F44E055DC0D334816311BD9D4B0BD41447F52FE7
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/arrow_gold0.gif
Preview:	GIF89a.....",.....t`2.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\arrow_green0[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 11 x 11
Category:	downloaded
Size (bytes):	48
Entropy (8bit):	4.381328385912461
Encrypted:	false
SSDEEP:	3:Cpr3llh3uJT+H:43ydUTm
MD5:	FBD0E6E9B04C2C0F0DE3B9B372EB91FF
SHA1:	FF07B76F9896AF9DCFD72E2DB5167C5C7064B0C9
SHA-256:	595D5753D57518C1235FAE639F2665608B8639BB8E12D12DE33339EC4CC9760A
SHA-512:	2D513B0C0A2A18CDB51BC04E8AC900A9B34C378CBFE70A3A0D764D92358F25F34EAEE2CA56AB80F3A314A4E8BBF347117EC05FBCA5C7E04FCDF2E132071E827B
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/arrow_green0.gif
Preview:	GIF89a.....>.r,.....t`2.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\button-sysc[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 149 x 121
Category:	downloaded
Size (bytes):	14621
Entropy (8bit):	7.825199065619867
Encrypted:	false
SSDEEP:	384:yTq9/R62zTbh9Nj5Jg8mf5FBh5R4xJWEEpRO/PK48:aq9gKI8mRFBSdf8
MD5:	BCF9D8B990427A3FD6076D8B828DC634
SHA1:	249E51075BA8E049CF92373FB31175F03950A54F
SHA-256:	2CADB2795C254C1BC18A7FC3E766D5AB760C9566F323E2DA3A60629E8028A88C
SHA-512:	910AE8C8A959BC19AB332916CFE338999121DA1D7450F0AE4BC1224DE1CC66030D92282DA0F4B6FE3B976C25B456286984E443DFC038E9104E04833BFBB51E3
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/button-sysc.gif

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\button-sysc[1].gif	
Preview:	GIF89a..y.....''&..!.....47(.I[.....|||.....CCCy..)3'Xdd...sYF...TWK.....v8E57E*WdT.....C71Rb+.....gtv+)#PQPCA<.....HSU...IU*...GTG...0+'.....<CB.....IS8...+,*+40iji.!....gO=.....T[7..."#!...qti...dddCHDEHIIKKgpI...<=9amk120...KIB.....QMG...~.|#)#.$!|bRRZZ.....qspad[...[\[$+):;1...k}.191.....GEB{_J.....DFGfa7.....YE9...iidGD=AJ*.....CJ<'".(%"glr.....V^`bhd3;8HMQRYR.....\[R...;3/p{z*..O\+.....|..?K3HK>...._hH.....RUW.....ple:>?.....AA4.....>O).....rt{.....358...~v\'.....03 .....WTQ>O5.{o...hea.....L@7...qxqIN2.....bghSMQ5-,;3:... ..@?>ifj...wvpYWX$"(.....0>)oooMGL,''.....!.....,.....y.@.....a.D.2..*\....#J.H..."EL...c."T....dE....M.k.".{.h..G%K.>rR.D..5=....d...Z..4e....N.F}*.....fEbUkU.Y.b.#...L4J-(e@-.:X~.8q.....(;q...:.Z....R.n..W.!C....d... .."GD.4)h.%...Y*4.....d8p.@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\carbon-monoxide[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=12, height=292, bps=158, PhotometricIntepretation=RGB, orientation=upper-left, width=600], baseline, precision 8, 515x251, frames 3
Category:	downloaded
Size (bytes):	129790
Entropy (8bit):	7.890919421015789
Encrypted:	false
SSDEEP:	3072:ie2ke28EzJw9Hew+CLsGU+/7jX94hXGLVjFrRk0:i1k18EzJGHew+CLso7jXOh2ZRrRV
MD5:	C83AD720C9E8C9FF4099CD8A74F63990
SHA1:	EB99ADBE8DC292769D7550A97A0236BDC2F46592
SHA-256:	176E7581B8833A56D160D6CA01B0C29D4951086689BB1293C767DC6F30725181
SHA-512:	55E9CA1348F7065B1D6495CEF4343106DB6ABE7C0DFE13EE216B2004711FD03AF7ABBC67D3A7F0EAAB5518753C987B5352BBECC52B4DC017A15523F237B853 5
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/carbon-monoxide.jpg
Preview:	.....Exif..II*.....X.....$.....(.....1.....2.....i..... .....'.....'..Adobe Photoshop 21.0 (Windows).2020:02:03 15:10:23.....0231.....n.....v...(.....~.....H.....H.....Adobe_CM.....Adobe.d.....N....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...1.....y.8X8.e.....X....;..h.....2....L1..X.W n....${P. .54.1.HFr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\coronavirus[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 525x295, frames 3
Category:	downloaded
Size (bytes):	54750
Entropy (8bit):	7.970078713308231
Encrypted:	false
SSDEEP:	768:dnY8WF3kuJcWl0OdwWFu9cWU6C+YQFgLVKwZLPpnyw60Ma5qbTRNliAQV2OXVB:/WleYwiu351F2JRnywTMbAPJf
MD5:	956167D6912A4B6EFC08FE7C6A8C1EDB
SHA1:	1B2D9ABD46E8F6CFC2F40D236592149A63AF6439
SHA-256:	AFD9A3BD4278B33407F7064C304320416ADF34F1C4CF0FE8198CCCDFD4803001
SHA-512:	8898335B7A458594C8521EE1BC591C61E4D58624513F8C171901568913AB4D3F45405F02CF65413C332F13843F085CDBECDB870587728BEBF561DD68F8ACE8F3
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/coronavirus.jpg
Preview:	.....Exif..II*.....Ducky.....<.....|http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164360, 2020/02/13-01:07:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="27E344336F4118BD4DD0D1DA5195F882" xmpMM:DocumentID="xmp.did:4762E0641D1111EBA05BB25D5D4E51D8" xmpMM:InstanceID="xmp.iid:4762E0631D1111EBA05BB25D5D4E51D8" xmp:CreatorTool="Adobe Photoshop 2020 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:9dbb5d76-670c-014a-b1c7-009a273515a6" stRef:documentID="adobe:docid:photoshop:cff643a1-c15d-9f45-bd4f-e8d01e934abd"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\covid19[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.136589458286182
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPjL8y+KqD:J0+ox0RJWWP0T
MD5:	8AB10AA878C6260D9465F86284A645E9
SHA1:	A3AECE8220D35AB422B15A254D976576CAD5221F
SHA-256:	D8C83817C808A1D7CD8CA3EF9D291C728FF566D3277718641AF8306E492D421A
SHA-512:	D31733023270C2C7715C2E71B925C59B95A98A4A732A2D80A530364882CB7EDDD446AC5C48D84AF6BA18A77B87A7AA9FA020178E9B02985E3C3A4A4740384A5
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\current-map-small[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 296 x 371, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	53362
Entropy (8bit):	**7.993417790305679**
Encrypted:	**true**
SSDEEP:	1536:7wjcii1HaGZ+xJqtUrNut7m1ktLSkBV9uN9Nsvm:scjZbZ+/qtUwwktLS0nyLsO
MD5:	B2A76796AD77608C8BB5C335A8BA63A9
SHA1:	CE5BA1744FE032CD0240612BB9251FA37929E6FD
SHA-256:	5B49CEB3EF060B51549A47694A8D59F61F72240E21CF1EDD34C27ECFAC7E1C18
SHA-512:	CA1010040FD21C4257A82336D5FE5E8CC7A290547998BB36EB1FEA7413CA42F8ADEB96484E25CAA44DC4052FCC167916DB69E838D2C7D73B4DE76C587EB1B0A
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/graphics/current-map-small.png
Preview:	.PNG.....IHDR...(...s.....,.z....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..`....0..jW... 3s...p..'m..^..k.z.^...zmzM.p.p.... ...YZ.2....HZ.d..d>u.yogggg.;..{..X..AAA..... ....GP.CAY.P.CAY.P.CAY.P.CAY.P.CAY.P.CAY.P.CAY..\..#.....`.V..d....9.;.n.\8....o.c\../`0..n.8..}H.....Q0...'..ZA_....s..q...h.....Q.y.....V.....>.3..:>..<.._.#...../.[..} ng...l.w.a...=..J]'.l.^.....m.\.....\.0..tk...^.....s{..K.l.p.....FzfN.y..S.....B~(.....t...O...}..q. .3..+....^....o.Y .....?,X...S....e..h.f.;...../...U..\{;._.m.Ft...i...Pw.].4]oq..>?...6..."W. Es.....:.G....}..E|.U....G?E..Y.....a.7.D:...?.....[,...V.....N.K...5.....iN.X.:..J...~.....rf..l.sW.l...{g.....iy...PV.*....u....22.H....#(.w....Zq..f.o...s....y.....[]].....C...n./ .w...u...o.W.S..E.>r@w.....f..Ga.n.....s...w*x.+..K._..S}....j...{wd.?.y...@..=[...s..zs2..F...MUW....!g+0.>Js....&8..C.....A.....m~.x..o.r.../.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\encodesanscondensed-bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 70596, version 0.0
Category:	downloaded
Size (bytes):	70596
Entropy (8bit):	**7.992124290610587**
Encrypted:	**true**
SSDEEP:	1536:uHsmb+/BmrCSStlF8kfpKhtTJvAiEK3rcwKcRK/9kS48:u3b+aAHF8yKhtFvAi13+2AiSr
MD5:	1CA756A9691BD7FAB6B37D5B4CFCD1CF
SHA1:	8762A8E359C72FCFF098468821E70B3240C2CF10
SHA-256:	795CCCA3255FA08FCDF3F55BE7D69D9D8D87234D5EA653C0074F7AB48676A382
SHA-512:	8B214F2827D0191185DFF85B929D0D0BE1804642ACB4540EA23DB47AF884EF3D990E2B27AB07BA84272E2CF1D7551EC919690268CA5192784ACC095D7226BB45
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-bold.woff
Preview:	wOFF.....DSIG.....GDEF.....f.f.GPOS...d..)Z..s."x.~GSUB..+.....).s.bcOS/2..<....R...`s..cmap..<.....2(.xcvt .....]......vfpgm.....vd .|gasp.....glyf..C.....T..thead.....6...6...Jhhea..... ...$.X..hmtx.....s.....loca...L...,...j.f..maxp...x... ... .name.....t..{post...../%UFT.prep.....s.2x...+..... .r.l.1.&.Jb.....7..*.....".Ia...]z....7I2.C<.....&."i!68..\.Knl.[{....ak>..?.WcH..Z..6....W.....>..C}..A1.m[.=..=.+{.O.9^!?^. *;.w..l....^>. ..$r:.m....\F...v-.l.....nv.{...;)..x..y.p.Uz..~-.F...^. Mn1...{eCt.4nS.b.....e....2..i...;u..._t.e\d\.X.c.u.-u....c...Y.+...M.n...v._.}..;1.YV....w....9.9.<.9'..E.....D..z.....Z..&"..D..H..wq.u..P...[P.y.....n/..n.]....*...n...../,.7....^...RO.b.&.t%... .0.F..G0.E..`.....X.....L....e.>..P.....`..&.&O.I7.....W.`...h.....&.&.LV.....&.\d.N.....M>a.i..\o.5.o..nr..F.....W.U.}._1....E.b4..Z.s:fb..(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\heart-month[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 515x250, frames 3
Category:	downloaded
Size (bytes):	38518
Entropy (8bit):	7.9666917785850115
Encrypted:	false
SSDEEP:	768:8CZFzY4kWAMvZ52+a+yUXBfYKBEOnguKIieeHSg75ncf:J3zY4kWA+pafKBEOgcix7Ra
MD5:	138058CA58F83B75F25F09454E7BF9BA
SHA1:	AD842387E5B44D3B08EB30A63E34D558AF87BF83
SHA-256:	F67797886731188273524 7A034E6A16E237992510302412FC3F1FEC723586246
SHA-512:	BFF4792ED6174E3CD7739300F460F66BDE930587202D11E26BFE21E8551DB7576C098210455F76A96124EBF3FA5DA65C80A7CE0D146CC061DCD523E6A356D11
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/heart-month.jpg
Preview:	.....Exif..II*.....Ducky.....<.....mhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:994155DDDDD4E5119D159C69CFEA293A" xmpMM:DocumentID="xmp.did:ADE14043014C11E8A225EFB984F909B2" xmpMM:InstanceID="xmp.iid:ADE14042014C11E8A225EFB984F909B2" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A0E157214C01E811B0E59950AED94F4C" stRef:documentID="xmp.did:994155DDDDD4E5119D159C69CFEA293A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\icon_flash[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\icon_flash[1].gif	
Size (bytes):	607
Entropy (8bit):	6.150874141816269
Encrypted:	false
SSDEEP:	12:+4fBVm3RLxgpY2CRBs1XGeozZtLTnsO6RSORKPwcXxBmG:+WBMhL+psRy1luXHvs04CBh
MD5:	F39970CEE0E709A2C6225C686E877E23
SHA1:	37193D45B1BD8C7B81F2B50B5BAF80DC3DFA998D
SHA-256:	74F8DF3D7341D6CD60F342F3EFD6433FEA89B34AB60BEBEE6EA17AD728B05360
SHA-512:	BA3AF5CD5A886530C2AB81B7EC6457FE3ECB842F9A552A199D55120F340F705AEDF1759C90203ABFF2B97FC7297B5FDBC98A6C11A3EA473E514E238E78C25E5 6
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/icon_flash.gif
Preview:	GIF89a.....R.....<A.JM.....[_.....tw.....up.IL.~x....xs.|v.<@.....`c....mi....rm.`a.....WZ.HL.....xr.....eb.....|.....@E.QV....9?....rt....5;... .xz.....?D.JO.\[.WY....:?.....!.....R.,.....RR PO.....PKNQ..K(..O N.....Q,5.ROQ.L.4%..Q.....L7$6..A.QO.Q3H.).....D..=;.BINK...8."G.10Q..+..O.....ML.....-.<..LLK.&.#9C'68q...}O|8(".G...#.Rq .....j..D.../x...K..&#y1."...D0.@)...;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery-1.2.6.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	55805
Entropy (8bit):	5.229448793359489
Encrypted:	false
SSDEEP:	768:0csXS2yYCzATBLK88E1o2z33c8yrtz0GBU3+ySk+f1:0cs1ySToR2T3Fyrt0GBG+Nk+t
MD5:	3D5C23458FF980BD76BEE32E76FAAC86
SHA1:	FE16C08BCEF433F057A253330C3548F46F2DFECF
SHA-256:	FF8FE30E152C0EDDAABEB0738FD227DABB8BF538773A7D5E58875C49B53A4A25
SHA-512:	872FCF4EC4BC114CFCECB16DF3352DA7E9D28B0249A7950183DE8CD90D99BDC4103B126976E22CC3D711019058AEC4282D12A4E3489F2111C68CF0F79637EE 0
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/js/jquery-1.2.6.min.js
Preview:	/*.. * jQuery 1.2.6 - New Wave Javascript.. *.. * Copyright (c) 2008 John Resig (jquery.com).. * Dual licensed under the MIT (MIT-LICENSE.txt).. * and GPL (GPL- LICENSE.txt) licenses... *.. * $Date: 2008-05-24 14:22:17 -0400 (Sat, 24 May 2008) $.. * $Rev: 5685 $.. */..(function(){var _jQuery=window.jQuery,_$=window.$;var jQuery=window.jQuery=window.$=function(selector,context){return new jQuery.fn.init(selector,context);};var quickExpr=/^[^<]*(<(.|\s)+>)[^>]*$\|^#(\w+)$/,isSimple=/^.[^:#\ [\.]*$/,undefined;jQuery.fn=jQuery.prototype={init:function(selector,context){selector=selector||document;if(selector.nodeType){this[0]=selector;this.length=1;return thi s;}if(typeof selector=="string"){var match=quickExpr.exec(selector);if(match&&(match[1]||!context)){if(match[1])selector=jQuery.clean([match[1]],context);else{var elem=do cument.getElementById(match[3]);if(elem){if(elem.id!=match[3])return jQuery().find(selector);return jQuery(elem);}selector=[];}}else..return jQuery(context).find(selector

