ECC Internal News

Malwarebytes Endpoint (Desktop) Protection

- Malwarebytes Enterprise was recently added to the arsenal of cybersecurity tools in use here at ECC
- It is designed to co-exist with and supplement other anti-virus software (such as Windows Defender)
- It has been extremely helpful in eradicating spyware, adware, malware (including cryptomining), and even ransomware from our systems here at ECC.
- Take a look at the snapshot below to give you an idea of what Malwarebytes has found and cleaned so far on our campus systems:

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>10,998</td>
</tr>
<tr>
<td>PUP</td>
<td>154,913</td>
</tr>
<tr>
<td>PUM</td>
<td>23,677</td>
</tr>
<tr>
<td>Ransomware</td>
<td>8</td>
</tr>
<tr>
<td>Exploit</td>
<td>100</td>
</tr>
<tr>
<td>Website</td>
<td>23,986,135</td>
</tr>
</tbody>
</table>

External News
Professor Warns: Amazon Echo is “Always Recording” Your Conversations

- A media professor (Nick Flor, an Associate Professor of Information Systems, Film, & Digital Media at the University of New Mexico’s Anderson School of Management) has warned that Amazon Echo and other such devices are “always recording” private conversations without the consent of their owners.
- This controversial discovery was revealed in a news story about a judge’s ruling which gave New Hampshire authorities permission to examine audio recordings from Echo in the case of a double murder where two women were stabbed to death:
  
- “Remember when Amazon claimed they only started recording when you said: “Alexa”. Turns out that’s a big freakin’ lie,” tweeted Flor. “These stupid devices are ALWAYS RECORDING.”
- It’s true, they only start recording when you say “Alexa”. What they don’t tell you is they NEVER STOP RECORDING after you say “Alexa” just ONCE!

Some shocking cybersecurity statistics for the year 2018

- 3.6 billion records exposed in data breaches until the end September 2018
- Healthcare targeted by 37% of all Ransomware attacks in Q3 2018
- Ransomware still the top malware threat during 2018 according to Europol
- By early 2018, 90% of all remote code execution attacks were associated with cryptomining
  - Cryptomining is the act of taking over your CPU and RAM to mine Bitcoins for profit
- 92% of all malware is still delivered by email and Phishing attacks are the most common exploit
  - Which is why we use the KnowBe4 Phishing Training software at El Camino!
- Fileless attacks are on this rise
  - Fileless attacks exploit software already installed on the victim's computer rather than attempting to download large executables (using Microsoft Office macros or Windows Powershell commands)
- Here is a snapshot from the quarterly Threat Landscape Report issued by Fortinet:
U.S. Higher Education Breaches For October 2018:
  • N/A

Other Significant U.S. Breaches:
  • Toyota (Oct)
  • Google+ (Oct)
  • Dept. of Defense (Oct)
  • U.S. Centers for Medicare & Medicaid Services (Oct)

Tip of the Month

How to Protect Yourself Against a SIM Swap Attack
  • A spate of hacked Instagram accounts. A $220 million lawsuit against AT&T. A bustling underground crime ring. They all have roots in an old problem that has lately found new urgency: SIM card swaps, a scam in which hackers steal your mobile identity—and use it to upend your life.
  • At its most basic level, a SIM swap is when someone convinces your carrier to switch your phone number over to a SIM card they own. They’re not doing it for prank call cover, or to rack up long-distance charges. By diverting your incoming messages, scammers can easily complete the text-based two-factor authentication checks that protect your most sensitive accounts. Or, if you don’t have two-factor set up in the first place, they can use your phone number to trick services into coughing up your passwords.
  • A sobering caveat: If a skilled SIM hijacker targets you, there’s realistically not much you can do to stop them, says Allison Nixon, threat research at security firm Flashpoint. “In most of the cases that we’ve seen, a sufficiently determined attacker can take over someone’s online footprint,” she says.
  • An example of the SIM swap circle of fraud:
The two main preventative measures are:
  - Hardening your cell phone account (separate PIN number)
  - Not using your cell phone number to link to online accounts

Read more about the steps you can take here: https://motherboard.vice.com/en_us/article/zm8a9y/how-to-protect-yourself-from-sim-swapping-hacks

Cyber Security Trivia

The trivia question for this month is:
  - What are the two most impersonated brands used in email Phishing attacks?
    - UPS and FedEx
    - Bed Bath & Beyond and Forever 21
    - Amazon and Microsoft
    - Apple and Walmart
    - Benny's Good Time Liquor and Dominos Pizza

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