TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

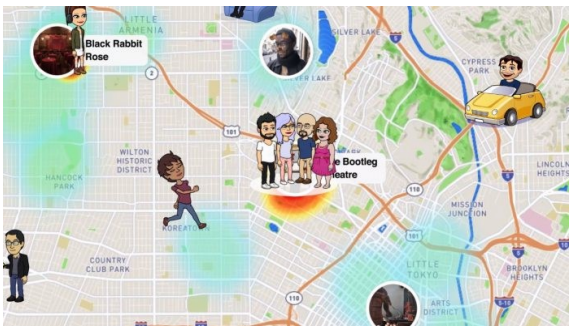
In the News:

- Police issue child safety warning over Snapchat maps update
  - The Telegraph
- Google can be forced to pull results globally, Canada Supreme Court rules
  - The Guardian
- Parliament cyber-attack hits fewer than 90 email accounts
  - The Guardian

current courses >>>

Non-Standard Communications

This course is designed to teach students how to communicate securely while protecting their identity by employing digital signature reduction measures and digital tradecraft through the use of commercial off-the-shelf technology (COTS), readily available open source technology, and best practices. Students will learn a variety of critical skills utilizing the host nation's commercial digital infrastructure.



Snapchat's Snap Map

Stalk your friends!

On June 21st, Snapchat added a new feature to it's array of picture taking features. If you are not familiar with Snapchat, it is an app that allows users to send each other self destructing messages or media to their friends. While the messages do self destruct within a certain time period, Snapchat should not be compared to apps like Signal which do it in a more secure fashion. Users also have the ability to add media to their "story" to share with their entire friend's list or publicly. If this app wasn't good enough with the massive amount of information they have on you (read the privacy policy), they have added the ability to share your location with your friends and the rest of the world. This is thanks to their purchase of Zenly, a social map app, for over 250 million dollars.

Users now have the ability to show their exact GPS location to their friends, selected friends or no one on the Snap Map. While your location isn't updated unless the app is open, your last location will be shown until updated. You can also post to "our story", which allows users to drop media in your current location for the public to view. If enough people post to "our story", a hotspot of stories is created in that area. This presents a privacy issue or an opportunity depending on which side of the fence you sit on. If you want to do OSINT on someone, it would be easy to become friends with them and track where they go in real-time or view hotspots in your location until you find who you are looking for.

There are a few saving graces, the first being that the feature is turned off by default. If you didn't know about the feature until now, your location is not being shared and you have nothing to worry about. If you have enabled the feature, you can still turn it off by enabling "ghost mode" in settings. This setting makes it so your location is only viewable by you while still allowing you to view the map. Remember that Snapchat still knows where you are until you disable your location services. Just because your friends can't see where you are doesn't make your location any more of a secret. Social media apps are one of the greatest privacy violators and we recommend that you stop using them if you care about your privacy. You can start with Snapchat: https://www.snapchat.com/a/delete_account

The Dangers Of USB Devices

On the way to work, you see a thumb drive laying on the ground with the label on it: "Important Documents". You decide to pick up the thumb drive —free thumb drive, right? You bring it back to the office and decide to plug it into your workstation. Worst mistake of your life. Several scenarios are possible, and 90% of those have a bad outcome. Here's a few possible scenarios:

1. Scenario one is you plug it in, format it and use it like normal and nothing bad ever happens. You added a new thumb drive to your collection for free.
2. Scenario two is you plug it in, a command prompt window flashes on the screen for a split second, and you know you messed up. Within the next few hours, your machine is being encrypted and a window pops up asking you to pay a ransom for your files to be decrypted.
3. Scenario three is much worse. As soon as you plug in the unknown thumb drive, a worm travels across the network infecting every machine in sight. Important and secret corporate documents are exfiltrated from the network and whoever's thumb drive you picked up now owns your company's network.