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.jshowoff.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6579
Entropy (8bit):	5.228753253129017
Encrypted:	false
SSDEEP:	192:O10Rasp42ZbGDt2rfIgINP/iVxQTA39KyJArB:g4pjZiu3/iv1t8B
MD5:	AF1015158867ECB3BC8B923ABA626215
SHA1:	DE5FB1BB2BF305F070A706DFBEFF57249753ECF3
SHA-256:	F40473668CB3C72EF3AC8EDDC7945A672DFF271BF54351F639E704FDE2101237
SHA-512:	FB6BE27AA9899FA322A971C11E8BFE248D5E66B7FDA37952372E45E0F7859FE26CB80444B63850E55BA70943FAC3E0CA39838114F3166D01EDAE0519617EB26D
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/js/jquery.jshowoff.min.js
Preview:	/*....Title:..jShowOff: a jQuery Content Rotator Plugin..Author:..Erik Kallevig..Version:.0.1.2..Website:.http://ekallevig.com/jshowoff..License: .Dual licensed under the MIT and GPL licenses.....*/....(function($){$.fn.jshowoff=function(settings){var config={animatePause:true,autoPlay:true,changeSpeed:2000,controls:true,controlText:{play :'Play',pause:'Pause',next:'Next',previous:'Previous'},effect:'fade',hoverPause:true,links:true,speed:10000};if(settings)$.extend(true,config,settings);if(config.speed<(c onfig.changeSpeed+20)){alert('jShowOff: Make speed at least 20ms longer than changeSpeed; the fades aren\'t always right on time.');return this;};this.each(function(i){var $cont=$(this);var gallery=$(this).children().remove();var timer='';var counter=0;var preloadedImg=[];var howManyInstances=$('.jshowoff').length+1;var uniqueClass='jshow off-'+howManyInstances;var cssClass=config.cssClass!=undefined?config.cssClass:'';$cont.css('position','relative').wrap('<div class="jshowoff '+unique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jshowoff[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3468
Entropy (8bit):	5.130714868268042
Encrypted:	false
SSDEEP:	96:gxhTzrJZwi5n3ao8FZpNNNisHrymo4dG4QjRk1:6TvJKi93ao8OHez

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jshowoff[1].css	
MD5:	EA8F627844489B0D84EA383588E13730
SHA1:	D86649EC726D7009B075FEA0DD76C87B73F28857
SHA-256:	28BBAE52F137499A252D25447764FB3A84EE0E6A1C46406C3A62B5E494A6BBBE
SHA-512:	F43F917A7B1E9B32D77017E1A37BD46B463CA829E304C7DAC29459ACC624E22FD7BBB7DA1F34AA211A499621BE92094B92BCD0DFB72132950DD39065E049878
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/jshowoff.css
Preview:	/*This CSS is for the home page slide show script */....img {...margin: 0;...padding: 0;...border: 0;..}....#features, #slidingFeatures, #labelFeatures, #basicFeatures, # thumbFeatures {...background: #efefef;...position:relative;...overflow: hidden;...width: 515px;...height: 250px;..}..../* These are used to round corners in Chrome and Fi refox...-webkit-border-top-left-radius: 6px;...-webkit-border-top-right-radius: 6px;...-moz-border-radius-topleft: 6px;...-moz-border-radius-topright: 6px;..*/......jshowoff {...wi dth: 515px;...margin: 10px 0;..}......jshowoff div {....width: 515px;...height: 250px;..}..../* These are used to round corners in Chrome and Firefox....jshowoff div, .jshowoff img , .jshowoff {...-webkit-border-top-left-radius: 6px;...-webkit-border-top-right-radius: 6px;...}.....#basicFeatures, .jshowoff.basicFeatures, .jshowoff.basicFeatures img, .jshowoff.basicFeatures div {...-webkit-border-radius: 0;...-moz-border-radius: 0;...}..*/......jshowoff div p, .jshowoff div h2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lg-screen[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	44485
Entropy (8bit):	5.189370576255165
Encrypted:	false
SSDEEP:	768:Xx6ueLyHrZ8gibyGuNDxM5471agocPo8/XJNrJuJeM8vpozzClIQFigfR5pjlrkD:gCiH8zoCW3
MD5:	DAD356F86F56E708A1C5FD5E7CB84AD8
SHA1:	FE76597102EC78611A459C7FCA92EA8CE25CB8F3
SHA-256:	982D717A4E58C664E5FAC75EE42D3DF8C7944A91F9075614FA5738E0477960DB
SHA-512:	2C8ED8F722D97FF144ED2BDCB6E36A5BE61A8F72A9227BBAA5D051AAF73504DEBAC7D566125AF77F47FE58792F7DDCC57991C50664A38E7E94D0D77559193AE5
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/lg-screen.css
Preview:	@charset "utf-8";....* {..margin: 0px;..padding: 0px;..}....@font-face {...font-family: 'encode-cond';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-medium.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-bold';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-bold.woff) format('woff');...font-weight: bold;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-black';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-black.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url(https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url(https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans-bold.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\mcm-logo[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 150x79, frames 3
Category:	downloaded
Size (bytes):	17436
Entropy (8bit):	7.969509409078188
Encrypted:	false
SSDEEP:	384:EqoYu66PdIkt3rziZM3jzl9sQ3YRYsAfSjebHrm2eG0bUNs/WxZfzCIC:9UPdIcrzyM3jzPICfSCi20oGexlzCP
MD5:	E561CBE87F6A44380263CA3ABB7C1E2C
SHA1:	DDD632CDD5F527DDE481A3FED8A2888E08D59045
SHA-256:	AFB1AB303CA752AEF90361ABF3F0357B6A84E7B99FD6A8540314A8B737BB9285
SHA-512:	AA4A0E08183659214E004A633FB88145F4ABF672A758F5C50107E368DB077D545FB1AEA91061D47075EF0E31A112DA0B8A9AA9FB1B3E5C90F29001753DA2643C
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/mcm-logo.jpg
Preview:	......JFIF.....d.d......Ducky.....d.....Adobe.d.....O..... .....!.1.AQa"..2B#.wq..r..4t.78.b3..(.....!...1.AQ.aq".2B..5...R.#.t..br.3s..$%...C6.c..d.u.7.....?...Y..:.f9.c1...u..s..c.f3.....9....\|:.R.. ..Z\|".....N....._R.i....f.p."...^`V....w..L.. .U.i..'#C...AT...k.\|.j.8.{...y..3B.:.....Uj.1E8.7.as..#e9.6.I..jjB..T$eRh.>y...5W..6.f..H....-W..+.1.>..[.S..L.t....e.....v..JH.....6+..9R.m..)v.:{.. m.(H..B&..V.$.....B..9...5.-.\\].ZI.q....H...2.s..~...U2T..K.#.o...MS...z....xm.3.-=.)a)N.....b..''PT.A\.Sa...$..m..8"..Q...*...Z..r`r...8..KdY.&..N....kJf.O..w.E.[.0...X.}.Z.b..e.$..oO... S...SI*.[\..*.y...*m.,.p'+...~..m.g.Ywk..m#Q Ed.u...*u.....k..E%.r.....L.[._....V.....y.r.....]2.I....5<....x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\menu-triangle[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 14 x 14, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1725
Entropy (8bit):	6.010293208125424
Encrypted:	false
SSDEEP:	48:2/6r11L4knA9WIiRw5V/c0871a3h3b4HHRy387KVH6p9bs9:2SB6knmWIiK5V/wCVsHR+VH6p9I9
MD5:	79F1FE2A0BC31410409C9DFCC2F7E76E
SHA1:	0927D2E088597BC195FCBC2C4638151B5F4A425A
SHA-256:	53C79F3AAE1173AD214BF0D3AADD33D3D83A595BAA45332B4C94110416B884DA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\menu-triangle[1].png	
SHA-512:	8051C3A6B20B4ED91F45F02E785971E524C57A07C18D562E3F356BE8211F279095D43999572B79AAE1A96CB545CE70F7525738C1801B3A9379FF28EEF84F4FDB
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/menu-triangle.png
Preview:	.PNG.....IHDR.....H-.....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmp:CreatorTool="Adobe Photoshop 21.1 (Windows)" xmp:CreateDate="2020-03-12T14:30:24-04:00" xmp:ModifyDate="2020-03-19T11:02:12-04:00" xmp:MetadataDate="2020-03-19T11:02:12-04:00" dc:format="image/png" photoshop:ColorMode="3" photoshop:ICCProfile="sRGB IEC61966-2.1" xmpMM:InstanceID="xmp.iid:52004830-5682-c041-919c-d66e2f27fcfc" xmpMM:DocumentID="xmp.did:ac96bb68-fb65-3e41-88dc-3c50d73e6f15" xmpMM:Original

