ID: 386160
Sample Name: COVID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:36:14
Date: 13/04/2021
Version: 31.0.0 Emerald

Table of Contents

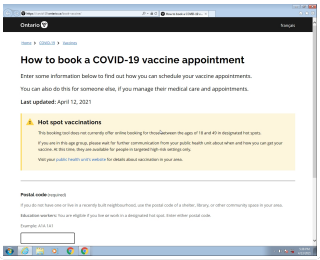
Analysis Report COVID-19 Vaccine Locations Booking S…

Overview

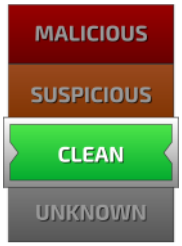
General Information

Sample Name:	COVID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx
Analysis ID:	386160
MD5:	14d9efc0e6bd70f..
SHA1:	a9d37cf22facbe7..
SHA256:	cbf87430a5ac83f..
Infos:	

Most interesting Screenshot:



Detection

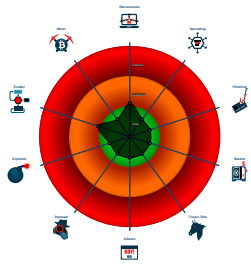


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- IP address seen in connection with o…
- 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 w7x64**
- WINWORD.EXE (PID: 1796 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- iexplore.exe (PID: 2616 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2728 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2616 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

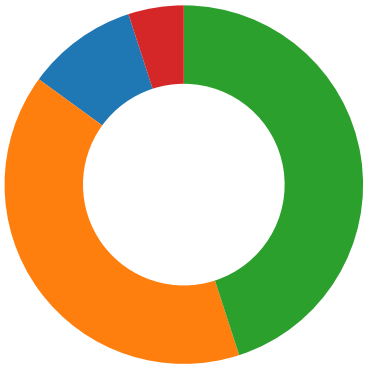
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

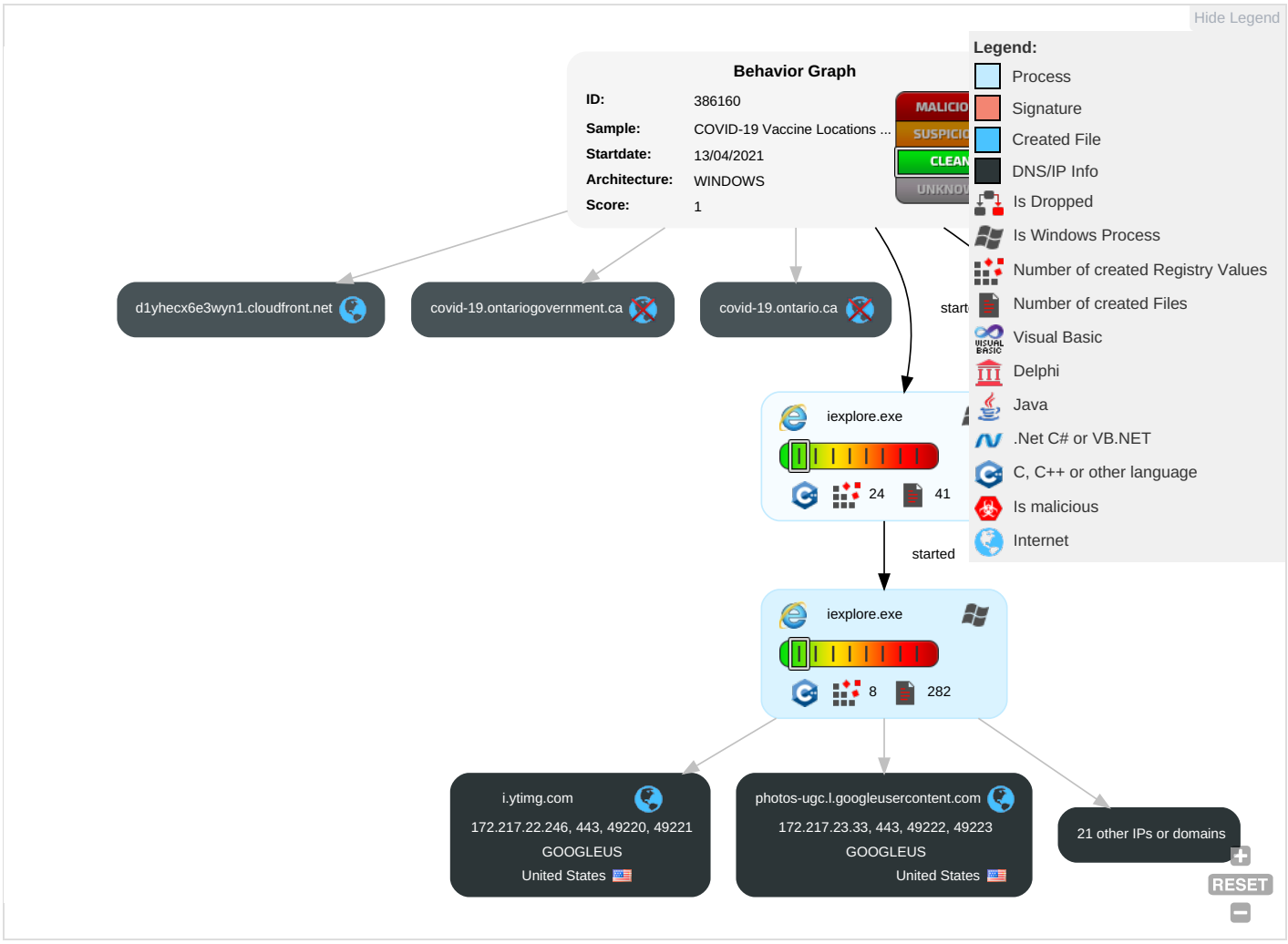
Click to jump to signature section

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

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	Impa
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 Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	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		Carri Billin Fraud

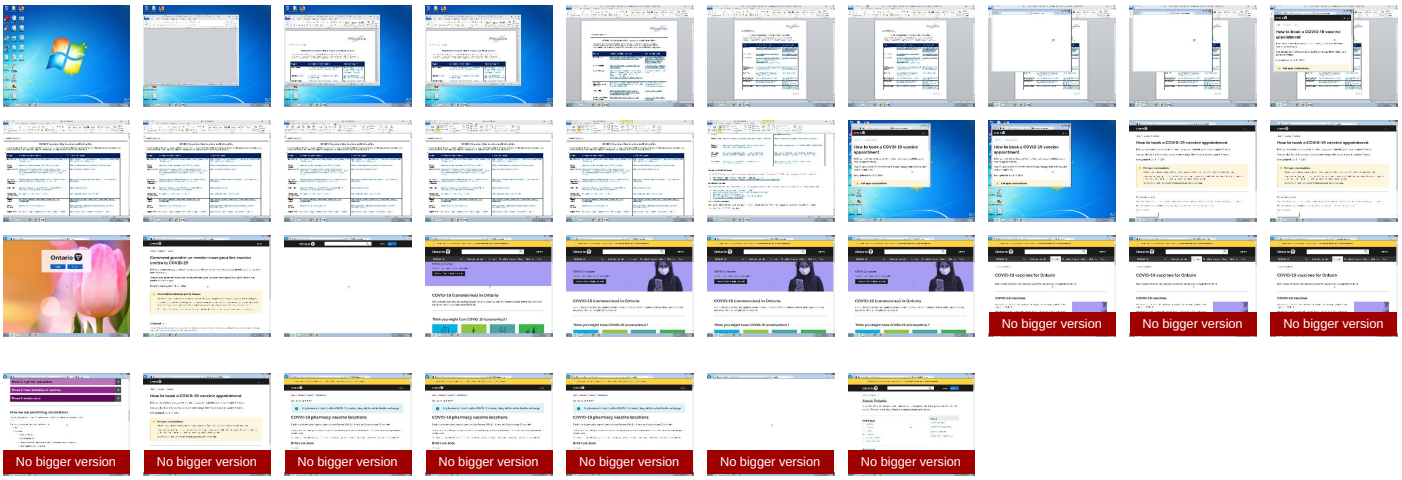
Behavior Graph

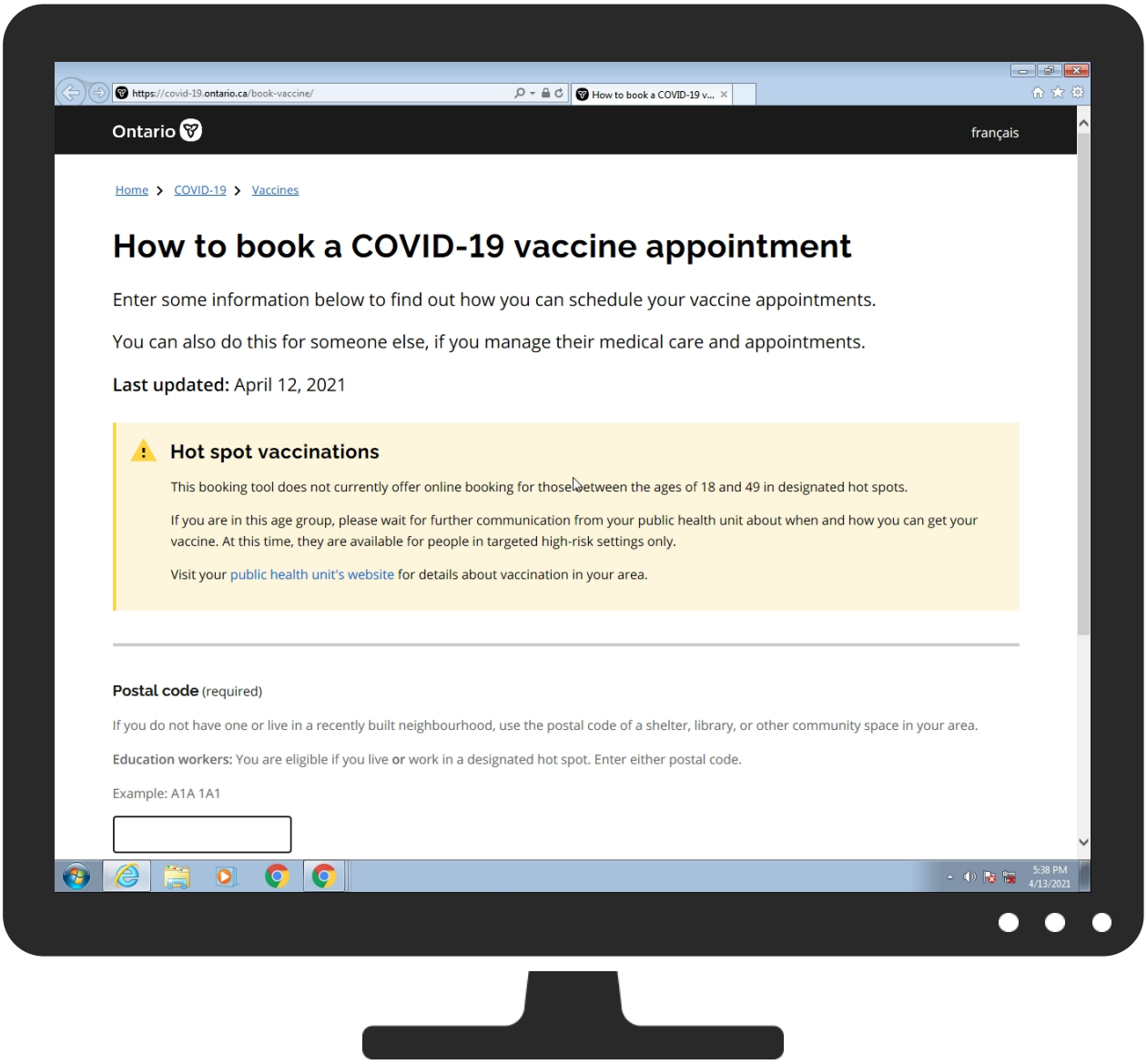


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.ndfht.ca	0%	Avira URL Cloud	safe	
http://www.whcacovid.com	0%	Avira URL Cloud	safe	
http://https://www.Pharmachoice.com	0%	Avira URL Cloud	safe	
http://https://hopitalmontfort.com/en/second-covid-19-care-clinic-opening-ottawa-east-thursday	0%	Avira URL Cloud	safe	
http://www.stevensonhospital.ca/news/index.html?id=265	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.womenscollegehospital.ca/assessmentcentre	0%	Avira URL Cloud	safe	
http://https://hpepublichealth.ca/covid-19-vaccines/	0%	Avira URL Cloud	safe	
http://www.hauserspharmacy.com	0%	Avira URL Cloud	safe	
http://www.bradysdrugstore.com	0%	Avira URL Cloud	safe	
http://https://hybridpharm.com/	0%	Avira URL Cloud	safe	
http://https://www.phdapps.health.gov.on.ca/phulocator/4Public	0%	Avira URL Cloud	safe	
http://https://CovidScreen.lacgh.napanee.on.ca)	0%	Avira URL Cloud	safe	
http://https://barriehealth.ca/	0%	Avira URL Cloud	safe	
http://https://www.rvh.on.ca/	0%	Avira URL Cloud	safe	
http://https://www.cmh.org/patients-visitors/service-resumption-covid-19/covid-19-testing	0%	Avira URL Cloud	safe	
http://www.health.gov.on.ca/en/pro/programs/publichealth/coronavirus/docs/Guidance_for_Prioritizing_	0%	Avira URL Cloud	safe	
http://www.metrodrugs.ca	0%	Avira URL Cloud	safe	
http://https://nygh.on.ca/covid-19-updates	0%	Avira URL Cloud	safe	
http://https://www.osmh.on.ca/covid-19/	0%	Avira URL Cloud	safe	
http://https://www.phdapps.health.gov.on.ca/phulocator/riovirus)	0%	Avira URL Cloud	safe	
http://https://assessmentbooking.simplybook.plus/v2/	0%	Avira URL Cloud	safe	
http://www.espanolaregionalhospital.ca/covid-19	0%	Avira URL Cloud	safe	
http://https://www.mahc.ca/en/services/covid19.aspx#	0%	Avira URL Cloud	safe	
http://https://portal.healthmyself.net/tehncovid/guest/#/g5x/book/type	0%	Avira URL Cloud	safe	
http://https://www.prhc.on.ca/about-us/covid-19-novel-coronavirus/	0%	Avira URL Cloud	safe	
http://www.hwmh.ca	0%	Avira URL Cloud	safe	
http://www.lakeridgehealth.on.ca	0%	Avira URL Cloud	safe	
http://https://testing.getcorigan.ca/	0%	Avira URL Cloud	safe	
http://www.rvh.on.ca	0%	Avira URL Cloud	safe	
http://https://www.msh.on.ca/	0%	Avira URL Cloud	safe	
http://www.HamiltonCovidTest.ca	0%	Avira URL Cloud	safe	
http://https://gbfht.ca/cac/	0%	Avira URL Cloud	safe	
http://https://www.grhosp.on.ca/	0%	Avira URL Cloud	safe	
http://https://psfdh.on.ca/2020/04/03/community-assessment-centre/	0%	Avira URL Cloud	safe	
http://https://stage.api.ontariogovernment.ca	0%	Avira URL Cloud	safe	
http://https://www.haltonhealthcare.on.ca/covid-19-info/booking-a-test	0%	Avira URL Cloud	safe	
http://www.libertymarketpharmacy.com/	0%	Avira URL Cloud	safe	
http://https://slmhc.on.ca/about/covid-19-information/covid-19-assessment-centre/	0%	Avira URL Cloud	safe	
http://https://www.wdgpublichealth.ca/your-health/covid-19-information-public/covid-19-vaccine-information/	0%	Avira URL Cloud	safe	
http://https://registration-mom.mychamp.ca/Live/Montfort/Booking/Account/BookRegister	0%	Avira URL Cloud	safe	
http://https://www.guardian-ida-pharmacies.ca/en/ontario/brampton/kennedy-medical-plex-pharmacy-ida-7027581	0%	Avira URL Cloud	safe	
http://https://www.medicineshoppe.ca/en/ontario/toronto/the-medicine-shoppe-pharmacy-134-7014226	0%	Avira URL Cloud	safe	
http://www.southstormontpharmacies.com	0%	Avira URL Cloud	safe	
http://https://www.porcupinehu.on.ca/en/your-health/infectious-diseases/novel-coronavirus/covid-assessment-	0%	Avira URL Cloud	safe	
http://https://southlake.ca/	0%	Avira URL Cloud	safe	
http://https://eohu.ca/en/covid-19-novel-coronavirus	0%	Avira URL Cloud	safe	
http://https://durhamregion.vertoengage.com/engage/generic-open-clinic?key=5f58a4fe-9e22-4fb8-b49a-b8fe1ca0	0%	Avira URL Cloud	safe	
http://https://www.myvisit.cmh.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d2khazk8e83rdv.cloudfront.net	143.204.11.64	true	false		high
productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com	34.198.74.185	true	false		high
googleads.g.doubleclick.net	172.217.23.34	true	false		high
d36pom45p27o8j.cloudfront.net	13.226.169.24	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
i.ytimg.com	172.217.22.246	true	false		high
photos-ugc.l.googleusercontent.com	172.217.23.33	true	false		high
www.phdapps.health.gov.on.ca	204.41.3.217	true	false		unknown
d1yhecx6e3wyn1.cloudfront.net	143.204.11.100	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yt3.ggpht.com	unknown	unknown	false		high
www.ontario.ca	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
covid-19.ontario.ca	unknown	unknown	false		high
api.ontario.ca	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
covid19.ontariohealth.ca	unknown	unknown	false		unknown
files.ontario.ca	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://covid-19.ontario.ca/	false		high
http://https://www.phdapps.health.gov.on.ca/phulocator/	false		unknown

URLs from Memory and Binaries

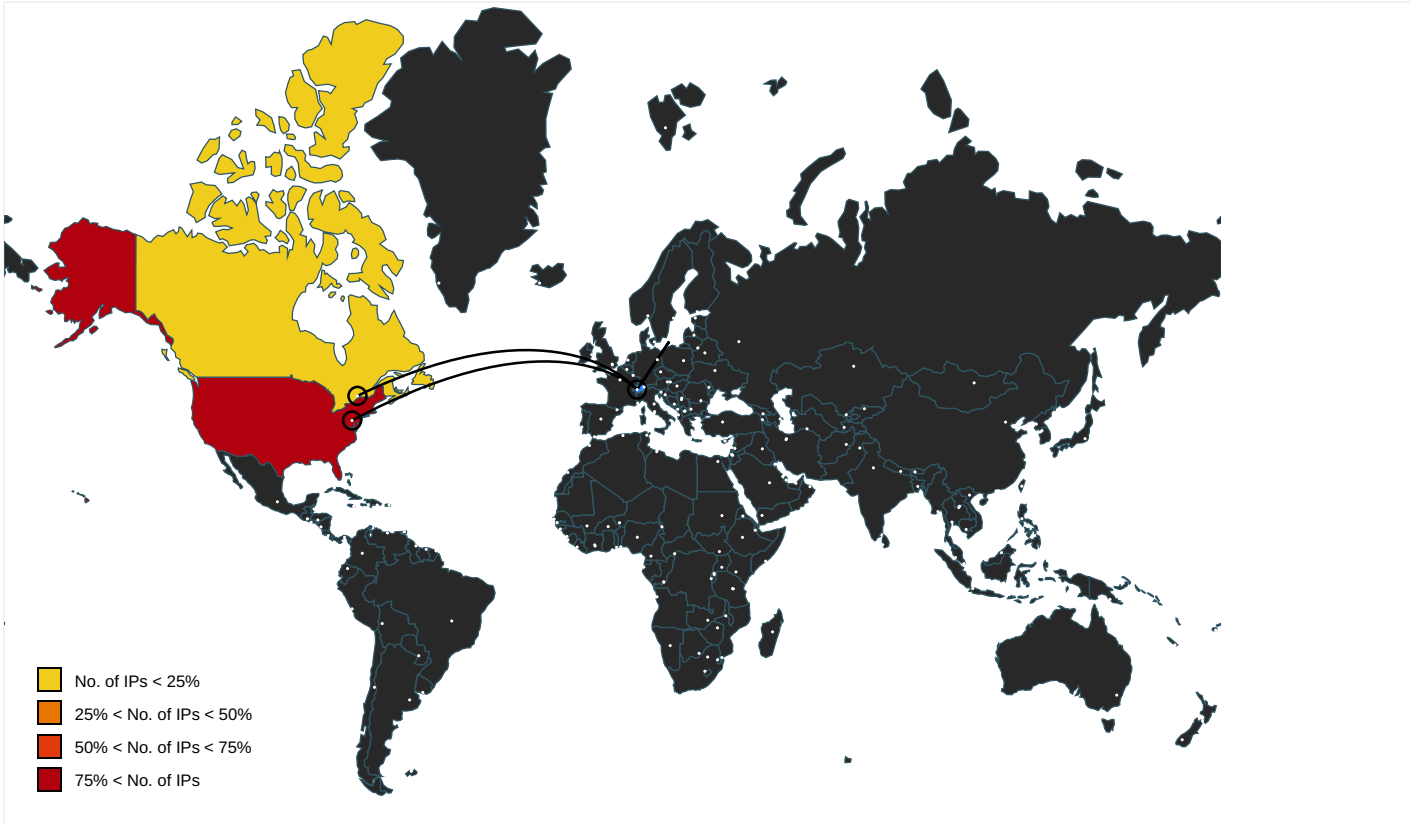
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ndfht.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ontario.ca/fr/page/accessibilite	rendezvous-vaccin[1].htm.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://www.ontario.ca/page/vaccines	ontarios-covid-19-vaccination-plan[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/get-covid-19-vaccine	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://covid-19.ontario.ca/index.html	RUKONSLK.htm.3.dr	false		high
http://https://www.ontario.ca/page/covid-19-support-people	ontarios-covid-19-vaccination-plan[1].htm.3.dr	false		high
http://www.whcacovid.com	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.Pharmachoice.com	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://hopitalmontfort.com/en/second-covid-19-care-clinic-opening-ottawa-east-thursday	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/c19-book-vaccine-assets/social_image_en.png	book-vaccine[1].htm.3.dr	false		high
http://www.stevensonhospital.ca/news/index.html?id=265	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.womenscollegehospital.ca/assessmentcentre	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://news.ontario.ca/search/en?keywords=covid19	RUKONSLK.htm.3.dr	false		high
http://https://hpepublichealth.ca/covid-19-vaccines/	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/covid-19-data/data-catalogue/ed270bb8-340b-41f9-a7c6-e8ef587e6d11.json	populate-front-page-data[1].js.3.dr	false		high
http://https://one.halton.ca/vab/s/	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false		high
http://https://covid-19.ontario.ca/book-vaccine/THowohealth.ca/os-covid-19-vaccinatm/embed/YrjmP_ueahQ?cont	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://www.hauserspharmacy.com	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.bradysdrugstore.com	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.york.ca/wps/portal/yorkhome/health/yr/covid-19/covid19vaccinationclinics	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false		high
http://https://hybridpharm.com/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.phdapps.health.gov.on.ca/phulocator/4Public	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://CovidScreen.lacgh.napanee.on.ca)	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	low
http://https://barriehealth.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.rvh.on.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/feedback/assessment-centre-locations	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://covid-19.ontario.ca/getting-covid-19-vaccine-ontario#phase-1	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/getting-covid-19-vaccine-ontario#phase-2	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/getting-covid-19-vaccine-ontario#phase-3	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://www.youtube.com/generate_204?cpn=	base[1].js.3.dr	false		high
http://https://www.cmh.org/patients-visitors/service-resumption-covid-19/covid-19-testing	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/covid-19-data/data-catalogue/8a89caa9-511c-4568-af89-7f2174b4378c.json	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-workplace-2020-12-21.png	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://www.health.gov.on.ca/en/pro/programs/publichealth/coronavirus/docs/Guidance_for_Prioritizing_	ontarios-covid-19-vaccination-plan[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.metrodrugs.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/covid19-cms-assets/2021-02/tools-check-results.svg	RUKONSLK.htm.3.dr	false		high
http://https://covid-19.ontario.ca/book-vaccine/	book-vaccine[1].htm.3.dr, ~DF1CE05EB0C3EFFAB1.TMP.2.dr	false		high
http://https://nygh.on.ca/covid-19-updates	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ontario.ca/page/accessibility	ontarios-covid-19-vaccination-plan[1].htm.3.dr, book-vaccine[1].htm.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://www.osmh.on.ca/covid-19/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/fr/le-plan-de-vaccination-de-lontario-contre-la-covid-19#phase-1	rendezvous-vaccin[1].htm.3.dr	false		high
http://https://www.hamilton.ca/coronavirus/covid-19-vaccine-booking	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false		high
http://https://www.phdapps.health.gov.on.ca/phulocator/riovirus)	~DF1CE05EB0C3EFFAB1.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assessmentbooking.simplybook.plus/v2/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.espanolaregionalhospital.ca/covid-19	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/fr/index.fr.html	RUKONSLK.htm.3.dr	false		high
http://https://www.mahc.ca/en/services/covid19.aspx#	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.ontario.ca/es/onesite	app.min[1].js.3.dr	false		high
http://https://portal.healthmyself.net/tehncovid/guest/#/g5x/book/type	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.prhc.on.ca/about-us/covid-19-novel-coronavirus/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ontario.ca/.ca/book-vaccine/	~DF1CE05EB0C3EFFAB1.TMP.2.dr	false		high
http://https://covid-19.ontario.ca/vernment-ontario	~DF1CE05EB0C3EFFAB1.TMP.2.dr	false		high
http://www.hwmh.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.ontario.ca	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr, print[1].css.3.dr	false		high
http://www.lakeridgehealth.on.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://testing.getcorigan.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ontario.ca/page/government-ontarioDGovernment	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://www.bchsys.org/en/covid-19-online-scheduling.aspx	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://www.rvh.on.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msh.on.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.HamiltonCovidTest.ca	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://youtu.be/	base[1].js.3.dr	false		high
http://https://gbfht.ca/cac/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://github.com/robloach/jquery-once	jquery.once.min[1].js.3.dr	false		high
http://https://www.grhosp.on.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://psfdh.on.ca/2020/04/03/community-assessment-centre/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/centres-depistage/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://covid-19.ontario.ca/ontarios-covid-19-vac	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high
http://https://covid19results.ehealthontario.ca:4443/	RUKONSLK.htm.3.dr	false		high
http://https://stage.api.ontariogovernment.ca	app.min[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ontario.ca/img/favicon.ico~	imagestore.dat.3.dr	false		high
http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-covid-alert-2020-12-21.png	covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/covid19-cms-assets/2021-03/getting-covid-vaccine-meta-1920x1080-en.jpg	ontarios-covid-19-vaccination-plan[1].htm.3.dr	false		high
http://https://covid-19.ontario.ca/fr/zones-et-restrictions	about-ontario[1].htm.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://www.ontario.ca/page/ethical-framework-covid-19-vaccine-distribution	ontarios-covid-19-vaccination-plan[1].htm.3.dr	false		high
http://https://www.haltonhealthcare.on.ca/covid-19-info/booking-a-test	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.libertymarketpharmacy.com/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://slmhc.on.ca/about/covid-19-information/covid-19-assessment-centre/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.wdgpublichealth.ca/your-health/covid-19-information-public/covid-19-vaccine-information/	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://news.ontario.ca/newsroom/en	app.min[1].js.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://registration-mom.mychamp.ca/Live/Montfort/Booking/Account/BookRegister	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.walmart.ca/en/stores-near-me/richmond-hill-south-supercentre-1116	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://www.ontario.ca/page/privacy-statement	ontarios-covid-19-vaccination-plan[1].htm.3.dr, book-vaccine[1].htm.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://covid-19.ontario.ca/book-vaccine/THowio.ca/ontarios-covid-19-vaccinatm/embed/YrjmP_ueahQ?con	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.guardian-ida-pharmacies.ca/en/ontario/brampton/kennedy-medical-plex-pharmacy-ida-7027581	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.medicineshoppe.ca/en/ontario/toronto/the-medicine-shoppe-pharmacy-134-7014226	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.southstormontpharmacies.com	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/covid-19-test-and-testing-location-information	ontarios-covid-19-vaccination-plan[1].htm.3.dr, 4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr, RUKONSLK.htm.3.dr	false		high
http://https://www.walmart.ca/en/stores-near-me/woodbridge-supercentre-1081	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://www.porcupinehu.on.ca/en/your-health/infectious-diseases/novel-coronavirus/covid-assessment-	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/	RUKONSLK.htm.3.dr, covid-19-vaccines-ontario[1].htm.3.dr	false		high
http://https://southlake.ca/	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid-19.ontario.ca/themes/custom/ds_theme/favicon.ico~&	imagestore.dat.3.dr	false		high
http://https://eohu.ca/en/covid-19-novel-coronavirus	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://trilliumhealthpartners.ca/assessment	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false		high
http://https://durhamregion.vertoengage.com/engage/generic-open-clinic?key=5f58a4fe-9e22-4fb8-b49a-b8fe1ca0	~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.myvisit.cmh.org	4178e9cc986fc140f048cd41cab70b6192963e31-551c0acc8f79274f589f[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/cs4qPsP6COA	{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat.2.dr, RUKONSLK.htm.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.11.100	d1yhecx6e3wyn1.cloudfront.net	United States		16509	AMAZON-02US	false
172.217.22.246	i.ytimg.com	United States		15169	GOOGLEUS	false
34.198.74.185	productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
172.217.23.33	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.226.169.24	d36pom45p27o8j.cloudfront.net	United States		16509	AMAZON-02US	false
172.217.23.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
143.204.11.64	d2khazk8e83rdv.cloudfront.net	United States		16509	AMAZON-02US	false
204.41.3.217	www.phdapps.health.gov.on.ca	Canada		808	GONET-ASN-1CA	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	386160
Start date:	13.04.2021
Start time:	17:36:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@4/274@14/9

