Monthly ECC Information Security Briefing
September 26, 2018

ECC Internal News

Have you heard about “The Vision Resource Center”?  
- All California Community College employees (faculty, staff, administrators and trustees) are eligible to access an entire library of training videos hosted by the California Community Colleges Vision Resource Center (formerly the Professional Learning Network).
- After you create an account you can access thousands of courses from Skillsoft & Lynda.com.
- If you’ve already registered with the Professional Learning Network, use the same account credentials to login to the new site.
- Register here with the CCC Vision Resource Center:
  - [https://visionresourcecenter.cccco.edu/](https://visionresourcecenter.cccco.edu/)

El Camino targeted by PowerGhost attack
- Recently, ECC was attacked by a large-scale outbreak of cryptomining malware identified as PowerGhost.
- The PowerGhost exploit was based on a stolen National Security Agency tool called “EternalBlue” which was part of a larger tool kit that was compromised when the NSA servers were hacked.
- The attack signatures are similar to that of the WannaCry Ransomware and NotPetya exploits that have wreaked havoc across the internet over the last 2 years and effectively shut down Facebook, Amazon, and other large companies for almost an entire day.
PowerGhost is categorized as “file-less malware” because it isn’t easy to detect, doesn’t leave much trace evidence behind, and uses Windows PowerShell scripting commands to infect other computers on the network.

The PowerGhost malware is designed to use the CPU, GPU, and RAM of your computer to mine cryptocurrency and send the proceeds to an encrypted e-coin wallet, which can often lock your system up due to all the resources being used.

Although trace amounts of the PowerGhost infection are still active, the majority of infections were squashed within the first 3 days of infection which spared ECC from suffering the usual extended downtime of systems expected from an attack of this magnitude.

External News

Trio of cyber criminals accused of hacking into thousands of computer systems and stealing info from 15 million credit cards arrested

- The Department of Justice announced that a trio of high-profile hackers linked to a “sophisticated international cybercrime group” known as Fin7 have been arrested.
- The cyber criminals allegedly breached computers in 47 states and stole details linked to 15 million credit cards.
- The three men, Fedir Hladyr, Dmytro Fedorov and Andrii Kolpakov, were arrested in Europe between January and June of this year. Hladyr is in U.S. custody, and U.S. authorities are seeking extradition of the other two.
- According to officials the international hacking group targeted more than 120 U.S. companies in order to steal customer card data and other information. “Since at least 2015, FIN7 members engaged in highly sophisticated malware campaigns targeting more than 100 U.S. companies, predominantly in the restaurant, gaming, and hospitality industries,” the DOJ said in a statement.
- The group breached systems operated by dozens of restaurants including Chipotle, Arby’s, Jason’s Deli, Red Robin and Chili’s through phishing scams that appeared to look legitimate. Hackers “carefully crafted email messages that would appear legitimate to a business’ employee, and accompanied emails with telephone calls intended to further legitimize the email,” officials said. The emails contained malware that would grant them access to customers’ credit card data.

Hackers breached US electric utilities

- Security analysts have discovered a new hacking group that has been successful in breaching networks of electric utilities in the United States.
- The new research from cybersecurity firm Dragos is yet more evidence that hacking groups are looking for ways to penetrate networks of critical infrastructure —potentially with the intention to stage disruptive or destructive attacks.
- The hacking group has been penetrating targets in the United States, as well as the Middle East, Europe and East Asia for at least a year, according to Dragos.
- In the United States, the group - which analysts at Dragos have named “Raspite” has been particularly focused on breaching companies that manage generation, transmission, or distribution of energy across the country.
• Hacking groups successfully breached networks of the companies’ business sides by using common tools and tactics like phishing emails and so-called watering hole attacks—a strategy in which a hacker infects a legitimate website that its target frequently visits.

Data Breach Watch

U.S. Higher Education Breaches for July and August 2018:
• Augusta University
• Clark University (MA)
• Eastern Maine Community College
• University of Kansas
• University of Pittsburgh Medical Center
• University of Wisconsin
• Yale University

Other Significant U.S. Breaches:
• Adams County, WI
• Animoto
• Boys Town National Research Hospital
• Instagram
• LabCorp Diagnostics
• LifeLock
• Macy’s
• Polar Fitness Trackers
• Reddit
• Sitter
• Timehop App
• T-Mobile
• U.S. Air Force

Tip of the Month

How to recognize & steer clear of Smishing attacks!!

• Smishing or SMS phishing scams are similar to your standard email phishing scam, with the exception that rather than email, the scammer attempts to trick the prospective victim via a text message sent to their phone.
• When you get a smishing text, you’ll likely see something asking you to call a phone number - or even worse - click a link to resolve an issue and providing your bank account, smartphone data plan or some other form of highly personal information.
• Calling a phone number could result in someone talking you into giving up your Social Security number, banking information or website login information.

• Click on a link in your text message and it could take you to a fraudulent website meant to make you think it's from something like your bank, wireless service provider or sometimes the Internal Revenue Service. Clicking that link alone may saddle you with malware on your smartphone, but if you actually enter your personal information on such a site, you could be turning it over to criminals who can then take over your private accounts.

• Say, for example, you give your login information for your smartphone data carrier. A criminal could then use that to capture your account and steal your phone number. They could then use that to bypass other forms of security you use, like text message-based and two-factor authentication, to protect your online accounts.

• The best way to avoid smishing scams is to simply ignore any texts you get from numbers you don’t recognize. But some scammers can spoof their numbers to appear as though the messages are coming from numbers you might recognize. So, if you want to be especially safe, simply avoid opening any links sent to you that ask for your login information. And if you’re told to call a number, don’t do it.

• If you think you’ve received a fraudulent text or call, contact your wireless carrier, or the institution the person on the other end of the line claims to represent. From there you can see if you’re being tricked, or you’ve got an actual issue. But in reality, chances are, it’s a scam. If you do happen to open a link sent to you via text message, be sure to download an anti-malware app for your smartphone and run it immediately to sniff out any threats that you may have inadvertently downloaded to your handset.

Cyber Security Trivia:

The trivia question for this month -

• What is a zero-day exploit?
  A. An exploit that takes advantage of no known fixes to stop it
  B. A really tasty candy bar
  C. An exploit that targets the “0” sector of a hard drive
  D. An exploit that triggers after counting down to zero

• 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