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\office[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 300x150, frames 3
Category:	downloaded
Size (bytes):	16557
Entropy (8bit):	7.956386766435145
Encrypted:	false
SSDEEP:	384:4/65fha80xWNegyyZioAFikUkJarKhSH/PiLwO9l2u6pb:1tU8yWNegXivF/UGITBO9h6pb
MD5:	D8CDC6D6E056F4A1FEED452196E47D89
SHA1:	E10CE7AB1ED5ED55BBE46EE18C2BF9DCBAEDAB32
SHA-256:	D803225F1F2A6E5B267C8DCF448605D5F7122DD30FF37FAAAC185E044FA291C2
SHA-512:	281DE0385296DC0C319ABF5FBE691BB346953DB1058726BFB631C4D4EFB11FADD77DCA2583BC21D177E85E3DE0028083B3CE4CE10646C4DDD2607E96F83F470
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/about/graphics/office.jpg
Preview:	.....JFIF.....H.H.....C.....C.....,.."..... .|..v.R$...|.$.I).9..#..$S.....WI.n..Z} ...<..6Wp.%[.|0.S....Z.%.w.H.R$..$=.ZM\I..8....zd..I...x...Z..0o..z.<..V\...\{..H.loC.)._.4:4[..p.m%...R.....%v3V.L.X.g.83A..#r.Ul.o:k.y..../x?=.$.K..e9.X.\.....yZO.=.|....!7...qD..!.W.[..1.a..ua.C:M.n.j.u...7....Pd/.{.0..Kf.....3..dz.....+..S.0....m.8.w..5..W."..=..EI.1..I....O$...J.c....*.....].HX4.4t.F...t4..B....Q..-.p.k..5`.....z.n.._T.}.....F...^...k..v.px....c.;"3G...&..k..]I....).([~..X..EQ.y.*..p...h.O].....+..W.....1..o8.&....c+...0.Nt.!..5.^lS.#}m.Z..8./...M..QM..H`x...I..L!.MMd..]...%...N....$...H.V...|W .:..}.AE...)7.I..+.XH....sa.A..."..T..m4..@un...=`.&8....4...no...M3.n..N.pr.....Q...."].Hs.Y.s.n..n.q..v.."v.}...q.2...{0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\print[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1015
Entropy (8bit):	5.201179617626621
Encrypted:	false
SSDEEP:	24:Po1/EPH0dRU5PNRxYIpm5t16DRW3BT/jmHTnhcJ1DA4hipBf+v:PoqUdS5FXg1D3B+HTGLAK4p+v
MD5:	32C7EB2120D98C96C282E7A824E7694E
SHA1:	7CDB846962FC7D84DEDE41B922AF71AB8E652134
SHA-256:	9136B91FAF455180E6E18CB97C04C2B79E812DA891B83EB84E30DE87E7BC108F
SHA-512:	7A210A3F212E7059D24174C35D4C265B5834CA820F34D51369FC194C21F3994CEC16A3D8A13978EA9D4A055E94B3104480BE3AA949128B5108B77568B2E6D7FE
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/print.css
Preview:	@charset "utf-8";../* CSS Document */...../*Reset Style*/..body {...margin:0;...padding:0;...line-height: 1.4em;...word-spacing:1px;...letter-spacing:0.2px;...color: #000;...font-size: 12px;...font-family: Arial, Helvetica, sans-serif;...background-image: none;...background-color: #FFFFFF;...}...../*Remove Element*/....nhgovheadercontainer, .headerNavbar, .headerNavbarDS, .agencyheadercontainer, #google_translate_element, #addresscontainer, #leftsidebar, #rightsidebar, .footercontainer {...display:none;...}..../*Show Elements */....contentnarrow {...display: inline;...}.....pagecontainer {...border-right-style: none;...border-left-style: none;...}...../* Show URL */...a:link, a:visited {...background: transparent; ...color:#333; ...text-decoration:none;...}.....a:link[href^="http://"]:after, a[href^="http://"]:visited:after {...content: " (" attr(href) ") "; ...font-size: 11px;...}.....a[href^="http://"] {...color:#000;...}...../*Break Page*/...#comments {...page-break-befo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\sm-screen[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	36845
Entropy (8bit):	5.191778062616621
Encrypted:	false
SSDEEP:	768:cx6u65i3b2rZOcDGoiXVGudMsi71agocPH8/KXEaIJNrJuJmM8vpozzClIQVDGeY:XiS8nokclL
MD5:	110D28B964599E5C1D4374333CCD4A28
SHA1:	3ED13E84CB7C8592C5F6F4FFE46C4C4F7D526A4F
SHA-256:	3F16367310BDE403841A1B9789F42936DE4B27A113821BBDA9921114B00B2C72
SHA-512:	78B69D8F6AC604AD07C52F5E13A7CE0F3270FC42023DD3E49EC901D36CCDD61460DFED35021A8D215CFCF63FBEC8597D66F971B95F67D2E520040A0B9771C8C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\sm-screen[1].css	
IE Cache URL:	http://https://www.nh.gov/covid19/css/sm-screen.css
Preview:	@charset "UTF-8";../* CSS Document */....* {..margin: 0px;..padding: 0px;..overflow-wrap: break-word;..word-wrap: break-word;..}....@font-face {...font-family: 'encode-cond';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-medium.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-bold';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-bold.woff) format('woff');...font-weight: bold;...font-style: normal;..}....@font-face {...font-family: 'encode-cond-black';...src:url(https://www.app-support.nh.gov/nhgov-fonts/encode-sans/encodesanscondensed-black.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url(https://www.app-support.nh.gov/nhgov-fonts/open-sans/opensans.woff) format('woff');...font-weight: normal;...font-style: normal;..}....@font-face {...font-family: 'open-sans2';...src:url

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\state-seal-20perc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 290 x 272, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	176189
Entropy (8bit):	**7.995265529394209**
Encrypted:	**true**
SSDEEP:	3072:Zg6TSbZaVpaMWowoFTELiokiPI2emGUhu30Y0gYl8kSpECwHImBwLP+IgLsIE7hl:ZDTSKaJoT/HiPI2WKxsQ1BO+Igrio0
MD5:	0B20ADAA7A352B28E7094F9CBD58B18B
SHA1:	0F8210B0491CDB022CA8E150A15E6F5793CBAA65
SHA-256:	E39A2FA14D90DE7F6FC614EFFBA41A5A523295DE9497F28949FAD44F30985FDF
SHA-512:	F40C9708761F96816167290255CD1E4C25E6764FA31544ABEC0CC5BEE8A2AA8EFE89705436CC2784619BF2351493FC1B69C9427C3C157FF1909F924B05F7C6DC
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/state-seal-20perc.png
Preview:	.PNG.....IHDR..."..........y.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..w|.U.....%.9.FB..R.....b..;vQ_.b...`.A.D.....jzo'...k.9I..~....._o...9S.^.Y.....o_.$.....w.&.. ?....d.b>t.....,_.N....2D;&..p...(..CX..@....Z....`{U!.W8. ...3"R...._C...W.....(.p.0.....]..1....&.....c..m8.....Y..t.f]'DQ.....;..Gm...V#'...e-t.n...o...2.{...Ep.....4Cg.....9..x.P.". ..d.&.....cxr....-.=.7Z..Cj..f.....`HB..\vQ)...9d:..e.v,\|.^4...:.....W_.....kTP...-...w.}'.6[ut...p.....'a..CoMD....o..~.....!.*.6.....UP.W.Y....$HllEz....D.5#.G.....Y.(...4..DzMU.m\.?... +.&.$~.....o...#..{...v..-.....).."mx..=.....Ct..H.Ev+to.dE....t...*....=..3.~..'f.....BX.*.....c^.8.."H..4.Xs...<..n.....Y.A..yF.N|mF.H...5!..'n~..L..C0Hs....j%#.|.....m....K..A~.3+._. &C...8.V4.....S7...d.....k.p.x.....-.1#.>.:cf.....o....F../..{W..d.....4.,!.....W..G....).l.U2..&.\..'.t..Oq.....0..').....~.....{.%..n..`u.N...R...*.....Wgo...0.m..y8R5.n_....Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\trirong-bold-italic[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 104636, version 1.0
Category:	downloaded
Size (bytes):	104636
Entropy (8bit):	**7.994372920279513**
Encrypted:	**true**
SSDEEP:	3072:UFMAyAJh4p6VbL0JGHXmAIaYH1lgIReZK:rAyAf4p6VHMG3FfYVpReZK
MD5:	B319D127DA5E19FFB74114611F565BA3
SHA1:	E679B91CB5E993D3F22FC6157DCE53961E29625E
SHA-256:	69CFCC5923557F154D05913A99D8A42349473C90591FCBB014E2D4049C1303B6
SHA-512:	C3B82228A2F0B36B43E8AF5AD5F986CF8B2631EEA96AB20C3DB4D1325CB86B39629A83426AE76430FB323EBC309C00BEBA66479B6453A010C2D3F017DA4D1CB
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-bold-italic.woff
Preview:	wOFF.....FFTM.....q...GDEF.....z..../.-?GPOS...,...F..0BU...GSUB...t...p....6.j.OS/2.....V...`_...cmap...<.....N..8=cvt .....f.....:.fpgm.. `..... ?...gasp..&$.....glyf..&,..E....0..head..k....4...6..zIhhea..k....#...$.K..hmtx..l.....|..loca..q.....xmaxp..y.... ... .name..y....}..7.C!].post...P.....X.<..prep.....?.z..... .=.....U.....j,hx.%....a.Dg..xQ...D4.~$.....b&g.....i.MGMY..U.....s..7..'....aFJ.....c..5/..K.Y.}...s..^.....\|..g"b..x..y..U...9.^..^w.=.Ig..1.$...#..d'd....h^.(tF.....g....[J\...Z..... ;....B.R..b&...s.{..5.N..k..w.{.}.....9...-*"..Cn.....m.....t..-...rIqU...w....o..!..o\..q=..j..*..l...n;"#...;|..A..+.:Z.w.\.....~.Z:.w.?3..3{.:.9.Rm..+.y._;..gm..R..:....[.....Q.m..557.U....0..x. .I...b..sE.4fZ+.-.....tQx...<...,F..IcY..gZ.p.aTfU..M...6..7...L.-...w..T.....o.....o...F*.q.(~Y?.8c.y.Kv.z.]..Z...n.....c...$.}.WW..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\trirong-bold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 92188, version 1.0
Category:	downloaded
Size (bytes):	92188
Entropy (8bit):	**7.994132078924214**
Encrypted:	**true**
SSDEEP:	1536:oj63PgyTzsCtGbDFZy+62kHiyk1QVeomuttkSV5j6rmLW2y7Mvqmy6BimyqCDgzc:oWthABZy+Ebk1QJmunvWysoqmDQmUgzc
MD5:	D06A96C19D63EEB1ECED3019275A55C3
SHA1:	2D67881AB1B55AFE06F30C3A319D1A171BDA9D00
SHA-256:	D00B15BE78ED504B4A71B0EB09A634C79D8722FD7D35487B4E4B50DD8619FEEE
SHA-512:	E17224EF3B7E323888E041B2DE4C5CE8F7BB457D8D66AA1582BFA3D292ED83EE9FB852ED6446FF9E71B2644D67370D6BAFF23634B09D79DB248FD77DDA64615B0
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-bold.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\trirong-bold[1].woff	
Preview:	wOFF.....h.....(T.....FFTM.....q...GDEF.....z..../.-?GPOS...,...-..0F..QGSUB...\...p....6.j.OS/2.....T...`_...cmap... .....N..8=cvt .....e.....;.fpgm.. D.....?...gasp..&.....glyf..&....M..qHs9..head..;`...2...6..zMhhea..;....!...$....hmtx..;....Z.....{loca..A.....maxp..H.... ... .name..I.....8...Hpost..[.....X.H..prep..gx.....?.z.....=.....U.g.....j,]x.%....a.Dg..xQ...D4.~$.....b&g.....i.MGMY..U.....s..7..'....aFJ.....c..5/..K.Y.}...s..^.....|..g"b..x..{..U...9.=..N...I&..;..B...$$0y.B.....*.....U.*.8K."..R...5K...?.e.[....1R..."..bz?.t.LO2....Vm...s.....s....F.*.I..Uk7..{.sH...=..RlqU.E.w....o.....]....u...;k0*&5.o..8...2.....h-..s.2.k3..k.....7{}:..F;.Qj-.{D3..kG.Y...l....j.4.h.5...DS{...h...*y..>iH..\%.f,S_.Q..U....+.>.j{...z...,.C..+.*..BfB..z.. ....._+xG.PC*.AK.....T....[.....;....CA_.KR....>....b.I+.M.....r.. ..|.|.|....'...y]U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\trirong-italic[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 97836, version 1.0
Category:	downloaded
Size (bytes):	97836
Entropy (8bit):	**7.992812856165301**
Encrypted:	**true**
SSDEEP:	1536:oztrIeRrHfnKXXlmskBvETVgmHT/TKzCcOmbhSszaetnPO+MyaRw4WT6z0YN/S:otEeR/neXrkq/THclzaetG+MRZOY0YN6
MD5:	8B9E98B92DCF4E9A700678A91745C669
SHA1:	6B40C2B9268FB260AFB3C294E77AF47968FE7356
SHA-256:	F9B1A7B8D47D2D7324A13B088BD6CCA6ED4B8BB105545F0F2E00D0FAA46484E8
SHA-512:	0473F5F4EBF3532DA731759A4364E2CED367D1713A05A6A244AF39C520CD1A53F7E43778DB9B36E174BCE51ED646F9F26E49AB9FF898EDB364882402F5A4D529
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-italic.woff
Preview:	wOFF.....~,.....2<.....FFTM.....q..2GDEF.....z..../.-FGPOS...,...../....GSUB.....p....6.k.OS/2...|...U...`^...cmap.....V....cvt .....b.....9.fpgm.....?...gasp..%.....glyf..%...<.....head..a....3...6..z4hhea..a....#...$...thmtx..b.....(.loca..g.....maxp..o.... ... .name..o.....8....post..q.....bf7..prep..}.....?.z.....=.....T.....j,.x.%.....Dg....J%.h(..BG.....s...Mv.....ud..@C...+W*...^y.....K.r&.*....r..\.[.*.)J.e..V...5.....;......"q..x..y..Gu._...cvg.`u....,dYWD...iY.V.-.....!@ Elc..R1.L.6.l....c.%(.^.C..."..2.....-.Eh..7...vWK.JU.....~.....{W....Sn..u.wJ.C.<!....CGd.$.*...FKb.[vN..[.mF....w.|g..D%q...NH..C7....G....vEL.....K.X...-.2.q{...NZ}nv.T.;.S.4.^q.w.....K_.....6}{0}2.\]k.L:sc.].'*...B..B.d..t,c..+.=...ep...=..D:..Y.....'c...ed.<....~~..[.5F...c.....~.....z0..A....k..w..*....G.{.~....e...S.6i...n)..V..p.. ...08.....=n]1.:...b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\trirong-regular[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 91200, version 1.0
Category:	downloaded
Size (bytes):	91200
Entropy (8bit):	**7.99415993124143**
Encrypted:	**true**
SSDEEP:	1536:8cemqsJMY88ViCR23M/yu4EUfM7gss4QOaRAUYQZJthAVA8Pu1Y2PxcFWE:8cemq8Vx23OyAUfM7gstQOjAHth4AQuO
MD5:	E69DE951CFE0745B7DD409C22361ABAB
SHA1:	EF6600CB946058DE66822725CFC60F536925E9DF
SHA-256:	FE728B3EF76B93A90F08C48B3CBEA9E3652F70DEDA41192120AB87DB4EB3C207
SHA-512:	58486D3D089DCB5BC216036C402D5FDA723296BFDA25E7937A2565B84E1A3E2BEF839BA66A4FBE2297AEA8D19D3FF6922877998E6FDE909F4B9E2D4B0390489
Malicious:	false
IE Cache URL:	http://https://www.app-support.nh.gov/nhgov-fonts/trirong/trirong-regular.woff
Preview:	wOFF.....d@.....<.....FFTM.....p..TGDEF.....z..../.-?GPOS...,...../....1GSUB.....p....6.j.OS/2...|...S...`^...cmap.....N..8=cvt .....d.....:.fpgm.....?...gasp..%.....glyf..%.....b.. |.head..7....2...6.xz0hhea..8....!...$....hmtx..84...B....HO.Tloca..=x.....klmaxp..EX... ... .name..Ex...Z..7..\.post..W.....X.H..prep..c.....?.z.....=.....U&a.....j,#x.%....a.Dg..xQ...D4.~$.....b&g.....i.MGMY..U.....s..7..'....aFJ.....c..5/..K.Y.}...s..^.....|..g"b..x..y.\Wu..=.=.Y.{f.].i..hC..,.....bY..Z..b.Z.U..B.(c.p.@.S...,....6f..bYm.....E...pM...pTB..=.z.#.H...*}.;.v....w.....F...Kj...[d...o?,.o.....\.\.rY.].%...[:d.k.7_.....zg..D%u.....C{o; ...8t@:..V.]<.(c...P..M...z..s]...9G...nnZ\..v.E...+...}.....aO.....7..6f.d.}.F.....}5r2..5&267.F:s.<.W...P.3.O4..''KrW!k.elU.>7..\#.m."w....-.....lx.....Z0.....*.....q8..lm.....Y...+.=..\.v.Sj..-...p'.....|.....[]...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\xls-icon[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded
Size (bytes):	1060
Entropy (8bit):	6.5523064400854745
Encrypted:	false
SSDEEP:	12:WnfJ2E8aiGIb63CYUEbTzgCO7adD7qfDXSct4SmgoM5DnElf37Zan8wmD5MGznIw:UAtf0RX1O7atS1fhDEF37ZsEINS5zTq+
MD5:	3DBE760EAE2C284187D535C8A88D4AA3
SHA1:	512CFF45B5F642A453EB5E8FFCFC855E4CF8A587
SHA-256:	ACEB0FFCA43ED21666E999200E07E44CD3C3EF35BCC899393BC47A06825CA6B6
SHA-512:	E938AD3A944D45579E7EB1C1184DFCD3F55E5ADFECF2962512E6239C0AAB2FB470B4BDBA356C434F865AD54AECA4D5C3A2B78A59B24C98DAB5748FF33353F60
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/graphics/xls-icon.gif
Preview:	GIF89a.....U..6k.c.T.....6j.....3u.5j.....}..n.[5i....E.....].H_.Ji.....W.V.....U....f..U.....U....`.U.....d.P.....t.]n.Y}..q.a.....j<t.H.:...O.....\.I.....M|.....tj.aq.]...H..b.b.....x.....7l....;n.3u.....B..3t.3u....X.D.....Az....d.Q...h.g...Z..R...qY.D.....e.WB|....@w.....k.a...p.h7x.L.....C..n.[...[.G...R.D.....|..u.gX.C7k.....d.W...`.KF..[..@q....K..H..L..k....I.2t.....f.Y..s...U.q.....A.....i.....c..Mz.f.Ss.l....v..mE.6.....!.....,.....e...H.A.">..S@.CY.....EhDj.....N.9Q...C.2pDcf...U.....KVd..@..YD....RJd.Y.....2f.X.d..Nwd.....+...q..D.Q.....A(T.8.#..G.... G.5I.....#Y..H....A].X..@R.Y..L..gN.&G.y...O.....u.N.L.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\1000x100-jpg-header06[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1000x100, frames 3
Category:	downloaded
Size (bytes):	17925
Entropy (8bit):	7.961742262047726
Encrypted:	false
SSDEEP:	384:OnDrAMst9mJecX6TYfTLSNyB+bNU0fxhy4dZXHmHdNvh:Ovzst9uXz7uEB+bD7Lavh
MD5:	5A2DC4F484EF0A7390493900283BF3EE
SHA1:	051CBC0963BB50413B4D30F156B4C4356A82F924
SHA-256:	6BBDA937684C997DDE4E58722C1E6A3EF7850689E47F774E8B36FA02E5ED10F9
SHA-512:	E58C1CF2F2F30C11E8FC017A40B3B66E670B73B3BB88779D8A8235AC53FEC3A93679E09F949B4C522D82C34440311034EA38D116F3B9021FB803E227936EBC2D
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/1000x100-jpg-header06.jpg
Preview:	......Exif..II*.....Ducky.....(.....)http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:A3E037A50DB911E4B50BCB33DADB8763" xmpMM:DocumentID="xmp.did:A3E037A60DB911E4B50BCB33DADB8763"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A3E037A30DB911E4B50BCB33DADB8763" stRef:documentID="xmp.did:A3E037A40DB911E4B50BCB33DADB8763"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....$$"$$53335;;;;;;;;;;.....%.....% #...# ((%%((22022;;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\button-glencliff[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 149 x 121
Category:	downloaded
Size (bytes):	16961
Entropy (8bit):	7.722181974036868
Encrypted:	false
SSDEEP:	384:0afxFf87Kr6PQeaKHSYheY+oLey9TuVnCLQoWql8cr0a5mI:tf7f82r41hevQru1o5rbUI
MD5:	C39C3037DA3701E35E53688A1BE5D566
SHA1:	D7CEF2CF7147252F060E80939F18B4557903129A
SHA-256:	1DAE627C236A85D5A1C4E0B5BDC8E8D086A0A4BD613670E75A9AC6FB04D702A2
SHA-512:	4C8A2B3AD40AA7B58D97D68E0946506D7C899A70F6B592564D651B677C2D0A4F8D527549C89DCEF8F08A05702450A29F022F6FBE13AA9D60F61D2B379066155F
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/button-glencliff.gif
Preview:	GIF89a..y....M7,..K...nh5.....VVVzzz56%...kV3y.O....{rMK..V$).....[.....n7FEFefe..Y..v..a7F+...*1!...FF5VY6...%)".....X.L.hh.QN....yYe6.....j...994...wwvE.{y..a.....?XWG..w...DC)GU5.srffD....zD..l....zT.... ....R3.ss..f.....zyU....giZeDZG5..I...W[_...=AE.xB.....G..b....j.|.....ujD..cdcW...[:@vwi..v.{..e...iuBwgg...fiq...{..m:..m...yt.|w....43...GQ+79F.xx..u^`bSKF.....q.rjVV+....k..i.kh...n[d.{Z...dC.zAIKQ.>E.uiyx..$ '.....OQR.....UH)4(#.....y.wd...iU.ut..irg..c...i.Q3uhU.....k.zD.NL....a:...%.%...mo.....".."..P..d.]`&%/.....,21..e.M....{{oss....J....vkqkt.f=.zs..i.....b\MRA...lsW....RWKX.ns1+0.....s..K.....I.....GB.....]`.....uv..D.....!.....,.....y.@.....(@..<x..*\....#J.H..E....X..G.....@.....x..f.&..... ".....##.E.Ae..M..hi1..1...2.D.%.-M.i.G.H..{.....&.rQb..G..h*.j...Z.Q."...s.....!.E..5.....{&.H.....%..S0.....>..Y....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\button-nhh[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 162 x 127
Category:	downloaded
Size (bytes):	13794
Entropy (8bit):	7.8213130255442085
Encrypted:	false
SSDEEP:	192:DYx89BJjCA890Z/K0B9Ljs7LtGGv/atK++BELUzaYIoSJ82s02Wkv9M29kAL3g:D6aJjC7wPjWLtD/h++BEgIvq2sMkvn7g
MD5:	8DF72335578FD65D2DA9759530E147FB
SHA1:	140CC7ACE1A5883659674FA2679C47F89B744412
SHA-256:	2790E88A1BF3D336DBDD2200DF5D072A6B7B9BC64EA577AFF2739DAC924FC840
SHA-512:	C4D02AFCF99CF0CF50487F3DFF71153E634B2F0A0CB88E8F95DA535EF54C2E7199E3CFF898168AA2DEFA72221186A07C446E9AB6A9CD67E6E9984563D13BF9F8
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/button-nhh.gif
Preview:	GIF89a.....DEBRjo...7GI...Zt.....q..3F1...PiOu..h.l.....BI:.....lmm.....5;6)5"...z.....#/.UVU...DYW.....)46...dwyu..uzwi.....#.....h.....28(BWB..}H^f$)$.....t.....$$...bh]s....u../=AZ..tsm@=7`xc.....^..PTL.....ANR..._mv..."-/...one...g..MMI.....y.....l..|.....0.(.....~~w.....^_ZP;>.....u.....U.....!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CS5 Windows" xmpMM:InstanceID="xmp.iid:929FEC153A1411E6A662F62ED57C5719" xmpMM:DocumentID="xmp.did:929FEC163A1411E6A662F62ED57C5719"> <xmpMM:Derived