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: https://covid-19.ontario.ca/book-vaccine/ • Scroll down • Close Viewer • Browsing link: https://www.ontario.ca/ • Browsing link: https://covid-19.ontario.ca/rendezvous-vaccin • Browsing link: https://www.ontario.ca/page/government-ontario • Browsing link: https://covid-19.ontario.ca/ • Browsing link: https://covid-19.ontario.ca/covid-19-vaccines-ontario • Browsing link: https://www.phdapps.health.gov.on.ca/phulocator/ • Browsing link: https://covid-19.ontario.ca/ontarios-covid-19-vaccination-plan#phase-1 • Browsing link: https://covid19.ontariohealth.ca/ • Browsing link: https://covid-19.ontario.ca/book-vaccine/ • Browsing link: https://covid-19.ontario.ca/vaccine-locations • Browsing link: https://www.ontario.ca/page/about-ontario
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 2.20.142.209, 2.20.142.210, 13.107.13.80, 204.79.197.200, 13.107.21.200, 131.253.33.200, 13.107.22.200, 172.217.23.40, 172.217.23.46, 152.199.19.161, 216.58.207.164, 216.58.207.131, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 172.217.20.238, 172.217.23.78, 172.217.22.238, 142.250.185.134, 172.217.23.67, 13.107.253.19 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, api.bing.com, afd.e-0001.dc-msedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, star-azurefd-prod.trafficmanager.net, dual.t-0009.t-msedge.net, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, www.gstatic.com, au-bg-shim.trafficmanager.net, api-bing-com.e-0001.e-msedge.net, dualstack.f3.shared.global.fastly.net, www.google-analytics.com, www.bing.com, e-0001.dc-msedge.net, www-google-analytics.l.google.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, fonts.gstatic.com, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, r20swj13mr.microsoft.com, static-doubleclick-net.l.google.com, dual-a-0001.dc-msedge.net, youtube-ui.l.google.com, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, t-0009.fb-t-msedge.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/386160/sample/COVID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
13.226.169.24	ACH REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	
143.204.11.64	scan-100218.docm	Get hash	malicious	Browse	
104.16.19.94	http://https://bit.ly/3hDDoTm	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://ninjutsu.4ryu.com/.well-known/pki-validation/zombaiogw_1_1/print_recipe.php?living=ytpr1h11zw0qw0&south=difference&slide=during	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://surl.me/vy4l	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://u15974653.ct.sendgrid.net/ls/click?upn=sKo8P2XHLOhqpgLcALrpHsAMymMPQ9pJ-2BnCP9l5luXmX2tau-2FkmeQME9D69RU7ffQBYwWBrDSW94kS5u6ig5BmkhgBhgQJfm-2BsLwvjPlmdPdsXD4ILOaqVNEwgY7GAZQPkafmgyIOS5FU-2B6124ooi1O-2FMB47qUlmVhTTnK6qV5fGlsBAy7itOSHfP1wikhvsiyeK_Y89n8cg5DiKkjVvtw-2FYSjk3JbqBqCNqd4QE5c0z9p4IJ6aN66chjxOUHcribC2kbrQ6ua83fMfn3Hnb3TofbErA9L2X-2BpZpbvzOnYxCl6WSRvjbd6cnTXhRnH1-2Btzg-2FEpNckJ170lMbhRvVxgpvwWV6rRyYLwNDxpt3lm1lgyNi-2B-2B86Pp03BP8O3y-2Bw2BSUYNj8fK3irR9dYwZuWCkvZJ3fJURjdr0uD0itVZut-2BhVs-3D	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/font-awesome/4.1.0/fonts/fontawesome-webfont.eot?
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://lokalny-biznes.eu/modules/mod_simplefileuploadv1.3/elements/reactivation/indextest.php?youll=enwht11p10sc0&picture=call&please=gave	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	Ug6Q3lejBj.exe	Get hash	malicious	Browse	• 104.16.19.94
	Mike-voip-18388.htm	Get hash	malicious	Browse	• 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	V3kT2daGkz.exe	Get hash	malicious	Browse	• 104.16.19.94
	setupapp.exe	Get hash	malicious	Browse	• 104.16.18.94
	C++ Dropper.exe	Get hash	malicious	Browse	• 104.16.18.94
	setup-1.exe	Get hash	malicious	Browse	• 104.16.19.94
	Five.exe	Get hash	malicious	Browse	• 104.16.19.94
	6BympvyPAv.exe	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde973.htm	Get hash	malicious	Browse	• 104.16.18.94
	Open Invoice & Statements.htm	Get hash	malicious	Browse	• 104.16.18.94
	securedmessage.htm	Get hash	malicious	Browse	• 104.16.18.94
	Three.exe	Get hash	malicious	Browse	• 104.16.18.94
	One.exe	Get hash	malicious	Browse	• 104.16.19.94
	Five.exe	Get hash	malicious	Browse	• 104.16.19.94
	Two.exe	Get hash	malicious	Browse	• 104.16.19.94
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 104.16.18.94
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 104.16.18.94
	FARASIS.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	FARASIS.xlsx	Get hash	malicious	Browse	• 104.16.19.94

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	inv_397145572_1781481758.xls	Get hash	malicious	Browse	• 50.17.5.224
	inv_397145572_1781481758.xls	Get hash	malicious	Browse	• 50.17.5.224
	P.O 0000237701.exe	Get hash	malicious	Browse	• 18.235.92.123
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• 3.223.115.185
	EUR 11,464.00 955PLA3210970613.PDF.exe	Get hash	malicious	Browse	• 50.17.5.224
	1koFD7T3Tv.exe	Get hash	malicious	Browse	• 100.24.251.71
	Ug6Q3lejBj.exe	Get hash	malicious	Browse	• 54.227.172.114
	Quot_466378-09.exe	Get hash	malicious	Browse	• 54.225.165.85
	Product_Samples.xlsx	Get hash	malicious	Browse	• 54.198.222.183
	MTCC169.DLL	Get hash	malicious	Browse	• 54.225.222.160
	originfile8.doc	Get hash	malicious	Browse	• 23.20.114.125
	yHm3PFVYHK.exe	Get hash	malicious	Browse	• 54.221.253.252
	commercial invoice & packing list doc.exe	Get hash	malicious	Browse	• 52.20.197.7
	V3kT2daGkz.exe	Get hash	malicious	Browse	• 34.238.79.100
	Bank Details.xlsx	Get hash	malicious	Browse	• 3.230.51.235
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• 52.206.71.220
	IntegraL.exe	Get hash	malicious	Browse	• 23.21.252.4
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 54.165.198.12
	remittance info.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	782kQ15aYm.dll	Get hash	malicious	Browse	• 54.197.173.238
AMAZON-02US	D@136.exe	Get hash	malicious	Browse	• 3.23.250.40
	bd.exe	Get hash	malicious	Browse	• 99.86.154.99
	bee.exe	Get hash	malicious	Browse	• 99.86.154.178
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• 52.58.78.16
	presupuesto.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	ghnrope2.dll	Get hash	malicious	Browse	• 13.225.75.73
	scan_745.htm	Get hash	malicious	Browse	• 52.219.98.146
	ntpxrxZCfL.exe	Get hash	malicious	Browse	• 3.13.255.157
	Ug6Q3lejBj.exe	Get hash	malicious	Browse	• 52.84.150.39
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 3.13.255.157
	Shipping-Documents.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	shipping documents. CI PL.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Original Invoice-COAU7229898130.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• 52.221.6.123
	swift note.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	RFQ3936.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Invoice-SRP0047459188e.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	BANKINV28032021VBNSINO.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	tmkfdBpwAx.exe	Get hash	malicious	Browse	• 3.22.15.135
AMAZON-02US	D@136.exe	Get hash	malicious	Browse	• 3.23.250.40
	bd.exe	Get hash	malicious	Browse	• 99.86.154.99

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bee.exe	Get hash	malicious	Browse	• 99.86.154.178
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• 52.58.78.16
	presupuesto.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	ghnrope2.dll	Get hash	malicious	Browse	• 13.225.75.73
	scan_745.htm	Get hash	malicious	Browse	• 52.219.98.146
	ntpxrxZCfL.exe	Get hash	malicious	Browse	• 3.13.255.157
	Ug6Q3IejBj.exe	Get hash	malicious	Browse	• 52.84.150.39
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 3.13.255.157
	Shipping-Documents.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	shipping documents. CI PL.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Original Invoice-COAU7229898130.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• 52.221.6.123
	swift note.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	RFQ3936.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Invoice-SRP0047459188e.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	BANKINV28032021VBNSINO.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	tmkfdBpwAx.exe	Get hash	malicious	Browse	• 3.22.15.135

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Order 100920-0087.pps	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Shipping-Documents.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	shipping documents. CI PL.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Original Invoice-COAU7229898130.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift note.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	RFQ3936.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Invoice-SRP0047459188e.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	BANKINV28032021VBNSINO.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	fileshare.doc	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	documents-122179384.xlsm	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	RFQ P39948220 Inquiry.ppt	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	documents-1982636004.xlsm	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	documents-466266883.xlsm	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_RFQ_Hongjin_.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Bank Details.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	Confirm Order for AKTEK Company_E4117.ppt	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 143.204.11.100 • 172.217.22.246 • 172.217.23.33 • 13.226.169.24 • 172.217.23.34 • 143.204.11.64 • 34.198.74.185 • 204.41.3.217 • 104.16.19.94

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	117192
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	3072:F2qSSwIm1m/QEBbgb1om2qSSwIm1m/QEBbgb1oQ:FJdwIm1m/QEOb1omJdwIm1m/QEOb1oQ
MD5:	2FEBC5EB397A71B7A4862D0DCC21CA5E
SHA1:	5568FBD6D7DB899850D3AAFF95FEC08952361678
SHA-256:	2E9BE05B763D01CB0CD6FDE8BC64432A012AD3ECD9A6F3099DDE740A2D148A13
SHA-512:	B7D42B634F3B0CDC81CB94F281C8BB743BB98421AE54E21005637F762292D865EB1D71D43C4FF96AEE824527E9F7FB94FE5F5A4D35A22363A2A86AF8ABE0C414
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.107162850663867
Encrypted:	false
SSDEEP:	12:hwTJ6HkPlE99SNxAhUe0hbHwTJ6HkPlE99SNxAhUe0ht:2okPcUQUPhUokPcUQUPht
MD5:	5366D69859421B1F9504AC783CF1C20E
SHA1:	FA3D38A914F18A307700B4805A0BF09E88D18C22
SHA-256:	E6926EC858898EA46A462FAA256E8A5D11246D9AAE7934F1CC7B96CD53710EA3
SHA-512:	28670C3C58701E4EF47A98BE5C12B6F57C2CB492ADFA519FB3186FDEE2B3B1C81E2C1E89AEAF9F018C206B4B20ABC129B7723CFCA13D2ADE5A4102524279617
Malicious:	false
Reputation:	low
Preview:	p..... .....t.RK.0..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... .....sK.0..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?...z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\MP98E46N\www.ontario[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	275
Entropy (8bit):	4.355403879931485
Encrypted:	false
SSDEEP:	6:JFK1rUFSC5EJVqGCj5xIQl1rFK1rFK1rFK1rFK1rUFSC5EJVqGCj5pTTNIQl1rFJ:JsrU775SQPrsrsrsrsU775pTiQPrsrS
MD5:	98F4D448FF72FE164BFFB31CD83DBEDD
SHA1:	95FF0E90375ECA00EC41C0552087D23B71BA4ECE
SHA-256:	CD5C6078FA0F906CF735E5ADB6C184F18A9216521CD81DAB418FA558281E7A59
SHA-512:	3E67F7FAAB3DF9E2B877DADE3010CEED6B0EE662056DE7D7346AB6FD90491C84B87A72E4ECED978AA9871123EB6271B9AD8E0563D7104F30B2679AA4F20AD35F
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="modernizr" value="modernizr" ltime="2056763168" htime="30879942" /></root><root></root><root></root><root></root><root></root><root></root><root><item name="modernizr" value="modernizr" ltime="2467383168" htime="30879942" /></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\Q3DXH6Q1\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2703
Entropy (8bit):	5.135318670078789
Encrypted:	false
SSDEEP:	48:0JQ53Q5io1TEhQIio1TEhQ3mhQIio1TEhQ3mhQ4QIio1TEhQ3mhQIio1TEhQ3mhk:uQtQ8gEhQHgEhQ3mhQHgEhQ3mhQ4QHgi

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\Q3DXH6Q1\www.youtube[1].xml	
MD5:	54BA69745A39CBBF2BEE75B4655AE5D1
SHA1:	2E5D4C1FE13EA9C1CA94AC1AA43572E8941C94D3
SHA-256:	022B441ABB234D5B720AA27E69923E45050115BD9FCD0D2E2309B57830241CAB
SHA-512:	E6533F99BAC24F3EE9E72DA815F6DA78D9E8233E748C73E28B094E882CB9FCC4D09A519509F9398654960D385D3D0E17F8B1584388A31C8D8F1BC65E7ADA213
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="__sak" value="1" ltime="2153713168" htime="30879942" /></root><root></root><root><item name="__sak" value="1" ltime="2207193168" htime="30879942" /></root><root></root><root><item name="yt-remote-device-id" value="{"data":"cc052f98-2bcb-46f5-a0cf-4a42a52c9f1e","expiration":1649896719994,"creation":1618360720007}" ltime="2208093168" htime="30879942" /></root><root><item name="yt-remote-device-id" value="{"data":"cc052f98-2bcb-46f5-a0cf-4a42a52c9f1e","expiration":1649896719994,"creation":1618360720007}" ltime="2208093168" htime="30879942" /><item name="yt-remote-connected-devices" value="{"data":"[]","expiration":1618447120165,"creation":1618360720165}" ltime="2209363168" htime="30879942" /></root><root><item name="yt-remote-device-id" value="{"data":"cc052f98-2bcb-46f5-a0cf-4a42a52c9f1e","expiration&q

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{854E3008-9CB9-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.8701640884212738
Encrypted:	false
SSDEEP:	96:MRKSKOpkJeaJq0tHhr38Ju2bYeXJuD6a8Hk73:MRKSKOpkJeaA0tN3LBRGa8S3
MD5:	47AC2EA2516136C68385AA6B40E6A96E
SHA1:	6314BC4BBF51088AFD7F3273CF44DBB01A0D114E
SHA-256:	FCA3F6BEB29A17154A08B434138A35B56274DCF822601EFAB2FB026DDC0E1BB5
SHA-512:	1752DCE3A93F4756CDE8844F4F2935D2B9EDD9AB72FD687E7B0EEF9292DCD7EF4FD3DCE07548329F2226D0C62A8D8E23CE6CB28C4BCC3CBC3C3067CBCF7028C
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\{854E300A-9CB9-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	350516
Entropy (8bit):	3.592168513572414
Encrypted:	false
SSDEEP:	3072:qn3w6shuNdfh3Mv0rMREtit8XN6kyxQU3PKXzq9bNtuL8DRm:a3Uydh3qiRwxQU3MzqzUL8m
MD5:	F3DD614EEF58E609EEC285F7AF8E04F5
SHA1:	28373EAE164FF657C5F17A08D4DDA7091C8BDD82
SHA-256:	8B71C22EC38FD60CFB779D582397445F7D94CD456C7337547F7A9CD73882485E
SHA-512:	0CD4FB7A8A5778B48E8DF3561CF62195A94A5A2F414A8096415CB5F6872AD4009C507D74845CA1068E7EBD3E219312A658F101596D1A7B9E4805FECD89572EFF
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\{A66EC5B2-9CB9-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5637341456158451
Encrypted:	false
SSDEEP:	48:IvQGcpUpGwpNoG4pPCGrapgStGQpZfG7HpCQTGIpG:MUKDb4JEeSX/u0EA
MD5:	54EEFE202B5D7727BAB7BF7A6636F52E
SHA1:	7F98D61A148989773228B01C8DDC07A774172047
SHA-256:	52FF1500054F2247889DD75BF50A530401814B04EB65A503870B86939E246C02
SHA-512:	3972259F81449D1EC5AE84AB5548127CA82480AFCFF86D21AB648F7746293062CCDDA9861D19CC79510FB038C81FFD0D42E7F911C7707726B0849953FD7DDB9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A66EC5B2-9CB9-11EB-ADCF-ECF4BBB5915B}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34748
Entropy (8bit):	2.9903169596750265
Encrypted:	false
SSDEEP:	192:c/pSGvHjgDv3XHQfYsynKaNsC4OnNq3XHQfYsynkaNsC48nNQpSGvHjgDK:wCbXmYsyBNL0XmYsyTNVKCW
MD5:	5C96CA226070C934556BE1E747319234
SHA1:	98FFB28A6A6FBF40475F68E642FA12436F174894
SHA-256:	DD698A9372B96C86AEA420C7A33F27E6E577EDEE1F4787E61431FACF35E844EA
SHA-512:	35AE976D3C9C2003C96C22C27605AD8CCF06BA04BE735558F4A4F901A4C220A713CF852FB152F510A1601D0D1F7863A57CA6A44374EE5797951772507C011FA9
Malicious:	false
Reputation:	low
Preview:	E.h.t.t.p.s.:././.c.o.v.i.d.-.1.9...o.n.t.a.r.i.o...c.a./.c.1.9.-.b.o.o.k.-.v.a.c.c.i.n.e.-.a.s.s.e.t.s./.f.a.v.i.c.o.n.-.3.2.x.3.2...p.n.g.8....PNG.....IHDR... ... .szz.....pHYs.....~... ..IDATX.W[(.Y..{....f\2n..7..(3[<.... .h<)e.<y..@.x@).9..a.t..(N....1..Y.j}.....\....}.o}.f3&..;....g.1.m.G...d..a.....k.3M.....Vb&.-`4.7.{..t..%.D...r.3..Ka.V.U.....wK...K..ma... .B.$7...aW....l.Y.O.BoU!<..;...n.....p...7b(...gH..{..j.P....%.=<<4.b..5..$.....).~~~.....t:!66Vc.#00.....BP<..".....r.....'P.....3.....v....#.....EHKK.1aH..I.,.s6 .....`kk....auu....uB.....666`nn.....z...2r.....>(@..{....*....kHf.....\.....{....cn.$.[.....S,Pl.C...1..&.....oFw.....M.....4'.....&j....f}}}|.....1:.....v.!++...../.,.#....p1 H....l.b.A7-JHH...s~...8xzz..8.....&f...iff.....I..[.q.....i.....-88."##u....4.GGG....j/...7.....z.....{rr..Abb"...r. ...IM`....T.B&..fZ.H.,(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\RUKONSLK.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	59312
Entropy (8bit):	4.696571424764276
Encrypted:	false
SSDEEP:	1536:jqn2E24AmTI/Diz0/7hcKsKZEO7+bYyc0fwVgFY72sn0KcLuUvwHCsYHKrjAz1Pq:Gn2eDucPMAz1PJlb93m6hL2h
MD5:	88DD819218D5F34C26C4785C363759DE
SHA1:	62959AA53A4696D10A8AB5721059247C4DA8F801
SHA-256:	B07620CAD28717FD7064196B485143A7A8A100F041F0B5BF74A88BCB0F401819
SHA-512:	1CADBBD4CF8E384E9BA5AAC0C90C3622FB40A7C28EFA37B31F20E5B102DE54118C3F02B9E355C862BD934F7731990BD285844A23517FB217EDE96F952680C7B B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid-19.ontario.ca/
Preview:	<!DOCTYPE html>.<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http ://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema# ">. <head>. Google Tag Manager -->. <script>. dataLayer = [];. (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':. new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],. j=d.createElement(s),dl=l !='dataLayer'?'&l='+l:'';j.async=true;j.src=. 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);. })(window,document,'script', 'dataLayer','GTM-5G4CS4L');. </script>. End Google Tag Manager -->. <meta http-equiv="Content-Type" content="text/html;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	852
Entropy (8bit):	5.518736472579191
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZy+KVCetE31tEsLqo40RWUnYN:VKEcixKoe21tFLrwUnG
MD5:	647F2FC22BA401C8613B8A168C02DB1A
SHA1:	CFF6FD91F3B18BC776591420B9B09C321ADA4406
SHA-256:	FE81E776D459F15B4DAEF2EA548D3150A761C08D33C3013DF60D929775548092
SHA-512:	AC598D3755CA8AD371AA8D42AA7DCC53EBC91AA206E80ADC6713ADF09B29EEF31A92CC39218D509FBE0C9274C51DE499B63E6A88A0D6B4CDD049BCF2B3AF 6B36
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\api[1].js	
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. *//(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('explicit');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/mrdLhN7MywkJAAbzddTIjTaM/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-zy6MpaK2q7ThL2mDEY0TbyvBJDr6lKK9SPTRcXRLbNIBZDn1zpbOT7nMFdXz9mci';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\app-data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	50
Entropy (8bit):	4.828758439731455
Encrypted:	false
SSDEEP:	3:YSAjKv8Lt/1QRc3en:YSAjKvax18cu
MD5:	EF2C86230634867F37EA2E4C6778CB2D
SHA1:	2A24277E89F9498B378A63D141A1F6AF3E085733
SHA-256:	B84C538D7F3BE14E5F46BCE49268C34F4479B22FD9997BAA7E6F4C74E177C2CC
SHA-512:	55DEC0004F8D95D4296ED5EEFC5FC5A929EF4F3F3F22FEAD7D552DE7E9C671B3362DE50885FFFB8EC0C4AF7EA5F4FD8B74CE874F34D8E7FAE56236ACC52116F
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/page-data/app-data.json
Preview:	{"webpackCompilationHash":"192fd53b9f665082e06a"}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\app.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	54690
Entropy (8bit):	5.4361647031728735
Encrypted:	false
SSDEEP:	768:3z5xKen7+bC2L1L+LDLvvPdQ60v0X9H48RQ+Y1r4lumyOS5SIQ/WuQ5+hXt/Vs:+b71gXvve6z9LR3lumyOSsNbQ0Ft/Vs
MD5:	90AE69F345F32CEE774C6033DAB3E6AE
SHA1:	DBEA9776D4E0AEFCAE87268E73922C03061DDEBE
SHA-256:	4E8EED0EBB68E95AB82B239AA510F85431D3EE6D0EF444EF1C1AF102BFC232A9
SHA-512:	F1711AE874F4129B617ACEC8997F1D68F6D3F7934C83457817AF6D77BF420303F6586A05C1FDE9F7611AA9CA61B5CBFFC2605FF0FB6E6875D0B983A3756805BC
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/js/app.min.js
Preview:	"use strict";!function(c){c(function(){function e(e){var t,a,i="tabindex",n=c("#"+e.attr("data-dropdown")),o=c(s,n);o&&(a=(t=o.eq(0)).attr(i),o.attr(i,"0"===a?"-1":"0"),"0"!==a&&t.focus()),"1"!==n.attr("data-accessibility-processed")&&(c(document).click(function(e){e.target!==n.get(0)&&!1===c(d,n).is(":focus")&&o.attr(i,"-1")}),n.attr("data-accessibility-processed","1"))}var s=["a[href]","area[href]","a.close-reveal-modal","input:not([disabled])","select:not([disabled])","textarea:not([disabled])","button:not([disabled])","iframe","object","embed","*[tabindex]","*[contenteditable]"].join(","),d=c(".f-dropdown").find(s).attr("tabindex","-1"),a="aria-expanded";c("a[data-dropdown]").on("click",function(){e(c(this))});function t(e){(e=e.find("h1:first-of-type")).length&&(e.is(":focusable")||e.attr("tabindex",-1).on("focusout",function(){c(this).removeAttr("tabindex"),"#ng-view"===window.location.hash&&(window.location.hash="")}),e.focus())}c(".reveal-modal").find(s).attr("tabindex","-1").e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-19-icons-physical-distancing-2020-12-21[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 104 x 96, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	1948
Entropy (8bit):	7.847009055709759
Encrypted:	false
SSDEEP:	48:Dx9KT/TK/8Ku9aRuwUPQA0XI59CLojba8PsAPBj9+5fOndMk:DKT/TfLaAjPam9wyba8PZv+qdj
MD5:	D06B5237DBB17375F1AD6E49BAF608F3
SHA1:	BBBF067097F5C188FA5A7D3895EA7381F01255D6
SHA-256:	4C7BACBC7729E1F782FD8A14409006E54AFB7F6EB29A1D6C18B6358D7ED0AE11
SHA-512:	789450AD63B4BBD499A088A1CA028435614718FFCD38530DB2E8F6C301FC7029AF74DB0D8E4DA5A999BA3106816FCCEC66D1AB4507AE1B1397E81C1859F4F7E9
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-physical-distancing-2020-12-21.png
Preview:	.PNG.....IHDR...h...`.....[F.G....bKGD.....UIDATx...{pT.....1ND..jLl.)e*I.X.....Va..N;(.....V.#.t..5@.....8.....".J1(M..$\..h...?v...M.].=K.=..o.>..d.9{.y..J.Yp..9..w.5f..gZ...c."z...j...f...Y..C...kJ\..!..%:\O.Em...."...!...W].c.q.6..7b.o..F.l.1."..S\c.k.mGVG...U.7Z\.Q...2+M.-..f...(r...m.ot..FN0^U.n.....9.=.&I...z]....-.p9?rt.s.l.&V...r...W.Ni^X....i..d#.B8bH..P..:.s.....B']....0.w..g.L.....z.XxV....T%.\|>.N1.Q..P)bf@=..B.B..!....#&..t5.!..'.....tZt.$x....P..=.....S!.:.....j.:..h.h.H..1%&...u.<.....B..8..".c.Z...`..1;..... ..k..d.b,.bx.~...Q~.....b6.08y.B.(.....&....[.uVh@7.v.Zk0..{..X.....C..~.\..".5..{...\C:.L...b.1..S...Ig.Kx... .g76.E"^...ZGu.|z..iK.Nv..c.=*R...U.AK.]z...=H..b.r...j=:.re.r&."......[....^....q5..B<.U.1...y...b*+C.....I....zL..A....~.!....!.....u...3...]~..C{.9GHA.8.znC..%K9B..`-B.D...!....'.].T(...lA...6.y.Q. ....3.k#.cjh.ZO.5|<<.9...M....l.U#.....t/"9h.d....G8...@..%@#...H...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-19-icons-self-assessment-2020-12-21[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	1777
Entropy (8bit):	7.779993403442084
Encrypted:	false
SSDEEP:	48:VKbm+NSVrllm8qP5oU1Yb5mj5qUTc1rZvhklfGy:QNS5Pq51ub8EUA1NvuZ
MD5:	3C19B7F5C2929C2FD3EFFD65F53370F7
SHA1:	95702B5DED97EB44842748ADCA5FA953EC59DBEF
SHA-256:	DDDC4D69E737AA49AEC21E18FB0C50C59DEC5E7127F32577328177D2AFDA4691
SHA-512:	B3F063B3CE5F533609A4FEF34B765CE1CABE7B18332CFACC178F3DCF0EEA9DC2CE8DE2F35553FA8EB3846F08443948E119CEAF57E0636BF2571EC6F317059E13
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-self-assessment-2020-12-21.png
Preview:	.PNG.....IHDR...`...`.....H.....bKGD.....IDATx..kl.U...-H1$\..D.../j.X#Q.R.piQj"....._..&RD.Xl..T4j.4.A.T,...c.%...f..rQ.....;.33;;.....y.3..\|.....+.Kk.....[..{....nn.fn..y.T...C.-..\!..vE.F....r.lX.....i..uJz.c.c..i\.T.~...U....zyZ..K3.....:{qL...g...T.U....TCI.....ZC...J.....o.V..t.N..Gy..~#.TW..@x..u...B..s."..:`...!....P....(....+A...w..Nv....) L...#A(.<.>..7vU.!0.....f...@@.....(.&.8...>.....P.....a..@-H.L30...$....i.>.p0....(.....P.].z..\..k..e... ...m..(...h..w...../..G...&.....2.....".a.G....<>U...CO.....}E..|.t.~.....={.O=....@{...r..y.H....{.+..[.Z...X....y.H.@qn...?T..{...<.....E...`...G'. .No.....D..C:...+...p..K..w'.r.5.....o....X...~..a.....p}j...w.G.`.(.!.>.L..X,..J....).....,Z....q...$.q..$...a..8."...x..U;D.).....G.B..`.}..^..!v...z..'...%U..!.....%....'...z...$....q. 0..5v.....3G..U$..... ..9..[.....?.....L.b. .2....}@>l|N..0f.+..O...p?....>....g..D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-19-icons-stay-home-2020-12-21[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	2224
Entropy (8bit):	7.854566193026311
Encrypted:	false
SSDEEP:	48:542YEZxCrZXskgX9nTjrfS3y7E+WY/zJQdCSzcjhdb2Vf6RdCEgr:7YUEZckgZTgxkACSIjfblylgr
MD5:	F90F5AF067A6638975D2480687329F91
SHA1:	107E1F4FA829FF14E50AF3B5E2678E71F0F8F1FE
SHA-256:	C41DB7A0402949CC5A46A292469CF5C94AE97A95639AA6808F9F05C2731C5B1B
SHA-512:	5142B81B10D03B927FBB44E42A427B3D38F1D2683511889D71BD1EF8794D8BCED22CFF291D4913FD16E219562349A9A28F94E1C9F45BF0CD3A2FAC8ADF0F05D
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-stay-home-2020-12-21.png
Preview:	.PNG.....IHDR...`...`.....H.....bKGD.....IDATx..{p.....Mx..GB..|.JgbG...c. E..h.Z.u....R.b...!.v....%..8."..#*..F.#.. .(x.7.P..HH..?.&.$.....'.f..~~.....H...h.Ql..E.I.....z%...q=..I..3..h!.i.#:P'.+.&.\'.3W.....C'....]....&.M..7.M.e.m..7...J5.y#...{..\_.vg.n...=...,..\|Ve..]..\|....{t.P~.z....>...h\|..!.2.u\|.....8...1....Y.....y.P.tc.....Zy~.x.AX.(.....sV..e2u...V#....x.A....u^..!z..Z....:.....K..[)..d.k9.....w....S./..Nm..n<.7...zWW!z..7.v...,r.%9.....Mo.y.@..A.W...ez.3. dS.....E\k.f.7.4.hE..9q.t.p..0..$.m."...+.....bj.1....a..S....B..g...9....."\..[..}r...7.s..F...z... .....#.O=.....R....a.... ...z.@_J5.o.N..l...k*B6.W....."..%.....r.....+..5I.....!a....K..9...#...O}..m..BI.....?4L.G.0+.....r..... ...@...w.y..[. |..@CB*L..S.2..+u.....tB..}#k.....p...B..3..f@|.').....+..hK..w!V.'.....r....q."...rF".....".r..oS.y.y,.C.....X@1.....R&.h...~...;.k.oN..~.... 6J..~...A6.j>...5/..(.s..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-19-icons-wear-a-mask-2020-12-21[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 98 x 96, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	3127
Entropy (8bit):	7.89265984599944
Encrypted:	false
SSDEEP:	96:P9RABuo2YCs4zoTCtNDiNICK5nty2H5mdgv3IS:PMuobyzoTCtNxn82H5wgv4S
MD5:	34C99D948AD789EDE4BE64F085FDE6FA
SHA1:	DF33A0C82B3A9D157C594CAF167F506313E5F6F2
SHA-256:	75FEDC6E4C13AE69F86749B351ACDF08D70120F6EE1A1A9B7830532D5FE38BE7
SHA-512:	E91DBF47105B2DEBE4C38A5CCC2D22872534195CC63C8B5283E88B8622FF2C78512F9724F6E0D335D7A352C4D59770B80C77D72B4EBB7447670E13C3EF8D387
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-wear-a-mask-2020-12-21.png
Preview:	.PNG.....IHDR...b...`.....Ldo.....bKGD.....IDATx..yT.u...@...S!u.B.X.....T.....m.1.qh&S.-s.4i,.....4n.oh.....w....5...q_.w..}..s.|...z..{..=.+R. ;.4...Z..V.LU.n*\.MU.2..k..<.48;...|d...<.*.\.j5:...R?T.V{.+.(.M...*..9V..[.F.Dn.4sl..0=h._...J.y._wJn7u..J..>....Q...B..*V+...LA=..T....WC.....=U\...,.r.F9P.PG+..E..,.2.R....$Wu..}....M...d3..(....CFga..at..x..i.X..=.A.Q.7..c..A...D...m%...3F....^.`.B2.....I2...M.0.....L..g_S]];..m.,.5E..."..N<..B/.ch..>...0v.^.....P...1..$..J).N.B4...\...y...&.B.....v.!..\....#.].4B.o...C{!Q.p...A..5.a.w.2.9.,..YU...P.o....Bh.. .Hmc/...f...Ah.1.~#.!..Fh|....<....X.@v.W.Sh$..6u...DhL6.9."4'..xK<...../....<. L... ..).`1..d.DQn7.1...O...(`;.....j.+..:mIE .q....x....QX. L...B=..p.&....`..0.....Ew.:....E.....mZ#4.#...y...c..y.E.....H..Q.a...J.!....}.b..!M.a…%.;m..P.G?V#...\.c}J]:...X.i}4....8.....3.]....EtDh@..{.p.....6s.c..!.....x.8.;..L[.2....ziG.~.i7../#.O0...q...=..zw'.d{....".1..v..EWF...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-vaccine-bg-light-purple-772x772-2021-03-04[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=5, orientation=upper-left, xresolution=74, yresolution=82, resolutionunit=1], baseline, precision 8, 772x772, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-vaccine-bg-light-purple-772x772-2021-03-04[1].jpg	
Size (bytes):	71741
Entropy (8bit):	7.96207803306499
Encrypted:	false
SSDEEP:	1536:heH9zLFMbrOSUDMV3oWI5ew6+ofWN8MS1Szw+GVKl:wH8UG3cew6+HwBVK
MD5:	FB5DFB12F7592D96B116A5B8A08DE140
SHA1:	23F4D7E7C1EE992CDD7B620DD7596F4BE0021AAF
SHA-256:	24062561765546D2361E615F15D242EFF88137C89BDC0FF6E71731CCF619DC82
SHA-512:	F738BFE8781D5300CA2A79092C89F00DC1947EEC9DC12185C07DE5CC42F49055AC14CC4192D9F706380A74B96DC149D237F16C0C8E2973A349E1BA806BE9745
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2021-03/co-covid-vaccine-bg-light-purple-772x772-2021-03-04.jpg
Preview:	......JFIF............bExif..MM.*...........................J..........R.(...C.................................%...#... , #&')*)..-0-(0%()(...C..........(...(((((((((((((((((((((((((((((((((((((((((((((((((..........".....................................O........................!1"AQ..2aq.B....#R...3b...$CrS....%4..c...6s.&5DT...1A!Q............?.... ....]D.S.<.2&u....b*.....,r.w.PD..vR).Ji......#...['.O..+b...\.G.N.g....T....6....U.v.9z.K.\z....3.:...K,.k...R ..,?+...m....t.6Y....c.......%.%...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\co-covid-vaccine-page-intro-tall-704x1050-2020-12-24[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, 704x1050, frames 3
Category:	downloaded
Size (bytes):	161050
Entropy (8bit):	7.94871675359959
Encrypted:	false
SSDEEP:	3072:bUnhvJHJ2qPGy0Vm0KRFiM16F4M0dg7p1X7faexTjpo+PFMN5FwW:AnhRHINaWM16FXsM1zPxRoOMuW
MD5:	120B3F99A74158F0128A3922B9E7CB08
SHA1:	17DAE2F38E08B0DE5336CADE57EA7B72D916E1D4
SHA-256:	4A1544507FF1E0A23A5D401CA13AD666748F15402D203BDB8E3EE6DAE4B4047D
SHA-512:	EB1C845358DBF652BE5C1AEF47DA578526901F7BCEBBE7337F77D1D31A6313D3C81E8B31759F87B1AC5FD3BA6B2A5FB0A06E76FC095EBB631EA4504945C3E9 6D
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-vaccine-page-intro-tall-704x1050-2020-12-24.jpg
Preview:	......JFIF.....d.d......Ducky.......d......Adobe.d... ....!.1..AQ.a"q.....2..B...R#..b3..r..S$45..C%...cs.Dd6..7....TtEeu&.8....................!.1.Aa..Qq...."2......B#3..Rb..r..$..S4%..Ccs.T56...........?..2.......P ..@(......P..@(......P..@(......P..@(......P..@(......P..@(......P..@(......P..@(......P..@(..........8...dd;.g5.@.f........d`W..?..>v..5J.....X..)..P.L.C...B....E^.+.1m..'.n..;'..m...........J.L8..t. l.1q..&...rm.\.\!....!..9s``;.wY...A^....Z.+.....r.L,f\..dG.s...z9....+,.4...u.)...8.+.$l...j.l....p.[r..-......-_.+G...8......Yl....L...~...F.%."...N.v.,..$.8/..q..`. ..Ms2.$..9.$..p.B....^..r..c..M..A.!r..r'. .>8.lNpYb?VW......;}V..l..d\..'.....v...-.Y.*..ij...W..*.6..(.x..y..?.I\2...U..r..k.....Z..%..c_..4$9.C...D..l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\component---src-pages-vaccine-locations-index-js-5583fc738e553f2ae798[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	5054
Entropy (8bit):	5.156297314551839
Encrypted:	false
SSDEEP:	48:lD58jX9pEF0uqgMEXRzU3J83fqDsdGV5sSCCsV1Y9q3Vk7EYf2jdy3YFBAmUvicY:wifqDMGjsSz8Gq3Vk7LI7XUv4nUCbqk
MD5:	028F5D96F2E0C40C886912D324FDA960
SHA1:	263AEE0B07DBA65AAE1D7846A5774B5D0E7DB353
SHA-256:	5E87C1827E16B519451E1D82F600EA35B5F6EB616986F4F60EB4960493F83328
SHA-512:	88E2DECEBBBE3E2C2B6E4B36AC74AB3F653A14DCD874B3909D7E3147EB8AC2314C68EEF2B43D0057F9DDB5D9FBD401691358792C6730927F89FEC76D048766 E0
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/component---src-pages-vaccine-locations-index-js-5583fc738e553f2ae798.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[7],{"4pj9":function(e,a,t){"use strict";t.r(a);var n=t("q1tI"),l=t.n(n),r=t("gd65");a.default=function(){return l.a.c reateElement(r.a,{lang:"en"},l.a.createElement(l.a.Fragment,null,l.a.createElement("h2",{className:"ontario-lead-statement ontario-margin-top-32-! ontario-margin-bottom-32-!"},"Find your closest pharmacy to get the AstraZeneca COVID-19 vaccine if you are age 55 or older."),l.a.createElement("p",null,"Starting April 1, 2021, select pharmac ies across the province are booking appointments for AstraZeneca COVID-19 vaccines for eligible people ages 55 or older in 2021."),l.a.createElement("p",null,"You must have an appointment to get vaccinated at a participating pharmacy. Contact a participating pharmacy near you to book an appointment."),l.a.createElement("h3",null ,"Before you book"),l.a.createElement("p",null,"You must:"),l.a.createElement("ul",null,l.a.createElement("li",null,"be 55 years old or older in 2021"),l.a.crea

