



## Cutting Through the Cybersecurity Noise

*Here's what's important this week: March 15, 2019*

---

### Take Action

- Warn your folks about the latest phishing/malicious email hooks. These include messages that
  - Appear to come from the U.S. Center for Disease Control (CDC) and contain fake flu warnings to distribute GandCrab ransomware.
  - Use the Boeing 737 MAX 8 crash as a lure to spread H-WORM-RAT malware.
  - Come from random [sender@mail.com](mailto:sender@mail.com) and contain threads from old (2015-2017) emails, most likely stolen from compromised accounts (threads where folks have replied to the email and make the new, malicious message look more legitimate). These generally contain a link to a website hosted by OVH Hosting in Canada.
  - Contain links to websites with the domain, moonfruit.com. This has been an on-going campaign since late 2018 to get user account credentials, usually via a fake Outlook Web Access sign in page. eMails usually arrive Tuesdays and Wednesdays.

---

### Be Aware

- Company officials at Facebook and Apple say their outages this week were not due to a cybersecurity, hacking, or DDOS issue. But security conspiracy theorists wonder...
- Malwarebytes wrote a good article, "The not-so-definitive guide to cybersecurity and data privacy laws."  
Reference: <https://blog.malwarebytes.com/security-world/2019/03/not-definitive-guide-cybersecurity-data-privacy-laws/>
- At last week's RSA conference, a few security vendors announced some interesting 2018 trends. See the attached threat brief for more info.

---

### Upcoming Events

- On Tuesday, March 26 at 1 pm Eastern, the InfraGard National Capital Region is hosting a webinar on CIS Controls, featuring Phyllis Lee, senior director for controls at the Center for Internet Security. You do not have to be an InfraGard member to attend.  
Registration: [https://zoom.us/webinar/register/WN\\_rnfB512-QSuhvEBgN4liuA](https://zoom.us/webinar/register/WN_rnfB512-QSuhvEBgN4liuA)
  - On Saturday April 6 from 1pm to 5pm, WestMEC is hosting a cybersecurity awareness event that is open to the public. See the attached flyer for more info.
-

## Reminders

The Arizona Counter Terrorism Information Center (ACTIC) and Urban Area Security Initiative issue this product to increase Arizona's awareness and cyber resilience. It's up to you to make sure you take the proper steps to secure your networks and devices. Although vendors, products, and/or services may be mentioned, we do not endorse any specific one.

Contact [ACTICCybersecurity@AZDPS.GOV](mailto:ACTICCybersecurity@AZDPS.GOV) with any questions, to provide feedback, or to be added/removed from this distribution. Please note that this email address is not monitored 24x7.

Report potential, suspected, and/or confirmed cyber threats to the ACTIC via:

- <https://www.azactic.gov/Tips/>
  - [ACTIC@AZDPS.GOV](mailto:ACTIC@AZDPS.GOV)
  - (602) 644-5805 or (877) 2 S A V E A Z (272- 8329)
-