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\calendar-graphic[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 126, 8-bit/color RGBA, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\calendar-graphic[1].png	
Size (bytes):	13037
Entropy (8bit):	7.9638596412762785
Encrypted:	false
SSDEEP:	384:7UUVbS3J79HLEmDVxE+i+HGWAXg0eV+V1fJkm1bT:gkbSTrDZx2+HJug0Y+ym9
MD5:	6452F1EC1866D5ED498BAC41660565B5
SHA1:	B1232C23FCC3A911400E6E6AB9437C14D20D72DD
SHA-256:	87D61DAD66681572B3AC12B40CC346BB37D0FFDB9BB83CCF9482C55CED44386C
SHA-512:	96281ADF7AAFB026E0824671ED1E6F04466CF919F772A78B1623F33C67609BEB9AC941548BE4D329FE1BFAFAE554B92AFA0B8D9E067DCCA2C87D86145712ABE4
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/calendar-graphic.png
Preview:	.PNG.....IHDR.....~..... .IDATx..w|.....i....)...J/.W@.C(.@..)6.zE..^D...(...E.....kTP.H.@.M...Bv.....$(...d..9.9g..y.3....?....?....?...g....\}..S'...=...~...*....Wb.T.....%W .V...w.N..RR^EX.....~."...\..$.r9@(P.T.~....-Q...Rd.'.C'...G..j.....*.HDr...[.r.%...EJJ.....%...RUQ.... .(.....-Q...OB]....K="a.?Q..`..-A.N...D...k.....+b.gyo..*...b.p..|..(/l.B....30. O}...O..a..g..$..0.....1.qa.....f.....8."..U...1A<ps#..G`... =+..K.0.#...4..t.j.W.~../j@.3..f.....}.Y.=.Ao.]..n....LY....({.*.MX.gbl..}p..Ub.R.{.c..X..(...5..#..p}W...m....U?`.. .a.. .'06.T.O.?k.r1Ag..R.%.....W...Li.O.y.....4..7....:[.+.6PXT.V+.....K.....}O...?}...7.GpL"_..d..S,{.vf.k./.....B.....8.Z.@.....Np.A*{}.p.&=.&:C..ub...`0F8..f..ov.X.!..q.....(.C`mt]..... <\|...IB.Z....U.'G7'.A3..tz....1.#..n...sW+...=.V.*....q..&c0F...2i.O.SKJ..!,.6...T.E..M..k~#.Q..C . ..6..0Bb.....?.....+.....`.K....av.DR.5...H?.....!$.A.....\.,.....eb.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\covid-19-collage[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1170x283, frames 3
Category:	downloaded
Size (bytes):	143308
Entropy (8bit):	7.973656679323932
Encrypted:	false
SSDEEP:	3072:5Jja7cG6rjN0cASdhuaCN0d4GetkLDUD2eMoLr6/3cRh3sSuBKN3KFZ:y7cz/N0cDdhuBN0d4GekNeMoL2/2h3sh
MD5:	26C0D88A73DDAF3A968D1843E51C6089
SHA1:	92500765685752564704229DDB3DB920F017C295
SHA-256:	4580309A26E683FFC37F95E1C0F2B5A7F9CB3F786E9E03BACB0A69F7C6E1CCAB
SHA-512:	AEAB175551D97FF2F50B5406AAEAB71916EDFF6D817F3BB1E06E39F675F32A4F3D40620EF76A99FB770C0E9E25396A0997F43B9E4A71AD66B3E0740E6C36063E
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/graphics/covid-19-collage.jpg
Preview:	.....Exif..II*.....Ducky.....K.....|http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164352, 2020/01/30-15:50:38 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:74a41400-ae58-8741-a221-759c506f2baf" xmpMM:DocumentID="xmp.did:635DF94A6DF211EAA057FEC637C4FF70" xmpMM:InstanceID="xmp.iid:635DF9496DF211EAA057FEC637C4FF70" xmp:CreatorTool="Adobe Photoshop 21.1 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4ce68ec7-9ab9-3548-b2a4-74b238e8ead6" stRef:documentID="xmp.did:74a41400-ae58-8741-a221-759c506f2baf"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\covid19[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	21687
Entropy (8bit):	5.047664886846948
Encrypted:	false
SSDEEP:	384:uhnOw8I44Wq6yzCjAO9eF3SofwQRLcPbDjNlCy:uFOU5zCjAOQQQWDvCy
MD5:	0B60D9DC633A3261EC79768E730832BA
SHA1:	BEA2EFD5CB5389E478190C74DC952C6B26D66E8C
SHA-256:	3658E067B02ACE6D9E8150C278C7CDC593332EBC6D083D774F00DEDCFD9CF7D0
SHA-512:	A076A11F12BA66D6AC04FDB93D8E11F7BFF49AF319AD5FEA52A2FCECA6EB4B36871C2E351C27351F728BD982F8BCDF95EDCB1234AF9A3058B0BCDB2508E51C98
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/
Preview:	<!doctype html>..<html lang="en"> InstanceBegin template="/Templates/main-w-box-new.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta charset="utf-8">.. InstanceBeginEditable name="head" -->..<title>Home | COVID-19</title>..<meta name="description" content="All Information on the Coronavirus Covid-19 in New Hampshire" />..<meta name="keywords" content="COVID, 19, coronavirus, New Hampshire, NH" />.. InstanceEndEditable -->... [if lte IE 8]>...<link href="/covid19/css/lg-screen-ie.css" rel="stylesheet" type="text/css" media="screen" />..<![endif]-->..<link href="css/lg-screen.css" rel="stylesheet" type="text/css" media="screen and (min-width: 730px)" />..<link href="css/sm-screen.css" rel="stylesheet" type="text/css" media="screen and (min-width: 320px) and (max-width: 729px)" />..<link href="css/cms.css" rel="stylesheet" type="text/css" media="screen" />..<link href="css/print.css" rel="stylesheet" type="text/css" media="print" />..<script type="text/javascript" sr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\cumulative-map-small[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 296 x 371, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	73630
Entropy (8bit):	**7.993771788542376**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\cumulative-map-small[1].png	
Encrypted:	**true**
SSDEEP:	1536:bqWhE2FDOvSxWE08YCmDcsh1HfqgSUd5dUopmtN9w4sthdO01nD:425OvSoEWCOcsagxUoEtAm+
MD5:	F4B170A46A69188BAC5F80B18592576B
SHA1:	2617C9F08505320375D737A8D3B2DA57A93243DE
SHA-256:	4EBD24BAC47AFF2EECFFA9C724898BC23931EFB9443520287A5C4FB984BFF45C
SHA-512:	DD55310011D9B9C483C6C451AB7552BC4E45B24189CB89B40F24C74CD884F755894AAB7325388DA4C7794AA638591797299F853BF0CB46F6387EDB51E790EF94
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/graphics/cumulative-map-small.png
Preview:	.PNG.....IHDR...(...s.....N.-.. .IDATx...|T...g..d.....!D$`.Yb.....R.Z/.Z.Uj..b...+-Z+.V..+m.Zl.t.*.. .l.U..% ..$!d_f....gf...D.....G23g.y....}..}.EUU..D".Ct.H$.pE..D".[.@I$..E..D".[.@I$..E..D".[.@I$..E..D".[..@y..p.YI6.E!v.d.8 >X.IEA...i....V.....^...h.Q..,*l.Zv.}....0[A.^...Zm...f...>...,)m.M..E.F.z7.d...%.6...d4n.y.....e...X..-.;.^....+.0.w...[...Yv.....l.....]q.o...I..5,. .d..6]..u.d~.}E....l.lc..!..l..8xn/.V.k.(...l.M6....>.b[...Z.....ju....FQ.i~hM.l.~..ly.k..`.>.]..J4.]......}..V.u...a3...2t.?a...G..8..d;[?+...mo>..y[\.....*.T%...6..e..xT.E..OW61.....=.Bwo-....G..r. ..~%Lz.E&...{...UE...{m$0...^/.....7%.V....d..\|.9.Q.....X..zS.....u>J.%..*j.^..>...7.i.G...0.....g2}.....5.6yJ..q.K....w....1....u.[..ES...rf~.@u\|.{.2.E.o{K.....vym...:n.y..@^..\|.X.... f.AC.....[u.....L.#....)..i.jJ+...n$^...w.H.>..#7..v.....*......./..G.3.L.?..tV=+W.....0,.G.....u>.5W^..~...y.q....o.....iL..m..1aB.V.n.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\ds[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 3
Category:	downloaded
Size (bytes):	41
Entropy (8bit):	3.4960271529727103
Encrypted:	false
SSDEEP:	3:CWoflBlll1nE:ow
MD5:	45FAFCED0B565CC5670032533B890B13
SHA1:	91CE14BEAE79694AC4E4BAA8961E92F8BA54A2CE
SHA-256:	7DF51310F47487A4B39B74D302FCDE64FE1AAFCA56299E3D05280965FC659C5F
SHA-512:	C083B8EFF67F31D5D8A77E522A1E04DE0AFED525F1FEBE53DF9B8F88E46741CD05235007143D43286003F25624E7DF45E866317D0EA8874F62912D6E16E5275E
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/ds.gif
Preview:	GIF89a.....@@@.....,.....DT.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\facebook-btn[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 42 x 42, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1051
Entropy (8bit):	7.784068898473082
Encrypted:	false
SSDEEP:	24:g5+eqQVZSnL0wOkwS9VmIAcIKSrT1lW2dsuL:g8nQswSi1cWT1tFL
MD5:	6248318A2E3768B22BC34535B7E4AEF1
SHA1:	FB41113AB2C8D731648039C78D9C956DC73C6B05
SHA-256:	7B7E5063A7E9A1A8ACC87AC9529D33A27EF1299E08FE7E792704F824E19C39B9
SHA-512:	D4E8F7B6CEF0B4624FC9A0EB6C9D5283702FB34EC9A8DF332D2C3818AFA50AADB3DD45E20014315882C2AEFE886395BB9E77A71ADDDA994517C4351D3E664(26
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/facebook-btn.png
Preview:	.PNG.....IHDR...*...*.....[....IDATX..]h.U...3.n..6.Y.M....[,)X...}.*.R.,.(.... ..*R....I@..>X..Z...M...i.n.~dC.6.f..n.cf|..v.3....L...;..9?.=....E$..... ..@._..]..r...~.#.h^*.W.>7r"..*...xo .h$.+fv9GfA.X..w....]....UF...$I...1.+....Y..]..rGw.CO<Mb F...}..O.....&....@.a4..fuE&y...ZB.%_@.y..3<....{.J.....2..-.#.H..$..!...W[U[.4...D#ADi[;....n ..CR..,h{..9km..z...@.... ...#...d....}%.L.f.W:.....I.b.A_80.{.#<.;f.pi.7....".H.}.[9.G^{..o.^._@..O.6<.}.'Z..pV..J..../.;f.r.a..9...M..}~.G.:...J~.....&%....s.>.[L...m..Q..=.Q.!.nl.4.....'..m.....d:k..'.zJ]....~ #Rr..7|7._.:_....!v.....P.9...*..C}6Pk.F.9DTt..a9mOnl;D.5.Nrc..Z.j.....E..m.....W.%...Z6UM'.Z.k..tg..xO.....h.f{....[...ua...).^K....-..6.Pg.fp.....]..=a2.2J.....i.\....Y,...e..1..9.r ..Y.....nb F.v.y..;...u.W.ZfAf1=1.h..<....y..g....{6.....M.s.?.....}..w.....?.....l:.M...4p....ZA.(0..a.'waT.D...J..<p.H.WL.u.W1j.ku@..>.....b.M.....>.%..`.O.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32x32
Category:	downloaded
Size (bytes):	3638
Entropy (8bit):	6.009925075904024
Encrypted:	false
SSDEEP:	96:Ojt6bYY7X9x0wVjcyvpx4GW8oAnUyu5o:OobYY7P0wVI8xL/Uyu
MD5:	819BA8DE904F2B86056DCC32A92874A4
SHA1:	5128B5AC8EC1CE19E81A928A516FDEE3C1DDA332
SHA-256:	5762EB82D249E88BAE39E8B719EB5F577EEA6C611313332721D7D3079C1ABB7D
SHA-512:	30A17BD3631201641F5D4AC42B327E7A18114ECD8CF54E56768BC0EFEE31FD11856BDFE13464FD69FAD1312F9FD6749B7BC63CE5A7EDBA640EA7E670AFBD3E 60
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico

