Monthly ECC Information Security Briefing
May 30, 2018

ECC Internal News

VPNfilter malware

- In case you missed the campus-wide announcement earlier this week here is the link to the original alert issued from the FBI and DHS:
  - https://www.us-cert.gov/ncas/alerts/TA18-145A
- Several people have asked if they need to replace their equipment at home, unless your network router is so old that the firmware is no longer upgradable, then there is no need to upgrade your hardware
- Also, there is a list from Symantec that identifies routers that are KNOWN to be at risk for the VPNfilter malware. Do not solely rely on this list in order to decide whether or not to take action.
  - Linksys E1200
  - Linksys E2500
  - Linksys WRVS4400N
  - Mikrotik RouterOS for Cloud Core Routers: Versions 1016, 1036, and 1072
  - Netgear DGN2200
  - Netgear R6400
  - Netgear R7000
  - Netgear R8000
External News

2017 Showed 270% Increase in Mac Malware


Twitter telling users to change their password after a bug left 330 million passwords exposed

- Twitter is advising all its 330 million users to change their password after a glitch left them exposed in the company's internal systems. Twitter discovered the glitch and did not find any "breach or misuse by anyone," the company said in a blog post. The bug left passwords in an internal log "unmasked," meaning that instead of showing up as an encrypted set of random set of letters and numbers, the password itself was displayed in plain text. Even though the company says it has no reason to believe anyone obtained any sensitive information, it is telling users to change their password "out of an abundance of caution."

Data Breach Watch

U.S. Higher Education Breaches for April 2018:

- Boise State University (related to recent Fresno State case)
Tip of the Month

Hordes of College Credentials for Sale on the Dark Web

- In March of 2017, the cybersecurity advocacy group, “Digital Citizens Alliance” identified 6.7 million higher education email addresses that were available on the Dark Web. Many of the email addresses, undoubtedly, would not function or grant a cybercriminal exploitable access to vulnerable systems. Some, however, could have helped a cybercriminal access valuable intellectual property or personally identifiable information. University credentials can be especially valuable as cybercriminals can use them to compromise university computer systems and then launch attacks against third targets from those systems, betting that targets are less likely to identify activities from university IPs as malicious.
- You should never use your elcamino.edu account for personal business or for setting up external accounts. Many ECC accounts have become compromised because of this, and it puts the entire school in danger of being hacked.

Cyber Security Trivia

The trivia question for this month is:

- What is the team name commonly given to a group of programmers that are tasked with exposing errors or security holes in software?
- Email your answer to: pyoder@elcamino.edu
Write in with your IT security questions:

If you have any questions about cyber security, please send them to: pyoder@elcamino.edu

All current and previous issues of the Monthly E.C.C. Information Security Briefing are posted online at:

- http://www.elcamino.edu/about/depts/its/techservices/infosec.aspx

Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District
pyoder@elcamino.edu