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\component.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	53285

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\component.min[1].js	
Entropy (8bit):	5.169887911708994
Encrypted:	false
SSDEEP:	768:sy+ta8OMxBTedmgGhnAuhxrZJCGGVbmY2O4BfwPZnuj8VddPm0PjXKYhAClg:LqlRoZjddOiXKYhACO
MD5:	31F620E726F456732B9A64BBE2BE7A40
SHA1:	517BE2F6D5C0537E1B1485803A280F232683D709
SHA-256:	5083CBFC6D40E35C5A2D800E0B1B0A0F624AF5E842D23C0985B4225011A26421
SHA-512:	209977E8F2F413322C62F85F0DA680D821D111DB59DFE90EEFB19E40DC12B39B18EB29C04F31ED6DCF7F7CD18EA1BCF780C43249440E20B992D46884CD9967
Malicious:	false
Preview:	"use strict";angular.module("onesite.component.directives",[]).directive("onesiteHeader",["$filter","$timeout","languageService","routeService","redirectService",function (e,n,i,o,a){var l={en:"page/government-ontario",fr:"fr/page/gouvernement-de-lontario"};return{scope:{contentNode:"=",search:"=",update:"="},restrict:"E",replace:!0,transc lude:!0,templateUrl:"/core_modules/component/partials/onesiteHeader.html",link:function(r,t){r.pathLogoHeader="/img/logo-ontario@2x.png",r.pathLogoPrint="/img/o ntario@2x-print.png",o.regulateRedirect(t),r.altLang=i.alternativeLanguage(r.contentNode.lang),r.update.header=function(e){r.altLang=i.alternativeLanguage(e.lan g),angular.isFunction(r.update.taxonomies)&&r.update.taxonomies(e.taxonomies),function(){var t=this;n(function(){t.click();var e=t.find("p.show-for-sr")[0];e&&angular.isF unction(e.focus)&&e.focus()},0,!1)}.call(t)},r.headerlogoAliasCollection=l,r.aliasToPath=a.aliasToPath,r.changeLangOnly=function(e,t,n){return function(e,t,n){var r=this;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\covidappbanner_240x182px[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	7664
Entropy (8bit):	4.174995504400109
Encrypted:	false
SSDEEP:	96:CxrHMjARBOhBILB/CUHoSxKY6/8VXZYKd6UWzsMIo94VRoMfvODJkH:6OUHokPXZYKcUOpIWsRoMfvOlkH
MD5:	B34EA8366EE6FBA1AAF196A6C002C57B
SHA1:	46352610A66407C8D4A51B9AAE5F9AE42F578170
SHA-256:	C3E2A241BC53BDDE45287BF91DE137F9DA0E768ADFCC22219EF980206EE8F30E
SHA-512:	80611C744F1C608E69FA5DA4CDD78896D0DE523E1AE1590C5E4EF782D7470F916E7392FD8201739D7F8EB69939E94D161A5DE1C7F698E2585175478778116176
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2021-02/covidappbanner_240x182px.svg
Preview:	<svg width="195" height="190" viewBox="0 0 195 190" fill="none" xmlns="http://www.w3.org/2000/svg">.<g clip-path="url(#clip0)">.<rect x="11.1429" y="39.1176" wi dth="66.8571" height="114.559" fill="white"/>.<path d="M65.834 10.0745H55.0441H41.2831H23.1435C17.514 10.0745 12.3536 12.4357 8.60064 16.2137C4.84763 19.9917 2.65838 25.3438 2.502 31.0107V49.1135L1.251 49.9005C0.938252 50.0579 0.625501 50.5302 0.312751 50.845C0.156375 51.1599 0 51.6321 0 52.1043V56. 0397C0 56.512 0.156375 56.9842 0.312751 57.299C0.469126 57.6139 0.781877 57.9287 1.251 58.2435L2.502 59.0306V67.2162L1.251 68.0033C0.938252 68.1607 0. 625501 68.6329 0.312751 68.9478C0.156375 69.2626 0 69.7348 0 70.2071V74.1424C0 74.6147 0.156375 75.0869 0.312751 75.4018C0.469126 75.7166 0.781877 76. 0314 1.251 76.3463L2.502 77.1333L2.34563 162.137C2.34563 167.962 4.69126 173.157 8.28789 177.092C12.0409 180.87 17.0449 183.231 22.8308 183.231H65.521 3C68.9615 183.231 72.4018 182.287 75.2165 180.712C78.0313 179.138 80.5333 176.777 82.4098

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\details.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text
Category:	downloaded
Size (bytes):	127
Entropy (8bit):	4.461489457578185
Encrypted:	false
SSDEEP:	3:UV9iSKVaJMJMvnFlHg1AoA7PC0lJYuN+KVuBgRllHkw/9V00eK:U/YJuH7llJzNzlHkw/3TeK
MD5:	A3D07AF30E7DC57B0647E417E27AC938
SHA1:	2EEB4A7E1DC2E86A6A0664BD6FC2FE7BA3009BAA
SHA-256:	F31746CBB75773ACC9358471805E24D2F80184A9686F2E4DFBF57530C3A583C0
SHA-512:	BF68F4D01D054F05E1B116CEC941C2B77662C8E950BC0961D256A88D55C39A9627BAE4355A3FDED12DCC4B155A8C89A232FFDF60D18EA7FE62114DB78053A0 3
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/details.module.css?qrgttk
Preview:	/**. * @file. * Collapsible details.. *. * @see collapse.js. */...js details:not([open]) .details-wrapper {. display: none;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\drupalSettingsLoader[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	519
Entropy (8bit):	5.161310412773144
Encrypted:	false
SSDEEP:	6:Uwq4VCi+5cGMKN0fGLB0PQwPoj/LR7nadOXCuhtdz2mySYuhtdz2myGy5mpq3Wja:UkaFN0fw0PKjNWdAbZbomvNXmirN5fgn
MD5:	49DBE4BAC61E9CA48A5951BCBE0D03E9
SHA1:	020EFEBBF1F6E97D39DDCDDC5262F34C1DB7807F
SHA-256:	5F8F69EC521F7998AF455985A8EDE6D8DCF3527B43795FE3D26F1F1B57A5A554

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\drupalSettingsLoader[1].js	
SHA-512:	C184CC753599864802BC90582698CF0D66E2E782D34ACD2E1EE26CA3F03BBA8C9D4FB2DB40E9B13FE0568DD9ABFE147EDC8A86FDD1B8EB5483AFA867C039C75
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/misc/drupalSettingsLoader.js?v=8.9.13
Preview:	/**.* DO NOT EDIT THIS FILE..* See the following change record for more information,.* https://www.drupal.org/node/2815083.* @preserve.**/..(function () {. var settingsElement = document.querySelector('head > script[type="application/json"][data-drupal-selector="drupal-settings-json"], body > script[type="application/json"][data-drupal-selector="drupal-settings-json"]');.. window.drupalSettings = {};.. if (settingsElement !== null) {. window.drupalSettings = JSON.parse(settingsElement.text Content);. }.})();

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\effect-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	16816
Entropy (8bit):	5.357184455434572
Encrypted:	false
SSDEEP:	192:5vTeXBVAInxCBhjX2sjhlStCsbiXcWzNvwu2LqQ6uZWs74:5vKXBVAWxC3jmQCCsbQ5IdGs74
MD5:	86F1E6B37CFAF2786F58619B88778717
SHA1:	96975EB34AA586AD9FA48C6F994A4AD2D87A0C60
SHA-256:	252B076ABB37EC8CEE93AA75EE776C45E01515D8361A9BAE2341EDFE02D875F7
SHA-512:	756F0D67A468BA5DAF96420DCFE493383A26833A392336180C1D2194190E995C409AD778A87429E0C84C41F77968852A4C0B0A239B473EF77A9BDEF03BDB1891
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/assets/vendor/jquery.ui/ui/effect-min.js?v=1.12.1
Preview:	/*! jQuery UI - v1.12.1 - 2017-03-31.* http://jqueryui.com.* Copyright jQuery Foundation and other contributors; Licensed */.!function(a){"function"==typeof define&&defi ne.amd?define(["jquery","./version"],a):a(jQuery)}(function(a){var b="ui-effects-",c="ui-effects-style",d="ui-effects-animated",e=a;return a.effects={effect:{}},function(a,b){funct ion c(a,b,c){var d=l[b.type]||{};return null==a?c||!b.def?null:b.def:(a=d.floor?~~a:parseFloat(a),isNaN(a)?b.def:d.mod?(a+d.mod)%d.mod:0>a?0:d.max<a?d.max:a)}function d(b){var c=j(),d=c._rgba=[];return b=b.toLowerCase(),o(i,function(a,e){var f,g=e.re.exec(b),h=g&&e.parse(g),i=e.space||"rgba";if(h)return f=c[i](h),c[k[i].cache]=f[k[i].cach e],d=c._rgba=f._rgba,!1}),d.length?("0,0,0,0"===d.join()&&a.extend(d,f.transparent),c):f[b]}function e(a,b,c){return c=(c+1)%1,6*c<1?a+(b-a)*c*6:2*c<1?b:3*c<2?a+(b-a)* (2/3-c)*6:a}var f,g="backgroundColor borderBottomColor borderLeftColor borderRightColor borderTopColor color columnRuleColor outlineColor textD

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1336
Entropy (8bit):	7.776296896714416
Encrypted:	false
SSDEEP:	24:2ELyu9N214knvN7rkS5PA3uEJHg1zTX6M4iQ7VfEVWnGrgbmVs/1:2Ee/ik17bZA3uEJA1zTXH4xEVWnMgya1
MD5:	BB3DEBD3FE12736EE94C99D20D42FFD3
SHA1:	C2C87994245FDAE0B3093B80614B202F90099D27
SHA-256:	EE877BF7E33D22CD354278EDBA7FB9DADCAAB3FABEA37CD8E3AFCA2FD824503D
SHA-512:	02AE48449B746503D22940E24F2796E44E14D52870B82C36DC3F7F902EBBA3D012DF9605BFB7083ABE1212452DEB82D89FFAF9220057A8BEDC2662ABC19D37D
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/c19-book-vaccine-assets/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .szz.....pHYs.....~.....IDATX.W[(.Y..{....f\2n..7..(3[<.... .h<)e.<y..@.x@).9..a.t..(N....1..Y.j}.....|....}.o}.f3&..;....g.1.m.G...d..a.....k.3M.....Vb&.-`4. 7.{..t..%.D...r.3..Ka.V.U.....wK...K..ma....B.$7...aW....l.Y.O.BoU!<..;...n.....p...7b(...gH..{..j.P....%.=<<4.b..5..$.....).~~~.....t:!66Vc.#00.....BP<..".....r.....'P .....3.....v....#.....EHKK.1aH..I.,.s6.....`kk....auu....uB.....666`nn.....z...2r.....>(@..{....*....kHf.....\.....{....cn.$.[.....S,Pl.C...1..&.....oFw.....M.....4'. ....&j....f}}}|.....1:.....v.!++...../.,.#....p1H....l.b.A7-JHH...s~...8xzz..8.....&f...iff.....I..[.q.....i.....-88."##u....4.GGG....j/...7.....z.....{rr..Abb"...r. ...IM`....T.B&..fZ.H.,(.9.....4....)....b.....!!...`}}.3hmm.....,PH....+..1pj.....Cjii..c@bL .....N.R..SWLLLp&...:.0...S..0.....?I.X.BWW.V.e&.l.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\hidden.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1359
Entropy (8bit):	4.625282671725046
Encrypted:	false
SSDEEP:	24:swlJfLWtQ6fATZXTSVEdOWcv3A5NxVKqMmd4lMO+GWNA3sEdy66gmNen:swlJfKt1fA1XWud6v3INxVWmClnHjdmI
MD5:	A40F4B74BED5FC5D74DF3DA6FDCAEE26
SHA1:	2B8F20E668877C8BB4203CE1506753570523734C
SHA-256:	144C2B996574A2F16003848858DE86DC5AD3486FB4FE14A5D5A79D134086E763
SHA-512:	9AA15667D962B0F618DE9C3B080059B49749C0440DAF47E6E1A267F2EE4CE8C3990BF6EF2820E55A29B7419C6625C84DE99439FDAFF1798BB88B30C04C98A18
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/hidden.module.css?qrgttk

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\hidden.module[1].css	
Preview:	/**. * @file. * Utility classes to hide elements in different ways.. */../**. * Hide elements from all users.. *. * Used for elements which should not be immediately displayed to any user. An. * example would be collapsible details that will be expanded with a click. * from a user. The effect of this class can be toggled with the jQuery show(). * and hide() functions.. */..hidden {. display: none;.}../**. * Hide elements visually, but keep them available for screen readers.. *. * Used for information required for screen rea der users to understand and use. * the site where visual display is undesirable. Information provided in this. * manner should be kept concise, to avoid unnecessary burden on the user.. * "!important" is used to prevent unintentional overrides.. */..visually-hidden {. position: absolute !important;. overflow: hidden;. clip: rect(1px, 1px, 1px, 1px);. width: 1px;. height: 1px;. word-wrap: normal;.}../**. * The .focusable class extends the .visually-hidden class

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\icon-alert-warning-white[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	205
Entropy (8bit):	4.780609430792005
Encrypted:	false
SSDEEP:	6:tI9mc4slzXdhyKjUhOqNsN6JASqrNPXA38:t4BdEKjUvGVLrBwM
MD5:	15B5EB20A77A2A1C3CA4CF355CFD49E9
SHA1:	D5F5C8F78E0450E145B7634A1AF79B51C406788E
SHA-256:	F9C8F16E9D72FDBF6555471BCB15D747C4802491D18938726E7B571CD9DDBD27
SHA-512:	916DE3E70C182BFFEF206547A22C140E10EBD3A76D4BBF7CF6ED36BF72569BD78A22EC8DEA00ADBD2CA282666C1A418F6D0A366BDBA043AB76F4BD7CD1A63 663
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/assets/icon-alert-warning-white.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" fill="none"><path d="M1 21h22L12 2 1 21zm12-3h-2v-2h2v2zm0-4h-2v-4h2v4z" fill="#fff"/><path d="M1 1 10h2v4h-2zm0 6h2v2h-2z" fill="#000"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ideas-to-combat-corona-virus[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	5107
Entropy (8bit):	4.8990878582239095
Encrypted:	false
SSDEEP:	96:bZ692TdGO6Tg6YtTWMDcKYSB7ejHNIMFoc+bQVM:bZuTTg6+yMDcKYBN9oc+k6
MD5:	3C1B5D98BF0309FC7F929CCF1EF87F66
SHA1:	E8D338AC254F7AF80EA79F84F6E7F30B4EE9B840
SHA-256:	15E131C58CEE40EAE3D7F1D2BD13E41C9E27F0A55ABCCC19036CCCFB4458948A
SHA-512:	EA325BA276A74F50B8C4530D50000C016DB7BEB1A892F4B76964238C15CFE9CDEE7C9C806B65CAA3FE39FEE939AA3110FB16008C0B7095F210EBE583FD43F8E E
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2021-03/ideas-to-combat-corona-virus.svg
Preview:	<svg width="359" height="136" viewBox="0 0 359 136" fill="none" xmlns="http://www.w3.org/2000/svg">.<g clip-path="url(#clip0)">.<path d="M27.3462 72.3929C27.3462 72.3929 -15.7078 72.3117 10.4176 60.6291C20.8352 56.0047 40.6937 52.5161 60.7964 49.9199" stroke="black" stroke-width="5" stroke-miterlimit="10" stroke-lineca p="round" stroke-linejoin="round"/>.<path d="M101.734 72.3929C101.734 72.3929 144.788 72.3117 118.663 60.6291C108.245 56.0047 88.3867 52.5161 68.2841 49.9199" stroke="black" stroke-width="5" stroke-miterlimit="10" stroke-linecap="round" stroke-linejoin="round"/>.<path d="M101.734 92.0261C101.734 92.0261 144.788 92.1073 118.663 103.79C108.245 108.414 88.3867 111.903 68.2841 114.499" stroke="black" stroke-width="5" stroke-miterlimit="10" stroke-linecap="round" stroke-linejoin="round"/>.<path d="M27.3462 92.0261C27.3462 92.0261 -15.7078 92.1073 10.4176 103.79C20.8352 108.414 40.6937 111.903 60.7964 114.499" stroke="black" stroke-width="5" stroke-miterlimit="10" stroke-lineca