IE Cache URL:	http://https://www.dhhs.nh.gov/favicon.ico

Preview:

.............h...&... ....(....... ....@..........................R...{....Is.B(B.....B}R.........{.s.s...kUc.)m...41.....1Ec.Ru{.........e..J.........)..AR.)}k.Z.k.J]R.....!}...U..c...Z...B]s.......
..B...),J.....9}..)01.JIc.)as..as.s.......9q{.R....u..k.s.Z....m{.!8Z.!Ms..<c.....!.{..Y..Rik.cq..9uc.{...........Ak.c...k.{.k...........u...e..Z.c.94J......().)ec.....!y......R.s.....s....M{.c...J.
..Juk.9}s..]..s...{....i..1u.............)AZ......Us.!]..k...c.c.R...Z....$1..M...Mk..]{.c.......{...c.s.Zys.J.{.............U{.!Ek.!U{.k...!ek.1Ys..u..)e......J]{.Jms.c...!,).....!<c..a...}..c.k.By..Zu......
........10J..Q{.)Ic..a...Y...Y{.)Qs.R...k...!.s.!i..s.s.)u..Ba{.R.k.................Y...e...i..JQc.)a{.)}s.........)u..1m..Z.k.s...s...............................Ik..Q{..]..!Qs.JEc..]{..q...e......c...Jqs.Z.
k.cu..c..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\footer_seal[1].gif

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 25 x 25
Category:	downloaded
Size (bytes):	936
Entropy (8bit):	7.566861187240718
Encrypted:	false
SSDEEP:	24:uDFM0rnx1/PBYjz8hxGmhKAKIqlIxL7Lqpg7NVzOQSAAo7fZv:uZMm1/PBYzgJ0AK9lenLqoNJpfzfV
MD5:	3EF0AE339337F22320D8CCAC504A8449
SHA1:	C747754A317B308869186DEBB10DDB77E756D7E5
SHA-256:	33A14A6CB3939700FE78DEAAFD649992667C7247A84639E627B7168902557367
SHA-512:	2D4B7D0FB58E8EB2A7AC364DACF57B2456317133CB3F24CBA9EFB005C9664486A63DE488326E0839FD5CBD04D3C22B53F02DCF81BD9D605806C647CFB9E324 C
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/footer_seal.gif

Preview:

GIF89a.......x-..7..B..S%|2..=..U..i..^).G*.G3.Q/.Z .d..]..@.=.NX!Bn-6x93.M%.YWJ.D.H#.X'.N-.gH.p..............s]'>.Nw.{p.p......n^.aq.u.e.W5.._..x............r.S=.b..............
[{]m4=..........]..........x..p.s@......8.zP..{.i8.s.].{t..s\V`]Vm..t..^NVzyt...[.zo...".pQN.3.w...~..m$.i..!..0..*..>..._gm;...s..T..M..>..{5VsI.n...G.8.[}~O...a...}[f..lu]{..agJ.k]Tqmu48
...!.......,.. !."....."..# $%&'&()*+,......-../.'0.01/234......566.77'8N..q#...x`p..B..,B.P.....8~.......x..... %ll..c..!..l.A$..]...*."..F.
q....v6.,x0.....x(Y....%C..i"DH.'1d<.2.@......"...*U...R.K.,Z.......P.PP.2.K....tQ@c..,X. ..*..0a..C.L.1\Bs1C$...(<.j...0i..Q#f..6m.q......]x....3n..Y.|N..t.P`0`. ..$8h.a..1......;g.Ph.J..
......"E.=[.........4...P.G.Q.A..]D...|......`......R..|.....W...X....HP`."H`...<....\."...A...4@....R...$.$..D....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\gcd-seal[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 180x64, frames 3
Category:	downloaded
Size (bytes):	4342
Entropy (8bit):	7.896707732925293
Encrypted:	false
SSDEEP:	96:dXLzANaWDn78v5e76bppPbea/wjGn36TBY9P3rBU:tLsNdn7K5i6bTfB3QBe3rBU
MD5:	07C2F782572AD5329109465D24EBD913
SHA1:	225F2226243AFFAF4BD532E5F648B2EFB7FA5ACF
SHA-256:	395DD501874DA9003C8A81010C9F8ABF42EAA7E4BE9BFB2012292777B6C088DD
SHA-512:	E29FD2215EDA48B98A8E9B6E8C4A775C2C21B17C056A078AB03B1C5F17B3C742DD91CDABFE06E314A5E0B2C181F5D883F9393BA25CC2C59E6C27BA99ED95E 8E
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/dcbcs/bds/graphics/gcd-seal.jpg

Preview:

......JFIF.....H.H.....C..""""""""""""...C...............   !   !!!   !!!!!!!!"""""""""""""""""""......@...O............................
!1."A.27QRaqt..#35Br......$4Usu.....Vb.......6CT................................(.......................1A...!Q2BRa."............?..m.o.'.Sa..}bkj..5.[i.M..RUT^......2................=.9..-7...y.....=...].T..
......Se..D$.u..Rv....}.T....fZ.........*..x.J...GM......o....+v\....`5.vs..jo.............<d.3..#..f...b.I.g..Kmj.)jD.DT..X.r.M...s..NQi..U...V...=.9..57...y..=6s...i..e..x.fJ..Ij&k..3Z.f.=.#~..DpS.
.tU3.1..Jg.VQ...q.n.v.v.x/W.bx...tbg.['J*2.....kX...o...T|I~^..............\m@I{.V..k..W.w.'d.......{;v!J..:.2...t.E...pUN)..<8<....q(..._.....g......A..X....QJ#.&D.rpT{/.|X...f%:.Y...lx@...
O.;..tZ..+.Xf.Z#3a.I..H.p...]%t.`...f..g..........v.B.T..X..0..7...$[.K..'.&.'C........|...%Z...@`..}./.'.=..f...\.LUP._...|..y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\icon-fb-like[1].gif

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 42 x 20
Category:	downloaded
Size (bytes):	1461
Entropy (8bit):	7.587767048114994
Encrypted:	false
SSDEEP:	24:R/MmkxSj6vKf4EQtdZ2VWN3+Qj5dejWfSZgDBsWgLhNk7pavk9HzU49t9iIo/E+n:cSjfytOVi++GC9CDLhNigigIo/31
MD5:	E8DFCB236B83526AF6EB96348B06F0C9
SHA1:	B741A536E0D2AE5C828D55DED39E17A60D5E1FA3
SHA-256:	614EB76A4DD29D91EA72883E702C609CE3E2AE3E12C2E5F96B2FCD32AA87860D
SHA-512:	4A64AB2C2A3B3705CB93D80ADF95A96EA5E257166C979972320884BA1105EFF25F1CD6FA15CBAAC7D31240F2FF09A5BCA8B93F6B5527F63D7631D9BF915194F
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/icon-fb-like.gif

