TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

# Digital Update


**CURRENT TOPICS >>>**

Wildcard Certificates Coming January 2018
**-Let's Encrypt**

Facebook Can Track Your Browsing Even After You've Logged Out, Judge Says
**-The Guardian**

Miscreants Have Been Pillaging Credit Cards From Trump Hotels' Booking System
**-Ars Technica**

**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.

## USG USB Firewall v1.0

### *USG is good, not bad*


For a long time, we have had many issues with USB and how inherently insecure they are. This is mostly due the amount of trust our computer gives to them. Plug-n-play insures that when we plug in a USB device, device drivers will be installed and the device will just work. Devices like the SyncStop are great because they physically disconnect the data pins and allow the USB device to charge without fear of something malicious happening to your device as it's charging. One uneducated employee could plug in a thumb drive he found on the ground and completely take down an entire company's infrastructure (See our last issue for a few examples of USB dangers). With USB devices having the ability to be this dangerous, almost everyone bans the use of them, which is the only thing they can do. It makes life difficult when you need to charge your phone or transfer some files between computers. In fact, in most jobs, it's a fire-able offense to plug a USB device into a company owned computer.

In comes the USG USB Firewall, a much better solution to this growing USB issue we have all throughout the world. It's name is a play on words, changing USBad to USGood making clear it's intentions already. The USG is similar in operation to the SyncStop, but allows data to pass through. Sounds dangerous right? No. The USG has two separate microprocessors on each end of the device that are connected via a serial link. The USG limits what can and cannot pass through the serial link to the other microprocessor. As always, a hardware solution is better then any software solution. In the case of the USG, it use two separate, physical chips on the device making it that much more secure.

The USG currently only supports mass storage devices with 512 byte sectors and a max size of 2 TB, mice with four buttons and a scroll wheel, and 101 key keyboards. If your device is not supported, it will be indicated by flashing lights on the USG. As far as transfer speeds, it runs USB v1.0 so transfer speed are quite slow, but it's worth transferring files slowly and safely, rather than loose and fast. You will still be able to use USB v3.0 devices with the USG, as USB is backwards compatible with the older versions.

# Is ____ Vulnerable?

We often talk about vulnerabilities or get asked if specific software is vulnerable and the answer is not always short and sweet. Yes, some vulnerabilities are easy to distinguish (ie. Internet Explorer), but others are not. For instance, how do we know Veracrypt is not vulnerable? In the case of Veracrypt in particular, it received a full audit that was funded by an independent company (OSTIF) in October of 2016. Before this audit, we had no way of knowing whether the software was safe to use or not, we were just trusting that the developers knew what they were doing.

On the most basic level, we can think of the security of a platform or piece of software in a series of layers. Layer one is the underlying protocol level. For VPN software, this would be OpenVPN, IPSec, PPTP, etc. VPN providers have very little control of what happens at this layer and can only make a good decision on which protocol they want to implement. In the case of OpenVPN, it has been fully audited and funded by the same independent company that funded the audit for Veracrypt. In this case, OpenVPN is the best protocol to implement into VPN software.

That brings us to the second layer: implementation. The protocol that software uses can be completely clean and perfectly written, but if the implementation of that protocol is not done in the same perfect way, the software can be compromised. Recently an implementation flaw was found in a GnuPG library that allowed researchers to compromise a RSA 1024 bit key and decrypt user data. This does not mean RSA (the protocol) is compromised, it means the implementation was not done correctly.

The final layer is user security. We talk about this a lot because it is very important. A piece of software, such as Veracrypt, can be absolutely perfect, but if you use the password "P@ssw0rd", Veracrypt is useless. Human beings are the number one security vulnerability, so if we don't exercise good security practices, it doesn't matter which software we use.

## EVENTS >>>

**BlackHat USA**

*July 22-27 2017, Las Vegas, NV*

**DEFCON 25**

*July 27-30 2017, Las Vegas, NV*

## READER QUESTIONS >>>

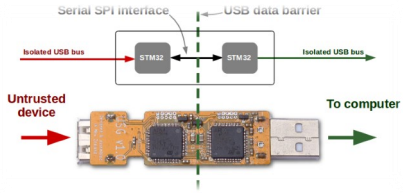
Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

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

Let us know at digitalupdate@tpidg.us

CONTINUED FROM PAGE ONE >>>




# USG USB Firewall

The USG has some very good rules in place that protect your computer against three major categories of attacks. Type 1 attacks consist of low level driver exploits. The USG only allows a certain amount of predefined rules through to your computer, so if an attacker tried to send something malicious, it wouldn't pass through. This type of attack would require a sophisticated attacker, but is definitely possible. Type 2 attacks consist of class changes after a device has been plugged in. A flash drive should not be able to switch to being a keyboard whenever it feels like it. The USG makes sure that if you plug in a flash drive, it stays a flash drive. It also prevents one device from being in two classes at once (ie. A flash drive and keyboard). In simpler terms, think of an Android phone and how it can switch between charging and being able to transfer data to your computer. This would not be possible when plugged into the USG.