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\item-list.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	285
Entropy (8bit):	4.505137324364592
Encrypted:	false
SSDEEP:	6:UuAVtvA7MmDGjudGj0XQKLt0Gj1IiGHt0GjjVwJ6Ivt0GjHCwJ6EAv:UumvyME/X1iiG9wY9wYPv
MD5:	8C9B6BEC7C9EBFB5351D874B356A38D1
SHA1:	87B4A1A6DB3220CF73F29F80DA1896605B396D74
SHA-256:	5251EC9A6D7F9CC54B205363D70EB38BF67517F8E02B3AE04E85C9CF5F908228
SHA-512:	4896DB2F629D7A2451B0A4A4BF722CA615BCC90F25D18FFF0B26486B51D0C26932294C756AAA6472B40FBA45C069F56CA998DB094CE6582419FDDA83098DD5E
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/item-list.module.css?qrgttk
Preview:	/**. * @file. * Styles for item list.. */...item-list__comma-list,..item-list__comma-list li {. display: inline;.}..item-list__comma-list {. margin: 0;. padding: 0;.}..item-list__comma-list li:after {. content: ", ";.}..item-list__comma-list li:last-child:after {. content: "";.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\js.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text
Category:	downloaded
Size (bytes):	402
Entropy (8bit):	4.560472448460017
Encrypted:	false
SSDEEP:	6:UqEIpVUIkj0EJt/c68eONnP6pjedLeMWuwRsvu1fev/Tez90EJtlQF6D1eONKDdp:UgLkr/vgOeE1RsVv/TuWKWXTEXjfK
MD5:	AC3A25C1A721FF659377D3B401A42F7D
SHA1:	0E8A6AFF9EECED7B68EEEE301A1594294E24F337
SHA-256:	132298C08776FAEA963092E83B7C30712BDE095C62530BD3A613322987C4663E
SHA-512:	0159995C7AA47E0DEBB1AA1C29BCC9F0EFED0277C0BDC67ACF501E07510A9C98D0EDF2EBEE7A5C1F136F136529F396EC23030A577451BA19945337309EBECE7A
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/js.module.css?qrgttk
Preview:	/**. * @file. * Utility classes to assist with Javascript functionality.. */../**. * For anything you want to hide on page load when JS is enabled, so. * that you can use the JS to control visibility and avoid flicker.. */..js .js-hide {. display: none;.}../**. * For anything you want to show on page load only when JS is enabled.. */..js-show {. display: none;.}..js .js-show {. display: block;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\mobile-chevron-right[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	191
Entropy (8bit):	5.03255814455634
Encrypted:	false
SSDEEP:	3:tRBRNqAR+4FcvW/D7SLvDmJS4RKb58ZSFuHEX7UL30eXFPQ8XX5CKOAwRAHFWFAy:tnrqlW/Dumc4slvIY7y0w3XX5lkAHw6y
MD5:	DB64144AF6DBB1EAF2ABE0E6272B2EFE
SHA1:	A0B6A72117F230E0515F97FD49DE956395F0179E
SHA-256:	6671A41C7316A80D630EF62A72BFD0D67EFD252F2D71D57412A016D7520758A6
SHA-512:	F0550C5AAE74BE35B075DB37C0196211976F3AF3B3176A012569801DA12039477213AD78E3D9C8C8FFA5E83558E9C6DF984BDC680F059B8EFFDC4BD31FD9907
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/images/mobile-chevron-right.svg
Preview:	<svg width="35" height="36" viewBox="0 0 35 36" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M16 33.3359L31.4485 17.6725L15.7851 2.22398" stroke="white" stroke-width="5"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\nowrap.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	96
Entropy (8bit):	4.428008466328818
Encrypted:	false
SSDEEP:	3:UV90vEW5jRP8mqy7LJMm/DPxJUH:UqE4znZ/rTi
MD5:	02DE344715C6EC9A3745FF2186D32B9D
SHA1:	F2F39B2CA9E9397B53AB76A7B3938EDC138A24CF
SHA-256:	4A4FA2A793D87C88F1509F370DBC40B6DEEC2188B6A918F92365F873B7BC566D
SHA-512:	F4146E324FCB514AD4658FF912B8DB937B61F5C4F438BBB9F136709CFD17EECCD2B91FE7B8BFDA3F6D0CA44DCC3E65C6931EE8FC464A2316919146AE1A3C19D8
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/nowrap.module.css?qrgttk
Preview:	/**. * @file. * Utility class to prevent text wrapping.. */...nowrap {. white-space: nowrap;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-angular-foundation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12118
Entropy (8bit):	5.139938442037991
Encrypted:	false
SSDEEP:	192:3NS2OSk1uTnbLykBo1kBo4OAdqzPKThxbMgfkBhcqj+/ggF:3kTSk8H2rNBAOPKTfMgsgggF
MD5:	A428F97770D2F8A1B1A002108F94EF4A
SHA1:	A2A5474D67225963FF8461867EC939FD5BF6949F
SHA-256:	BF9AC2D327C40986A4837C865C29A8F08B37107A94B1F1C4DB4489FF2CB6480B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-angular-foundation.min[1].js	
SHA-512:	A59DD0018A893AC8B7CC27259B0599E493AE605ABFC68E76A509F5A0D1B314E0BA150F66F83BCADE6B29382FD36682F4D70F5CB5AB4E15B70A26821FADAA16C
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-angular-foundation/onesite-angular-foundation.min.js
Preview:	"use strict";angular.module("onesite.angular.foundation",["onesite.angular.foundation.directives","onesite.angular.foundation.controllers","onesite.angular.foundation.services","onesite.angular.foundation.filters"]);."use strict";angular.module("onesite.angular.foundation.directives",[]).directive("onesiteAccordion",[function(){return{scope:!1,restrict:"A",replace:!0,transclude:!0,template:'<ul ng-transclude class="accordion"> ',controller:["$scope","$attrs",function(e,n){this.broadcast=function(){e.$broadcast("true"===n.oneOpen?"oneOpen":"multiOpen")}}]}}]).directive("onesiteAccordionGroup",["$compile","onesiteFoundationService","analyticsEventService","analyticsTypeaheadService",function(e,u,d,f){var a;return{scope:{heading:"@",isOpen:"@",toggleOpen:"@",templateUrl:"=",analytics:"=",data1:"@",data2:"@"},restrict:"A",replace:!0,require:"^onesiteAccordion",transclude:!0,templateUrl:(a=/^'(.*)'$/,function(e,n){var t=angular.isString(n.templateUrl)&&""!==n.templateUrl.trim()?n.templa

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-body.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3607
Entropy (8bit):	5.057955488770076
Encrypted:	false
SSDEEP:	48:TlJsFGIr0kZVPH4rRVF7GflXv+aEGU7/Jw1NbnW3AMCdvghtd2V9tOAYj2:Tlm3BGRG13U+jMAMCdohtd20vj2
MD5:	9BAC30FFB14C5F96B77117810CCB530A
SHA1:	E3599BF9EB70BAEB73BA0001395B5206CBCBC32D
SHA-256:	40AA79EDB0A65748F49A0089EA387BA2DD987E205BB9B230956A0BDF4EF2B9B1
SHA-512:	6BBCC8BE97091C7A8508C751E8E45B49319BF09AB978E4DDB2FB5732947909B3A025C759B5205F26E5DCC3004CD7C020C3205E02DB1EEF6CA0994857FBD306B
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-body/onesite-body.min.js
Preview:	"use strict";angular.module("onesite.body",["onesite.body.services","onesite.body.directives"]);."use strict";angular.module("onesite.body.services",[]).factory("bodyService",["componentApiService","dataBindingService","apiEndpointConfig","redirectService","lazyloaderFactory","lazyloadFiles","callbackService","apiKeys","$q","$location",function(l,s,e,a,t,n,r,i,o,u){var c={};r.setupGoogleMapApiCallback();var d={onesiteGooglemap:{regexp:/<onesite-google-map (.*=.*?)>/,handler:function(){var e=o.defer();return function(){var e=o.defer();if(window.loadGoogleMapApi(!1))e.resolve();else{var a=document.createElement("script");a.type="text/javascript",a.src="https://maps.googleapis.com/maps/api/js?v=3&key="+i.googleMaps+"&libraries=places&callback=loadGoogleMapApi&region=CA",$("head").append(a),window.loadGoogleMapApi(e,"/vendor/google-markerwithlabel/src/markerwithlabel.js")}return e.promise}().then(function(){(function(){var e="onesite.google.map";return t.load(t.instantiate("module",e),{nam

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-contact-us.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	4213
Entropy (8bit):	5.0419075599097765
Encrypted:	false
SSDEEP:	96:KTfORuzFDubr04doJaveTCzll8Tt90Sh1:KjQyJD0M37
MD5:	2E45C11110BE0B34805211925E828627
SHA1:	473DDAE6DFEA23DB1B1866EAF15F29432BE38F9B
SHA-256:	9EEE3D778CD03BAD9DEA05343FD1DB44AE38D1802EB1D72B5F6B5F57F8E45C3D
SHA-512:	B097225C21F436CADD4C709FFE151A2F92F57D46AB784E3436D3A8F28D783EED0ADD60A5A3589805D777407284199D0033DF687A29EA3362DF6F166EA6166CE
Malicious:	false
Preview:	"use strict";angular.module("onesite.contact.us.services",[]).factory("contactUsService",["remoteStorageService","sessionService","dataBindingService","apiEndpointConfig","componentApiService","redirectService","$q","$parse",function(a,e,t,c,s,d,u,l){var r={};return r.getContactNode=function(r,n,e){var i="/"+c["onesite.app"].apiService,o=c["onesite.app"].apiServiceCrossDomain,a=u.defer();return function(e,t){var r="/"+c["onesite.app"].apiService,n=c["onesite.app"].apiServiceCrossDomain,i=u.defer();return s.getEntity({url:d.respectProtocol(t.useRelativeUrl?r:n+r)+"/url/"+e,method:"GET",withCredentials:t.withCredentials}).then(function(e){var t=angular.isArray(e)?l("und[0].id")({und:e}):e.id;t?i.resolve(t):i.reject()},function(){i.reject()}),i.promise}(e,n).then(function(t){if(angular.isString(t)&&""!==t.trim()){var e=encodeURIComponent(t);s.getEntity({url:d.respectProtocol(n.useRelativeUrl?i:o+i)+"/"+e+"?fields="+r,method:"GET",withCredentials:n.withCredentials}).then(function(e){a.reso

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-moment.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18921
Entropy (8bit):	5.1828626911292055
Encrypted:	false
SSDEEP:	384:Ak1AdDaYLsp6fL8Ra1p5OZBmf54OMpUgv8SfcBY2Q/VsOgEpK:OuZRcpHR4O+v8Sfcc/2TEpK
MD5:	F4C2C7DCE7F310308F3202F7672E0FBC
SHA1:	3B9A391C9B34E13A9323895F27E30C6C58D803C4
SHA-256:	F9D8A28DA9F0AF8B8BADA0B6CF7A09141E58302062FDA2FD047B2280B10567F5
SHA-512:	44BB499A1905FC467DBDD678598631C71E8E1B00A8680150BEBBDC6CDC85EEB1D932B75D9C0E9764353DF2AFE9918FBB850AEA60BA7675CFBCBAB45ACE0A1147
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-moment.min[1].js	
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-moment/onesite-moment.min.js
Preview:	"use strict";angular.module("onesite.moment",["onesite.moment.services","onesite.moment.controllers","onesite.moment.factories","onesite.moment.directives"]);."use strict ";angular.module("onesite.moment.controllers",[]).controller("OnesiteDateAddImpl",["stringService","timeService",function(i,u){var o=this;o.add=function(n,t,r,e){var a=i. strToDate(n);angular.isNumber(t)&&(a=u.addYear.call(a,t)),angular.isNumber(r)&&(a=u.addMonth.call(a,r)),angular.isNumber(e)&&(a=u.addDay.call(a,e)),o.date=a}}]) .controller("OnesiteDateSelectorImpl",["stringService","timeService",function(i,n){function c(n){return angular.isNumber(n)&&!isNaN(n)}var h=this;h.stringToInteger=functi on(n){var t=(n=angular.isString(n)?n.trim():null)&&""!==n?parseInt(n):null;return c(t)?t:null},h.daysInMonth=n.daysInMonth,h.monthCollection=i.monthCollection,h.dateExist s=function(n,t,r){return r<=h.daysInMonth(n,t)},h.updateModel=function(){var n=h.validateYear(h.year),t=h.validateMonth(h.month),r=h.validateDay(h.day),e=angula

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite-search.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	46362
Entropy (8bit):	5.079097575525367
Encrypted:	false
SSDEEP:	768:8aWN6+8H8Jaav94am51J829kaRbY85YEOHI5Y1Or4GbOnsQ+zcHmzn46SOtVO9Uo:rWNi39kah5n15y6bPQbp6TO9Us0qoFD6
MD5:	9565D9F801992F78AF690B0818F049CD
SHA1:	95DD71F0064D3D10F9D06B19FAF312DB5AD477BD
SHA-256:	5037C5517FB4B285AA35D13EF405625BDDC6D0DA4FC0DA8D1D027BB735973086
SHA-512:	BABEF137038286D66F6A546A3184594F3F2F347CC43938FD139DDE2435EC6F92904F0B7E986CF2025F880193839777E1337B81913E746E110265D5A03CB8C16D
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/onesite-search.min.js
Preview:	"use strict";angular.module("onesite.search",["onesite.search.services","onesite.search.factories","onesite.search.directives","onesite.search.controllers","mm.foundation "]);."use strict";angular.module("onesite.search.factories",[]).directive("onesiteSearch",[function(){return{restrict:"E",scope:{type:"@",lang:"@",title:"@",search:"=",in ternalTagList:"=",nodeId:"@",resultStatus:"="},replace:!1,template:['<onesite-search-impl ng-switch="type">',' ','<onesite-search-main ng-switch="subType">','<onesite-search-main-tag ng-switch-when="tag"></onesite-search-main-tag>','<onesite-search-main-external-tag ng-switch-when="externalTag"> </onesite-search-main-external-tag>',"<onesite-search-main-default ng-switch-default></onesite-search-main-default>","</onesite-search-main>"," ",'<onesite-search-gazette ng-switch-when="ontario-gazette"></onesite-search-gazette>','<onesite-search-land-registration ng-switch-when="land_registration_all">',"</onesite-search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteBreadcrumb[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	375
Entropy (8bit):	4.393870368051338
Encrypted:	false
SSDEEP:	6:G4dRWV63KlRjHUF21Q6AoWSEVjeFvvB1vivkL+nXNvvgY+je/EKAM4qv:G4/WV6KlRjHc3oWRVjanB1qrXNnd+a/H
MD5:	89C524074C61840A965E575AE45D8B0E
SHA1:	5DE067E7A4E8FDE9C4A08CFB16D533111EAF6B5D
SHA-256:	AA2A2EFEF33D1B542AA54E40B7A5404FD65432374F85115DBD9C05F06ADD2986
SHA-512:	EBD12E60F0444888A828F89F0069D4D1EC07CC34AB6881C671D8F80923B0AF35282FD0BB53F26A11638C7671C2D03780294DE3D13F98B6EF1665DB9D50D27CB
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/component/partials/onesiteBreadcrumb.html
Preview:	<ul class="breadcrumbs breadcrumbs-ul-no-padding" aria-label="breadcrumbs">. <li ng-repeat="crumb in breadcrumb" class="breadcrumbs-font-size">. . {{ crumb.name }}. . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteFootnotes[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	876
Entropy (8bit):	4.478318989033825
Encrypted:	false
SSDEEP:	12:mHHIqC3jlclqvQfawoTbaWju6RPvhXmIzDuqUwwBNr33d+LPqs6HiG7kQh0fYMR:mIJ3jl/wITZRPvNm0yLr33kT+HE45MR
MD5:	6217180C101F83B59264D9D7E28892CC
SHA1:	99A180CA8096917C551F4CE9EA3091DFABBF6A1D
SHA-256:	186BAB01224AF5776B1BAC4175F67B99CA966E9D3EF15090C1A69BD6B6AF7C7C
SHA-512:	5073BCC98B42195766A862BC890D8B9BFBDAB562A781D7F6BAF185106F2882143779758D339C1C4842674D40FFD18962EB462766FF05838E96A596B59F1E9F52
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/component/partials/onesiteFootnotes.html
Preview:	. . . <h2 class="h3">{{ 'Footnotes' | translate }}</h2>. <ul cl ass="footnotes">. <li ng-repeat="footnote in footnoteList". id="foot-{{ footnote.id }}">. {{ 'footnote' | translate }}. [{{ footnote.id }}]. . {{ 'Back to paragraph' | translate }}. ^. . . . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteSearch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text
Category:	downloaded
Size (bytes):	990
Entropy (8bit):	4.630884483312336
Encrypted:	false
SSDEEP:	24:Qyk2vEeAs78s7416W2iF5EMiyLX4C69YKFdyUM6F:ZEeAsF744xCuZOlWevh
MD5:	DDDBAE6448E24EC4A536374EEFF3185C
SHA1:	64667B5FD631CF48F2412A09642285566391717E
SHA-256:	2569F28379560234D7DF645CBE8936F997B3E9E6D77ED467BA17CC833614C876
SHA-512:	64445923963719812969699799EFC0E0F8C836B1DEAA497E531D6D0BADF368E79103CC03550B7ACBEFE71D14134B19DEE92B2DECED9DDA67F54803610D9BB9F 0
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/landRegistration/onesiteSearch.html
Preview:	<form name="landRegistrationForm". ng-submit=". onesiteSearchImpl.enableScreenReaderTotal = false;. init(true).then(focusOnSearchButton).then (enableScreenReaderTotal);. current.keyword = onesiteSearchImpl.filterHandler.query.keyword.model.input;. selected.result = [];. ". ng-init=". last= {};. selected = {. result: []. };. current = {. keyword: null. };. ". scroll-to-detail="true">.. <link rel="stylesheet" href=" /css/hideHeaderSearch.css">.. Search Input -->. . <div class="small-12 medium-8 medium-push-4 end columns". ng-include="'/onesi te_modules/onesite-search/partials/landRegistration/searchInput.html'">. . .. Filters, results, related links -->. <div class="row main-content". ng-incl ude="'/onesite_modules/onesite-search/partials/landRegistration/filters/control.html'">. ..</form>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteSearch[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text
Category:	downloaded
Size (bytes):	615
Entropy (8bit):	4.49011483029449
Encrypted:	false
SSDEEP:	12:5EDNpc37vpC/uHIqC1iF9rc9HvTSuHIqCkFhs+clwgB:e0+J1iF2xT0JkFhf2wS
MD5:	EAAFFC219089C0001EABBD74D2D81CFC
SHA1:	3639184610DB0A35ABE088C0526FF69B3A108913
SHA-256:	8E10F5009F4C90622399F62425FD80F368FD182B60038CE8248C3EC7F33BF338
SHA-512:	92D1D7A6D147C5DD41CB3185E9117E6B92ABC9D74211EE830B64A870C8A473E09B031BC707290336E62775F0868C60A927BCCB605AD852D1752D1555E9C815F
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/orderInCouncil/onesiteSearch.html
Preview:	<div class="row". ng-init=". last = {};. selected = {. result: []. };. current = {. keyword: null. };. ". scroll-to-detail="true">.. Search Filter -->. <div class="small-12 medium-12 large-4 columns". ng-include="'/onesite_modules/onesite-search/partials/orderInCouncil/control.html'">. . . Result List View -->. <div class="small-12 medium-12 large-8 columns". ng-hide="selected.result[0]". ng-include="'/onesite_modules/onesite-sear ch/partials/orderInCouncil/results.html'">. ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteSearch[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	1737
Entropy (8bit):	4.7896091906288865
Encrypted:	false
SSDEEP:	48:DvuYV79bsFypmy1dsSAIF25OqxTDr6flpCX6dLH64:DrNswpmy1dJuOOTDr6flpD3
MD5:	6D56B4B349496CFF5EAE548C9F2CBD04
SHA1:	8380311034E856AEDC0E7357D450F5076F841152
SHA-256:	85AFC2E3CAA73BF31D45B4F7E3ADBF2DDDB09B61EB022E6D564148F5E208CD74
SHA-512:	D6A5E6705D62EE7FFB8594301F5086ECAB3EB4833FCEE1E1C0F8FDECEF34639870F07DD81FA14E997FC3FACA4B6611DAFF9A4DDAD7A558918C7DD056F9541 64
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/faqs/onesiteSearch.html
Preview:	<div ng-switch="onesiteSearchImpl.lang". ng-show="onesiteSearchImpl.total > 0">. . . {{ 'Frequently asked questions' | translate }}. .. <div onesite-accordion. class="faq h4". ng-init="last={}">.. TODO: accessibility -->. <div ng-repeat="paginate in onesiteSearchImpl.pagination | limitTo: onesiteSearchI mpl.pageIdx + 1". ng-init="$last ? (last.paginate = paginate) && (last.remaining = onesiteSearchImpl.total - paginate.idx * onesiteSearchImpl.config.pageSize) : null". aria-hidden="{{ !$last }}">. <div onesite-accordion-group. heading="{{ ::faq.title | html }}". is-open="false". toggle-open="true". analytics=" {category: 'faq', event: null, label: faq.title}". ng-repeat="faq in (onesiteSearchImpl.resultList | slice:paginate.fromIdx: paginate.toIdx)">. <compile-html htm l="'::faq.content". category="faq">. </compile-html>. . <

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteTaxonomies[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesiteTaxonomies[1].htm	
Size (bytes):	583
Entropy (8bit):	4.565084925266924
Encrypted:	false
SSDEEP:	12:xZ94poJ2q+W/jftNEG0MAyguNhA5LlBN4trTo+QfNPd+Gun/CTfQo:xdJ2PWLftJthwL4trUtflkZI
MD5:	65CC91DF803A37DAD0C9E92C3E1AE3F2
SHA1:	180937AA316F515034DD3F579B8075CE2D5C5135
SHA-256:	CA370086F2C8F70B93FA5C36D0C928374E40C7A3E34F6E99D007F71ECCDC567C
SHA-512:	1B2474D84B29C01E514C05B72B84D838361316F4A8B5B6D7BF2148563D6345E65FED576F26BA15E47EB28DF84DA924180A504008960B994261B3028D98CE773A
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/component/partials/onesiteTaxonomies.html
Preview:	. <h2 class="h4" id="menu-jump" ng-show="vocabularyList[0]">. {{ 'Topics' | translate }}. </h2>. <nav role="navigation" aria-label="{{ 'Primary navigation' | translate }}">. <ul class="no-bullet">. <li ng-repeat="vocabulary in vocabularyList">. . {{ ::vocabulary.name }}. . . . </nav>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\onesite[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 48360, version 1.0
Category:	downloaded
Size (bytes):	48360
Entropy (8bit):	6.38943268154998
Encrypted:	false
SSDEEP:	768:z0Zqlr9O272i5zdZVWIE1aFvtZYUKXylaqR2akcPYec87o5kVYTDF3VGVpvpeIBP:z0Zqlr9/dzHVWIvtWUKXQR2akcPYeZ71
MD5:	C3A096A96DCD188F89A38E4156BC099C
SHA1:	4369F0CC5C86B33799DB72254FD842601E8295EC
SHA-256:	B050C96C1880A23F6FDC8CC513CDD646029872488A0A0A612CADBD2EF549DAD7
SHA-512:	7E89D167AF1F28115BB9D6149B74F2CA243553C2AA5A33B0A3893A69DC18023E3F150548081C596CA6F6AD0513A4D68E79650E7B92787E16CFCA78B7E5B2B32A
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/fonts/onesite.woff?2lmqj5
Preview:	wOFF.....OS/2.....`...`....cmap...h...T...T.V.Mgasp.....glyf.....<...<..\.head.....6...6"..1hhea...8...$...$....hmtx...\...,...,\..loca.....maxp... ... ...name...@.....P..post..... ... .3.....@.....@...@..... .....8..... ....79.....79.....79.....@.....%...#".....3!26764'%#535#.3...J.....J.....I.....R.....".....". .@.....%...I.w.5.?.P.|....747635476?.676;.54763!2.....+. ...#"'&5#...#"'&5#"'&5.35#.....327654'&#".....;.....;.276=.3276=.4'&+.54'&+."....#".....327654'&#"..%.....q....\.....n++<=++.++<=++I...m.[..p..I.....%.....m..... .....m.....q.....n...<++++<<++++<.....o.....n.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ontario-a11y[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2276
Entropy (8bit):	4.842280177369027
Encrypted:	false
SSDEEP:	48:Z5Ur6H64sY4Y59QTGb2IMfY6rx7fU83JOdMCKQwjJD:Z51zQ6MfY+Q83J0nKR5
MD5:	587E5E0F1229A2F93D642B87E7F71AF5
SHA1:	F1DB88F7ABA4F1ED5BB5EC67C147A14B9EE994E2
SHA-256:	79CA829DA1BA9E0623352EA06C78BA00E7EF528F312A80BEB2B4281F1FFC17DE
SHA-512:	E432322BC8DC806E5F6E13D3CBB674B5E274E37EBBD9F9B15D285AE5899B61EEC9829515DA944B0E23527D0EA22CA4D709D9032F7AA9F1D150808E4C8158B5A 0
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/js/ontario-a11y.js?v=8.9.13
Preview:	/**. * A11Y handling. */.var KEYCODE = {. TAB: 9,. ENTER: 13,. ESCAPE: 27.};..function addA11y(element) {. element.setAttribute("aria-hidden", true);.}..function removeA11y(element) {. element.removeAttribute("aria-hidden");.}..function addA11yVisiblity(element) {. element.style.visibility = "visible";. element.setAttribute("aria-hidden", false);. element.setAttribute("tabindex", -1);.}..function removeA11yVisiblity(element) {. element.style.visibility = "hidden";. element.setAttribute("aria-hidden", true);. element.removeAttribute("tabindex");.}..// keyboard utility to Trap focus.function focusUser(config) {.. if (!config) {. throw new Error("Unable to initialize focus-trapping - missing config");. }. var element = config.element,. escapeCallback = config.callbackOnEscape;.. if (escapeCallback && !(escapeCallback instanceof Function)) {. throw new Error("Unable to initialize focus-trapping - callback is not a function");. }.. var focusableElements = el

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ontario-icon-alert-warning[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1033
Entropy (8bit):	7.530310454588132
Encrypted:	false
SSDEEP:	24:sbFhgwnhbRnrAiH7Kf5k8K3pNIlMqAnfVG5gCrKNp:14h9rAiHefk3pShA9G5Rw
MD5:	8A54B1F276942D771612AFC3902789BC

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ontario-icon-alert-warning[1].png	
SHA1:	F0DDA961C0ED6EA32B936F688B8350BD1C1459F1
SHA-256:	3D831607D0E657E0D4A5C445914645678E92592038FECCBDF66B84ECE56EC281
SHA-512:	BAD13771BFBBFF0F7385BAE0E40C80853DF3AA04A2FFF5D4AFBD1046724AF3B4F6A7CF09A14652437DFC4BE41EF68DD2F82BC3CCF7FC12B45816FB34AF18F853
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/c19-book-vaccine-assets/ontario-icon-alert-warning.png
Preview:	.PNG.....IHDR...`...`.....w8....pHYs..,K..,K..=.....sRGB.....gAMA.....a.....IDATx...m.@.E...o. .'....A.:.;p:p.)!. ..@^.q....fI..`....!....K.../.j.%"EQ.EQ.EQ.At.}..iH0.$....O.....I....1).@.B.H .c...}..p.~.Uu.>.0d&.6.../~.v..@.%`8.k.5~#.Vo..!/.5}.....Q..k..u=s....#A.J.....ijKB.3..G.r....%..D,...8}-.1..##...sk.'<...'....f.....Z.?....iC@-e=..v.,..4.1X/.lOA#.=...'....^..-.Z.2.....1.O....@.l.....n....=.../.%.Y./.....iF....l....Z.'....+}."...i}R..D<.PG....d.....4#....|.J....e..8kF.?P^_.[..,.....E....Q...e.O.5cGAT....M.....Rf....hF.E.e..../oQ~....M@:."...6...'...VC.v..|.....2.....E6}.'..?8.K_....(2.K.....s.....|..._..p.r{...rA.%..fD.,.....(`.....H_&.@q.../...F..Er}.6.B.0...2Y.XjF...e..l.T;m$,.I..X3.H./.OA./+.F....._3.H./.....i'..q.....B9..[.$..$P3....k...{B..A....QD.K....(.....kF.A..k...(..._....Qx...7b.....G...Wo...wuO..Nw<.....Qx.K.)H.{.q...,_3.p...X.fDa...X.fDa)/..X.fD1./GOA+.(&..x...QL...h..2./...../.U.E

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ontario@2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 360 x 91, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6667
Entropy (8bit):	7.942048147330949
Encrypted:	false
SSDEEP:	192:EiBKxzrvo5MCO922wdtBDRYMJvVHbU76yFYO89VqniGGdk:EiKPo5M922qBDR1L7jyyFGirk
MD5:	46718AF8157A5B51C395EEC77FB087E3
SHA1:	3DBC339CF8F44B8C87A0426911F3075AFB1CB464
SHA-256:	F9B9CFB8AFA75DB50F7544B8FF0510B8385FCB0BB83C8BEF5A2688F9FA74E6DF
SHA-512:	3399BE3B0A97D5BA3C4EBBED9E74B52C63880F0F8A56D5B2E855AB8F298AF57B128EFEAA95C6C065C459B77D45933C83D82C9CFC5892F9B5FBA5F74518C42DB8
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/ontario@2x.png
Preview:	.PNG.....IHDR...h...[.....^|.b....IDATx.....^.....l...^.m.62.0..qV..l.ii6..c.....s.|..r.c..VZX.(.K..%3d....r@N.99/.>.sr\...Y'.d.....D..mo?...b..L..rN....#9&.e.T.P...E@...=.T...M2T2.)...%#...).%9P...5e...[/..h..*....6)&...@....`.....Y....[R.@.:.a.G,.-%..@.\..bG%.@.....1.....T..b.....ho.PI.p[...7...+b_.....I....".`...Cs....j....L.....4.pg..`..~Y]..]...."......*....tK.....p.u.s.#!...j..1...b.9.n.eYQ...cil....e.O.pI....K.O...L+./.S.oK...iG~5.i.....o..+X....c...k7...u...Z6}..]@Gum..?. .....B.....]q.....^...P.....>.?wr...Cr.Z.b3..._N...H....E.B..W^x..Lh.....#..@.O.n.M.....t...?@.:...}?.>.H9d.0....{..._[.l}N.?.QK.5i....z:.v...k....5.T./.[4iJ...w.~....h.".y.$....[>.5K.y.a9s.....r....-+.....k...|1(....Z.....\x.....O..~++W..d.~.z.={....r..7.....n=}=.H.ea3...Fa...8..."..2J.By....s...5k$....r..7h.z..`T...N]..{n..;.@..;...~.0j.%..c...SO...1F.y....K]@..q....C.V@a..r.....%..#.....p..L8j07..k0....'.(.|.....:5k.....hx.'