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\icon-fb-like[1].gif	
Preview:	GIF89a*.....v.....u.....n.....r..r.....q..h~.....x..... .....x.....~.....q.....y.....s.....|.....Uo.....y.....|..... .....k.....s.....w.....!.....,....*.....}J.....OB.X.....#J..(.?. .Zh....-6zl,.%..(S.,w..?,....I.J..!l..7c...@.....D.I;i.!".c8.J.Ju.~BX$..oG.g!\T.K.*..S.....d...Z..Y.3.p.....<i.).M#9.`.Y..}5h..`....l.4...nk.5...)".<.`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\icon-sp[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 19 x 29
Category:	downloaded
Size (bytes):	62
Entropy (8bit):	4.478946144941852
Encrypted:	false
SSDEEP:	3:Cq//RewltxIu3uXU1xn:T2KU1xn
MD5:	BE84D93A3126CAFBBA9E92D25F139F7B
SHA1:	55F18DA72A71AC3F4CF7B4A6FB3053ED0169FFA1
SHA-256:	B264D426F9B80C2C02B49123C628B62AC446AAEAD5F4874780F900AB024228AA
SHA-512:	98089AA6627FFEA2E2B302B1E5B29CB8B64518183D124B66FA731A1B9B40D771C4E5882E3B7350AE547AAA6EF73BF55E32BED5CB3738464FDC2E88220FB36DB 7
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/icon-sp.gif
Preview:	GIF89a.....!.....,.....Hn..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\icon_pdf[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded
Size (bytes):	603
Entropy (8bit):	6.298893633281494
Encrypted:	false
SSDEEP:	12:U6LzEJau3+MTkA0iZzRnwAjM3s9RR0KoRxW:U6SLbh9HAsaK0xW
MD5:	47FD53FA9278B645A64B42C31F0A7068
SHA1:	E4293C1BA08413FBCCCA5CC67733F2A972A31869
SHA-256:	72293FE33F7F462A579E0297AB625D20AA53470ABF7A77B5E0AE5112FADA4F4C
SHA-512:	92D277ABA7A5B8F8BCEE6285285B055C5E1CD7125651EDEBF33955665B5483E6FF4A481A312A57CDFF438D78AC8964CE8B895FF273CA7DE281652B5AD645D24 4
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/icon_pdf.gif
Preview:	GIF89a.....U.....^S.....e].....8-....le.nf.|v.z.....t....UL.i`.....vi....UO.....h].UP.....um..j`.....qm.x.....B=.....PF.yr.}w...s.vl. .....!.....U.,.....UU0SR.....SPQT..P+..RQ.=8..."T,@.URT.N(....T..)....-!...*.TR.TQ$ 6QP.A....T2O....1.TB.9.....7. '.T.....E&5%..J.K.P.L.M>G?C..t..5..$..D.0....2` b.....A..GI..,...)..,@.R.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\iconseal[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 25 x 25
Category:	downloaded
Size (bytes):	936
Entropy (8bit):	7.566861187240718
Encrypted:	false
SSDEEP:	24:uDFM0rnx1/PBYjz8hxGmhKAKIqIlxL7Lqpg7NVzOQSAAo7fZv:uZMm1/PBYzgJ0AK9lenLqoNJpfzfV
MD5:	3EF0AE339337F22320D8CCAC504A8449
SHA1:	C747754A317B308869186DEBB10DDB77E756D7E5
SHA-256:	33A14A6CB3939700FE78DEAAFD649992667C7247A84639E627B7168902557367
SHA-512:	2D4B7D0FB58E8EB2A7AC364DACF57B2456317133CB3F24CBA9EFB005C9664486A63DE488326E0839FD5CBD04D3C22B53F02DCF81BD9D605806C647CFB9E324 C
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/iconseal.gif
Preview:	GIF89a.....x-..7..B..S%|2..=..U..i..^).G*.G3.Q/.Z .d..]..@.=.NX!Bn-6x93.M%.YWJ.D.H#.X'.N-.gH.p.....s]'>.Nw.{p.p.....n^.aq.u.e.W5.._..x.....r.S=.b..... [{]m4=.....]....x..p.s@.....8.zP..{.i8.s.].{t..s\V`]Vm..t..^NVzyt...[.zo...".pQN.3.w...~..m$.i..!..0..*..>..._gm;...s..T..M..>..{5VsI.n...G.8.[}~O...a...}[f..lu]{..agJ.k]Tqmu48 ...!.....,..... !."....."..# $%&'&()*+,.....-../.'0.01/234.....566.77'8N..q#...x`p..B..,B.P.....8~.....x..... %ll..c..!..I.A$..]...*."..F. q....v6.,x0.....x(Y....%C..i"DH.'1d<.2.@....."...*U...R.K.,Z.....P.PP.2.K....tQ@c..,X. ..*..0a..C.L.1\Bs1C$...(<.j...0i..Q#f..6m.q.....]x....3n..Y.|N..t.P`0`. ..$8h.a..1.....;g.Ph.J.. ....."E.=[.....4...P.G.Q.A..]D...\|.....`.....R..\|.....W...X....HP`."H`...<....\."...A...4@....R...$.$..D....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\index[1].htm	
Category:	downloaded
Size (bytes):	11358
Entropy (8bit):	5.081230966440111
Encrypted:	false
SSDEEP:	96:1AAl6lD3R0m3BGTvVrGNI643LJ7jIWqqyapxC8bB4/fxvLLmyySbxo93ILPlUIiK:SaMR0m3mz9oRHa9R54uEBukeX2oK
MD5:	7FAC353FD6E72A2C75820F2276D522D5
SHA1:	DEEC13C8F8CFB6A44E92FE15A5BBB4D18D1EB539
SHA-256:	B8FF55F1551A2611F3890196A3E6EA69D579D2DF441AA6AD6141F84F39511238
SHA-512:	CFF7AEA083A5B873FEB9F8D122BF4C02705FF7FE21135F7D13AAE5AC79A57879E2F56F07A22D5938B8B2C12B6B504E2381A5789347D5F5C2677837C802F1DE81
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/about/index.htm
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml"> InstanceBegin template="/Templates/main.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />.. InstanceBeginEditable name="doctitle" -->..<title>About Us | New Hampshire Department of Health and Human Services</title>..<meta name="Description" content="The New Hampshire Department of Health and Human Services is the largest agency in New Hampshire state government, responsible for the health, safety and well being of the citizens of New Hampshire." />..<meta name="Keywords" content="about, health, human, services, dhhs, new, hampshire, nh, nh medicaid, tanf, child care, substance abuse, wic, child support, food stamps" />.. InstanceEndEditable --> InstanceBeginEditable name="head" --> InstanceEndEditable -->..<link href="../css/base.css" rel="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mental-health[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 515x250, frames 3
Category:	downloaded
Size (bytes):	33303
Entropy (8bit):	7.974316717561031
Encrypted:	false
SSDEEP:	768:0Oqj4xMlnGpUqpxt29uVPD/4M7DWXM5Vz2fWQhVhz:a4elnGLtCy/3OXeqvz
MD5:	96D4920CFCAF9ABFDCAA8522656A3137
SHA1:	7B2B2F6ED65D0F633DE370711A2F762D18D9AE59
SHA-256:	18F1A2D6CB258D5F92E9EC463EC03D785EBDAC35A24A63B213FAB634871D7570
SHA-512:	E4A4DFB75D01B676383026B81A826C90CAE51AAF64257FC12093A806FAB2D96531A4126537F35B13503B349C312BFCC4B7A9164D99260972343C5FAD0C24E016
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/mental-health.jpg
Preview:	......Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164360, 2020/02/13-01:07:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:64228f6a-a50e-46b2-b829-8abc1f531c88" xmpMM:DocumentID="xmp.did:5636845C1E1011EB8809AFE341815D76" xmpMM:InstanceID="xmp.iid:5636845B1E1011EB8809AFE341815D76" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:aa4471f1-b7a0-ed43-97bc-895485e21ba5" stRef:documentID="adobe:docid:photoshop:db8248d2-086c-6a48-94d3-0a1aa0928de9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\pdf-icon[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded
Size (bytes):	1302
Entropy (8bit):	6.880653223666133
Encrypted:	false
SSDEEP:	24:8Sal1he91WwylZ82lYSqMHY1yVUNT3byJvGY8Rov+P:iqQinNuWy6NKJvL8yv+P
MD5:	0E58756A31693898401D549A6FD8747F
SHA1:	6AE148BAE1D9B4EA9CF8353B5A563FD96C2DB62F
SHA-256:	733985E128D61935A5CBFC671CB6A8A055952FFF6503A69DE543BF98F980DF2A
SHA-512:	87F4FBEE7AE08899B26BED3EEC36E72B205BA5A69AC2E90CB93F25CAF63641A4625E2E836970C8DC5491D67082374F747BAD8ACC38A34C29416F540930C68E8F
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/graphics/pdf-icon.gif
Preview:	GIF89a..... .MMh..y.....s...88.....>>i...UU...!..XMP DataXMP<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:9570A76A214211E39888F760BBA09AA4" xmpMM:InstanceID="xmp.iid:9570A769214211E39888F760BBA09AA4" xmp:CreatorTool="Adobe Photoshop CS3 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:C792EF2B1576E2119B42C2924AD253AB" stRef:documentID="uuid:D01E3487E275E2119B42C2924AD253AB"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\school-safety[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 49, 8-bit/color RGBA, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\school-safety[1].png	
Size (bytes):	10253
Entropy (8bit):	7.972468978592324
Encrypted:	false
SSDEEP:	192:eMFTvtFRw3WygedNX9P9+5z51HN4dil0c7aQWIAhCRdBnthIsTb4BVsECF7:1FLtPYWwHW9HmtaQnAhavzIsb44Ei
MD5:	4E5DEEFA8F279F99BB93C9EBECFC7B11
SHA1:	C335E28675D5623D124DB3C6874E09DFCA2E4C0F
SHA-256:	51A3393B9B1D0D215CBE3AECC4B772679AFF02C9581B07DF09035B1D0AA2C651
SHA-512:	627CE68930400103E8D3DFBB0FF91F504609442192732D431AB98DF9815B478D8EDB2C2F313F89F8009FC5915F8B4F279DA25D1AA3B43B9907C8263A8C200DA5
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/school-safety.png
Preview:	.PNG.....IHDR.....1.....8.P... .IDATx...t.....[..M6.C.$!!...z...W..\E...6@..''\EE..A.I.{EE....B.5$..4.7.lv.;3.....?gI.y.>...f..B..C...Sy...Z...../.$.....@dpH.4....@V&....Oww.z7lv;.CVZ ....~...+(.... ..!.G.%....'.....P..Z..q.n^].1#z.....4....&...3}.G.....).0.L..EX..<4.5^.?.....f.s..\|.....j !2.....3.Gi...<G.W+.{...h...D%1y.<.>.,l#.....q..c... ..2..:...w.u{...,.6:%4.K#QT^.I..... <..>..q1.]....s2/...D..r.l.....e+.....l....._..FL`.-''.o.g...EK.....P:'.....OO.<...R.$.V...H;|.C9g..5....8x.....kF\hXm.2.....9!.~.i'r..s.3...P{'';.....Mq..F.k.[XZ.....'.ss.P^V..l.@AE9 ..cp.....M{....G..I....i.^.|..\..9..l=....@.&.@..8.q.Oo/.B`.....DbLlm..Y..9u.....T..x....,^....:.Mu...C...CG.[.....=i...;M.....1#..{.[n.C...ae%..M.h.-....~.V.}.....}+ArsAT.@.H..[.....;{.zn1. ..V.V...,Hi-..:Rg.}.yP`D<.....o..../.7.....q.b....M_. .K...:.....(..V.....K..''N.6....E.....E.. .R.....D..J...c. ''H...)...;.;...F..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\seniors[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	13573
Entropy (8bit):	4.988504258614964
Encrypted:	false
SSDEEP:	96:1AAN6R0m3BGTvVrGNI643LJ7DoWK3aS6pxVHbh4DfxvLLmyySOLrgneinOI6VHtt:SnR0m3mz8Y8RH+/EUh1ymGDb242oK
MD5:	884814DBA14EF841EC18FADE7145DDF7
SHA1:	F8B9924FD70BA0B42959DF852C0FDB2F6B6980B3
SHA-256:	D2A61C184CC788FC32DCE676C1E0D8FB6DE2EA465981069C875E50A60812EA76
SHA-512:	584E41FDC4A54866B919A5802A19632C6CA36B108C86C5F93043B4456CD43AAA3BA9EF2581712D4FD76B672BE3593D556836361227E3A75ECFBC58C37D85AFF
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/foryou/seniors.htm
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml"> InstanceBegin template="/Templates/main.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />.. InstanceBeginEditable name="doctitle" -->..<title>Services for Seniors | New Hampshire Department of Health and Human Services</title>..<meta name="Description" content="DHHS services for seniors." />..<meta name="Keywords" content="seniors, elderly, health, human, services, dhhs, new, hampshire, nh" />.. InstanceEndEdit able --> InstanceBeginEditable name="head" -->.. InstanceEndEditable -->..<link href="../css/base.css" rel="stylesheet" type="text/css" />..<link href="../css/contrib ute.css" rel="stylesheet" type="text/css" />..<link href="../css/print.css" rel="stylesheet" type="text/css" media="print" />..<script type="text/javascript" src="../scri

