TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

CURRENT TOPICS >>>

[Roomba Maker Preparing To Sell Maps Of Your Home To Advertisers]
-Bleeping Computer

[An Amazon Echo Can't Call The Police– But Maybe It Should]
-Wired

[95% Of All Ransomware Payments Were Cashed Out Via BTC-e]
-Bleeping Computer

[Apple Removes VPN Apps From The App Store In China]
-Techcrunch

CURRENT COURSES >>>

Open Source Intelligence

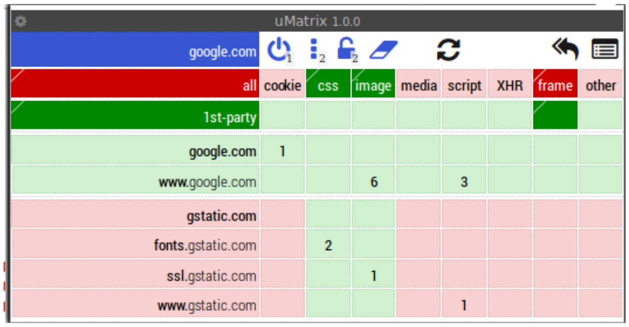
The Open Source Intelligence (OSINT) course teaches students how to leverage publicly available data sources to gather intelligence on both themselves and potential targets. Students are taught how to use online search engines, people engines, social media platforms and more to gather as much information as possible. Students are given access to our website that hosts proprietary OSINT tools that leverage paid and free APIs. Students will leave with practical knowledge of finding information and linking online accounts.

uMatrix

Matrix-based Firewall

uMatrix is a point-and-click matrix-based firewall addon that allows you to block entire classes of requests based on domains names or categories. It was originally part of the HTTP Switchboard, but the developer decided to split it into two addons: uBlock Origin and uMatrix. It has a built-in list of classes to block, but can be modified to suit your needs. By default, CSS and images are allowed globally as these are very low on the threat level. Things like cookies, media and scripts are only allowed for first party sites by default and iframes are blocked globally.

If you open a page to google.com (pictured below), your browser will be able to run scripts from google.com and www.google.com, but will block scripts from gstatic.com and www.gstatic.com because these are third-party sites. This is indicated by the green (allowed) and red (denied) boxes and the numbers correspond to the amount of items per category that need to run on your current page. To allow a selective category, such as scripts on gstatic.com, click on the top half of the category box to allow scripts to run on that domain.



all	cookie	css	image	media	script	XHR	frame	other
1st-party								
google.com	1							
www.google.com			6		3			
gstatic.com								
fonts.gstatic.com		2						
ssl.gstatic.com			1					
www.gstatic.com					1			

If you want everything to run from gstatic.com, click on the top half of the labeled "gstatic.com" and everything other than globally blocked elements will be allowed to run. If you do it this way, all subdomains will also be able to run things, ie. www.gstatic.com, ssl.gstatic.com, etc. And if you want all of one category to run globally, such as scripts, click on the top half of the box labeled "scripts" and all scripts will be allowed to run on any sites you visit and any third party sites they link to. It is better to be very selective with this, as allowing everything globally defeats the purpose of even using the addon in the first place.

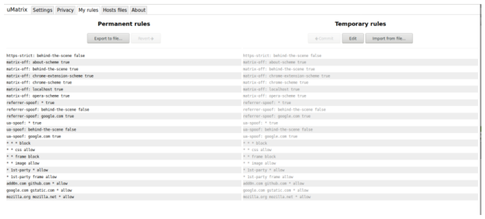
All settings made on a page are regarded as temporary rules unless you make them permanent by clicking the lock icon before leaving the page. Be very careful with this, anything that you changed will be added to permanent rules if you click the lock not just specific classes or specific domains. The

THREATS AND VULNERABILITIES >>>

The Easiest Target—You

When we think of computer security, we think Anti-Virus, Anti-Malware, firewalls, etc. While these tools do help protect our computers from being compromised, they are absolutely useless if we can be manipulated into bypassing these safeguards. Phishing (email), Smishing (SMS) and Vishing (Voice) are very good examples of this. In these instances, an attacker either calls, texts or emails you pretending to be someone else to try to get some private information out of you or they try to get you to do something, such as run some obscure file they send you. You can have a 128 character password, and feel like you're the most secure person on the planet, but as soon as you send that to someone who claims to "need" it to access your account, your security is completely null and void. This also works on the business side as well, if you have that same 128 character password, and an email and phone number you only use for that specific account, but the customer service representative doesn't take the proper steps to verify it is you calling to access your account, your security is useless. An attacker could call customer service, say they are you and even if they don't have access to your phone number or email, the customer service representative may give them access through alternative means such as personal information which an attacker could easily find online. If an attacker were to send you a file and give you a legitimate reason to run the file (ie. view your bank statement), more than likely you will trust that it's safe to run without a second thought. All of your safeguards are useless when you specifically gave that file permission to run on your machine. There are no takesies backsies after running that file. There's only so much your computer can do for you if you make a bad decision. There is no hardware or software solution to prevent humans from being compromised by other humans. The only hope we have is to educate users on best practices and make them more skeptical when asked for information.

CONTINUED FROM PAGE ONE >>>



Permanent rules

```
https-strict: behind-the-scene false
matrix-off: about-scheme true
matrix-off: behind-the-scene true
matrix-off: chrome-extension-scheme true
matrix-off: chrome-scheme true
matrix-off: localhost true
matrix-off: opera-scheme true
referrer-spoof: * true
referrer-spoof: behind-the-scene false
referrer-spoof: google.com true
ua-spoof: * true
ua-spoof: behind-the-scene false
ua-spoof: google.com true
* * * block
* * css allow
* * frame block
* * image allow
* 1st-party * allow
* 1st-party frame allow
add0n.com github.com * allow
google.com gstatic.com * allow
mozilla.org mozilla.net * allow
```

Temporary rules

```
https-strict: behind-the-scene false
matrix-off: about-scheme true
matrix-off: behind-the-scene true
matrix-off: chrome-extension-scheme true
matrix-off: chrome-scheme true
matrix-off: localhost true
matrix-off: opera-scheme true
referrer-spoof: * true
referrer-spoof: behind-the-scene false
referrer-spoof: google.com true
ua-spoof: * true
ua-spoof: behind-the-scene false
ua-spoof: google.com true
* * * block
* * css allow
* * frame block
* * image allow
* 1st-party * allow
* 1st-party frame allow
add0n.com github.com * allow
google.com gstatic.com * allow
mozilla.org mozilla.net * allow
```

uMatrix

changes will only pertain to that specific webpage you were on when you changed the rules. For instance, if I allow gstatic.com on google.com, next time I visit google.com, gstatic.com will be able to run scripts, however if I visit facebook.com, gstatic.com will be blocked as a third-party site. You have the option to revert back to permanent rules by clicking the eraser icon in case you accidently allowed too many sites or you broke the site by blocking too many classes. You can also open up the settings dashboard, click on the "My rules" tab, and commit all temporary rules to be permanent rules. This means every rule you modified during your browser session will stay the same the next time you open your browser.

uMatrix has some other features, such as user agent string spoofing, which can be turned on to make your browser look like a different browser to everything website you visit. The list of user agent strings it uses is quite old (2012) and would probably make you look way more unique. Thankfully, you can modify the list with your own user agent strings that will make more sense for your specific needs. uMatrix can also force strict https on sites, so no unencrypted traffic can come from third party sites, but this will also break a lot of sites. It can also do referrer spoofing, which prevents sites from knowing which site you came from before landing on their website. There is also a built-in block list of known tracking, advertisement and malware domains that works very well with no configuration necessary.

uMatrix on the surface seems very similar to noScript in the sense that it blocks scripts on websites, but unlike noScript, first party sites are still allowed to run scripts unless you change that global setting. uMatrix also seems a bit more user friendly than NoScript with all of the color coding and the ability to see exactly what you are blocking and allowing by class and domain. uMatrix is available for Chrome, Firefox, and Opera. For questions or comments, contact admin@tpidg.us

EVENTS >>>

Techcrunch Disrupt

Sep 18-20 2017, San Francisco, CA

Microsoft Ignite

Sep 25-29 2017, Orlando, FL

READER QUESTIONS >>>

Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

Want to **contribute** to the digital update?