Type 3 attacks are under development, but would consist of predefined rules based on the device you plug in. For instance, if you plug in a flash drive, one of the rules could be a limit on the amount of data that can be transferred in one session. You could also set all flash drives to be read only so an infected computer couldn't exfiltrate data onto your flash drive (this is currently an open issue on Github). If you plug in a keyboard, you could have a rule that limits the amount of keys per second that could go through. This would prevent the dreaded keystroke injection attack that the USB Rubber Ducky or any other keyboard emulated flash drive or other device can do when plugged in.

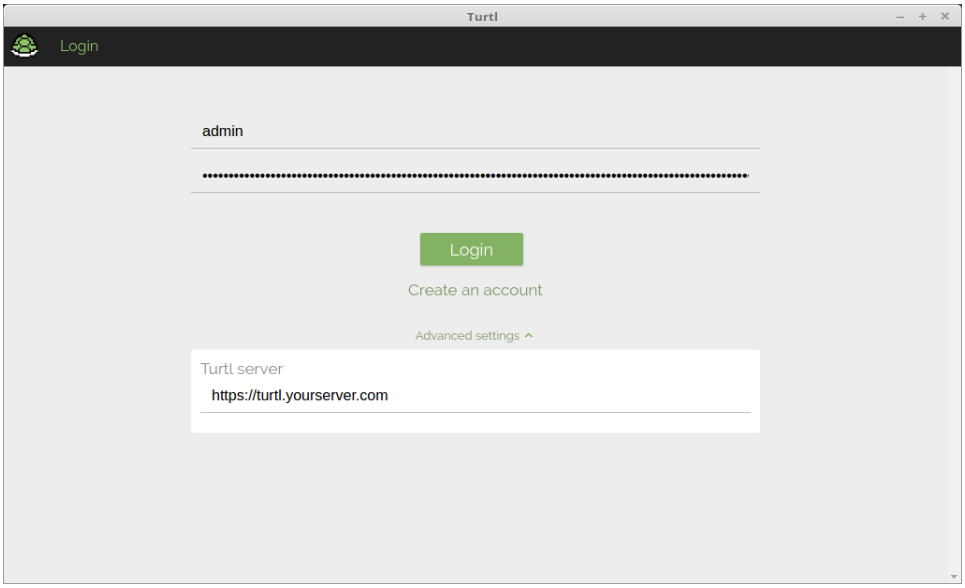
It seems that this device is soon going to be a must if we keep heading in the same direction with the massive amounts of ways USB can be compromised. There definitely is a ton of potential for this device and we look forward to seeing future features added. For more information or questions about the USG, contact admin@tpidg.us

BONUS MATERIALS >>>

# Turtl Server

## *A Self Hosted Notes Server*

We have mentioned Turtl in a previous issue and we still recommend it as a cloud based note taking app that supports Windows, Mac, Linux, Android and iPhone. Turtl is a very well put together zero-knowledge, encrypted note taking application. The only issue we have had with it is it leverages someone else's server. This presents two possible issues: 1. turtl has quite a few users making compromising the server much more worth it and 2. turtl's servers may not have 100% uptime and you may be unable to access your data. This is obviously worst case scenario and we trust the developer of turtl, but for absolute certainty, it would be nice to host a standalone version. Luckily it is possible, although a little bit difficult, to host it on your own server and connect your turtl client to your server without sacrifices to any convenience aspects. This also gives you the ability to choose usernames that were previously taken.




The setup portion is not easy and not recommend for the average user, but it is completely self sustainable after setup and requires no intervention on your part. Although everything turtl does is encrypted, it would be a good idea to get a TLS cert for your server before connecting your turtl client to your server. It can also be placed behind a webserver proxy if you want to connect your client to a subdomain such as turtl.yourserver.com. It is also possible to make the turtl server completely local by either running it in a local webserver, in a virtual machine or by grabbing one of the pre-built docker images. We teach turtl server setup as part of our non-standard communications course. Contact admin@tpidg.us for further information. Instructions on turtl server setup can be found here: https://turtlapp.com/docs/server/

UPDATE CORNER >>>

# Website Updates

Updates to https://www.tpidg.us for the month of July. For comments or suggestions email admin@tpidg.us

## Main Page Changes

- Added instructions on how to blur your house on Google and Bing under digital privacy category
- Added password reset guide for Windows, MacOS and Linux under forensics category (only accessible to limited users)

## OSINT Changes

- Added the following APIs:
  - Google Maps
- Adding Google Maps street view-images to Pipl advanced search
- Improved phone number search by added Whitepages lookup to Twilio API (very accurate)