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\open-sans-400-d0bad741aefb909e4be56d188b6f02b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 14260, version 1.1
Category:	downloaded
Size (bytes):	14260
Entropy (8bit):	7.955023552448444
Encrypted:	false
SSDEEP:	384:V0ZkWiwHBFDPthd/jO+yk0iwCebLvVgYGpn/qZOSO7O7RWf5z4Oc:V0hRbVFykgNSnSsSSSRWR8/
MD5:	D0BAD741AEFB909E4BE56D188B6F02B9
SHA1:	1547224E0A0BE06E5178815718797BD6607169A4
SHA-256:	4194A431CCA6678145F2C4D7D2E597087E2A76A4878C26B66315B2BA4F4EA393
SHA-512:	33FB0A386FD3ED97ADA0A6612D818530FED61E8688A0C38BCE29031076430C7FC2AA075C5AA8003E2E091D80C64602FE7A8D7F3B7380601EFB3CEC20285B50D
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/static/open-sans-400-d0bad741aefb909e4be56d188b6f02b9.woff
Preview:	wOFF.....7.....^L.....GDEF...X.....GPOS...p.....GSUB...|...Y...t...OS/2....._...`.>..cmap...8.....gasp.....#glyf.....$Y..3..~.head..'<...6...6...=hhea..'t.....$....hmtx..'.....l..Y.kern..).....loca..3.....C.O.maxp..5`... ... .d..name..5.....2../Jpost..6,.....(..j.....x...5.A...../0.E....-..E.m....2..mz.....)@.]-R...X...@..DN^Q].Md`....]h.,4s...../.....x.c`f..8.....u..1...<.f.....{...h..... 0t.vf.....&.O.....)B..q>H..u..R``.....9.x.c```d`.b.....@Z.A.....`..d.c8.p..?.!c0.1.[Lw.D.....\.J..(.....T..... .ja.....jK.....?.....=.s.....}.....Ly.. ...@w...@G7.....x..z.\S...=so.j.....R.!.....V..*RDD*Z...J.*E.*...H.R.j...R.^k...Z[...W.$.w.....~.~...9..9.r...8.....9..9...F|..#M.f....Y....}.g...\qf.....^..J...;.'..~.h..P?.@..4.....2r.....^./..'....!.1?!..s.H.8.3..U..\g.eP./=/.\@....^...W...W.-...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\phone[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3983
Entropy (8bit):	3.9233631757088947
Encrypted:	false
SSDEEP:	96:AFxvRl2OV1d/UaGgX2phUt1nExHaQEET+u7hO7VC:yvRlll/UaGgXwhc10HQEiEOo
MD5:	79DEF050C85931B2A5F387892E013F8C
SHA1:	A2AB876984106052B752A224B780C8B2FD58342E
SHA-256:	3D2AF2899747E4C51E45AC7EB1EAA0FDEE399022C94D8F4721922FB8AC740E8C
SHA-512:	2A90F626B9B9ABD202087D1361311863A331662E0ECC67BD4DD067A189E523CCE4E0963FEE27FE454A8531589B67ADCDE9ABF1B3223C368BB83CB1F83C318BF0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\phone[1].svg	
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2021-02/phone.svg
Preview:	<svg width="104" height="104" viewBox="0 0 104 104" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M82.1171 64.4242C79.988 62.2073 77.4199 61.022 74.6981 61.022C71.9982 61.022 69.4081 62.1853 67.1912 64.4023L60.255 71.3165C59.6843 71.0092 59.1136 70.7238 58.5649 70.4385C57.7747 70.0434 57.0284 69.6702 56.3918 69.2752C49.8947 65.1486 43.9901 59.7708 38.3271 52.8127C35.5833 49.3446 33.7395 46.4253 32.4006 43.4621C34.2005 41.8158 35.8687 40.1037 37.493 38.4575C38.1076 37.8429 38.7222 37.2063 39.3368 36.5917C43.9462 31.9822 43.9462 26.0119 39.3368 21.4024L33.3444 15.4101C32.664 14.7296 31.9616 14.0272 31.3031 13.3248C29.9861 11.9639 28.6033 10.5591 27.1765 9.24214C25.0474 7.13495 22.5012 6.0155 19.8233 6.0155C17.1454 6.0155 14.5553 7.13495 12.3603 9.24214C12.3384 9.26409 12.3384 9.26409 12.3164 9.28604L4.85345 16.8149C2.04386 19.6245 0.441519 23.0486 0.0903206 27.0216C-0.436477 33.4309 1.45122 39.4013 2.89991 43.3084C6.4558 52.9005 11.7677 61.7902 19.6916 71.3165C29.3057 82.7963

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\phus[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	14179
Entropy (8bit):	5.188193851128604
Encrypted:	false
SSDEEP:	96:mFWaR9De/V2l12cLqueeL0WeFSu+IBoaY7UtEXctUtYJtv9TuPwdNeMAXVgoyw/:OR9Det2lvL0WeFKtaY7fqtv9TuYVOLyk
MD5:	45559C2BC574E469047CFB109459D30B
SHA1:	58B6F1850C52F4E4CA2E058E40B3A5FCC6BD6505
SHA-256:	96C67525EE0088F5E938646461BA6116B5632375812446E0BEC9716A4F2D8177
SHA-512:	389931FB5430F61E52400F0A20CE768E62DBDB6F7EDFCD91C598CF2086B4045EA2441286DAA090FA2BE205AB61D763723D72CDD5B024902C4E6822CAA538677
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/c19-book-vaccine-assets/data/phus.json
Preview:	[{"id":"1","name":"District of Algoma Health Unit","on_portal":"No","phu_tool":"http://www.algomapublichealth.com/disease-and-illness/infectious-diseases/novel-coronavirus/covid-19-vaccine/vaccine-clinics-in-algoma/#clinics","phu_call_centre":"Yes","phu_phone":"705-541-2332","phu_general_phone":"705-541-2332","phu_general_web":"http://www.algomapublichealth.com/","r3_en":"http://www.algomapublichealth.com/disease-and-illness/infectious-diseases/novel-coronavirus/covid-19-vaccine/vaccine-clinics-in-algoma/#clinics","r3_fr":"http://www.algomapublichealth.com/disease-and-illness/infectious-diseases/novel-coronavirus/covid-19-vaccine/vaccine-clinics-in-algoma/#clinics","age_threshold":"60"},{"id":"2","name":"Brant County Health Unit","on_portal":"No","phu_tool":"https://www.bchu.org/ServicesWeProvide/InfectiousDiseases/Pages/COVID-19-Vaccine-Clinic-Appointments.aspx","phu_call_centre":"Yes","phu_phone":"519-753-4937 ext. 416","phu_general_phone":"519-753-4937 ext. 438","phu_general_web":"h

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\position-container.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	95
Entropy (8bit):	4.220495863964869
Encrypted:	false
SSDEEP:	3:USQTWqVYb1MVNMNQMXm/1JrYv:UVtYbymQt/frYv
MD5:	A203BFB5819742D466B5E99AF480009A
SHA1:	CC0323B65FD726EF89264B2A7A6D3D7C4999A5E2
SHA-256:	92931CEB6A0AD1C9B3E8FC6F335B9DFD6F0C7C8EE36F089BB10241C142A78FAA
SHA-512:	D12FB20EDE3211C3C3469D5DC86E2BE654A3D5ACE2FE3F20D3E959596106E0775369CB1A5A1886447497508DD572F4D61A47291EDD25910DD8713883AD01518
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/position-container.module.css?qrgttk
Preview:	/*. * @file. * Contain positioned elements.. */...position-container {. position: relative;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\postalcodes[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2786378
Entropy (8bit):	4.307469615088594
Encrypted:	false
SSDEEP:	12288:sPd86m8RsO98KBBBPqqjDaVasEr3/tBibyYKBilSTq1XjOG29:c2n8xguaG7/tnu1XCr
MD5:	BE1588D543EAA359C95DE4C948280691
SHA1:	A1CF4E81AA166CD80D89419D9F6F9B24DEF4D19F
SHA-256:	63EABDD03EB72721BBE660F6B0E108467BFADDB93FC150EC86A0B7778C7C3C78
SHA-512:	DEE6F0ACFEA6ADC556420726D896D8F5959F0C1043D3A94CF79EF20741EBED995D1D1A4AC8E4D95C42980931E02B981CDB1A8CE19AB34E2F9832C35F4534CFD
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/c19-book-vaccine-assets/data/postalcodes.json

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\postalcodes[1].json	
Preview:	{"id7":["B0T1B0","N0A1A0","N0A1B0","N0A1G0","N0A1J0","N0A1L0","N0A1N0","N0A1N1","N0A1N2","N0A1N3","N0A1N4","N0A1N5","N0A1N6","N0A1N7","N0A1N8","N0A1N9","N0A1P0","N0A1S0","N0E1C0","N0E1J0","N0E1M0","N0E1P0","N0E1T0","N0E1X0","N0E2A0","N0J1K0","N1A0A1","N1A0A2","N1A0A3","N1A0A4","N1A0A5","N1A0A6","N1A0A7","N1A0A8","N1A0A9","N1A0B1","N1A0B2","N1A0B3","N1A0B4","N1A0B5","N1A0B7","N1A1A1","N1A1A2","N1A1A3","N1A1A4","N1A1A5","N1A1A6","N1A1A7","N1A1A8","N1A1A9","N1A1B1","N1A1B2","N1A1B3","N1A1B4","N1A1B5","N1A1B6","N1A1B7","N1A1B8","N1A1B9","N1A1C1","N1A1C2","N1A1C3","N1A1C4","N1A1C5","N1A1C6","N1A1C7","N1A1C8","N1A1C9","N1A1E1","N1A1E2","N1A1E3","N1A1E4","N1A1E5","N1A1E6","N1A1E7","N1A1E8","N1A1E9","N1A1G0","N1A1G1","N1A1G2","N1A1G3","N1A1G4","N1A1G5","N1A1G6","N1A1G7","N1A1G8","N1A1G9","N1A1H1","N1A1H2","N1A1H3","N1A1H4","N1A1H5","N1A1H6","N1A1H7","N1A1H8","N1A1H9","N1A1J1","N1A1J2","N1A1J3","N1A1J4","N1A1J5","N1A1J6","N1A1J7","N1A1J8","N1A1J9","N1A1K1","N1A1K2","N1A1K3","N1A1K4","N1A1K5","N

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\raleway-modified-400-79edfeb2a0670adbccb268d3b8f344f4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18244, version 4.20
Category:	downloaded
Size (bytes):	18244
Entropy (8bit):	7.979202840632488
Encrypted:	false
SSDEEP:	384:glcBMfNkCPEVHO5tI+gJqVZ2TlPdIKoJ06nrKJ/mHf5F5gpynNYoe:gy3HP+gJUo5PSKoC6nLHf5fgMnyn
MD5:	79EDFEB2A0670ADBCCB268D3B8F344F4
SHA1:	1D164B4EA5D0CF0747934A42A3C0207EAD3A0404
SHA-256:	7CBDEB6D81C204683D29DACDE6CD1DE7C0B50B2389EAEC166B046A8FABC89067
SHA-512:	E493E91346A3829EDA94541AB2982CE694D85B43AD4361AD108B7D4F1D6437AEAF7D376580A85CBAD3A05E5D4E8F405E0FC67CE4F523973EDC77005CA7E37C3
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/static/raleway-modified-400-79edfeb2a0670adbccb268d3b8f344f4.woff
Preview:	wOFF.....GD.....FFTM...0.....$/.GDEF...L..... ."..OS/2...I...I...`..p.cmap.....bd..xgasp.....glyf.....6c..nx..D{head..:....1...6....hhea..:D... ...$.\..hmtx..:d....._,.loca..<.....5bQ.maxp..>..... ....name..>....s.....post..Ed.....Ldnx.c```d..3.....n.0..H..V..x.c`d``..b...`b`../@...1.....'..x.c`b..8.....i..>C.....0"s.2.R.....R....d``>.....I..:.R``.....x.c```f.`..F .....1...,..@.....e.cX...1..../.1.[Lw..(.(.(H).)(().)X).(.(T*,VX.....$.$.$.$.....?...i.....M.....4a.....i.`.J..+F.M...&.5-.h.....?.....;...o.r=..`.m..>..`...<.|.....x...{...w..{+.M.....F6....L@..].0.YX..98..yx.....ED..%$..ed.....UT..54..ut.....ML..-,..ml.....]\..=<..}|.....CB..#"..cb.....Z.:.&M..h..K..X.r..uk.o.e....v....0%5.J....G....g~(..%...5.)..j..;..s.3||.S...2...3g/^:w~..#7.^...C.....M=.}..z.Le.<{...O.00...J..rU.9.....x..}.|[...eY{\.....-o[...$...NH .B.e'.....(-m...-.P..>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\raleway-modified-400[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18244, version 4.20
Category:	downloaded
Size (bytes):	18244
Entropy (8bit):	7.979202840632488
Encrypted:	false
SSDEEP:	384:glcBMfNkCPEVHO5tI+gJqVZ2TlPdIKoJ06nrKJ/mHf5F5gpynNYoe:gy3HP+gJUo5PSKoC6nLHf5fgMnyn
MD5:	79EDFEB2A0670ADBCCB268D3B8F344F4
SHA1:	1D164B4EA5D0CF0747934A42A3C0207EAD3A0404
SHA-256:	7CBDEB6D81C204683D29DACDE6CD1DE7C0B50B2389EAEC166B046A8FABC89067
SHA-512:	E493E91346A3829EDA94541AB2982CE694D85B43AD4361AD108B7D4F1D6437AEAF7D376580A85CBAD3A05E5D4E8F405E0FC67CE4F523973EDC77005CA7E37C3
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/scss/base/ontario-design-system/fonts/raleway-modified-400/raleway-modified-400.woff
Preview:	wOFF.....GD.....FFTM...0.....$/.GDEF...L..... ."..OS/2...I...I...`..p.cmap.....bd..xgasp.....glyf.....6c..nx..D{head..:....1...6....hhea..:D... ...$.\..hmtx..:d....._,.loca..<.....5bQ.maxp..>..... ....name..>....s.....post..Ed.....Ldnx.c```d..3.....n.0..H..V..x.c`d``..b...`b`../@...1.....'..x.c`b..8.....i..>C.....0"s.2.R.....R....d``>.....I..:.R``.....x.c```f.`..F .....1...,..@.....e.cX...1..../.1.[Lw..(.(.(H).)(().)X).(.(T*,VX.....$.$.$.$.....?...i.....M.....4a.....i.`.J..+F.M...&.5-.h.....?.....;...o.r=..`.m..>..`...<.|.....x...{...w..{+.M.....F6....L@..].0.YX..98..yx.....ED..%$..ed.....UT..54..ut.....ML..-,..ml.....]\..=<..}|.....CB..#"..cb.....Z.:.&M..h..K..X.r..uk.o.e....v....0%5.J....G....g~(..%...5.)..j..;..s.3||.S...2...3g/^:w~..#7.^...C.....M=.}..z.Le.<{...O.00...J..rU.9.....x..}.|[...eY{\.....-o[...$...NH .B.e'.....(-m...-.P..>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\report-price-gouging-during-corona-virus[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6814
Entropy (8bit):	4.082683189957993
Encrypted:	false
SSDEEP:	192:zmzBdEFaqO6JpO5+2wiR0WB4+z3H/VqTF+W3TY:zYdEFaqO2pO5+2wRk8F+W3TY
MD5:	22BB5F4589A65EC0D626A05E687D25C4
SHA1:	44836538FEF4DFFCD1C992A447208A934844E2EA
SHA-256:	D04BE8D3F4F462D8568629AB858610E2119F06229AA29137968274AF240B8FB9
SHA-512:	7619B907D6562D3CF630631A17636C48714A6EC58DEFD436B6229110CEA7F03498725419AAB33F4FAB7E527957824CFA5E4E607FF2C08AFAFBC40C4A17B6A81E
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2021-02/report-price-gouging-during-corona-virus.svg

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\report-price-gouging-during-corona-virus[1].svg	
Preview:	<svg width="140" height="151" viewBox="0 0 140 151" fill="none" xmlns="http://www.w3.org/2000/svg"><path d="M97.3 98.325H51.4V98.4249H5.60001L10.9 14 8.225H51.4H92L97.3 98.325Z" fill="white"/><path d="M51.4 149.925H10.9C10 149.925 9.30001 149.225 9.20001 148.425L3.90001 98.625C3.80001 98.125 4.00001 97.625 4.30001 97.325C4.60001 96.925 5.10001 96.725 5.60001 96.725H51.1C51.2 96.725 51.3 96.725 51.4 96.725H97.3C97.8 96.725 98.3 96.925 98.6 97.325C98.9 97.725 99.1 98.125 99 98.625L93.7 148.525C93.6 149.425 92.9 150.025 92 150.025H51.7C51.6 149.925 51.5 149.925 51.4 149.925ZM12.4 146.525H51.1C51.2 146.525 51.3 146.525 51.4 146.525H90.4L95.3 100.125H51.7C51.6 100.125 51.5 100.125 51.4 100.125H7.50001L12.4 146.525Z" fill="black"/><path d="M51.4 100.125H1.7C0.7 100.125 0 99.325 0 98.425C0 97.525 0.8 96.725 1.7 96.725H51.4C52.4 96.725 53.1 97.525 53.1 98.425C53.1 99.325 52.4 100.125 51.4 100.125Z" fill="black"/><path d="M42.9 148.825C42 148.825 41.2 148.125 41.2 147.225L38.5 99.6249C38.4 9

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\secondary-navigation[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2607
Entropy (8bit):	4.779907926046658
Encrypted:	false
SSDEEP:	48:YTfAAmKryfJmz/8Rzm62eGTr9dRcCUeQA1NG:Y7AAmg2JmT8Rzcjr3RkSG
MD5:	CE60BE9D9B0E25B5F2E494193DBA554F
SHA1:	D05ADE985C9AF9C24509EB8B07BF1329D4C41748
SHA-256:	A2FD667C55478849BAB73195417AD57A9224C1750C64DE2760852B8F6E4086B6
SHA-512:	F019812C182C9EBD084E8E70D44B78F91DB8021930FD1E2D5C84A18F30F341EFBF24BA74D9F6847FAB675C7149981A6FB30A6A083E59236DA68FD37A36CD414
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/js/secondary-navigation.js?v=8.9.13
Preview:	(function ($) {. let activeNavListItem = $('.ontario-list-item-active');. let navListItem = $('.ontario-navigation__list-item');. let navListItemAnchor = $('.ontario-navigation_ _list-item > a');. let subNavContainer = $('.ontario-sub-navigation__container');.. let activeMobileNavListitem = $('.ontario-mobile-list-item--active');. let mobileNavListItem = $('.ontario-mobile-menu__list-item');. let mobileNavListItemAnchor = $('.ontario-mobile-menu__list-item > a');. let mobileSubNavContainer = $('.ontario-mobile-sub-nav igation__container');. let mobileSubNavActiveAnchor = $('.ontario-mobile-list__sub-nav-item--active > a').. navListItemAnchor.on('click', function(e) {. if($(this).next('div ').hasClass('ontario-sub-navigation__container')) {. e.preventDefault();.. $(this).parent().toggleClass('ontario-list-item--active');. $(this).parent().siblings(). removeClass('ontario-list-item--active');.. ($(this).parent().hasClass('ontario-list-item--

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\splash[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	1316
Entropy (8bit):	4.734902870803483
Encrypted:	false
SSDEEP:	24:icZ9fY0mIwC4HheXxvG6wiwkHJ9V9KACYgdZ8hgYnJMH:VmIUH0BtX9QdKhJJu
MD5:	E2F448F78AD6C5A64571929FCEA5E8F7
SHA1:	C0AA5F6FE4D7506432FA9086264BE09D671C60BF
SHA-256:	50DAD750CA6081A33EF23150705E86E1D4B319CB76416FFE0BC1AA88385865ED
SHA-512:	06BE9EC4B56BC1B9E6B404F5BE69246DB0BC353445E27187B91CC0242EB6D5AE615235BE47601F3B76C527F1D31D1ED5A7721F2E4B77E1780C1B1704606EA35 E
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/content-type/partials/dashboard/splash.html
Preview:	<style>. body {. background: url("/img/assets/splash/spring-2021.jpg") no-repeat center;. background-size: cover;. height: auto;. }.. .top-margin-6x {. margin-top: 6 rem !important;. }.. .site-logo {. width: 315px;. height: auto;. }.. @media screen and (min-width: 64em) {. .panel--semitransparent .button {. min-width: 9.5rem;. }. }.. @media only screen and (max-width: 40em) {. .top-margin-6x {. margin-top: 3rem !important;. }.. .button {. margin-right: 0;. }. }.. @media print {. .t ext-center {. text-align: center;. }. }.</style>..<main>. . .. . . <img alt="Government of On tario | Gouvernement de l.Ontario" src="/img/ontario@2x.png" class="site-logo">. . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\spring-2021[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	64293
Entropy (8bit):	7.846351923438243
Encrypted:	false
SSDEEP:	1536:Fma7QnNHsXD4679zsPckbbtVwWRQOIzdH5sl4ueSd6n1kg:d2NHsmrbEWmfdH50g
MD5:	508FD6E64738121024290EBD8E7A6A74
SHA1:	002BE4D4876CD81414B945DB4FB77E4A65B42C02
SHA-256:	FB969147A45B36F77DA9C817E8199F5A2C7DC24164E08BC5207156DA52455143
SHA-512:	C0671B8DB8A92879A84E0137BE230FC653443D4E82D51B56FFB82780C053845DF346BC96A54A58626150420F6132296A71C413EB31E98B1B3CA2BBB9AC623139
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/assets/splash/spring-2021.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\spring-2021[1].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 116.164766, 2021/02/19-23:10:07 "> <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="7604F6EC7101F9F3A6EBDB708AB235C7" xmpMM:DocumentID="xmp.did:538CC97A88F611EBB8D7BA14A11AA145" xmpMM:InstanceID="xmp.iid:538CC97988F611EBB8D7BA14A11AA145" xmp:CreatorTool="Adobe Photoshop 21.1 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4f6e4f4a-9343-47ca-b280-5c7c6d910e7f" stRef:documentID="adobe:docid:photoshop:ea19256a-bce7-cf40-9d50-1aabf33ba4b6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\template-page[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	2725
Entropy (8bit):	4.41239041853077
Encrypted:	false
SSDEEP:	48:/bhS6xLzOoTMEffMqMRZvLUCwqJWd/MhPV1NQzMqz2zR4u5GUE:NHoEJ4/q/SR/GUE
MD5:	76EBE1801AC566AF044887388AFF2DB6
SHA1:	4A6337C7C3238DA616CB64F8C0B775F483C1BCB4
SHA-256:	66A139CB816CE3D4FE46B69B4BA5B77A01234198C56009DEA8048A3C02E1402C
SHA-512:	D27AA8C429282AF84ECAD3E66D266E37BFE7E4152C39C1A90BEDA3DFA4D83D0E7434FCB74FD780286E5E6AAAAAECDC4530F239866F232836BF59830744A09E8A
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/content-type/partials/page/template-page.html
Preview:	<main>.. <onesite-optimization-banner>. </onesite-optimization-banner>.. <onesite-archive>. </onesite-archive>.. <onesite-intro>. </onesite-intro>.. . . . <compile-html html="mainController.node.content.greyBox">. </compile-html>. . . .. <div class="row". ng-init=". asideEnabled = mainController.node.content.right || mainController.node.content.archive_status === 'associated';. resultStatus = {};. ">. <div class="main-content". ng-class="{'large-8 medium-12 columns': asideEnabled, 'small-12 columns': !asideEnabled}">.. <onesite-toc toc-style="mainController.node.content.tocStyle". toc-list="mainController.node.content.toc". include-faq="resultStatus.total > 0". alias="mainController.node.content.params.alias">. </on

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\trillium_6[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 144x144, frames 3
Category:	downloaded
Size (bytes):	8660
Entropy (8bit):	7.889806609797456
Encrypted:	false
SSDEEP:	192:aknOiayY7s/y3yL8YKPKhU/zplFG8LtTusd3KCNllctSIky5:pnx5K3yL8kIbFG8Lhusd3VSSIkm
MD5:	A18E8422462335FC0879495809189094
SHA1:	F941AC2B0E6086C2D779B5D7093D9D478E68BAF0
SHA-256:	6EFB43B92424429C270E1D5B773A2E999F1231A6A7BA59096171EF475F7D97FF
SHA-512:	30E5D7A8F457CAA353446DC5FAFD2397E231895A8928DDFE8A9C1483966FB99D6D21426F33EF9CD60C40548D1BD4F2DB25A00860EAE7FAF1C0938474372EF85
Malicious:	false
IE Cache URL:	http://https://files.ontario.ca/trillium_6.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 5.5-c021 79.155772, 2014/01/13-19:44:00 "> <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/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmpMM:DocumentID="xmp.did:B82A61F6110911E5B5AE9E5C9EA152F0" xmpMM:InstanceID="xmp.iid:B82A61F5110911E5B5AE9E5C9EA152F0" xmp:CreatorTool="COOLPIX L1V1.2"> <xmpMM:DerivedFrom stRef:instanceID="228B4BD8679281BAB641C70E4070908B" stRef:documentID="228B4BD8679281BAB641C70E4070908B"/> <dc:creator> <rdf:Seq> <rdf:li>Karen Labonte</rdf:li> </rdf:Seq> </dc:creator> <dc:title> <rdf:Alt> <rdf:li xml:lang="x-default">Trilliums</rdf:li> </rdf:Alt> </dc:title> </rdf:Description>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\www-player[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	365477
Entropy (8bit):	5.242167915306127
Encrypted:	false
SSDEEP:	1536:BDQI0irpHrpj/fn8Mq5G04XGqUDrzltPljuvEMFfyUOP5FRrDJciM/ByDN4A6D65:TijDrzxCQgayRsLb
MD5:	2D4D90F855A60199EE25043D26066129
SHA1:	3E62A44ACF2768ABCCCE8ECCD1736C2D6F67AFFE
SHA-256:	E76089910B3A72BB157C377AF94E140AA5BA385BE2DAD47D13D5E80F3F3C5100
SHA-512:	37F74371CC28C1584DF9A3F308CBF97810CE5D77C7C1624CD9538D274B240ED36D927962E76FEBB30443D8040CF9084790C282D169A139B402F72AFE14305CAD
Malicious:	false
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;text-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000}.ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);-webkit-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);transition:color .1s cubic-bezier(0.0,0.0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0.4,0.0,1,1);-webkit-transition:color .1s cubic-bezier(0.4,0.0,1,1);transition:co