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\smallA[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 13
Category:	downloaded
Size (bytes):	185
Entropy (8bit):	6.185375227859527
Encrypted:	false
SSDEEP:	3:CxatOa/FA2P/OOlllMJRfyazQy38lDKKNkaaaRrExZd/7S17/Johi13sdvaDw3rR:ZtOW/OKQRfyyYDK18pExZde17Bohi9s9
MD5:	6F8CB4A1EFB4DF5320B6E70E53577E59
SHA1:	22845864135E6938A5DD1B7CE5C7AA44624F1318
SHA-256:	0C45128E99EE08762E4CBB4333C5FFB0C95149B8C3BCCED7A84FB37423CE8C33
SHA-512:	BAADE3D47511B8FC9BFE0EAB9C60AAF9104749544B7A24C7A8BE076B1F3F4DD4C2CDAF9902E8C096907CED9B7FDA11CABF6951A45BB758947DFD429498A94 BE7
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/css/graphics/smallA.gif
Preview:	GIF89a.....999.....vvv...SSS.....cccllll.....UUU.....BBBWWW.....<<<???...!.....,.....6.'.di.h..$...7.A\...&.....XA''.I...T,..&..hD.N.#.y....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\teens[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	12135
Entropy (8bit):	5.0121308162835
Encrypted:	false
SSDEEP:	96:1AA1GR0m3BGTvVrGNI643LJ7DoWK3aS6pxVHbh4DfxvLLmyySCM5hlAea2c9Wcy0:SLR0m3mz8Y8RHNvkth62oK
MD5:	2705710F50F1FCD80BBE013CFAF39709
SHA1:	31A4D90A2A00B3C49F16FB0997601E47C2B53E01
SHA-256:	7DDE0955645983167AD367FA1C4997027D8DC8743E7DD25556DFAB48C8FF680F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\teens[1].htm	
SHA-512:	6A108689C5B6C5A1295BCFA241E49A0801493D57A76CFA9DF08B2D6C15C91DE97AFE0FB1F65C0EF002C54ADDC126F1529066FCDDAF85E8623BFCBA290CADCA5
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/foryou/teens.htm
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml"> InstanceBegin template="/Templates/main.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />.. InstanceBeginEditable name="doctitle" -->..<title>Services for Teens | New Hampshire Department of Health and Human Services</title>..<meta name="Description" content="DHHS services for teens." />..<meta name="Keywords" content="teen, health, human, services, dhhs, new, hampshire, nh" />.. InstanceEndEditable --> InstanceBeginEditable name="head" -->..... InstanceEndEditable -->..<link href="../css/base.css" rel="stylesheet" type="text/css" />..<link href="../css/contribute.css" rel="stylesheet" type="text/css" />..<link href="../css/print.css" rel="stylesheet" type="text/css" media="print" />..<script type="text/javascript" src="../scripts/textsize

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\textsizer2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	9400
Entropy (8bit):	5.085927853718149
Encrypted:	false
SSDEEP:	192:0VKJv9DBzBv6YMTFQOln1aCj9ZWL270OLyodQXtK2PYvC8RrR0Y3UpHqsh:0VKJlDlV6YMxhEKbOEyodQXtK8n
MD5:	FA5AFDC96A59C9AA5A98DF57BC45A39F
SHA1:	5E596B4E91600A002A11F7CA90B8D55CC9FBE0DA
SHA-256:	656F1D9D07AAB96BAD6BF14A06A823837AD32C79F94B4082AE01221E233B26BD
SHA-512:	1D059FB79C04E90F56B1309C92500EEEF1922683BE8334F7A9F4DEE6A8978F6E61F59CCD457CB90180054374C449FFF453F1A9864F9BC75F2953DDDDFD573B8A
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/scripts/textsizer2.js
Preview:	// JavaScript Document..../* ..** ----------..** text sizer State of NH, Web Services Division..** created: 02 Nov 2010..** ---------- /..../* ..** ********** ..** BEGIN user-variable section..** DO NOT change code outside of this section..** ********** ********** ..*/..../// Specify stylesheet elements to exclude from resizing..// these should be identical to the individual elements specified in the styleshee t..// ie., classes should be '.classname', id's '#idname', tags, such as div 'div'..// Note: if an element in the exclude list appears anywhere in a stylesheet definition ..// the entire defition exluded; ..// Example, excluding tag 'div' means the following stylesheet definition ..// would be excluded from resizing: body, div, p {font-size: 20px;} ..// ..var arrExcludeStyleSheetElements = new Array('.search

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\textsizer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	5219
Entropy (8bit):	5.046059813833912
Encrypted:	false
SSDEEP:	96:8IRZqnvtiIkyEwmNeYMvAxerL5J6B82o231/BgYrCDgZrSvJLj0zE3bdCAHEsh:8IRZsv0E5mNofr6rF3Ra8CpR0Y34AHE2
MD5:	62BC4FEA155137DB1B998918DD1E30BF
SHA1:	D91108573500AD5AF21159209A97A4C097B43737
SHA-256:	6C4417DE30F53EB52ED26D95EB080F7A14F9F3DA1E522901443A8EAC5B3A8F0D
SHA-512:	1F714211545A997C483622B23D54AC2BD8AFEF12223ACBD5DF9427D860DDAD9C82A8EECC9BF4E59539F66A76C6005FD673F17EA8E006C2C1D27743387AEFE26
Malicious:	false
IE Cache URL:	http://https://www.dhhs.nh.gov/scripts/textsizer.js
Preview:	/*----------...Document Text Sizer- Copyright 2003 - Taewook Kang. All rights reserved....Coded by: Taewook Kang (txkang.REMOVETHIS@hotmail.com)...Web Site: http://txkang.com...Script featured on Dynamic Drive (http://www.dynamicdrive.com)......Please retain this copyright notice in the script....License is granted to user to reuse this code on ...their own website if, and only if, ...this entire copyright notice is included...----------*/..//Specify affected tags. Add or remove from list:..var arrTags = new Array('table','span','div','class','td','tr','a','p','h1');..../Specify spectrum of different font sizes:..var arrSizes = new Array('8pt','10pt','12pt','14pt','16pt');..../ global cookie name..var strCookieName = new String("SIZEPREF");..../********* begin functions section *********/..../ this function just calls the regular one without any fuss, did this so can customize

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\1095b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 515x250, frames 3
Category:	downloaded
Size (bytes):	38861
Entropy (8bit):	7.965890707861492
Encrypted:	false
SSDEEP:	768:0E0ydRJvF/yLfSRIrdGXij8NNLSwfNM5YFv1eMa:Xja2pSjGZHfG29a
MD5:	0EE5FD39F46045C84BB6EBECBF8035D6
SHA1:	8BC1DEF29E22D9F2480272E0948644564F6480F9
SHA-256:	79B552F5C7B43E7184AE479DE4E41DFDF311D326400FAC2AA60A895C02C0E3E9
SHA-512:	9E431D5D89D3B7966838A0F9BE231400B0DA798B7600C83D09C9923607C029B00C04F51523BCAD5BDD304A048409B8E473C4A3AE51B0671968E933CC1A0AA0E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\1095b[1].jpg	
IE Cache URL:	http://https://www.dhhs.nh.gov/graphics/slider/1095b.jpg
Preview:	......Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164360, 2020/02/13-01:07:22 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:64228f6a-a50e-46b2-b829-8abc1f531c88" xmpMM:DocumentID="xmp.did:8BB39165601311EB89E3DE696AE0C59F" xmpMM:InstanceID="xmp.iid:8BB39164601311EB89E3DE696AE0C59F" xmp:CreatorTool="Adobe Photoshop CS5 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:6558f1de-c874-3144-b2b8-91ae52843863" stRef:documentID="adobe:docid:photoshop:db8248d2-086c-6a48-94d3-0a1aa0928de9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\a-med[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 13, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1101
Entropy (8bit):	6.1898529070992145
Encrypted:	false
SSDEEP:	24:UKr1he91WwylZ82lYSqMHYmV0+T3byJCpkrsGp+qqxk:dqQinNuLu+KJpQiq+
MD5:	2198620B55C9E0808BD423C218843660
SHA1:	B1976497D135C384A95412550A6579FF96459935
SHA-256:	5E51CC6743CA4A799CF3C90E5B39563AFEFBA89216DB4937CA127068E6260810
SHA-512:	631A13D759EBB57E77F4053B70338E299B0F513F9E9EC0E7ACCED6614CFB9BD8393297307B4615E0E71E679C25E6AA747122A77DAD997AD917A62D879043EB2
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/a-med.png
Preview:	.PNG.....IHDR.....$....tEXtSoftware.Adobe ImageReadyq.e<...iiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:53E95500C81811E4A644EEFA9DDD0BCD" xmpMM:InstanceID="xmp.iid:53E954FFC81811E4A644EEFA9DDD0BCD" xmp:CreatorTool="Adobe Photoshop CS3 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:7392920C0151DE118F1C842F631D718C" stRef:documentID="uuid:156814919CEBDC11A2CFD38C7E53D8A9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>..OQ...zIDATx.b...?.%...B@.U@.r.n.*@^.....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\a-small[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 13, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1119
Entropy (8bit):	6.171306254385598
Encrypted:	false
SSDEEP:	24:UKr1he91WwylZ82lYSqMHYjAQqV1Q+T3byJCpkrsG5vlM94b9:dqQinNu3zTDKJpQl94b9
MD5:	185F7A43C690C8A0D73568B61A751161
SHA1:	FB523EDD5FB90035890C85AE341A6F1661410D97
SHA-256:	F8A7A8A27A10AAB2211459D24E83D801F3FE140D898E47417A85E00A8E3DA5B0
SHA-512:	8EA917CEFE5ACAA3C1C0F8406AA2748130C8F6EA02B1AC850CDED26CE7785A84860036FE35BE54359CCE0E47440D76CEFBD4F87914FB2F14FDD10D8E2664D32
Malicious:	false
IE Cache URL:	http://https://www.nh.gov/covid19/css/graphics/a-small.png
Preview:	.PNG.....IHDR.....$....tEXtSoftware.Adobe ImageReadyq.e<...iiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:69539324C81811E49A758A5BB4F8D573" xmpMM:InstanceID="xmp.iid:69539323C81811E49A758A5BB4F8D573" xmp:CreatorTool="Adobe Photoshop CS3 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:7392920C0151DE118F1C842F631D718C" stRef:documentID="uuid:156814919CEBDC11A2CFD38C7E53D8A9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....IDATx.b...?.%...B@..,x...../.....8.... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\adults[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	12691
Entropy (8bit):	5.051305468378174
Encrypted:	false
SSDEEP:	96:1AAzGR0m3BGTvVrGNI643LJ7DoWK3aS6pxVHbh4DfxvLLmyyS4MRc/jl0Meqm7mM:S/R0m3mz8Y8RHvksqjBT3T2oK
MD5:	85B0F79695E7ED054B29DB8302CA25D5
SHA1:	658F62645B373DFDBEC811C65C03EC4C86251468
SHA-256:	191244EEE601C101C32E698C4D89F0AF93254DD857A98C205EC63F68985FEEA1
SHA-512:	EE9AC9A00284C15B5983E0E47FAB8095D6F085E24A47CAFE1F0C6DC9C6094CE80681976B4A707522254FB1FAE8B7946F4D14B7AA4EC45351AB98BE1D36F73FA3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\adults[1].htm	
IE Cache URL:	http://https://www.dhhs.nh.gov/foryou/adults.htm
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml"> InstanceBegin template="/Templates/main.dwt" codeOutsideHTMLIsLocked="false" -->..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />.. InstanceBeginEditable name="doctitle" -->..<title>Services for Adults | New Hampshire Department of Health and Human Services</title>..<meta name="Description" content="DHHS services for adults." />..<meta name="Keywords" content="adult, health, human, services, dhhs, new, hampshire, nh" />.. InstanceEndEditable --> InstanceBeginEditable name="head" -->..... InstanceEndEditable -->..<link href="../css/base.css" rel="stylesheet" type="text/css" />..<link href="../css/contribute.css" rel="stylesheet" type="text/css" />..<link href="../css/print.css" rel="stylesheet" type="text/css" media="print" />..<script type="text/javascript" src="../scripts/texts

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.5515864823583705
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	COVID19open_closedPodsVACCINE_LETTER2B.docx
File size:	22673
MD5:	e65769cca6ce8214adf674a8001d83b4
SHA1:	d3800da27e0aa660f04da269b5392fb3f4c26eb5
SHA256:	b0ecb837f4df662ff941ce2cdb64cea78b07c22b1e9ad0d328229aa9dd9f1996
SHA512:	4fb1b69222aa92bd97145eb707a9249ea97a9dfd535cb4adbd0b0debc6c5ca715534d1409db3046d922281187e76eb215e540141d2cbc7a2db444aa9150537a6
SSDEEP:	384:T18xovaJhkQ80FRJNtdpzUbXA530bw0uBGM/xhQl9lce0DIdPuO:BcMaJhkQ9T1eXwEbwZxhQlwe0kd/
File Content Preview:	PK.....!.i...o.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:22:12.025783062 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:12.026664972 CET	49724	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:12.174304008 CET	80	49723	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:12.174515963 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:12.175271034 CET	80	49724	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:12.175415993 CET	49724	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:12.611895084 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:12.764082909 CET	80	49723	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:12.764265060 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.104409933 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.252722979 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.252826929 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.263142109 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.415457964 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.415497065 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.415649891 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.415676117 CET	49725	443	192.168.2.5	199.192.8.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:22:13.415740013 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.653018951 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.661058903 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.807749033 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.807909966 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.823383093 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823434114 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823455095 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823474884 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823494911 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823512077 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:13.823714018 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.823772907 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:13.983458996 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.000679016 CET	49727	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.002768993 CET	49726	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.057692051 CET	49724	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.058132887 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.124123096 CET	49728	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.125866890 CET	49729	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.126341105 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.126430988 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127008915 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127039909 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127062082 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127079964 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127088070 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127113104 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127121925 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127134085 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127150059 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127187967 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127213001 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127314091 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127338886 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127362013 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127365112 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127399921 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127410889 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127424955 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127449989 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.127453089 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.127499104 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.128088951 CET	49730	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.145584106 CET	443	49726	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.145872116 CET	49726	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.147062063 CET	443	49727	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.147326946 CET	49727	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.199623108 CET	80	49724	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.199675083 CET	80	49723	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.199862003 CET	49724	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.199923038 CET	49723	80	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.270086050 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270126104 CET	443	49729	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270144939 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270308018 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.270359039 CET	49729	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.270360947 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.270649910 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270685911 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270708084 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270728111 CET	443	49725	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.270735979 CET	49725	443	192.168.2.5	199.192.8.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:22:14.270798922 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.271720886 CET	443	49728	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.271858931 CET	49728	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:14.276675940 CET	443	49730	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:14.276870966 CET	49730	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.399796009 CET	49730	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.400649071 CET	49727	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.401540041 CET	49728	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.403879881 CET	49729	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.405005932 CET	49726	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.407011986 CET	49731	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.407972097 CET	49732	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.433610916 CET	49725	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.541562080 CET	443	49730	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:15.541749001 CET	49730	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.542059898 CET	443	49729	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:15.542177916 CET	49729	443	192.168.2.5	199.192.8.2
Feb 16, 2021 16:22:15.543102026 CET	443	49727	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:15.543135881 CET	443	49726	199.192.8.2	192.168.2.5
Feb 16, 2021 16:22:15.543224096 CET	49727	443	192.168.2.5	199.192.8.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:21:28.131097078 CET	62060	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:28.180052996 CET	53	62060	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:28.544234991 CET	61805	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:28.592845917 CET	53	61805	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:28.710880041 CET	54795	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:28.759525061 CET	53	54795	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:28.892354965 CET	49557	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:28.941030979 CET	53	49557	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:29.845263004 CET	61733	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:29.893956900 CET	53	61733	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:30.836529970 CET	65447	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:30.888127089 CET	53	65447	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:31.821074009 CET	52441	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:31.854044914 CET	62176	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:31.869800091 CET	53	52441	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:31.913322926 CET	53	62176	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:33.086740017 CET	59596	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:33.138250113 CET	53	59596	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:34.419207096 CET	65296	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:34.470812082 CET	53	65296	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:35.419163942 CET	63183	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:35.478086948 CET	53	63183	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:36.419938087 CET	60151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:36.480293989 CET	53	60151	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:38.013650894 CET	56969	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:38.074920893 CET	53	56969	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:38.718040943 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:38.779277086 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:39.733527899 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:39.793543100 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:40.512177944 CET	54757	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:40.563683033 CET	53	54757	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:40.734600067 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:40.806994915 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:42.734707117 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:42.796477079 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:46.735449076 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:46.786978006 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 16:21:53.062922955 CET	49992	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:21:53.123383999 CET	53	49992	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:22:05.905042887 CET	60075	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:05.953649044 CET	53	60075	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:09.147198915 CET	55016	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:09.205722094 CET	53	55016	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:11.948128939 CET	64345	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:12.005139112 CET	53	64345	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:15.669120073 CET	57128	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:15.734307051 CET	53	57128	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:17.736448050 CET	54791	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:17.804577112 CET	53	54791	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:18.391002893 CET	50463	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:18.452732086 CET	53	50463	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:23.981286049 CET	50394	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:24.038399935 CET	53	50394	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:25.465296030 CET	58530	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:25.522521019 CET	53	58530	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:26.797080994 CET	53813	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:26.855427027 CET	53	53813	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:39.140122890 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:39.188878059 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:40.138379097 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:40.146007061 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:40.187081099 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:40.194535017 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:41.151881933 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:41.153476954 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:41.200995922 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:41.202064037 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:42.166739941 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:42.215450048 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:43.161668062 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:43.210333109 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:44.162380934 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:44.214438915 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:46.466605902 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:46.529272079 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:47.163561106 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:47.212179899 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 16:22:48.207211018 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:22:48.255954981 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:22.715972900 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:22.773077011 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:26.959098101 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:27.016474009 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:28.360130072 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:28.655316114 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:33.064213991 CET	60516	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:33.153119087 CET	53	60516	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:34.064987898 CET	51649	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:34.126828909 CET	53	51649	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:34.983330965 CET	65086	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:35.045672894 CET	53	65086	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:35.891943932 CET	56432	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:35.951744080 CET	53	56432	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:37.687438011 CET	52929	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:37.736282110 CET	53	52929	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:38.429588079 CET	64317	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:38.478140116 CET	53	64317	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:39.342247009 CET	61004	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:39.390860081 CET	53	61004	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:39.630076885 CET	56895	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:39.681757927 CET	53	56895	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:40.224020958 CET	62372	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:40.291549921 CET	53	62372	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 16:23:40.358491898 CET	61515	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:40.423881054 CET	53	61515	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:41.419723988 CET	56675	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:41.479847908 CET	53	56675	8.8.8.8	192.168.2.5
Feb 16, 2021 16:23:42.253778934 CET	57172	53	192.168.2.5	8.8.8.8
Feb 16, 2021 16:23:42.311949968 CET	53	57172	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 16:22:11.948128939 CET	192.168.2.5	8.8.8.8	0xfe31	Standard query (0)	www.dhhs.nh.gov	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:22.715972900 CET	192.168.2.5	8.8.8.8	0x8993	Standard query (0)	www.dhhs.nh.gov	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:26.959098101 CET	192.168.2.5	8.8.8.8	0x4606	Standard query (0)	www.nh.gov	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:28.360130072 CET	192.168.2.5	8.8.8.8	0x949b	Standard query (0)	www.app-support.nh.gov	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 16:22:12.005139112 CET	8.8.8.8	192.168.2.5	0xfe31	No error (0)	www.dhhs.nh.gov	www.dhhs.state.nh.us		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 16:22:12.005139112 CET	8.8.8.8	192.168.2.5	0xfe31	No error (0)	www.dhhs.state.nh.us		199.192.8.2	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:22.773077011 CET	8.8.8.8	192.168.2.5	0x8993	No error (0)	www.dhhs.nh.gov	www.dhhs.state.nh.us		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 16:23:22.773077011 CET	8.8.8.8	192.168.2.5	0x8993	No error (0)	www.dhhs.state.nh.us		199.192.8.2	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:27.016474009 CET	8.8.8.8	192.168.2.5	0x4606	No error (0)	www.nh.gov		199.192.8.2	A (IP address)	IN (0x0001)
Feb 16, 2021 16:23:28.655316114 CET	8.8.8.8	192.168.2.5	0x949b	No error (0)	www.app-support.nh.gov		199.192.8.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dhhs.nh.gov

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49723	199.192.8.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 16:22:12.611895084 CET	1266	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.dhhs.nh.gov Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 16:22:12.764082909 CET	1267	IN	HTTP/1.1 302 Found Date: Tue, 16 Feb 2021 15:22:12 GMT Server: Molly and John Location: https://www.dhhs.nh.gov/ Content-Length: 208 Content-Type: text/html; charset=iso-8859-1 Set-Cookie: priv=1p; path=/ Set-Cookie: pub=91; path=/ Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 68 68 73 2e 6e 68 2e 67 6f 76 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	199.192.8.2	80	192.168.2.5	49724	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 16:22:14.199623108 CET	1298	IN	HTTP/1.0 400 Bad request Cache-Control: no-cache Connection: close Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71 75 65 73 74 2e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><body> 400 Bad request Your browser sent an invalid request.</body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 16:22:13.415649891 CET	199.192.8.2	443	192.168.2.5	49725	CN=dhhs.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 17:39:02 CET 2019	Sat Mar 13 20:01:06 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:23.071377039 CET	199.192.8.2	443	192.168.2.5	49749	CN=dhhs.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 17:39:02 CET 2019	Sat Mar 13 20:01:06 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:27.320533037 CET	199.192.8.2	443	192.168.2.5	49750	CN=nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Jan 07 16:51:01 CET 2021	Thu Sep 09 14:46:05 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
							Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		

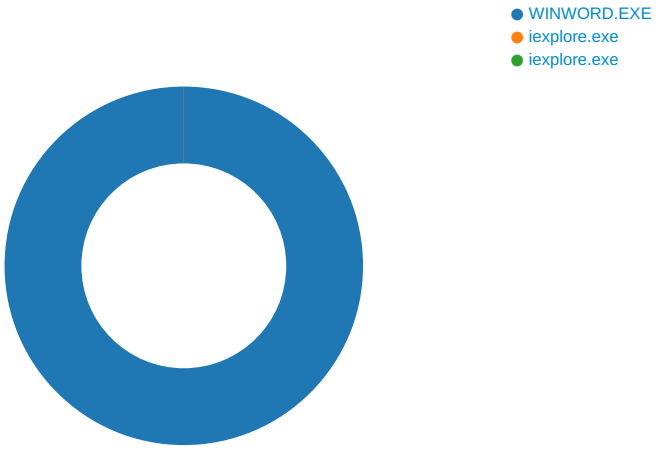
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Feb 16, 2021 16:23:27.322099924 CET	199.192.8.2	443	192.168.2.5	49751	CN=nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Jan 07 16:51:01 CET 2021 Wed Nov 21 01:00:00 CET 2018	Thu Sep 09 14:46:05 CEST 2021 Tue Nov 21 01:00:00 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Feb 16, 2021 16:23:28.950881958 CET	199.192.8.2	443	192.168.2.5	49760	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 16:41:10 CET 2019 Tue Aug 02 12:00:00 CEST 2011	Sat Mar 13 14:51:11 CET 2021 Tue Aug 02 12:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:28.951427937 CET	199.192.8.2	443	192.168.2.5	49761	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 16:41:10 CET 2019 Tue Aug 02 12:00:00 CEST 2011	Sat Mar 13 14:51:11 CET 2021 Tue Aug 02 12:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:28.952521086 CET	199.192.8.2	443	192.168.2.5	49762	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 16:41:10 CET 2019 Tue Aug 02 12:00:00 CEST 2011	Sat Mar 13 14:51:11 CET 2021 Tue Aug 02 12:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:28.959393978 CET	199.192.8.2	443	192.168.2.5	49764	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Jan 14 16:41:10 CET 2019 Tue Aug 02 12:00:00 CEST 2011	Sat Mar 13 14:51:11 CET 2021 Tue Aug 02 12:00:00 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 16:23:28.970336914 CET	199.192.8.2	443	192.168.2.5	49763	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	Mon Jan 14 16:41:10 CET 2019	Sat Mar 13 14:51:11 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:28.971134901 CET	199.192.8.2	443	192.168.2.5	49765	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	Mon Jan 14 16:41:10 CET 2019	Sat Mar 13 14:51:11 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:29.259805918 CET	199.192.8.2	443	192.168.2.5	49767	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	Mon Jan 14 16:41:10 CET 2019	Sat Mar 13 14:51:11 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		
Feb 16, 2021 16:23:29.261260033 CET	199.192.8.2	443	192.168.2.5	49766	CN=app-support.nh.gov, O=State of New Hampshire, L=Concord, ST=New Hampshire, C=US	CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	Mon Jan 14 16:41:10 CET 2019	Sat Mar 13 14:51:11 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Organization Validation CA - SHA256 - G2, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Aug 02 12:00:00 CEST 2011	Tue Aug 02 12:00:00 CEST 2022		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 6304 Parent PID: 792

General

Start time:	16:21:35
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0xfb0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6675977C	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\698A8F31.png	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66685805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9766F8FA-474A-4D26-9B90-1E4FEFAFF644}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66685805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$VID19open_closedPodsVACCINE_LETTER2B.docx	success or wait	1	66685805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\698A8F31.png	0	6897	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 25 00 00 01 27 01 03 00 00 00 d5 61 c7 3f 00 00 00 06 50 4c 54 45 00 00 00 ff ff ff a5 d9 9f dd 00 00 00 01 62 4b 47 44 00 88 05 1d 48 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 1a 84 49 44 41 54 68 81 7d 9a 7d 74 1b d7 75 e0 07 82 2c ca 5d db 50 d6 49 4d 37 12 47 f9 d8 ba 7b da 54 f2 f1 d6 24 4b 12 a3 8d bd b5 7b 76 bb ea 9e fe 93 f4 23 92 e2 34 6c b6 75 20 07 3e 02 61 7e 3c ca b4 45 7b fd 81 ec 71 1a 49 87 12 c7 e9 76 9b 9e dd a4 52 ca 6c 48 96 14 07 0c 12 c1 3e 16 39 da 3a 6b 8b 06 c9 01 0d 99 63 57 04 06 d0 48 98 19 ce 9b 77 f7 be 19 80 5f 92 33 47 07 14 30 bf 79 ef ce 7d f7 dd 77 ef 7d 4f 80 2d 17 15 84 d0 d6 df 6c e1 56 e8 56 ec 16 4a f0 af 86 5f 4e e5 05 c9 ff 24 bf	.PNG.....IHDR...%...'.....a.?....PLTE.....bKGD....H....pHYs.....+.....IDATh.}.}t..u....,].P.IM7.G...{.T...$K.....{v.....#..4l.u .>.a~<..E{...q.I....v....R.lH.....>.9.:k.....cW...H....w....._.3G..0.y..}..w.}O.-.....I.V.V..J..._N....$.	success or wait	1	66685805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9766F8FA-474A-4D26-9B90-1E4FEFAFF644}.tmp	unknown	2	08 00	..	success or wait	1	66685805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID19open_closedPodsVACCINE_LETTER2B.docx	5963	6897	success or wait	1	66685805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66698A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66698A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66698A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\247AE	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66685805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	66685805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI	binary	02 0B 05 02 04 02 04 02 02 03	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\247AE	247BE	binary	04 00 00 00 A0 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 A0 E7 F2 C2 04 D7 01 BE 47 02 00 AE 47 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	66685805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-02-16T16:22	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	66685805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1380974600	1380974601	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000000F01FEC\Usage	ProductFiles	dword	1380974601	1380974602	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	66685805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	66685805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\247AE	247BE	binary	04 00 00 00 A0 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00	04 00 00 00 A0 18 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00	success or wait	1	66685805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 A0 E7 F2 C2 04 D7 01 BE 47 02 00 AE 47 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BE 47 02 00 AE 47 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Analysis Process: iexplore.exe PID: 5696 Parent PID: 792

General

Start time:	16:22:07
Start date:	16/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff63cb80000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4368 Parent PID: 5696

General

Start time:	16:22:08
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5696 CREDAT:17410 /prefetch:2
Imagebase:	0x50000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly