in this issue >>> *V.1.20*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- [New Critical Bug Fixes for Windows and Flash](#)
  - Krebs on Security
- [Several Netgear Routers Have an Exploitable Vulnerability: Patch Today](#)
  - Lifehacker Security
- [Millions of Android Devices Imperiled by AirDroid App](#)
  - Ars Technica
- [A Beginner's Guide to Becoming More Secure Online](#)
  - Ars Technica
- [Thieves Can Guess Your Secret Visa Card Details in Seconds](#)
  - Ars Technica

UniFi Video

IP Camera Management Solution

UniFi Video is an IP camera management system that is capable of supporting multiple sites of multiple cameras into one centralized user interface. With UniFi Video, you can set up your own video server on a server or always-on computer (even a Raspberry Pi), rather than buy the NVR that Ubiquiti sells. Each Ubiquiti camera needs to be set up in "managed mode" and pointed to where you have your UniFi Video server, then UniFi will add it to your interface with the rest of your cameras. From there you can set resolution settings, motion detection, recording intervals, reboot the camera and monitor various statistics. Email alerts can be set up for events such as motion or camera disconnects to prevent any mishaps.

The user system works well, allowing several user accounts each with separate logins and email addresses for alerts. Users can be segregated very easily by creating groups and adding users to the group that gives them the permissions they need. Permissions can be micro managed down to which cameras they can view up to which recordings they can delete from each camera. Each camera can have their own designated motion zones to record only when they detect motion so you don't waste disk space with static footage. You can map out all your cameras on the interactive map to keep track of which areas are monitored and where your blind spots are.

Currently UniFi Video only supports running on Debian 7, Ubuntu 12.04, Ubuntu 14.04, Windows 7 and Windows 8. Hopefully soon they will add support for more platforms, such as Red Hat based Linux distros (Fedora, CentOS) and Windows 10. A way around this for now would be to set up a Virtual Machine to run UniFi Video rather than replace your host operating system. This would also protect your host system in case the video server were to ever get compromised. Overall, UniFi Video is a spectacular camera management system that works very well with organizing cameras across the globe in one nice, intuitive user interface. For additional info or questions, contact admin@tpidg.us *set the stage >>>*

Firefox Focus iOS Browser

Firefox Focus

Search or enter address

Automatic private browsing.
Browse. Erase. Repeat.

Advertised as the browser where you should do your embarrassing web searches, Firefox Focus is a free, privacy-focused browser that is currently available only for iOS. We have worked with this browser for a couple of weeks now and have found some big benefits and some disadvantages.

The downsides first: this browser is not ideal for heavy internet use. It does not support tabbed browsing, meaning that if you want to look at a different page you have to close whatever you're currently viewing. If you want a very basic browser for those sensitive search queries, this might be it, but it is definitely not a full Safari replacement.

In spite of the disadvantages, Firefox Focus offers some impressive features on a very simple interface. Open the browser and tap the settings icon in the upper-right side of the interface. Under "Privacy" there are four options: Block ad trackers, Block analytics trackers, Block social trackers, and Block other content trackers. The functions of these options are intuitive and up-front. You are warned that enabling the "Block other content trackers" may break some websites(i.e. videos may not play, etc.). Keep this in mind if you encounter a site that won't work on your mobile; you may have to temporarily disable this feature on those sites.

The most interesting feature of Firefox Focus, however, is the "Safari Integration" option. Enabling this setting allows all the same content blocking capability to be used in your default iOS browser (Safari) and effectively turns Firefox Focus into a browser extension. We really like this because there is no way to change your default browser and if you accidentally click a link on a website or either in a text message or email and it is opened in Safari, you will still have the protections of Firefox Focus.

We don't view Firefox Focus as a full replacement for Safari, but it has some good privacy protection. Even if you don't use the browser itself it's worth installing just for the Safari Integration.

Upcoming Events:

Law Enforcement Intelligence Units

May 1-5 2017, Bloomington, MN

National Technical Investigators' Association Annual Training Conference

July 12-23, Tampa, FL

Associated Locksmiths of America Expo

June 16-22 , Rosemont, IL

The easy button >>>

SnowHaze iOS Browser

Where Firefox is a very lightweight browser, SnowHaze brings some serious capability to the table. SnowHaze offers many more power-user features (or at least as "power user" as you can get on iOS). This app is security-focused and allows very granular control of website behavior.

Upon opening the app, tap the Settings icon in the lower-right corner of the screen. The first list of settings are labeled as "General" but these are mostly security-related. The first is JavaScript which you can completely disable. Preventing scripts from running greatly reduces the likelihood of malicious code executing on your device. You can disable automatic media playback, require HTTPS, and block "popovers" (new tabs that open up when you click a link).

The next block of settings are related to privacy. The first allows you to manage Website Data and let's you manually delete all website data, caches, cookies, and data stores. The User Agent setting allows you to choose multiple user-agent strings that constantly rotate, making you harder to track online. The History setting allows you to forget all history, or to forget history only on "Private Sites" (adult-themed websites), and to clear all history on demand. Tracking Protection lets you block HTTP referrers, block tracking scripts, and block HTML5 canvas access.

If you enable all the protections of SnowHaze your browser will be very secure. Unfortunately many of your favorite websites are likely to be broken. SnowHaze has a very cool solution for this: you can set your browser up for maximum security, but customize these settings on a case-by-case basis for each website you visit. Tap the green shield icon beside the URL bar and SnowHaze will allow you to disable certain settings for that website instead of disabling globally.

We generally don't recommend alternative browsers for iOS, but SnowHaze has made us rethink this position. This is one of the most impressive browsers we've seen yet. SnowHaze is available for iOS only and costs $2.99. For more information visit **https://snowhaze.com/en/**.