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8a89caa9-511c-4568-af89-7f2174b4378c[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1405
Entropy (8bit):	4.846601528666309
Encrypted:	false
SSDEEP:	24:YPOTSNBcZCiyIiUvK0+W1Z0V4g1Z0V4gUj0VrCVIBmg9PgT5lHpHmB:YPlQZC5IFK0/1Z0V4g1Z0V4gUj0Vhmgf
MD5:	3432B63D4176808AEB89100F06AE626E
SHA1:	BBD46C3E5790D727611A522F947A40F52CCCCF9D
SHA-256:	77ABF5EB84978F86BE2E216362CEDD5939E06A0E4121A05ED8D3C4EB5559D9D9
SHA-512:	AC0C61540C39CC855C042565E0718006E4E2E0696CC95B7F5822CBC8636034E682F4EC71EAFBA203FBBE9381A4DB1279E848241098B67BFE9130DA62C64E7BD
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-data/data-catalogue/8a89caa9-511c-4568-af89-7f2174b4378c.json
Preview:	{"help": "https://data.ontario.ca/api/3/action/help_show?name=datastore_search", "success": true, "result": {"sort": "report_date desc", "include_total": true, "resource_id": "8a89caa9-511c-4568-af89-7f2174b4378c", "fields": [{"type": "int", "id": "_id"}, {"info": {"notes": "", "type_override": "timestamp", "label": ""}, "type": "timestamp", "id": "report_date"}, {"info": {"notes": "", "type_override": "", "label": ""}, "type": "text", "id": "previous_day_doses_administered"}, {"info": {"notes": "", "type_override": "", "label": ""}, "type": "text", "id": "total_doses_administered"}, {"info": {"notes": "", "type_override": "", "label": ""}, "type": "text", "id": "total_doses_in_fully_vaccinated_individuals"}, {"info": {"notes": "", "type_override": "", "label": ""}, "type": "text", "id": "total_individuals_fully_vaccinated"}], "records_format": "objects", "records": [{"_id":106,"report_date":"2021-04-13T00:00:00","previous_day_doses_administered":"95,692","total_doses_administered":"3,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\PHULocator[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1542 x 184, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	36711
Entropy (8bit):	7.9276537058951995
Encrypted:	false
SSDEEP:	768:nx/NXRsI7/eGgiR/lVc8DcztTx/3TrjoY0vJJpo0MC:nzwliR/lcpTVPtipo0R
MD5:	7EAF9A26FEC2DF8ED8E036759D405A54
SHA1:	7749C2328B8EB5EA92631BA23B2CE43FEE866CB5
SHA-256:	34E31E2B94ABB45BBBFE70B2678D14A61E78C19E7D5960F97306106FA3E1DB4C
SHA-512:	7343664D9AD88C32B5148BBE2652E483EF67BDD053F21573EDDA406731CB02A8BF239F849619D05E0EF592749629ECFCF1ABAEB9C2C297569A1678439660B1B1
Malicious:	false
IE Cache URL:	http://https://www.phdapps.health.gov.on.ca/phulocator/images/PHULocator.PNG
Preview:	.PNG.....IHDR.....(.W.....sRGB.....gAMA.....a.....pHYs.....IDATx^....S.....tN..8.&t".].S...D.tQ#tE*.t.DM..I....!MQ.!..B..!.....R.....>...Z{}.g...|.w..}=..../..}....uY..!. .B.!..B.!..b. ..B.!..B.!..B.1..c@.!..B.!..B.!..A.1 ..B.!..B.!..B. ...B.!..B.!..B.!f.r..!..B.!..B.!..3.Z.....-^.s7o.n.....Ork.q.{..t..v.$I.$I.$I.$I.$I.aG..]..:vv.....e....$I.$I.$I.$I.$.wa ..._}9..8.*..:_L&T.$I.$I.$I.$I.$I....=..\|....8...7\.L.$I.$I.$I.$I.$I.$I...<v.^)v...E.H.$I.$I.$I.$I.$I.48a..I.....m....K.$I.$I.$I.$I.$I.4xa..~_B.c...W..6:9..$I.$I.$I.$I.$I.$I.'.....w..c.O....$I.$I.$I .$I.$I.4....{..h.....w..c@..I.$I.$I.$I.$I.$I.p...j.m...jY.;..1...%I.$I.$I.$I.$I.$i8.:.L..sx.._M.c.~...$I.$I.$I.$I.$I.$i..r..:..?M.c`...N.....f.>..t.e..nsw.y.{...k.*..B.!..B.!..B.....c_.....NN... s[..I:..8....v.....-Z..E.!..B.!..B.!.....{h....0.q..Z.L%..Xg./N..n..=.....Z!.!..B.!..B.!..._..c.....@..V.S...8..N..6.Wi..=.B.!..B.!..B.!.....t).@'.z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Raleway-700[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16436, version 1.1
Category:	downloaded
Size (bytes):	16436
Entropy (8bit):	7.973528132200105

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Raleway-700[1].woff	
Encrypted:	false
SSDEEP:	384:BNebrtrBElie10zsjs72g8Ds9ofyEVL7oVFQ54Fo:BsXbEYHWJqwBos5V
MD5:	E4F290693D69F0CA08871D256363EE9A
SHA1:	3FB6D354094ABB99AFDF80B45086FA7B0F073690
SHA-256:	72FFF1685DFB2C91A5AD93B3028E6B53789A4CA50C738B8590ECFC9EB002B25F
SHA-512:	847CA2BE6BDE8C9B9D174399AB5ACF63ED1C6778953EB412EE548B4DD0AAB63B7235378B120E8EA18D68D7DFD054B0D02B3A379EF9E092C3BBD6D5AD72F287A6
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/fonts/Raleway-700/Raleway-700.woff
Preview:	wOFF.....@4.....D.....GPOS...0...*..14.D.rGSUB...\...\...t...OS/2.....[...`.H..cmap.....gasp.....glyf.....*m..Nv-...head..9@...6...6.QP.hhea..9x.....$. ..ihmtx..9....*...x.. .loca..;.....1.Xmaxp..=\|... ... .:...name..=.....'.@.post..>.....%...#x.L..l.a....w.m{.g.m...`.m{..A.....j..... ..G.Q....p...PYF.C.@h`.8.P`.;..K.{.....E....y.A....%Q. ..+.....Q).....;...B..m.....J../...J.9..)....;.^+.g.F?....A....z;..f.....e.....B,..J<.P..4..MiF+Z....=..H':..../...@.0.a.g.....2..L`*..Lf1.9.c!.X.....b5kX.:..-..0.8...q.....x.#..<.5ox....B4..L..d.e..D..fff....".....p..e..e.g.y.2>ffFQ.....[U.....P..n..X4..).r..Z.Y..+Tu.MI..il.4-3Z...m.&....>N.8.&a.....=#.....l...o...4u.z[e...:._.1.AM.I.y...4.....4....."G.N. h.}....:@}...z@K..*...8..G/.4._.?..ghN..,...Ec....Q...&.Aob8....V3..h...>.K.=...}.....:kTZ..E..{.....J..$...YC.....N...Zl..'..j.1..c.bm..{'+I....z.|..5@...wF...Q..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Z3VCRLT7.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	8405
Entropy (8bit):	5.0746341151683
Encrypted:	false
SSDEEP:	96:EGsHG+NLuC/XnuEsejOfrBsrbCspsrbp4IpwVS70qXVTdyrNGz7TzvBAkbfNMhjs:EGsH3IC/XnL8M8uIzybI8jSVg2O+S43
MD5:	0953A2B6FB1D331EFA2AAD3FF8E2DC99
SHA1:	33D9EA08EEFB81ABE8934754EA434A33437B227C
SHA-256:	38BF2EB71CE159B99E4A9C680FED3427D8193EB5DC44CE8A75A684EB00A9F820
SHA-512:	4EDECE89518BDEF904871B360E510F6645E631F1FBF9BE5BC4883131827E4F3B7D1169754E73FC1E27526D78378CB3E37D495B7E3DE7F7280F4D6DE908EB5082
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/
Preview:	<!doctype html> <html class="no-js" lang="en"> <head> <meta charset="utf-8"> <meta content="width=device-width,initial-scale=1" name="viewport"> <meta content="IE=edge" http-equiv="X-UA-Compatible"> <meta name="sha" content="d43396df38048fbb44731befe641f3dfc221eaf3"> <title></title> <base href="/"> <link href="/css/combined.css" media="screen" rel="stylesheet"> <link href="/css/print.css" media="print" rel="stylesheet"> <script src="/vendor/modernizr/modernizr.js"></script> <script>!function(a,e,o,n,c,i,t){a.GoogleAnalyticsObject=c,a.ga=a.ga||function(){(a.ga.q=a.ga.q||[]).push(arguments)},a.ga.l=1*new Date,i=e.createElement(o),t=e.getElementsByTagName(o)[0],i.async=1,i.src="//www.google-analytics.com/analytics.js",t.parentNode.insertBefore(i,t)}(window,document,"script",0,"ga"),ga("create","UA-21003310-6",{cookieDomain:"auto",allowLinker:!0}),ga("create","UA-48649528-1",{cookieDomain:"auto",allowLinker:!0,name:"ServiceOntario"}),ga("require","linker"),ga("linker:autoLink",["serviceont

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ajax-progress.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1035
Entropy (8bit):	5.00154723082934
Encrypted:	false
SSDEEP:	24:0wn7OrsH9HAxr4TAkZxrh794kRxr3yp3XrFgAn6Umey52M9Y:0/MHA94TAE9x94kR9i1FS52+Y
MD5:	C39F9F1EBB648940FC7C7C78FD171595
SHA1:	6BE470262F71975CF7E01C209ADF412B0E43721E
SHA-256:	018BC192232B968B662399F1CB800C44EE22B64285A6334366C667F7EBFEA058
SHA-512:	E0DBB0F400C2D82DF607987057DE053AA74791367BB633CE39FE07F944429F6125FE5A5DF44A3AA3C6DBF29407B39ABFC44AE7911410DB73793241E87862552E
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/ajax-progress.module.css?qrgttk
Preview:	/**. * @file. * Throbber.. */...ajax-progress {. display: inline-block;. padding: 1px 5px 2px 5px;.}.[dir="rtl"] .ajax-progress {. float: right;.}..ajax-progress-throbber .throbber {. display: inline;. padding: 1px 5px 2px;. background: transparent url(../../../images/core/throbber-active.gif) no-repeat 0 center;.}..ajax-progress-throbber .message {. display: inline;. padding: 1px 5px 2px;.}.tr .ajax-progress-throbber .throbber {. margin: 0 2px;.}..ajax-progress-bar {. width: 16em;.}../* Full screen throbber */..ajax-progress-fullscreen {. position: fixed;. z-index: 1000;. top: 48.5%;. /* Can't do center:50% middle: 50%, so approximate it for a typical window size. */. left: 49%; /* LTR */. width: 24px;. height: 24px;. padding: 4px;. opacity: 0.9;. border-radius: 7px;. background-color: #232323;. background-image: url(../../../images/core/loading-small.gif);. background-repeat: no-repeat;. background-position: center center;.}.[dir="rtl"] .ajax-progress-fullscre

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\align.module[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text
Category:	downloaded
Size (bytes):	484
Entropy (8bit):	4.609557654572897
Encrypted:	false
SSDEEP:	12:Uo/uby0Ehl5oXozfz03jKqKfvXkICf8y53jfZT:AW0EDm+A3jKvUIEvL
MD5:	8628052440E532F890CFC00D4A682FA6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\align.module[1].css	
SHA1:	E52C3AF92E150EACDA721A2343791BA41535781F
SHA-256:	97FE5992208187911C3DAFF7FE8556EE254CA0A340AB9AF0E3BA04CE7E40E2E3
SHA-512:	95ED5289C7BB858F837CCB83018D3DA5F6577AE027689DE8503FE934B097E818ADE79CC7EB89742C93859BB64BA4984F52BFB16D5210D3E757614FF7FD01A67
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/core/themes/stable/css/system/components/align.module.css?qrgttk
Preview:	/**. * @file. * Alignment classes for text and block level elements.. */...text-align-left {. text-align: left;.}..text-align-right {. text-align: right;.}..text-align-center {. text-align: center;.}..text-align-justify {. text-align: justify;.}../**. * Alignment classes for block level elements (images, videos, blockquotes, etc.). */..align-left {. float: left;.}..align-right {. float: right;.}..align-center {. display: block;. margin-right: auto;. margin-left: auto;.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48759
Entropy (8bit):	5.5215063523389265
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfsce5XqY1TyPnHpX/KWY3SoavPVRhwmCgYUD0lgEw0stZc:/y9gZfA5h1UHpXxY3Soiuw0sU
MD5:	0A4E309B5F2D7439B4F8876B19F37FC7
SHA1:	7AC30F933A2B889EDBE5D3449F4EC90049B0E2A9
SHA-256:	F79723478F4C48501CD49AC52B81D6244A6562B9D3F08CE8AB208A8B8878D4C4
SHA-512:	891337D9CD308331BD0166BAA7C99C2B856D47F0ADE8AF596F71AFFC962546BBE0952554C51CC9A10E28BB4CEE3648AEC819D83A8935E69E95F53F5CBF141C4
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\app-a9735616a727a9b1be92[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with NEL line terminators
Category:	downloaded
Size (bytes):	145914
Entropy (8bit):	5.33693860599627
Encrypted:	false
SSDEEP:	1536:OA6yRUvHc0r8JZafx/UmLOCQ+mmwZaNbdKibCrPqKO6:jUv8qfx/1OJmlEibCzn
MD5:	6FA4401E25B9F872925DF833A0AEFB2A
SHA1:	2DC0549BC5570185ED5BF734298C22EE71DE9430
SHA-256:	0667759FF26F12E1E7B6594C495B4FA16A3A03A2954078728C489F093E767183
SHA-512:	20F7BA8AC3E044E18F6E98178C50C1C0E2E92572DF95188129D2FEACBE937F73D63B7B42003507F1F474520729C7A7F096B039B18FBEC95C47B2615D3ACA6846
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/app-a9735616a727a9b1be92.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[2],{"+VNo":function(t,e){t.exports="\t\n\v\f\r .....\u2028\u2029\ufeff"},"+ZDr":function(t,e,n){"use strict";n("n7j8"),n("OeI1"),n("JHok"),n("WevN"),n("TAD1"),n("sC2a");var r=n("TqRt");e.__esModule=!0,e.withPrefix=d,e.withAssetPrefix=function(t){return d(t,"/covid-19-ac-assets")},e.navigateTo=e.replace=e.push=e.navigate=e.default=void 0;var o=r(n("8OQS")),i=r(n("pVnL")),a=r(n("PJYZ")),u=r(n("VbXa")),c=r(n("17x9")),s=r(n("q1tI")),l=n("YwZP"),f=n("LYrO"),p=n("cu4x");e.parsePath=p.parsePath;var h=function(t){return null==t?void 0:t.startsWith("/")};function d(t,e){var n,r;if(void 0===e&&(e=""),!v(t))return t;if(t.startsWith("./")||t.startsWith("../"))return t;var o=null!==(n=null!==(r=e)&&void 0!==r?r:"/covid-19-ac-assets")&&void 0!==n?n:"/";return""+((null==o?void 0:o.endsWith("/"))?o.slice(0,-1):o)+(t.startsWith("/")?t:"/"+t)}var v=function(t){return t&&!t.startsWith("http://")&&!t.startsWi

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\back_to_top[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	529
Entropy (8bit):	4.819517992623224
Encrypted:	false
SSDEEP:	12:wm5GQ1j4R3NTDhuyguA2sGjFr1HHL1YsWp8m5GW1u86rHL:56/Dn1ACF1Hr1HWjKrr
MD5:	1539CD1795DA850B1FE05E3D979DFDD3
SHA1:	92DCA6BE12A6906FBEECF2955C731807565CBBA1
SHA-256:	AD501F10C168FD148081CD3533E3C621FCAC63CBB32E36CBE832655C541996C1
SHA-512:	81BBE4965F472A7D22D3823785D1E9A62619EC61507D2ADBA762E5531AEBE645B14D8B233DD26B8DD5621282BAD1F72FCDCDA1F97E091D502806579EF2E853B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\back_to_top[1].css	
IE Cache URL:	http://https://covid-19.ontario.ca/modules/contrib/back_to_top/css/back_to_top.css?qrgttk
Preview:	#backtotop {. background: url(../backtotop.png) no-repeat center center;. border: 0;. bottom: 20px;. cursor: pointer;. display: none;. height: 70px;. position: fixed;. righ t: 20px;. text-indent: -9999px;. width: 70px;. z-index: 300;.}..#backtotop:hover {. opacity: 0.8;.}..#backtotop:focus {. opacity: 0.6;. outline: none;.}..@media (-webkit-min-device-pixel-ratio: 2),.(min-resolution: 192dpi) {. #backtotop {. background: url(../backtotop2x.png) no-repeat center center;. background-size: 70px 70px;. }.}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\back_to_top[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1237
Entropy (8bit):	4.59414829644007
Encrypted:	false
SSDEEP:	24:2v/WFCy5VKm2WNcklMHdl2W9cnxcm4LAwEM8ecnxcmqS/cuDlPWSlFGlxqaunv:F5MmOka9nKd4EwrfKdX/pdPGyaG
MD5:	919FAD4E6F86603BBAF5A7606E8F6D02
SHA1:	7A3EF573004FF5DD49BD15DAFC2776066DEC009C
SHA-256:	34FE1A9D6C921F918BC8D1D37913A4DEBE03BF81F2A01CDBFA7897565E819794
SHA-512:	C8F9EF62C17F717C70484D58ECF7CA0049C9BD662C175379F7965B75ACB8E8016A97D50529CBE9AB39AFE4FB1F91E8D7256D5F9952B3BD3355B6169353653066
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/modules/contrib/back_to_top/js/back_to_top.js?v=8.9.13
Preview:	(function ($) {. Drupal.behaviors.backtotop = {. attach: function (context, settings) {. var exist = $('#backtotop').length;. if (exist == 0) {. $("body", cont ext).once('backtotop').each(function () {. $('body').append("<button id='backtotop'>" + settings.back_to_top.back_to_top_button_text + "</button>");. });. }.. backToTop();. $(window).scroll(function () {. backToTop();. });.. $('#backtotop', context).once('backtotop').each(function () {. $(this).click(function () {. $("html, body").bind("scroll mousedown DOMMouseScroll mousewheel keyup", function () {. $('html, body').stop();. });. $('html,body').animate({scrollTo p: 0}, 1200, 'easeOutQuart', function () {. $("html, body").unbind("scroll mousedown DOMMouseScroll mousewheel keyup");. });. return false;. });. });.. /**. * Hide show back to top links.. */. func

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\banner-icon-alert-xsmall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 35 x 35, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	684
Entropy (8bit):	7.561648097484827
Encrypted:	false
SSDEEP:	12:6v/7sYYX5dVmWzel3kMAvpK2Wm3G8Swqf3lOy39rIlh7fnRb:JYU5dVteSZ7q8SwMl9BIX5b
MD5:	9C107EF16D799B14DF23AC4F2BAC0820
SHA1:	F6D0961B1AE9086F3682CC9A302E4B197D150B3B
SHA-256:	B0ED8B23CF003933CA5E0D8C1A7254FAEF9C16458BE3BCEBE1E094CC1E240603
SHA-512:	903BAF4D512B792034E8D50216B24BE15E232686E228A13C1E4D41179E1B6F76EF2F605B35CEB90D9159DFE31E2FAD6AE04E6D4B178929F405BDF59CE09E898
Malicious:	false
IE Cache URL:	http://https://files.ontario.ca/banner-icon-alert-xsmall.png
Preview:	.PNG.....IHDR...#...#.....Y....pHYs.....~....^IDATX..1h.P....AC.\.A..... ....t..sp.D.4..v..w..(....p..."q...]qh..).!.%..;..K....n...../..^%.".J5.%.....#..\..z..u.J...4.)@...7.. zNG.F5.&`...k...J.....Q..q.KJ.....jX.`D}.YbY]Y...].m...;\.|!+.#.Z.0".n..x..&../...._...jX.4g.y.Y]Y.z^.q)od-..4.jX&...U...r..|T.F.....w...?e...4....`..'Ea6T.Z....px.....pF26S..o!..~.>.. ZY>..Nd~.K...6.....Y..[]..2.\.^...."J..d.....[.....|.....*Q.....`M_....;.Q..2.....`:.W.....s\..g..=.m..n.i;O5Y.....`M_...kE].N..w>.!";..n..4....1..=..... /'..SC...2.*.z.zN.t. 5.8T.H.D9..w. .Y . 0.@:...b.x.z.-{%b...(r...H+..@.~&6...v....n..Eg.i.x..s..xX.ToI.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1644380
Entropy (8bit):	5.579185646972128
Encrypted:	false
SSDEEP:	12288:vNetzXRr0KR2GRMzKBZcmknN7TTSacwH2AvJRa9DOc9uzP:1et10KfMzKBZcmkN7Te1EsJwzP
MD5:	A3F4FCB79410AB0223E07AF957F25866
SHA1:	658770C407CB2D1C9F66AC5FA8831A9F33831E7E
SHA-256:	4B76A2DD7B5DBE0AAAE16DC3C414486896335CCB82F0C9A4E0F0FF3739FBDDC7
SHA-512:	AC6E586AD3814528853224257832 4E4283B8702C7F20DD08503BD22BE8ECDE3FE75690CCCE1B83045F88380E07C4CAB6BDCA50D94349C719E3420CCFCC7063
Malicious:	false
Preview:	var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var ba,da,aaa,ia,ka,la,pa, qa,ra,ua,va,wa,baa,caa,xa,ya,daa,za,Ba,Ca,Da,Ea,Ia,Ga,La,Ma,gaa,haa,Wa,Xa,Ya,iaa,jaa,Za,kaa,$a,ab,laa,maa,cb,jb,naa,qb,sb,oaa,xb,ub,paa,vb,qaa,raa,saa,Fb,Hb,Ib, Jb,Mb,Pb,Qb,Tb,Zb,ac,ec,fc,ic,kc,lc,vaa,mc,nc,oc,wc,xc,zc,Gc,Nc,Oc,Sc,Qc,zaa,Caa,Daa,Eaa,Xc,Yc,$c,Zc,bd,ed,Faa,Gaa,dd,Haa,kd,ld,md,nd,qd,rd,sd,ud,Jaa, vd,wd,Ad,Bd,Cd,Dd,Ed,Fd,Gd,Hd,Jd,Md,Nd,Pd,Rd,Sd,Laa,Td,Ud,Vd,Wd,Xd,Yd,ee,ge,je,ne,oe,ve,we,ze,xe,Be,Ee,De,Ce,Qaa,le,Qe,Oe,Pe,Se,Re,ke,Te,Saa,Xe,Ze,We, af,.bf,cf,df,ef,ff,gf,lf,mf,nf,Taa,sf,of,uf,xf,yf,Ef,Bf,Cf,Uaa,Ff,Df,Gf,Hf,Vaa,If,Jf,Kf,Lf,Mf,Of,Nf,Pf,Qf,Yaa,$aa,aba,cba,Uf,Vf,Wf,Yf,$f,bg,hg,ig,lg,dba,og,ng,pg,eba,xg,yg,zg,fba,A g,Bg,Cg,Eg,Fg,Gg,Hg,gba,Ig,Jg,Kg,hba,iba,Lg,Ng,Mg,Pg,Qg,Tg,Rg,kba,Sg,Ug,Vg,Xg,Wg,mba,lba,Yg,oba,nba,pba,ah,qba,ch,dh,eh,bh,fh,rba,gh,sba,tba,ih,xba,jh ,kh,lh,yba,nh,ph,sh,yh,Ah,xh,th,Bh,zba,C

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\book-vaccine[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	114036
Entropy (8bit):	4.88625280764325
Encrypted:	false
SSDEEP:	768:YKo9BNvyFBGnbdrFnQQLWRxmk/Y5hfVNp/cOh5fn+Rh0cbyF6QlKA6mPPg/P:YKo9BNvybGbdZnQDxmzmRGjEHP
MD5:	F994B6380BA1CE89DD0EFFF5069DED0C
SHA1:	B2EA52F328956DBCAFB313D8F1303523A5283444
SHA-256:	79CA3D4D80368302418D7BADD8C9D2C046E5179362C0BFDCB962B8E9863338E8
SHA-512:	8512A0EC0D96F0D07F767CD66BF20BBD1EB47BC039EAD85492057613CA10E5DC994AEB81E0EA8E9EB9D9E8139B2872554CCBDB20540FAAF39BF4A58F7EA318 24
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/book-vaccine/
Preview:	<!DOCTYPE html>.<html lang="en">. <head>. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge">. <meta name="viewport" content="width=device-width, initial-scale=1.0">. <meta name="description" content="Find out how you can schedule your COVID-19 vaccine appointments">. <meta property="og:locale" content="en-CA">. <meta property="og:site_name" content="@ONThealth">. <meta property="og:title" content="How to book a COVID-19 vaccine appointment">. <meta property="og:url" content="https://covid-19.ontario.ca/book-vaccine/">. <meta property="og:type" content="website">. <meta property="og:description" content="Find out how you can schedule your COVID-19 vaccine appointments">. <meta property="og:image:url" content="https://covid-19.ontario.ca/c19-book-vaccine-assets/social_image_en.png">. <meta property="og:image" content="https://covid-19.ontario.ca/c19-book-vaccine-assets/social_image_en.png">. <meta name="twitter:title" con

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\co-covid-19-icons-workplace-2020-12-21[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 101 x 101, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1734
Entropy (8bit):	7.135004662670737
Encrypted:	false
SSDEEP:	48:4NkKoAuPnrPTrurr+iDobpMPuBLSqS05znEH+SoH:4BD0TLSqfpnp7H
MD5:	630DC64C876E8AA078295DD8B9CEB640
SHA1:	5455A8DB103AF0DE27ADF7825EA0ADDE32D94BFC
SHA-256:	A3ABD4483DE4E1B314DDBB09DCBCB7A8DF8716E2F6A098994AD710682D055D7C
SHA-512:	06D674A9D10261FBCE64C121A2A7BF8E23E6F847CBA4BFAF6FE76E97FC7C34F7EAFA1EEACC7B27FF0C86428285B380395DEE74E5E75702E13703F6D9D31175B B
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid19-cms-assets/2020-12/co-covid-19-icons-workplace-2020-12-21.png
Preview:	.PNG.....IHDR...e...e.....c.....(PLTE..... .....$$$)))...333666???BBBEEE HHHMMMRRRSSSUUUVVV\\\fffkkkpppwww.....`"....tRNS..... "#$%)*+,-./0123789:;<=>BDFGHIJKLMNabdefjloprstuvw..... .....M.....bKGD...;g....IDATh...WW.A...E.T.Gl.P.....F..j.@@.$HI.D...HGQ@..DQ..O.{^.-.$[f...*.sv.....T".i..j...+.Y...[i..<.&%..x.9.T.Jb cJ.HHM....";H..0F..s.d..lc.9.a.<._...../.I4.....w..t..KBB*@U.....2..^...:..w.[.CZ.<....%..= ;..)/..P.`K}..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\component.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	53285
Entropy (8bit):	5.169887911708994
Encrypted:	false
SSDEEP:	768:sy+ta8OMxBTedmgGhnAuhxrZJCGGVbmY2O4BfwPZnuj8VddPm0PjXKYhAClg:LqlRoZjddOiXKYhACO
MD5:	31F620E726F456732B9A64BBE2BE7A40
SHA1:	517BE2F6D5C0537E1B1485803A280F232683D709
SHA-256:	5083CBFC6D40E35C5A2D800E0B1B0A0F624AF5E842D23C0985B4225011A26421
SHA-512:	209977E8F2F413322C62F85F0DA680D821D111DB59DFE90EEFB19E40DC12B39B18EB29C04F31ED6DCF7F7CD18EA1BCF780C43249440E20B992D46884CD9967
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/component/component.min.js
Preview:	"use strict";angular.module("onesite.component.directives",[]).directive("onesiteHeader",["$filter","$timeout","languageService","routeService","redirectService",function(e,n,i,o,a){var l={en:"page/government-ontario",fr:"fr/page/gouvernement-de-lontario"};return{scope:{contentNode:"=",search:"=",update:"="},restrict:"E",replace:!0,transclude:!0,templateUrl:"/core_modules/component/partials/onesiteHeader.html",link:function(r,t){r.pathLogoHeader="/img/logo-ontario@2x.png",r.pathLogoPrint="/img/ontario@2x-print.png",o.regulateRedirect(t),r.altLang=i.alternativeLanguage(r.contentNode.lang),r.update.header=function(e){r.altLang=i.alternativeLanguage(e.lang),angular.isFunction(r.update.taxonomies)&&r.update.taxonomies(e.taxonomies),function(){var t=this;n(function(){t.click();var e=t.find("p.show-for-sr")[0];e&&angular.isFunction(e.focus)&&e.focus()},0,!1)}.call(t)},r.headerlogoAliasCollection=l,r.aliasToPath=a.aliasToPath,r.changeLangOnly=function(e,t,n){return function(e,t,n){var r=this;

