



Monthly E.C.C. Information Security Briefing

Date: April 26, 2017

ECC Internal News:



Barracuda Spam & Virus Firewall 600



- Do you have any idea how much volume our email Spam Firewall handles?
 - As I was walking through the parking lot one day (I think there's a song in there somewhere), someone stopped me and asked about the spam situation here on campus. I told him about the recent upgrade to the new Barracuda 600 series spam firewall and that spam prevention had actually *improved* since the upgrade.
 - The reason that it seems that so many spam/phishing emails get through is because it's simply a numbers game. The volume of spam/phishing emails is increasing year by year, and that translates into greater numbers of fake/junk mails getting through.
 - Here is a snapshot of activity during just **one day** of monitoring:

Email Statistics [inbound]			Help
	TOTAL	DAY	HOUR
Blocked	1,336,788	14,828	489
Blocked: Virus	16,613	49	1
Quarantined	87,138	1,093	37
Allowed: Tagged	243,258	2,844	73
Allowed	1,311,372	19,874	508
Total Received	2,995,169	38,688	1,108

- We hope to add an additional feature to our spam firewall in the near future, called Advanced Threat Detection. This will allow us to block more advanced malware, zero-day exploits, and targeted attacks.
- Please continue to send us your spam & phishing emails that get through to (not the ones marked [BULK] – you can simply delete those):

spamalert@elcamino.edu



- **Write in with your IT security questions:**

- If you have any questions about cyber security, please send them to:
 - pyoder@elcamino.edu
- Any questions that may be of interest to a wide audience will be posted the following month!

External News:

- **Pennsylvania Democratic Senate Attacked by Ransomware**

- Full story:
 - <http://www.nbcnews.com/news/us-news/senate-democrats-pennsylvania-are-being-held-cyber-hostage-n728901>

- **IRS tool for filling out FAFSA application breached**

- The tool that lets you connect to the IRS for auto-filling your tax information into the Free Application for Federal Student Aid (FAFSA) form has been breached. The IRS has disabled the use of the tool until October, 2017 and has sent out notices by mail to those who are suspected of being affected by this breach. So far, it is estimated that some 8000 fraudulent tax refunds totaling \$30 million have been issued as a result of this breach.
- Full story:
 - http://www.chronicle.com/blogs/ticker/breach-of-financial-aid-tool-may-have-compromised-data-on-100000-taxpayers/117659?cid=wcontentlist_hp_latest

- **Apple Mac OS Malware Spiked in 2016 Q4**
 - Threat actors are increasingly expanding their targets to include the Mac OS
 - So much for a Mac being considered safer than a PC!
 - Full story:
 - <http://www.darkreading.com/attacks-breaches/apple-mac-os-malware-spiked-in-q4-/d/d-id/1328591>

- **Higher education breaches for March, 2017:**
 - Daytona State College
 - University of Georgia
 - Lane Community College Health Clinic
 - University of Idaho
 - University of North Carolina Health Care

Tip of the Month:



- **Beware of the Meitu!**
 - A popular photo-editing app for Android & iPhone called Meitu has been downloaded over a billion times. The problem is, it is collecting data from your phone including photos, calendars, contacts, and your geolocation.
 - It also collects your phone's IMEI number – a 15-digit serial number (like a computer's MAC address) that verifies the phone's country of origin, the manufacturer, and the model number. With this IMEI number, hackers can actually “clone” your phone which will give them access to your texts, emails, calls, and everything else stored on your phone. And, get this - once your phone is “cloned” to another device, there is no way for service providers to block the porting of cellphone numbers (except if you're using Google Voice)!
 - **Suggestion:** Delete this app from your phone immediately if you already have it!