The moral of the story is: do not ever plug any unknown USB device into your laptop, smart phone, workstation, etc. USB devices of all shapes and sizes can be modified in a variety of different ways to exploit victim's computers. Theses USB devices can be wired mice, keyboards, webcams, thumb drives, etc. If it uses a USB connection, it can and will be used by an attacker. In our next issue, we will review a device we believe is the answer to this ongoing problem, but no amount of hardware will ever be a 100% solution. User alertness and education is the ultimate solution. If an unknown USB device never gets plugged into a computer, there will never be a problem.

Upcoming Events:

National Technical Investigators' Association (NATIA) Annual Conference

July 12-23 2017, Tampa, FL

BlackHat USA

July 22-27 2017, Las Vegas, NV

DEFCON 25

July 27-30 2017, Las Vegas, NV

16TH ANNUAL NORTH CAROLINA DEFENSE AND ECONOMIC DEVELOPMENT TRADE SHOW

Aug 7th 2017, Fayetteville, NC

Ultimate Router Configuration Pt. 2

Configured with security in mind

In the last issue, we covered settings that can make or break your router security. Remember that your router is what stands between your devices and the internet, so it is very important that it be as secure as possible. We will cover a few more settings that are important, but a bit more overlooked than last issue's settings.

UPnP: While necessary for certain applications to function, this protocol allows applications to open ports on your router without permission or authentication. This creates a bit of a security issue, so we recommend just turning this feature off.

MAC Address Filtering: We have covered this in previous issues and courses, so by now you should know our stance on it: you should not rely on it. This is why defense in depth is so important. If you use this along with other security features it may be worth it, although it could be a bit inconvenient for you. No matter what you do, do not rely on this option.

Content Filtering: Just because you cannot go to a certain site does not make you any less vulnerable. This option normally filters on domain names which are easily bought for ten dollars or less. If you block one domain, ten more will pop up in it's place.

DMZ: Short for Demilitarized Zone, this option allows you to completely expose a local device on the Internet. This has its use cases, but if you don't know what those use cases are, your best bet is to make sure that it is turned off.

Wi-Fi Transmit Power: Your signal strength should be strong enough for your devices, but not strong enough for someone in your neighborhood to either "borrow" or hack into your Wi-Fi from the comfort of their home or car. This option is not available on all Wi-Fi routers.

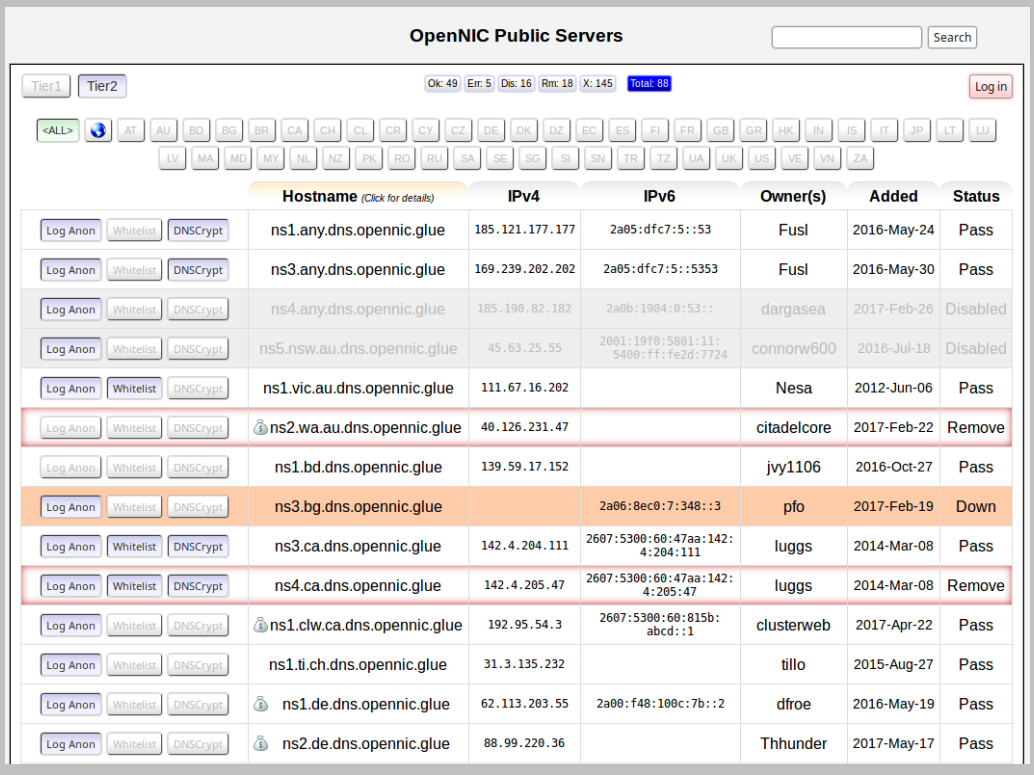
Bonus Materials >>>

Private DNS Servers

Maintained by the community

If you use an Internet Service Provider's modem, chances are you use their DNS servers as well. You may think it's not that big of a deal because you use a VPN, but not all VPN providers have a solution for DNS and your DNS requests may still be going through your ISP. Your ISP may not be able to tell what you are doing, but they can definitely tell where you are going. Another big issue is a lot of ISPs will restrict access to sites at the DNS level. Because they own the DNS servers, they can choose whether or not they want to respond to certain domain names.

In comes the OpenNIC project with community hosted DNS servers. They offer a list of DNS servers with both IPv4 and IPv6 support, no logs, DNSCrypt and multiple locations. It is best to pick a DNS server that has been up for a while, stores no logs and is hosted in a trusted location (ie. not the UK). If you use one of OpenNIC's DNS server, you gain access to more TLDs (Top Level Domains) including .geek, .libre, .dyn, etc. Be sure to add a secondary server just in case the one you choose goes down. If you do not have a DNS server, you will not be able to access sites with their domain names.



Update Corner >>>

Software Updates

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

VeraCrypt

Version: 1.20

Released: June 29th 2017

VeraCrypt Setup 1.20.exe
7725e6dc9358dec14fb7bb852c5e45cffa6736fb9438bf8413db8a6721e86f0a
VeraCrypt_1.20.dmg
63b186cd9d117a13bf249445b9d0551391babf12512a974978baf44a65bcfd37
veracrypt-1.20-setup.tar.bz2
7725e6dc9358dec14fb7bb852c5e45cffa6736fb9438bf8413db8a6721e86f0a

TOR Browser Bundle

Version: 7.0.1

Released: June 13th 2017

torbrowser-install-7.0.1_en-US.exe
d9a07c2cb50523056cfa8dc792e498cf8fc032512d34aae84d9ae65e7e0ece97
TorBrowser-7.0.1-osx64_en-US.dmg
7ebbede7a17fe69767f313181da7b1a55cfac5dda749bc7a5a9eeb7b37464a50
tor-browser-linux64-7.0.1_en-US.tar.xz
49bb80d7ba864a2b4701ba1765d78cf4d61e5a481c179dd92fa8adbb82fbacfe

TAILS Live ISO

Version: 3.0

Released: June 13th 2017

tails-amd64-3.0.iso
676f1322166536dc1e27b8db22462ae73f0891888cfcb09033ebc38f586e834a

KeePass

Version: 1.33/2.36

Released: June 2nd/9th 2017

KeePass-1.33-Setup.exe
03901b363cbfdb2d8c1840ae580cbf5346fafa5c6f94fd4aaa99b25536801935
KeePass-2.36-Setup.exe
6e34391f83870404d21666b6689b2a34521b4db2ab1b007d9347f81b5f7e288b

Firefox

Version: 54.0.1

Released: June 29th 2017

Firefox Setup 54.0.1.exe (64 Bit)
b402cd79a6db9e42c24609f369e3211aeeb979003d47c2f5842241ecd54d0440
Firefox 54.0.1.dmg
5ec2a1bac1059932399bdbbc9fb64fdd51f069db8768f2b52b080218eb019773
firefox-54.0.1.tar.bz2 (64 Bit)
aee55fb841e37b2e1da84d8a35f4f1bfda1fd93fe9256911d5a4d75ee3d136bb

coming soon >>>

In Future Issues...

Signatures

USG USB Firewall

What is randomness?