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\covid-19-main-theme[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\covid-19-main-theme[1].css	
Category:	downloaded
Size (bytes):	144817
Entropy (8bit):	4.993832219720816
Encrypted:	false
SSDEEP:	768:r8/jk31n3cumEPWbhJKTpydeEFNV5n9fXboaGoswm4lHgKGYsjh+cefR8i:Abssur1EFNVHnGoswm4lHgKGYsjh+cs
MD5:	085E2441EC091BAD5A18860D5762DD73
SHA1:	5544BC5CE438A323882B2C25C9203504F72EED1C
SHA-256:	C4A3F28EAF72B342036F69183E0DE6D708B31F19154ABE583BEE35540D673CB9
SHA-512:	B00D40DC553146187923A461F2816FE3E5DD1EDEE5B1E125A9A8BCD385F85683B5168EC08121F7026099FFE99BC96B23AEC23BC89F78F862584ED01B5B61ECA
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/refactored-css/covid-19-main-theme.css?qrgttk
Preview:	.ontario-button:active,.ontario-button:focus,.ontario-header-button:focus,.ontario-input:active,.ontario-input:focus{box-shadow:0 0 0 4px #009adb;outline:4px solid transparent;-webkit-transition:box-shadow .1s ease-in-out;transition:box-shadow .1s ease-in-out}.ontario-h1,.ontario-h2,.ontario-h3,.ontario-h4,.ontario-h5,.ontario-h6,.ontario-sidebar--left>ul>li>a:first-of-type,h1,h2,h3,h4,h5,h6{font-style:normal;font-weight:700;text-rendering:optimizeLegibility;margin-bottom:1rem;-webkit-font-feature-settings:normal;font-feature-settings:normal;font-family:Raleway,Open Sans,Helvetica Neue,Helvetica,Arial,sans-serif}.ontario-h1,h1{font-size:2rem;letter-spacing:.04rem;line-height:1.2;margin:2.25rem 0 1.5rem}@media screen and (min-width:40em){.ontario-h1,h1{font-size:2.5rem;letter-spacing:.04rem;line-height:1.29}}.ontario-h2,h2{font-size:1.6875rem;letter-spacing:.03rem;line-height:1.33;margin:0 0 .75rem}@media screen and (min-width:40em){.ontario-h2,h2{font-size:2.0625rem;letter-spacing:.02r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1336
Entropy (8bit):	7.776296896714416
Encrypted:	false
SSDEEP:	24:2ELyu9N214knvN7rkS5PA3uEJHg1zTX6M4iQ7VfEVWnGrgbmVs/1:2Ee/ik17bZA3uEJA1zTXH4xEVWnMgya1
MD5:	BB3DEBD3FE12736EE94C99D20D42FFD3
SHA1:	C2C87994245FDAE0B3093B80614B202F90099D27
SHA-256:	EE877BF7E33D22CD354278EDBA7FB9DADCAAB3FABEA37CD8E3AFCA2FD824503D
SHA-512:	02AE48449B746503D22940E24F2796E44E14D52870B82C36DC3F7F902EBBA3D012DF9605BFB7083ABE1212452DEB82D89FFAF9220057A8BEDC2662ABC19D37D
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/covid-19-ac-assets/favicon-32x32.png?v=95d5a2a6253850552d499cd53df6b4a2
Preview:	.PNG.....IHDR... ... .szz.....pHYs.....~.....IDATX.W[(.Y..{....f\2n..7..(3[<.... .h<)e.<y..@.x@).9..a.t..(N....1..Y.j}.....|....}.o}.f3&..;....g.1.m.G...d..a.....k.3M.....Vb&.-`4.7.{..t..%.D...r.3..Ka.V.U.....wK...K..ma....B.$7...aW....l.Y.O.BoU!<..;...n.....p...7b(...gH..{..j.P....%.=<<4.b..5..$.....).~~~.....t:!66Vc.#00.....BP<..".....r.....'P .....3.....v....#.....EHKK.1aH..l.,.s6.....`kk....auu....uB.....666`nn.....z...2r.....>(@..{....*....kHf.....\.....{....cn.$.[.....S,Pl.C...1..&.....oFw.....M.....4'. ....&j....f}}}|.....1:.....v.!++...../.,.#....p1H....l.b.A7-JHH...s~...8xzz..8.....&f...iff.....l..[.q.....i.....-88."##u....4.GGG....j/...7.....z.....{rr..Abb"...r. ...IM`....T.B&..fZ.H.,(.9.....4....)....b.....!!...`}}.3hmm.....,PH....+..1pj.....Cjii..c@bL .....N.R..SWLLLp&....:.0...S..0.....?I.X.BWW.V.e&.l.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 3 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	15406
Entropy (8bit):	2.2429689033058424
Encrypted:	false
SSDEEP:	96:Ml3XHQgQw4F2VF8InOanFxRvYaNsKQZA4/mnNe:63XHQfYsyneaNsC4enN
MD5:	09BD5B5426A668D935E28A5E7B667AC9
SHA1:	1555B05E7D4BE697F795F148D157872361779375
SHA-256:	AEB3B21855F07B7E9E2632483B0A24488A8F294A152E2D64B96C8A4145A55B51
SHA-512:	B57B5ECA260F7B5EEC154969FAACC5224D5ABBC922B1F033F0ADB667AE77544E0002659BA010216D52C634A1ED2B490C5D1E4A2BF3A92D60FF030F2FB276F5I 8
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/favicon.ico
Preview:	......00.... .h&..6... .... .(....&..... .h....7..(...0...`..... .....,...J...j.....j...J...,..... .....5...z.....z...5..... .....I.....I.....i..... .....i.....$.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\footer-default-supergraphic-logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	655
Entropy (8bit):	5.4192569642679995
Encrypted:	false
SSDEEP:	12:TMHdPhGi/nzVJ/KYf3nwnTDHLdudmT6vb7bULtsXKX:2dMATLf3wnTDrtCg2KX

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\footer-default-supergraphic-logo[1].svg	
MD5:	A5F24D16C913DF02269E8AA8515411FB
SHA1:	230ADB5E203A9DDFB0847640A73CCB37A28D4BE9
SHA-256:	CBF618B92A9CDFBC7A976BA731D29E190E08C1F98C4D8A315EFE6F946FEB02FF
SHA-512:	C61FD75534E3D7ACCF1B060E5A1BD50BA61C478E008939AC6FF451D8C814329CCF37924D7A54B6B62BBC89D0D33EB659EE5D86A8379E6FD65D4E207699B438 8
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/scss/base/ontario-design-system/logos/footer-default-supergraphic-logo.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 25.0.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. viewBox="0 0 4410 4093" xml:space="preserve" height="4093" width="4410">.<style type="text/css">...st0{fill:#1A1A1A;}.</style>.<path class="st0" d="M2494.4,0C1689.4,0,805.7,218.5,0,772.3l362,856.2c590-449.3,1330.4-725.9,2131.5-725.9..c299.5,0,601.5,45.4,880.6,118.1c-227.9,821.4-749.4,1560.5-1556.8,2054l99,1017.9c1586.7-773,2382.7-2252,2493.7-3652..C3831.3,161.3,3177.6,0,2494.4,0z"/>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\foundation-6-dropdown[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1646
Entropy (8bit):	4.864857788902514
Encrypted:	false
SSDEEP:	24:SUkoiiJBoVwvR1E1ioJfFAjNAEGZr18ApxlQS9EQyKFWaEEd:NiiJNvEtJiuEGZr18ApxlQvQyKFWaEEd
MD5:	1997E1D1A551670EF3A501A65AFAEA60
SHA1:	52B6AE1D335EC323A267A9C0573CC0AE1CDEDA89
SHA-256:	31763C3827BF8E1BA940B539BBD396D090D39BD6BEFB4A01F663BBC5E8770924
SHA-512:	5BB67346AD6A57179ECC8FC158ED2681894FF65A7656E03AC8E1D430C2ECA931BFC6C6CC87568BDB0E6D550DB5FBE9E5EB34852DAA220BADF40E9ADFE6A9 E03
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/vendor-assets/styles/foundation-6-dropdown.css?qrgttk
Preview:	@charset "UTF-8";./**. * Foundation for Sites by ZURB. * Version 6.6.1. * foundation.zurb.com. * Licensed under MIT Open Source. */....button.dropdown::after {. display: block;. width: 0;. height: 0;. border: inset 0.4em;. content: '';. border-bottom-width: 0;. border-top-style: solid;. border-color: #fefefe transparent transparent;. position: relative;. top: 0.4em;. display: inline-block;. float: right;. margin-left: 1em;.}...button.dropdown.hollow::after,..button.dropdown.clear::after {. border-top-color: #1779ba;.}...button.dropdown.hollow.primary::after,..button.dropdown.clear.primary::after {. border-top-color: #1779ba;.}...button.dropdown.hollow.secondary::after,..button.dropdown.clear.secondary::after {. border-top-color: #767676;.}...button.dropdown.hollow.success::after,..button.dropdown.clear.success::after {. border-top-color: #3adb76;.}...button.dropdown.hollow.warning::after,..button.dropdown.clear.warning::after {. border-top-color: #ffae00;.}...button.d

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514 B
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\libs.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	415978
Entropy (8bit):	5.237457563501528
Encrypted:	false
SSDEEP:	6144:NO16SvjX9kv4VgkVr/H+Ef0/W9sY6pNaZLutgUJ:NVYtkA3jPsYDyiUJ
MD5:	49763D93C2BABB3D39CF2FECC55E651F
SHA1:	F9CCC005BC35C2DD1ED7D116C2DC9811B3BAD4CA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\libs.min[1].js	
SHA-256:	6875D73440C8B7D1F3CC68CE7AF3BEBAE7A5F87424D704608FD1CF2899A53AB6
SHA-512:	6B59C94425CEC12FC1B4D4135E707968B416E3237F713B198616DE279BBCDA35BFF220A23B16664351EC75D6A9E2A85DF1B3B2B8963916B1858B726D8087B457
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/js/libs.min.js
Preview:	"use strict";var _typeof="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbo l&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t};!function(c,l,n,a){var t,e;t=["foundation-mq-small","foundation-mq-small-only","foundation-mq-medium","foundation-mq-medium-only","foundation-mq-large","foundation-mq-large-only","foundation-mq-xlarge","foundation-mq-xlarge-only","foundation-mq-xxlarge","foundation-data-attribute-namespace"],(e=c("head")).prepend(c.map(t,function(t){if(0===e.has("."+t).length)return'<meta class="'+t+'" />'})),c(function(){"undefined"!=t ypeof FastClick&&void 0!==n.body&&FastClick.attach(n.body)});function d(t,e){if("string"!=typeof t)return c(t,e);if(e){var i;if(e.jquery){if(!(i=e[0]))return e}else i=e;return c(i. querySelectorAll(t))}return c(n.querySelectorAll(t))}function i(t){var e=[];return t||e.push("data"),0<this.namespace.length&&e.push(this.namespace),e.push(this.name),e.j

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\logo-serviceontario@2x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 314 x 76, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3429
Entropy (8bit):	7.890173045368409
Encrypted:	false
SSDEEP:	48:C/6BjsSsRFT00zid+42Av1T51eeGM21wq5CBJj/BbpCIdazdCTEetQj4LFBBxxoj:CSBwSC50Kisi+CNbpC6azm+j4Llkj
MD5:	140AB78A5FD95A567C1E91E8BDA59E72
SHA1:	C36C77A4C3D2AD9C926DA8C6A18280BC007BC1E7
SHA-256:	ADE4510791D1B4997FE624230C4621811B9B7624394262500C8B592607AEC214
SHA-512:	4EE41DD144C7F16B5A614279AB7D345BBB7C7C7A94980F35B2051AE1A1C1D60314A7A77A4773D4437147AF94265B166657479D61A5CC1BD2EF3FA3EA3D18733
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/logo-serviceontario@2x.png
Preview:	.PNG.....IHDR...:...L.....N{4....pHYs.....tEXtSoftware.Adobe ImageReadyq.e<....IDATx..?.]G..-7.$.P..HX..R..H.....$.(..H...o*..."R8U..48R6JJ.LC..F.....HA..P`.)$e..Xg s3.3w.}s.|..y..}w...9s...d...AX]..... .+.... ..... .":A.... ...N..AD'.. ...A.... ...A.... ...A.Dt. .":A.... ...N..AD'.. ...AD'.. ...A.... ...A.Dt. ..qdV?.....k...}.....{.....fryse.lzr....x.?.6.. .....sp....y.Wo..l.iGD.c..G...6.o>.....k..l...i.....AWrz...'../.|...'.kv..s.}.j ?A.....~...r..E.-.....<.|../....?7y...w....!....v.m.&9....4.>u.7.....".0.GG.z.....`.v..T...'.=.....y#/ ..Bvk.~:.1Yn...t.L.s.aV...'<.;...9.S.S.=...%Yfp...+9...Gr...[;!..7...y.K*y..`.g...:.a.<..n.....\.%..0h....M^.<.....~....>..$;.vx...F%:/OBY.X.#.+..Gh%..KU....E.[.....K.b..f)g.9...<W$W>.!... ..7.).1..+}Ze...G..\....uo.d...;zw...\II...n\..j..a#..p..s.Z6.L.$.....0..~N.l...Sj.w.fv..f.yU]^.... ...Q..._..g.....w.....~..Jy....c...<.}.E0.T~..y;..u.z..G..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\logo-serviceontario@3x[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 828 x 188, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	24516
Entropy (8bit):	7.971561164547846
Encrypted:	false
SSDEEP:	384:yCr/t9JbCkqYQ7rgwk321q5cnq+iq37GTiu9uoozt3mdPh/o51ol7XES5DkE1p1s:yCr//Ju/7rgwxFnqlq37GOztoPS5Kl7g
MD5:	40F71798A45166F3E7D8BEFEC0B0E792
SHA1:	160114222E6595D2FE99B3105F7E1AC4CA0E035D
SHA-256:	B49B863CD7D397BE87B95E00D87BCB29B6A6754EBA20A4A98B65344F0C240CF2
SHA-512:	D254944F64B316DA42EB7695B24EF23177C7E5F5701814FEEE1EB547F5441EA9761B245AECBD39212F08B3660635E70E5AB1D27F2F5F215B62D1BF2BD9C795EE
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/img/logo-serviceontario@3x.png
Preview:	.PNG.....IHDR...<.....sBIT....|.d.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<... .IDATx...w`..?....I....%..I.w.m06.t..@B.....B.$.o8.wI..q).....b....mY.eY....2 ..C.C\..]i....H..y.I..g....0xd.n.B.!..B.T%".....0..Z!...t..E.!..B.!.1..cT..<0.;)."..B.!...@..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[. ..B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B. !$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[...B.!..B...<..B.!...E..!..B.!$lQ.C.!..B..[..^.!dja..z.....%.(...+.AX.!...cX.y%.....v...(.ae$.Q.3...A....P*x.....W...<.....x ...Q.....!. B..... =2...v....V4.t.aed..X.*...)..8(9..Hp...`...k....K..#..nxE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\mainstylePHealthPortal-en[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	183016
Entropy (8bit):	5.350996575136658
Encrypted:	false
SSDEEP:	1536:npXGjUEJk15LDm4oUB5eXXmwDm4oUB5el/7kQ:pXcdJkBB567B5s7kQ
MD5:	19B829E81CBE2523FC9BA03C18DA3FE9
SHA1:	E97FAF1F9C6B26629D20AE560288E2076B0658E9
SHA-256:	BBF22F54AB8486ED6CBAAA3BBD09E81A1FB262B2B340868AECA7E4B458FEAEAA
SHA-512:	72C754C622D73063CDA15B6D758018BEDD798873B4E83D209BAAFAA8AA5A4BE329F301B5AA036C42FCA4FA62AB1D0A2CCB3EAB1EABB3685B1A8F9669A67AB DE6
Malicious:	false
IE Cache URL:	http://https://www.phdapps.health.gov.on.ca/phulocator/Style/mainstylePHealthPortal-en.css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\mainstylePHealthPortal-en[1].css	
Preview:	/***** begin PLUMTREE PORTAL 4.5ws STYLES *****/..A..{COLOR: #000000;}...inputBox..{FONT: 10px verdana,arial,helvetica,"sans-serif";}...linkCap..{FONT: 10px verdana,arial,helvetica,"sans-serif"; TEXT-TRANSFORM: uppercase; COLOR: #000000;}...linkCap A..{TEXT-TRANSFORM: uppercase; COLOR: #000000;}...wizBckgrndCldNarrow..{BACKGROUND-COLOR: #F4F4F4;}...wizBckgrndCldWide..{BACKGROUND-COLOR: #CCCCCC;}...bnr..{FONT: bold 10px verdana,arial,helvetica,"sans-serif"; COLOR: #FFFFFF;}...bnrDate..{FONT: 10px verdana,arial,helvetica,"sans-serif"; COLOR: #FFFFFF; TEXT-ALIGN: right;}...bnrHead..{FONT: bold 14px verdana,arial,helvetica,"sans-serif"; TEXT-TRANSFORM: uppercase; COLOR: #FFFFFF;}...bnrHelp..{FONT: bold 10px verdana,arial,helvetica,"sans-serif"; TEXT-TRANSFORM: uppercase; COLOR: #FFFFFF;}...bnrHelp A..{FONT: bold 10px verdana,arial,helvetica,"sans-serif"; TEXT-TRANSFORM: uppercase; COLOR: #FFFFFF; TEXT-ALIGN: right; TEXT-DECORATION: none;}...bnrSubHead..{FONT: 12px verdana,arial,helvetica

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\modernizr[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	51351
Entropy (8bit):	4.6306630219418095
Encrypted:	false
SSDEEP:	1536:9RCJ6/KpVsnUMxvXmET56JYFE7qbe/7Y8fjWWy+4GrkfwuXxJ44ipW/VPRLq277a:9j/FjzarzCT71Pts
MD5:	C1FF1650BBA6E39089834E708129D723
SHA1:	7D1CEA058027485E9CCF1A92E38823ACB05C0659
SHA-256:	7DFC3EF73C1284C7AFF3C5CDAC3812D212C8B899037D7860C8BA20A1DEFB9A7F
SHA-512:	94EB43018F4A313D561FD171E894AE64B1F18C2F30988071B0D14BEA024F686EEC2C856848EF720AB6963B0A8B2D7FADC6C3B0D21D9C1EF71426524FBCC968E
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/vendor/modernizr/modernizr.js
Preview:	/*!. * Modernizr v2.8.3. * www.modernizr.com. *. * Copyright (c) Faruk Ates, Paul Irish, Alex Sexton. * Available under the BSD and MIT licenses: www.modernizr.com/license/. */../*. * Modernizr tests which native CSS3 and HTML5 features are available in. * the current UA and makes the results available to you in two ways:. * as properties on a global Modernizr object, and as classes on the. * <html> element. This information allows you to progressively enhance. * your pages with a granular level of control over the experience.. *. * Modernizr has an optional (not included) conditional resource loader. * called Modernizr.load(), based on Yepnope.js (yepnopejs.com).. * To get a build that includes Modernizr.load(), as well as choosing. * which tests to include, go to www.modernizr.com/download/. *. * Authors Faruk Ates, Paul Irish, Alex Sexton. * Contributors Ryan Seddon, Ben Alman. */..window.Modernizr = (function(window, document, undefined) {.. var version = '2.8.3',..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-analytics.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3387
Entropy (8bit):	5.059305558706283
Encrypted:	false
SSDEEP:	96:N/vaLKsMcz+O7ExvPw9DNLPcjPiB99fkMD5Cp5mCqI+durVi:NkMQuE1oi
MD5:	C39507E3A4CDA01C1BD9B02103241886
SHA1:	828E2A9DCE54355640A572487982A171CA367B45
SHA-256:	91AD764A124D3068A6656221CCE93607FAB7D3C51B4126344D6707F18F228C58
SHA-512:	F3BE53E35E97BBECD2663D6A6BB0F5C58186E979A1B8198994BCC33D547A023EE5542E5D530C299E9F45119F92F157F8A4C9986952DDAE8249CD43210420C5F
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-analytics/onesite-analytics.min.js
Preview:	"use strict";angular.module("onesite.analytics",["angulartics","angulartics.google.tagmanager","onesite.analytics.directives","onesite.analytics.filters","onesite.analytics.services"]).config(["$analyticsProvider",function(e){e.settings.trackRelativePath=!0,e.registerEventTrack(function(e,t){if(t.category=t.category||"missing-category",t.value){var n=parseInt(t.value,10);t.value=isNaN(n)?0:n}if(window.ga){for(var i={eventCategory:t.category,eventAction:e||null,eventLabel:t.label||null,eventValue:0===t.value?0:t.value||null,nonInteraction:t.noninteraction||null},a=1;a<=20;a++)t["dimension"+a.toString()]&&(i["dimension"+a.toString()]=t["dimension"+a.toString()],t["metric"+a.toString()]&&(i["metric"+a.toString()]=t["metric"+a.toString()]);ga("send","event",i)}})}]);."use strict";angular.module("onesite.analytics.directives",[]).directive("scrollToBottom",["$window","analyticsTypeaheadService","analyticsEventService",function(n,c,t){return{restrict:"E",scope:!0,template:['<div ng-init="si

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-health.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2716
Entropy (8bit):	5.191556252285694
Encrypted:	false
SSDEEP:	48:/0MiqXssrzHoSbzpDlDvpcijZiWU2LLafkI1HbZ8GVLMDyOlnbxN09Xp2fn:/WszFbzNlDvv02LL211GGV/Olnb052f
MD5:	9CD27F9A2902AC378467C824DB978A5B
SHA1:	05D4E5D36B35783E034ACC6A5268D28E2E69082C
SHA-256:	EC78B2DC4F57E8D83AE6244B7C6DECD315C0544811D137F3D96D92C842F0B845
SHA-512:	EB25B8A78245E0DD88B4A9918CE7BCD4BC9F79DC61D4DF6FE7607D083FBBA0C77182E563F4968C56E55E86D0C8C8AC3CD35C40D79464DC71DA64FE5155B4E0E
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-health/yellowCard/onesite-health.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-health.min[1].js	
Preview:	"use strict";angular.module("onesite.health.yellowCard",[]);."use strict";!function(){function e(o,n,r){var t=this;t.component="phuForm",t.phuInfo={},t.errorMessage="",t.errorOccurred=!1,t.iconAvailable=!0,t.setComponent=function(e){t.component=e},t.getHealthUnit=function(e){return l(),e=n.transformPostalCode(e),n.validatePostalCode(e)?n.queryForPHU(e).then(u).catch(h):(i(a),o.resolve(!1))},t._setError=i,t._clearError=l,t._formatPostalCode=c,t._isOnIcon=s,t._handleResponse=u,t._handleAPIError=h;var a="We couldn.t find that postal code in Ontario. Please use one of these formats: M5V 3Y3 or M5V3Y3.";function c(e){return e.slice(0,3)+" "+e.slice(3,6)}function i(e){var o=e!==a?"api":"malformed";window.ga&&ga("send","event",{eventCategory:"icon-lookup",eventAction:"error",eventLabel:o}),t.errorMessage=e,t.errorOccurred=!0}function l(){t.errorOccurred=!1,t.errorMessage=""}function s(e){switch(e){case"https://drhd.icon.ehealthontario.ca":case"https://hrhd.icon.ehealthontario.ca":case"https

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-holiday-pay-calculator.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	7106
Entropy (8bit):	5.247064945099283
Encrypted:	false
SSDEEP:	96:vBu1+zG/20SAclNek4zNvIkLCEBcNUaFKTVQcuNQOCCHhQ+H+IF/ms:X0OeBzKkmEFZqZuLK6+eXs
MD5:	1E8EA161887BDB34E5719CFB6E6B3D98
SHA1:	0D1A12896A87757326A6D7E6750C5FBFE44D786D
SHA-256:	3B6FD807B693AA20CB3A9A80410E9A3EE1950F2E7D7D6B7A2317EA66680060DB
SHA-512:	95AFD64FEB218445A632F63F9B675242725564E3DA3DBCC954B6846FB61A0593EDFA930B6EAF223A13AFE20712CFCC2E1A540578231C2CC94D1FEDC1A14E602D
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-holiday-pay-calculator/onesite-holiday-pay-calculator.min.js
Preview:	"use strict";angular.module("onesite.holiday.pay.calculator",["onesite.holiday.pay.calculator.services","onesite.holiday.pay.calculator.controllers","onesite.holiday.pay.calculator.directives"]);."use strict";angular.module("onesite.holiday.pay.calculator.directives",[]).directive("onesiteHolidayPayCalculator",["weekLabels","getDateObject","languageService","daysFromToday","selectedCheckboxes","formatDateForAnalytics","differenceInDays","subdayOptions",function(a,t,o,l,s,c,i,r){return{restrict:"E",scope:!0,replace:!0,templateUrl:"/onesite_modules/onesite-holiday-pay-calculator/partials/onesiteHolidayPayCalculator.html",link:function(e){e.language=o.currentLanguage.get(),e.weekLabels=a,e.daysFromToday=l,e.getDateObject=t,e.selectedCheckboxes=s,e.formatDateForAnalytics=c,e.differenceInDays=i,e.subdayOptions=r}}}]);."use strict";angular.module("onesite.holiday.pay.calculator.controllers",[]).controller("OnesiteHolidayPayCalculatorImpl",["$scope","holidaysOfTheYearService","languageService

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-live-chat.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2509
Entropy (8bit):	5.094125766726055
Encrypted:	false
SSDEEP:	48:d/fhCajQVjQVsyKIcOtqEL2tQp4ojMDkeNzBIVTRAm+/9Rf35z8xLu:dnrj2jHyJcIjrVT45z3
MD5:	9E632AD1FEA5C87150A0EB8734EBF28C
SHA1:	C8F783A25FD2BFB5F73BBAE5FBB96B638DA21245
SHA-256:	4114DD2B4A8CA98EB097AFD2D5673D0FBE89BE50E54DAED20490646D9127D32F
SHA-512:	2180583E252D4707362003EE94125739016D0C99A7AE403004249EC42CC806D6082F3444C3FBBB99FE07D8407AA1E59F711B477E21A3B969737EBE89E08109E4
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-live-chat/onesite-live-chat.min.js
Preview:	"use strict";angular.module("onesite.live.chat",["onesite.live.chat.directives","onesite.live.chat.services"]);."use strict";angular.module("onesite.live.chat.directives",[]).directive("onesiteLiveChat",["redirectService","liveChatService","scopeService","stringService","$parse",function(a,i,n,l,e){var o=e("node.content.id"),r=e("node.content.lang"),s={en:"https://www.webchat.ccm2.gov.on.ca/EO_Webchat/iceMessagingWeb/Chat.html?destinationURI=sip:im_990a_sw03@ccm2.gov.on.ca&lang=en-CA",fr:"https://www.webchat.ccm2.gov.on.ca/EO_Webchat/iceMessagingWeb/Chat.html?destinationURI=sip:im_990a_sw03@ccm2.gov.on.ca&lang=fr-CA"},c={en:"page/employment-ontario-live-chat",fr:"fr/page/clavardage-avec-emploi-ontario"},u=["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"];return{restrict:"E",transclude:!0,scope:{title:"@"},replace:!0,templateUrl:function(e,t){var a=angular.isString(t.type)?angular.lowercase(t.type.trim()):null;return"body"===a?"/onesite_modules/onesite-live-chat/p

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-moment.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	18921
Entropy (8bit):	5.1828626911292055
Encrypted:	false
SSDEEP:	384:Ak1AdDaYLsp6fL8Ra1p5OZBmf54OMpUgv8SfcBY2Q/VsOgEpK:OuZRcpHR4O+v8Sfcc/2TEpK
MD5:	F4C2C7DCE7F310308F3202F7672E0FBC
SHA1:	3B9A391C9B34E13A9323895F27E30C6C58D803C4
SHA-256:	F9D8A28DA9F0AF8B8BADA0B6CF7A09141E58302062FDA2FD047B2280B10567F5
SHA-512:	44BB499A1905FC467DBDD678598631C71E8E1B00A8680150BEBBDC6CDC85EEB1D932B75D9C0E9764353DF2AFE9918FBB850AEA60BA7675CFBCBAB45ACE0A1147
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesite-moment.min[1].js	
Preview:	"use strict";angular.module("onesite.moment",["onesite.moment.services","onesite.moment.controllers","onesite.moment.factories","onesite.moment.directives"]);."use strict ";angular.module("onesite.moment.controllers",[]).controller("OnesiteDateAddImpl",["stringService","timeService",function(i,u){var o=this;o.add=function(n,t,r,e){var a=i. strToDate(n);angular.isNumber(t)&&(a=u.addYear.call(a,t)),angular.isNumber(r)&&(a=u.addMonth.call(a,r)),angular.isNumber(e)&&(a=u.addDay.call(a,e)),o.date=a}}]) .controller("OnesiteDateSelectorImpl",["stringService","timeService",function(i,n){function c(n){return angular.isNumber(n)&&!isNaN(n)}var h=this;h.stringToInteger=functi on(n){var t=(n=angular.isString(n)?n.trim():null)&&""!==n?parseInt(n):null;return c(t)?t:null},h.daysInMonth=n.daysInMonth,h.monthCollection=i.monthCollection,h.dateExist s=function(n,t,r){return r<=h.daysInMonth(n,t)},h.updateModel=function(){var n=h.validateYear(h.year),t=h.validateMonth(h.month),r=h.validateDay(h.day),e=angula