NoScript Security Suite

The Ultimate Security Add-On

Anyone who has taken one of our courses that deals with digital security knows that we advocate the use of a Firefox add-on called NoScript Security Suite. We recommend NoScript because it is the most comprehensive ad-block and script blocker available. Unfortunately using NoScript can be a major headache if you aren't familiar with it. Even if you are familiar you may need a refresher. This article will cover setting it up.

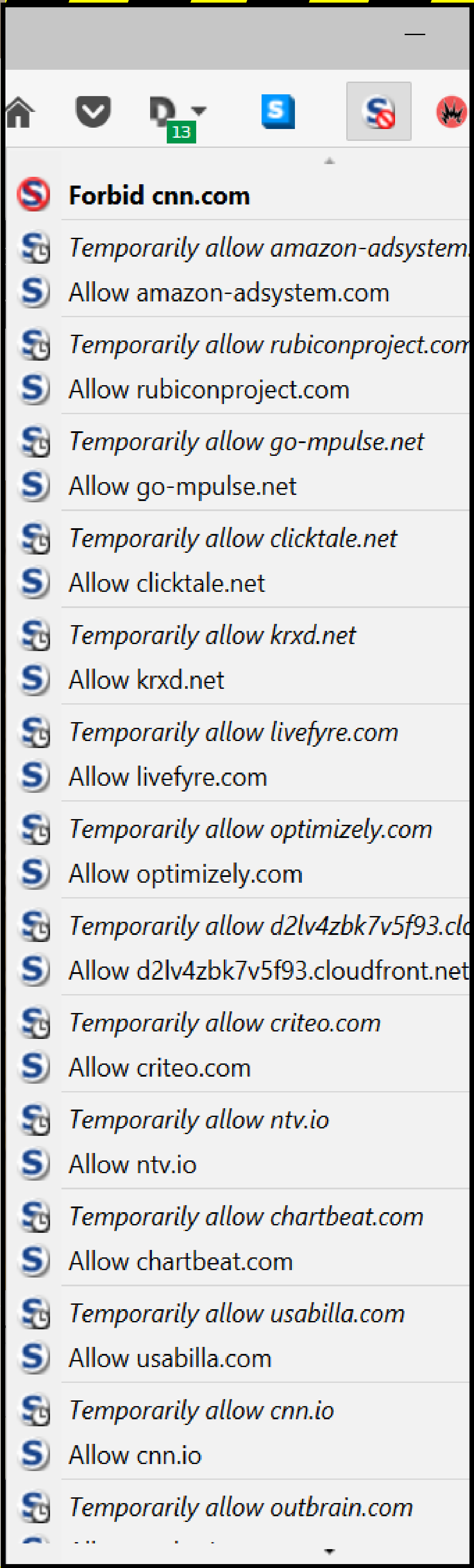
The image on the right shows the scripts that NoScript is blocking on cnn.com. All of these attempt to collect data about your visit or serve you advertisements, and some may even be malicious. NoScript prevents these from running on the page. The problem is that the website probably doesn't work as intended; with all script blocked videos will not play, forms cannot be filled in correctly, and other necessary content may not be displayed. To solve this NoScript allows you to selectively enable scripts individually instead of letting them all run.

When you visit a website, click the NoScript "Options" button at the bottom-right of your screen. A list of scripts like the one shown here will appear. If this is a site that you only plan to visit once, we recommend only enabling scripts temporarily. This basically involves a process of trial and error until you find the combination of scripts that allows the page to function correctly without allowing everything else.

Because there are millions of websites we can't tell you exactly what scripts to allow for each one, but we can give you some rules of thumb. First, you will probably need to allow the site itself. If you are going to Bank of America's website you would click "Allow" or "Temporarily allow" bankofamerica.com. If the page still does not function, look for any other scripts from the same site. If you are visiting sites that serve audio or video, look for scripts that contain "cdn" (content delivery network). For example, if you are going to listen to an audio file on soundcloud.com, you may also have to allow "soundcloudcnd.com".

You may wish to set up sites that you visit frequently on a permanent basis. We still recommend going through the initial setup process by temporarily allowing scripts until the site works correctly but is not permitting any unnecessary scripts to run. Once you have found this balance, click "Make Page Permissions Permanent" in the NoScript options.

We admit that NoScript can be frustrating but we highly recommend using it because of the security it affords, and no other browser extension even comes close. Once the sites you use on a daily basis have been set up it becomes much less frustrating, so be sure to give it a fair chance. For more information on NoScript please visit **https://noscript.net/**.



Forbid cnn.com

Temporarily allow amazon-adsystem

Allow amazon-adsystem.com

Temporarily allow rubiconproject.com

Allow rubiconproject.com

Temporarily allow go-mpulse.net

Allow go-mpulse.net

Temporarily allow clicktale.net

Allow clicktale.net

Temporarily allow krxd.net

Allow krxd.net

Temporarily allow livefyre.com

Allow livefyre.com

Temporarily allow optimizely.com

Allow optimizely.com

Temporarily allow d2lv4zbk7v5f93.cl

Allow d2lv4zbk7v5f93.cloudfront.net

Temporarily allow criteo.com

Allow criteo.com

Temporarily allow ntv.io

Allow ntv.io

Temporarily allow chartbeat.com

Allow chartbeat.com

Temporarily allow usabilla.com

Allow usabilla.com

Temporarily allow cnn.io

Allow cnn.io

Temporarily allow outbrain.com

coming soon >>>

In Future Issues...

Phone Number Masking

Mailfence

Wire