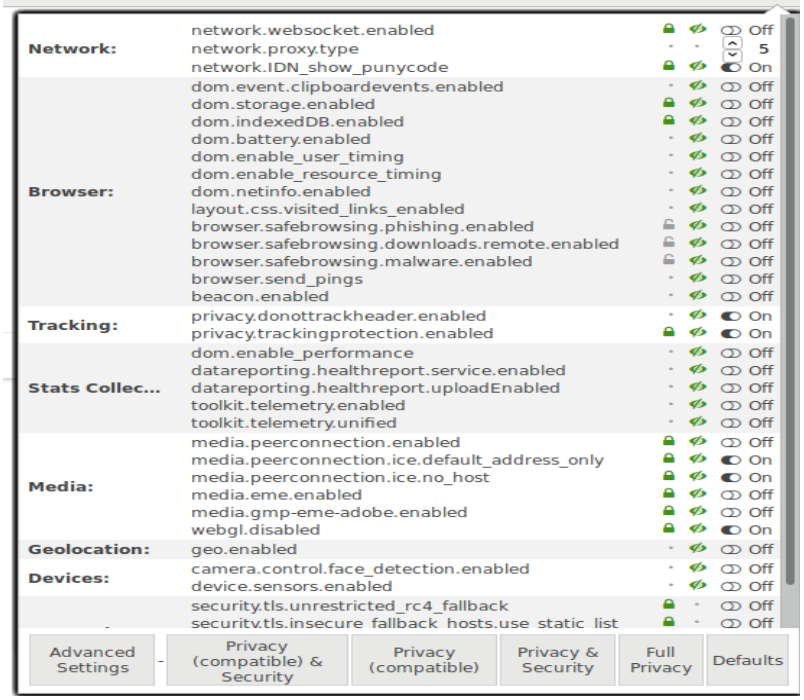
Let us know at
digitalupdate@tpidg.us

BONUS MATERIALS >>>

Privacy Settings Addon

A Firefox Privacy Addon

Firefox provides a lot of desirable privacy settings which is why we always recommend using it as your default browser. While there are a lot of settings on the surface like telemetry or search engine settings, there are many settings that are buried in the about:config page in Firefox. For instance, if you want to turn off WebRTC to prevent your browser from leaking your private IP Address, you have to search through about:config to find the rule that shuts it off as there is no button in Firefox settings.



Network:	network.websocket.enabled	🔒	Off
	network.proxy.type		5
	network.IDN_show_punycode	🔒	On
Browser:	dom.event.clipboardevents.enabled		Off
	dom.storage.enabled	🔒	Off
	dom.indexedDB.enabled	🔒	Off
	dom.battery.enabled		Off
	dom.enable_user_timing		Off
	dom.enable_resource_timing		Off
	dom.netinfo.enabled		Off
	layout.css.visited_links_enabled		Off
	browser.safebrowsing.phishing.enabled	🔓	Off
	browser.safebrowsing.downloads.remote.enabled	🔓	Off
	browser.safebrowsing.malware.enabled	🔓	Off
	browser.send_pings		Off
	beacon.enabled		Off
Tracking:	privacy.donottrackheader.enabled		On
	privacy.trackingprotection.enabled	🔒	On
Stats Collec...	dom.enable_performance		Off
	datareporting.healthreport.service.enabled		Off
	datareporting.healthreport.uploadEnabled		Off
	toolkit.telemetry.enabled		Off
	toolkit.telemetry.unified		Off
Media:	media.peerconnection.enabled	🔒	Off
	media.peerconnection.ice.default_address_only	🔒	On
	media.peerconnection.ice.no_host	🔒	On
	media.eme.enabled	🔒	Off
	media.gmp-eme-adobe.enabled	🔒	Off
	webgl.disabled	🔒	On
Geolocation:	geo.enabled		Off
Devices:	camera.control.face_detection.enabled		Off
	device.sensors.enabled		Off
	security.tls.unrestricted_rc4_fallback	🔒	Off
	security.tls.insecure_fallback_hosts.use_static_list	🔒	Off

With the Privacy Settings addon, all of the rules that correspond to privacy and security are put into an easy to access list with switches to turn them on or off. The addon also provides presets for full privacy, privacy and security, compatible privacy, and compatible privacy and security. The full privacy setting is preferred, but breaks some sites like Protonmail which require access to some DOM settings that are turned off.

Remember that this is yet another addon that could be either another attack surface or a way to positively identify your browser via browser fingerprinting. The good thing about this addon is it makes switching these settings very easy, but everything can be done manually as well if you don't want to add another addon. The privacy settings addon can be found here: https://addons.mozilla.org/en-US/firefox/addon/privacy-settings/

UPDATE CORNER >>>

Software Updates

We preach updates in every class, so here's a list of security software updates for the month of July accompanied by sha256 checksums.

VeraCrypt

Version: 1.21

Released: July 9th 2017

VeraCrypt Setup 1.21.exe

6cff2cce52eb97321b1696f82e9ccefa7c80328d91c49bf10b49e3897677896e

VeraCrypt_1.21.dmg

cbd3f80eca753edce40be134ccbd288805c93643b21d8cf21fd72c0fd544f377

veracrypt-1.21-setup.tar.bz2

594acbe5215032005ec65e4814fa69e7dc8b36a61a37082b057b0c612aa518b3

TOR Browser Bundle

Version: 7.0.2/7.0.3

Released: July 3rd/27th 2017

torbrowser-install-7.0.2_en-US.exe

48aa8f59a197c1bc5bc12b42840cae9872f741b36fd190c0d2c94750ffa1c545

TorBrowser-7.0.2-osx64_en-US.dmg

122161eac00af4ce65c0415133240b80625b790469b8d80f91637b0e8e43760f

tor-browser-linux64-7.0.3_en-US.tar.xz

0ce22ee15a65502515f46dd1643d902baad7bce0e9aabb4a12a37760fad721dd

TAILS Live ISO

Version: 3.0.1

Released: July 5th 2017

tails-amd64-3.0.1.iso

5805604801bb7e49627168b3a02fefc5857209a30b8e2c04936c481ed2d08a57