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesiteContentDate[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	367
Entropy (8bit):	4.605116063766543
Encrypted:	false
SSDEEP:	6:nsZCdW5KLTeb4am5rKgJq9TRGHKgJWk3TRa+YNWbyRXTuTHRM/:naCV31arQd05D4xy
MD5:	B734290BF6C29ACD25F37BF6AE7C74A6
SHA1:	DD46AB64053914894DBA40EED5991CA9021CD036
SHA-256:	DD1F871501A564211AEF5F7603BC12B2AD7C2C85CEA48EF06E2C43F1BF47A090
SHA-512:	0ACF6894D03AFF6427EBBFFC2584E82CD1AA2BF22BF76ADA4300AB0655E45604CE5E391545A87C63410185A6AC279EE1C663272FB7F4199E012EC639EAF9047
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/core_modules/component/partials/onesiteContentDate.html
Preview:	. <small class="right". ng-switch="language">.. . {{ text | translate }} : {{ date | date: 'd' }} {{ date | date: 'MMMM' | translate }} {{ date | date: 'yyyy' }}. .. <span ng-switch-default>. {{ text }}: {{ date | date: 'MMMM d, yyyy' }}. .. </small>. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesiteSearch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	2666
Entropy (8bit):	4.837246446994693
Encrypted:	false
SSDEEP:	48:5WhhtO+eV79QPdsCDghJsnFO+b+ax25Aqqb6VLH6y4VWQ:5JmPdob1aKX9yVh
MD5:	9458FFA88509BE41D5770C3F17FFCBAC
SHA1:	772F52826CA4A7E6FDDB77A66B44C1842F00A8E1
SHA-256:	C9C63FAFA69AC1298BFB069000050FAFFCB1D7124698B2E469FB632BC133286A
SHA-512:	2EBFA960F6F3B5E6DEDD3AF1FE10975C7B370814D83E62E91FD21C9BA4CE313DEF69DE9E98914B36B69C346386AD562A3CF6B563DC1756EDA83937E63E6A41 4
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/landing/onesiteSearch.html
Preview:	.. <div class="small-12 large-8 medium-12 columns main-content". ng-init="last={}". ng-switch="onesiteSearchImpl.lang">. <h2 class="hi dden-for-small-up">. 1-{{ pagination[0].size | formatNumber:onesiteSearchImpl.lang:0 }}. {{ 'of' | translate }} {{ onesiteSearchImpl.total | formatNumber:onesit eSearchImpl.lang:0 }} {{ onesiteSearchImpl.total === 1 ? 'page' : 'pages' | translate }}. </h2>.. <div class="results-page". ng-repeat="paginate in onesiteS earchImpl.pagination | limitTo: onesiteSearchImpl.pageIdx + 1". ng-init="$last ? (last.paginate = paginate) && (last.remaining = onesiteSearchImpl.total - paginate.idx * onesiteSearchImpl.config.pageSize) : null". aria-hidden="{{ !$last }}". ng-class="{last_range: $last}">.. <div class="search-results". ng-repeat="result in (onesiteSearchImpl.resultList | slice:paginate.fromIdx: paginate.toIdx)">. <div ng-include="'/onesite_modules/onesite-

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesiteSearch[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text
Category:	downloaded
Size (bytes):	1046
Entropy (8bit):	4.767655045044842
Encrypted:	false
SSDEEP:	24:hSk2vEu874Qn6WnFXKM0Nr1iFXByxT0JkFX1NnFXBIMv6F:huEN74XKaz1CW+gV0
MD5:	85A46B07F39569490C6F241998C2D57C
SHA1:	830063ABC7535A4ACCCE58C5F766B5DC639BCED6
SHA-256:	8D3F2276D6BABD9F5CC64F8BF7B9A1CBA1125603DF96C189154DC4981ABFD165
SHA-512:	398C297448116031EB815B2FD382A4012A84AB5091EDFEC85739E7E2DC95C7B04884EBA55FA4F5E86D8BA555ACA43181FFEC11B7F13486A655D9264D4CF4D19
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/openData/onesiteSearch.html
Preview:	<form name="filterForm". ng-submit=". onesiteSearchImpl.filterHandler.dirty = true;. init(true).then(focusOnSearchButton);. ">.. <link rel="stylesheet" hre f="/css/hideHeaderSearch.css">.. Keyword Input -->. . <div class="small-12 columns". ng-include="'/onesite_modules/onesite-search/partial s/openData/searchInput.html'">. . .. <div class="row". ng-init="last={}">.. Search Filter -->. <div class="small-11 end medium-12 large-4 columns". ng-include="'/onesite_modules/onesite-search/partials/openData/filters/control.html'">. .. Result List View -->. <div class="small-12 medium-12 large-8 columns". ng-include="'/onesite_modules/onesite-search/partials/openData/result/listView.html'">. .. Related Links -->. <hr class="thick">. <div class="small-12 columns". ng-include="'/onesite_modules/onesite-search/partials/openData/filters/relat

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\onesiteSearch[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text
Category:	downloaded
Size (bytes):	420
Entropy (8bit):	4.753591950889029
Encrypted:	false
SSDEEP:	12:52cCj6HHIqC1iF1FEOyUMi4vTO6HHIqCkF1FEoDMZ:c56lJ1iFjhyUMikTO6lJkFj5MZ
MD5:	C47FF73E533D3EEC271F37C3248881FB
SHA1:	8764E00EFC0D7231DC7D2F80E25ED01740597239
SHA-256:	58D184A6213BEFF13D2ED89F3A0E5C0918E6B7E618220A1030FEEE0873C90B41
SHA-512:	75E03044D07C193BE1CF86C66268276295674CFE2ABED7530BED9DAD76176D25F6AC6C1D91B63BD4FBB017273DFB2E6A270E4BDCA81649D7BE39CC356E3383
Malicious:	false
IE Cache URL:	http://https://www.ontario.ca/onesite_modules/onesite-search/partials/tradeCalendar/onesiteSearch.html
Preview:	<div class="row". ng-init="last={}">.. Search Filter -->. <div class="small-12 medium-12 large-4 columns". ng-include="'/onesite_modules/onesite-search/partials/tradeCalendar/filters/control.html'">. .. Result List View -->. <div class="small-12 medium-12 large-8 columns". ng-include="'/onesite_modules/onesite-search/partials/tradeCalendar/result/listView.html'">. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ontario-header[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	6222
Entropy (8bit):	4.844898050083307
Encrypted:	false
SSDEEP:	96:kBZanKVWpDMRcOjUQ7scwYduZLsknKYidfoeF2:kuAa1F
MD5:	BE99F97DEF9F761341863B11742BD8B7
SHA1:	2DA2BF5C7C092012710C2E2C5E28FA99C0C605EE
SHA-256:	FDFDFF5841C35FCB333180DB8B7D5443B39746D4B9A02A2E70CB4474410E9C8E
SHA-512:	A0DBACB887A904F1111E4AC5EF56A15E44E80F651FB6D90BF1AFD692F68783301140DFAA7C9CB2CFF1BD054978BF31056BCFB496C7D42C7376CB4289ABFF09C
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/themes/custom/ds_theme/c19-assets/js/ontario-header.js?v=8.9.13
Preview:	// Utils.function getClosest(element, selector) {. while (element) {. if (element.matches(selector)) break;. element = element.parentElement;. }. return element;.}..// run asynchronously.function deferInFn(fn) {. if (typeof fn === "function") setTimeout(fn, 0);.}../*.Header.*/.(function () {.. "use strict";.. // review browser support. if (!("addEventListener" in window) || !document.documentElement.classList) return;.. var navPanelSelector = "ontario-header-navigation",. isReadyClass = "ontario-header-navigation--is-ready",. isActiveClass = "ontario-header-navigation--open";.. var header = document.getElementById("ontario-header"),. nav = document.getElementById(navPanelSelector),. openBttnToggler = document.getElementById("ontario-header-menu-toggler"),. closeBttnToggler = document.getElementById("ontario-header-navigation-close-toggler");.. var currentTogger = null,. currentDomEl = null;.. function showNavPanel(navpanel) {. hea

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ontario-icon--error[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	510
Entropy (8bit):	4.8430341235609795
Encrypted:	false
SSDEEP:	12:tvG1W9ocVn7eSZjocTCccTidtxLJXRit5:tu1OVKSZjoScONLJhit5
MD5:	F6BC09EAE0718AE9A3BB69F9AD988059
SHA1:	CA56C9D304B28E584BB203251E15CE8A7D84EE7A
SHA-256:	2CE06C836E10362D58478F672E0A3A106696419D6A07348A8DEA496D2E8AD7D6
SHA-512:	1C15D76F2809B7FA6DE25F88FEE6C6C4FD97C9F82E1486188F037A5F0613AD8FB9E1C2795F1703D34ABADD2A562E17476F5ED72590CDE21A62817E3D9248076
Malicious:	false
IE Cache URL:	http://https://covid-19.ontario.ca/c19-book-vaccine-assets/ontario-icon--error.svg
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 36.67 36.67">. <defs>. <style>. .cls-1 {. fill: #cd0000;. }. </style>. </defs>. <path class="cls-1". d="M684.91,385.94h-3.67v-11h3.67Zm0,7.33h-3.67V389.6h3.67Zm-1.83-27.5a18.39,18.39,0,0,0-7,1.39,18.67,18.67,0,0,0-5.95,4,18.34,18.34,0,0,1,0,31.3,13,18.39,18.39,0,0,0-5.37-13,18.28,18.28,0,0,0-13-5.37Z". transform="translate(-664.74 -365.77)" />.</svg>

Static File Info

General

File type:	Microsoft Word 2007+

General

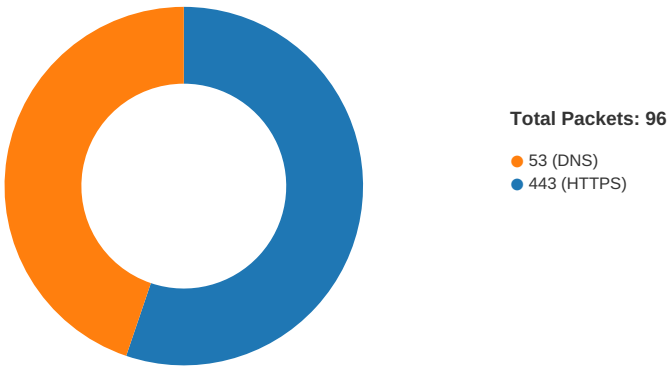
Entropy (8bit):	7.746354233936926
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	COVID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx
File size:	56869
MD5:	14d9efc0e6bd70f11db15709caffe72f
SHA1:	a9d37cf22facbe7ceda7dec88b983b5092597b5f
SHA256:	cbf87430a5ac83f27e1152f1cbe3b867400ccc68895c9a596697e8e64196c0ef
SHA512:	88f2f4db40640edcafe6f0bd172045a07cdfd03d575cf46e2a19e07c0506c2d26a9bdf112f8441b1b2f3b2332c350aa51bea2adc648e477340d2c2cd11d2200f
SSDEEP:	1536:7QVomU8A9ppjEmIohQbXbmr22FKBLiJkA:7Q7UFpJhCXaKBOyA
File Content Preview:	PK.....!..9r=....\.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 13, 2021 17:37:28.675700903 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.675729036 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.721920013 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.722011089 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.722209930 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.722273111 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.732255936 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.734021902 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.779342890 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.780551910 CEST	443	49165	143.204.11.100	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 13, 2021 17:37:28.785106897 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785135984 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785151005 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785181999 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785187960 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.785211086 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785224915 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.785233974 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.785253048 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.785275936 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.785310984 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.787437916 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.787508965 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:28.788871050 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:28.788942099 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:29.013139963 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:29.057571888 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:29.058262110 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:29.058320999 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:29.225094080 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:29.270390987 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:29.270466089 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:29.270632029 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.240710020 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.285125017 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287348032 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287430048 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.287692070 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287734985 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287754059 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.287770033 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.287776947 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287816048 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.287827015 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.287869930 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.288978100 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.289028883 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.289028883 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.289067984 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.290196896 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.290240049 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.290268898 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.290302038 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.291449070 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.291486979 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.291501045 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.291523933 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.292660952 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.292751074 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.292794943 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.292808056 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.292849064 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.293915987 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.293950081 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.293962002 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.293989897 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.371340990 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.372037888 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.372901917 CEST	49171	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.373473883 CEST	49172	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.374049902 CEST	49173	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.374774933 CEST	49174	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.417599916 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.418087959 CEST	443	49165	143.204.11.100	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 13, 2021 17:37:33.419528961 CEST	443	49171	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.419672966 CEST	49171	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.420114040 CEST	443	49172	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.420198917 CEST	443	49173	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.420238972 CEST	49172	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.420258045 CEST	49173	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.420995951 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.421057940 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.421084881 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.421118021 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.421169043 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.421226025 CEST	443	49165	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.421241999 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.421281099 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.423657894 CEST	443	49174	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.423753977 CEST	49174	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.425187111 CEST	49171	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.426290035 CEST	49165	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.442434072 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.442466974 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.442559958 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.442950964 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.442975998 CEST	443	49166	143.204.11.100	192.168.2.22
Apr 13, 2021 17:37:33.443017960 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.443461895 CEST	49166	443	192.168.2.22	143.204.11.100
Apr 13, 2021 17:37:33.444190025 CEST	443	49166	143.204.11.100	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 13, 2021 17:37:26.678884029 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:26.737647057 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:28.538772106 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:28.646919966 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:30.086622953 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:30.135772943 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:30.159277916 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:30.175677061 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:30.200001955 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:30.208498955 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:30.237185955 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:30.270998955 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.633934975 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.644654036 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.661407948 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.663750887 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.668757915 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.671240091 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.676074028 CEST	63009	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:32.696254969 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.710105896 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.717278004 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.718313932 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.728718042 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.733338118 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:32.750011921 CEST	53	63009	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:33.287211895 CEST	59319	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:33.338939905 CEST	53	59319	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:33.619843006 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:33.677005053 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:37.998157024 CEST	59770	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:38.070590019 CEST	53	59770	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:57.885875940 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:57.934639931 CEST	53	61523	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 13, 2021 17:37:57.960015059 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:58.017174006 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:58.893093109 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:58.949901104 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:58.971065044 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:59.034408092 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 13, 2021 17:37:59.953943968 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:37:59.987288952 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:00.013740063 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:00.044300079 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:03.004673004 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:03.004935026 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:03.053291082 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:03.053498983 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:05.771576881 CEST	50667	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:05.838373899 CEST	53	50667	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:07.006160975 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:07.006346941 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:07.057245016 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:07.058006048 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:49.005299091 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:49.100181103 CEST	53	54129	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:51.028285027 CEST	65329	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:51.094017029 CEST	53	65329	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:51.346478939 CEST	60718	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:51.351878881 CEST	49157	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:51.395221949 CEST	53	60718	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:51.400609970 CEST	57391	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:51.444817066 CEST	53	49157	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:51.460114956 CEST	53	57391	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:52.104582071 CEST	61858	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:52.167088032 CEST	53	61858	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:56.606880903 CEST	62500	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:56.692657948 CEST	53	62500	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:57.585875988 CEST	51652	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:57.635529995 CEST	53	51652	8.8.8.8	192.168.2.22
Apr 13, 2021 17:38:57.988244057 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:38:58.052541018 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:00.983897924 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:01.014990091 CEST	54609	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:01.040110111 CEST	58101	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:01.055013895 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:01.066914082 CEST	53	54609	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:01.105257988 CEST	53	58101	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:06.780910015 CEST	64329	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:06.790235996 CEST	64881	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:06.848330975 CEST	53	64329	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:06.857075930 CEST	53	64881	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:20.587256908 CEST	55327	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:20.660142899 CEST	53	55327	8.8.8.8	192.168.2.22
Apr 13, 2021 17:39:24.787085056 CEST	59150	53	192.168.2.22	8.8.8.8
Apr 13, 2021 17:39:24.922920942 CEST	53	59150	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 13, 2021 17:37:28.538772106 CEST	192.168.2.22	8.8.8.8	0xd575	Standard query (0)	covid-19.ontario.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:49.005299091 CEST	192.168.2.22	8.8.8.8	0x64c2	Standard query (0)	covid-19.ontario.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.028285027 CEST	192.168.2.22	8.8.8.8	0x7c48	Standard query (0)	www.ontario.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.351878881 CEST	192.168.2.22	8.8.8.8	0xce3b	Standard query (0)	files.ontario.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.400609970 CEST	192.168.2.22	8.8.8.8	0x21ad	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 13, 2021 17:38:56.606880903 CEST	192.168.2.22	8.8.8.8	0x9672	Standard query (0)	api.ontario.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:57.585875988 CEST	192.168.2.22	8.8.8.8	0xf95	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:57.988244057 CEST	192.168.2.22	8.8.8.8	0x20ed	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:00.983897924 CEST	192.168.2.22	8.8.8.8	0xac13	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:01.014990091 CEST	192.168.2.22	8.8.8.8	0x2d5a	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:06.780910015 CEST	192.168.2.22	8.8.8.8	0xb3c2	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:06.790235996 CEST	192.168.2.22	8.8.8.8	0xbef0	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:20.587256908 CEST	192.168.2.22	8.8.8.8	0xe641	Standard query (0)	www.phdapps.health.gov.on.ca	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:24.787085056 CEST	192.168.2.22	8.8.8.8	0x57e2	Standard query (0)	covid19.ontariohealth.ca	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	covid-19.ontario.ca	covid-19.ontariogovernment.ca		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	covid-19.ontariogovernment.ca	d1yhecx6e3wyn1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.100	A (IP address)	IN (0x0001)
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.124	A (IP address)	IN (0x0001)
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.101	A (IP address)	IN (0x0001)
Apr 13, 2021 17:37:28.646919966 CEST	8.8.8.8	192.168.2.22	0xd575	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.38	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	covid-19.ontario.ca	covid-19.ontariogovernment.ca		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	covid-19.ontariogovernment.ca	d1yhecx6e3wyn1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.101	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.124	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.100	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:49.100181103 CEST	8.8.8.8	192.168.2.22	0x64c2	No error (0)	d1yhecx6e3wyn1.cloudfront.net		143.204.11.38	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	www.ontario.ca	www.ontariogovernment.ca		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	www.ontariogovernment.ca	d36pom45p27o8j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	d36pom45p27o8j.cloudfront.net		13.226.169.24	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	d36pom45p27o8j.cloudfront.net		13.226.169.36	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	d36pom45p27o8j.cloudfront.net		13.226.169.100	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 13, 2021 17:38:51.094017029 CEST	8.8.8.8	192.168.2.22	0x7c48	No error (0)	d36pom45p27o8j.cloudfront.net		13.226.169.33	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	files.ontario.ca	files.ontariogovernment.ca		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	files.ontariogovernment.ca	d2khazk8e83rdv.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	d2khazk8e83rdv.cloudfront.net		143.204.11.64	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	d2khazk8e83rdv.cloudfront.net		143.204.11.28	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	d2khazk8e83rdv.cloudfront.net		143.204.11.53	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.444817066 CEST	8.8.8.8	192.168.2.22	0xce3b	No error (0)	d2khazk8e83rdv.cloudfront.net		143.204.11.15	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.460114956 CEST	8.8.8.8	192.168.2.22	0x21ad	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:51.460114956 CEST	8.8.8.8	192.168.2.22	0x21ad	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:56.692657948 CEST	8.8.8.8	192.168.2.22	0x9672	No error (0)	api.ontario.ca	api.ontariogovernment.ca		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:56.692657948 CEST	8.8.8.8	192.168.2.22	0x9672	No error (0)	api.ontariogovernment.ca	productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:56.692657948 CEST	8.8.8.8	192.168.2.22	0x9672	No error (0)	productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com		34.198.74.185	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:56.692657948 CEST	8.8.8.8	192.168.2.22	0x9672	No error (0)	productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com		52.71.121.103	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:56.692657948 CEST	8.8.8.8	192.168.2.22	0x9672	No error (0)	productio-nodeelas-1po85c440amc1-224777076.us-east-1.elb.amazonaws.com		3.224.191.206	A (IP address)	IN (0x0001)
Apr 13, 2021 17:38:57.635529995 CEST	8.8.8.8	192.168.2.22	0xf95	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:38:58.052541018 CEST	8.8.8.8	192.168.2.22	0x20ed	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:39:01.055013895 CEST	8.8.8.8	192.168.2.22	0xac13	No error (0)	googleads.g.doubleclick.net		172.217.23.34	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:01.066914082 CEST	8.8.8.8	192.168.2.22	0x2d5a	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:39:06.848330975 CEST	8.8.8.8	192.168.2.22	0xb3c2	No error (0)	i.ytimg.com		172.217.22.246	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:06.857075930 CEST	8.8.8.8	192.168.2.22	0xbef0	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 13, 2021 17:39:06.857075930 CEST	8.8.8.8	192.168.2.22	0xbef0	No error (0)	photos-ugc.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:20.660142899 CEST	8.8.8.8	192.168.2.22	0xe641	No error (0)	www.phdapps.health.gov.on.ca		204.41.3.217	A (IP address)	IN (0x0001)
Apr 13, 2021 17:39:24.922920942 CEST	8.8.8.8	192.168.2.22	0x57e2	No error (0)	covid19.ontariohealth.ca	covax.azurefd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 13, 2021 17:39:24.922920942 CEST	8.8.8.8	192.168.2.22	0x57e2	No error (0)	covax.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:37:28.787437916 CEST	143.204.11.100	443	192.168.2.22	49166	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020	Wed Apr 06 22:01:43 CEST 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:37:28.788871050 CEST	143.204.11.100	443	192.168.2.22	49165	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020	Wed Apr 06 22:01:43 CEST 2022	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:37:33.476855040 CEST	143.204.11.100	443	192.168.2.22	49171	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:37:33.495132923 CEST	143.204.11.100	443	192.168.2.22	49173	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:37:33.496412992 CEST	143.204.11.100	443	192.168.2.22	49172	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:37:33.502901077 CEST	143.204.11.100	443	192.168.2.22	49174	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:48.716222048 CEST	143.204.11.100	443	192.168.2.22	49184	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:48.716419935 CEST	143.204.11.100	443	192.168.2.22	49183	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:51.199331999 CEST	13.226.169.24	443	192.168.2.22	49187	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:51.201241016 CEST	13.226.169.24	443	192.168.2.22	49186	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:51.428680897 CEST	13.226.169.24	443	192.168.2.22	49188	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:51.519992113 CEST	13.226.169.24	443	192.168.2.22	49189	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:51.527255058 CEST	13.226.169.24	443	192.168.2.22	49190	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:51.530602932 CEST	13.226.169.24	443	192.168.2.22	49191	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:51.584839106 CEST	143.204.11.64	443	192.168.2.22	49194	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:51.597486973 CEST	143.204.11.64	443	192.168.2.22	49195	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:51.598572016 CEST	104.16.19.94	443	192.168.2.22	49196	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 13, 2021 17:38:51.599118948 CEST	104.16.19.94	443	192.168.2.22	49197	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 13, 2021 17:38:56.951251030 CEST	34.198.74.185	443	192.168.2.22	49203	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:56.952672005 CEST	34.198.74.185	443	192.168.2.22	49202	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Fri Nov 26 14:15:53 CET 2021 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:57.588958979 CEST	143.204.11.100	443	192.168.2.22	49206	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:57.591905117 CEST	143.204.11.100	443	192.168.2.22	49204	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:38:57.592259884 CEST	143.204.11.100	443	192.168.2.22	49207	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:38:57.593218088 CEST	143.204.11.100	443	192.168.2.22	49205	CN=covid-19.ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Apr 06 21:31:44 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Tue Jul 07 19:25:54 CEST 2009	Wed Apr 06 22:01:43 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Sat Dec 07 18:55:54 CET 2030	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		
Apr 13, 2021 17:39:01.158274889 CEST	172.217.23.34	443	192.168.2.22	49214	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 13, 2021 17:39:01.158406019 CEST	172.217.23.34	443	192.168.2.22	49215	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 13, 2021 17:39:06.964034081 CEST	172.217.23.33	443	192.168.2.22	49222	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:39:06.964189053 CEST	172.217.23.33	443	192.168.2.22	49223	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 13, 2021 17:39:06.964595079 CEST	172.217.22.246	443	192.168.2.22	49220	CN=edgestatic.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:13:20 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:13:19 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 13, 2021 17:39:06.965059042 CEST	172.217.22.246	443	192.168.2.22	49221	CN=edgestatic.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:13:20 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:13:19 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 13, 2021 17:39:21.100017071 CEST	204.41.3.217	443	192.168.2.22	49226	CN=www.phdapps.health.gov.on.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Wed Apr 15 16:50:31 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Mon Sep 22 19:14:57 CEST 2014 Mon Nov 27 21:23:42 CET 2006	Sun Apr 24 17:20:30 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Mon Sep 23 03:31:53 CEST 2024 Fri Nov 27 21:53:42 CET 2026	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		

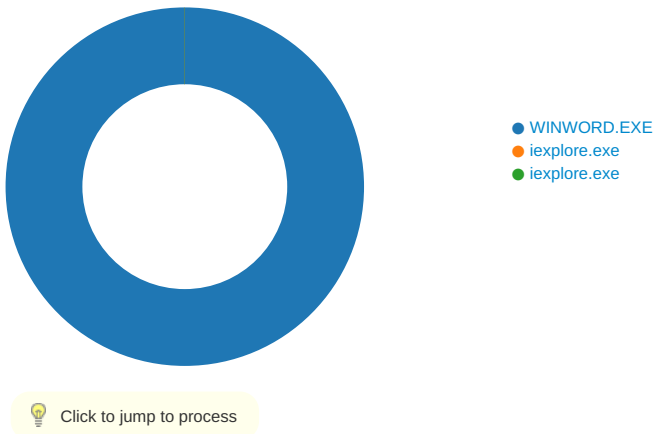
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Mon Sep 22 19:14:57 CEST 2014	Mon Sep 23 03:31:53 CEST 2024		
					CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Mon Nov 27 21:23:42 CET 2006	Fri Nov 27 21:53:42 CET 2026		
Apr 13, 2021 17:39:21.109054089 CEST	204.41.3.217	443	192.168.2.22	49225	CN=www.phdapps.health.gov.on.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Wed Apr 15 16:50:31 CEST 2020 Mon Oct 05 21:13:56 CEST 2015 Mon Sep 22 19:14:57 CEST 2014 Mon Nov 27 21:23:42 CET 2006	Sun Apr 24 17:20:30 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Mon Sep 23 03:31:53 CEST 2024 Fri Nov 27 21:53:42 CET 2026	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Mon Sep 22 19:14:57 CEST 2014	Mon Sep 23 03:31:53 CEST 2024		
					CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Mon Nov 27 21:23:42 CET 2006	Fri Nov 27 21:53:42 CET 2026		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 13, 2021 17:39:32.663588047 CEST	13.226.169.24	443	192.168.2.22	49232	CN=ontario.ca, OU=Government of Ontario, O=Government of Ontario, L=Toronto, ST=Ontario, C=CA CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Nov 26 13:45:55 CET 2019	Fri Nov 26 14:15:53 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Tue Jul 07 19:25:54 CEST 2009	Sat Dec 07 18:55:54 CET 2030		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1796 Parent PID: 584

General

Start time:	17:36:29
Start date:	13/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f0d0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$VID-19 Vaccine Locations Booking Sites_April 12 (8eb60eb7-3115-41f6-bcc5-3e70c62319dd).docx	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C045F79E.png	0	25735	success or wait	1	7FEE90A9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings	binary	05 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	F4D27	binary	04 00 00 00 04 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 28 4C 40 4E C6 30 D7 01 27 4D 0F 00 27 4D 0F 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	success or wait	1	7FEE90A9AC0	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 FF FF FF FF				

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\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1384972334	1384972335	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1384972335	1384972336	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4D27	F4D27	binary	04 00 00 00 04 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 28 4C 40 4E C6 30 D7 01 27 4D 0F 00 27 4D 0F 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 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	04 00 00 00 04 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 00 00 00 00 00 00 00 00 27 4D 0F 00 27 4D 0F 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 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	success or wait	1	7FEE90A9AC0	unknown

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				

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 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 FF FF FF FF				

Analysis Process: iexplore.exe PID: 2616 Parent PID: 584

General

Start time:	17:36:59
Start date:	13/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13fda0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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: 2728 Parent PID: 2616

General

Start time:	17:36:59
Start date:	13/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2616 CREDAT:275457 /prefetch:2
Imagebase:	0x1140000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly