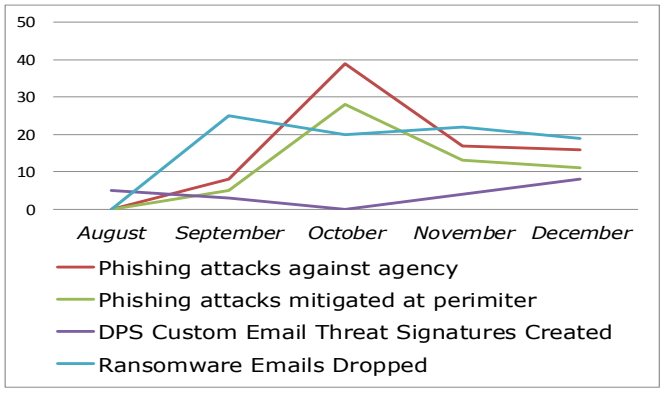
NEWS
Cyber Security
Vol. 2 | Issue 1
Jan/Feb 2017

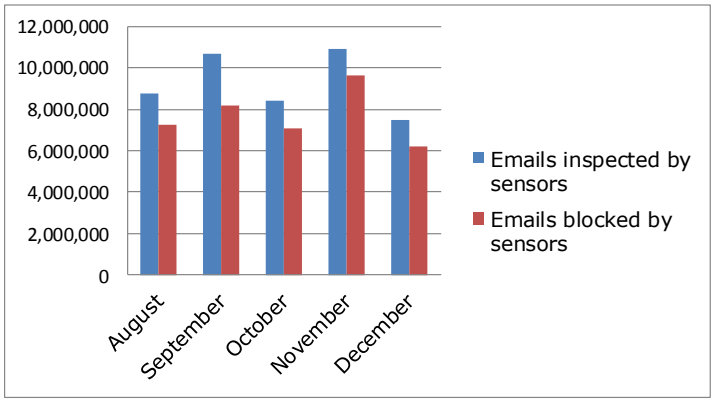
Year in Review

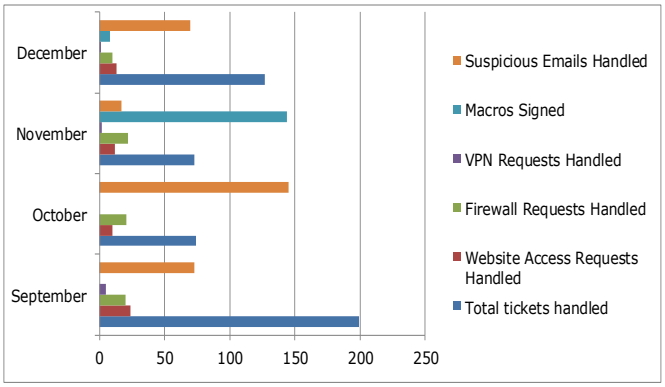
2016 was a year of many events - from the energetic Rio de Janeiro Summer Olympics; Brexit Referendum; Falcon 9 vertical landing; nail-biting Presidential election; and of all things, Russian hackers! It presented changes, and challenges to each of us, but above all else, it is important we remember the personnel, friends, and service members who worked around the clock to make Texas safer. Successfully executing the Department mission is no small feat, and I believe we all know a few persons worthy of applause.

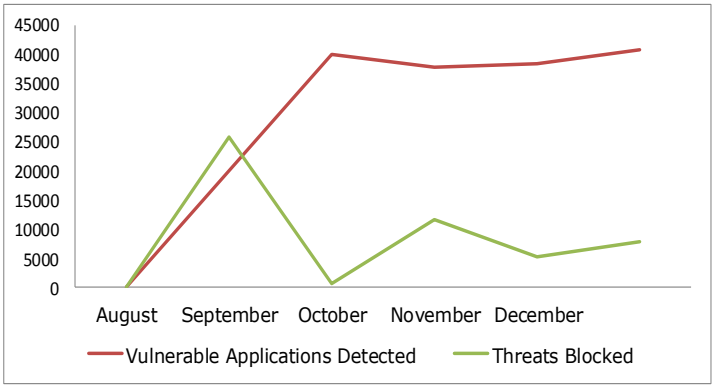
This article includes our aggregated end-of-year performance stats; highlights from 2016's most impactful data breaches; and a farewell toast to a Cyber Security staff member called to arms. Cyber Security hopes the future brings many opportunities to our readers, and you enjoy our Cyber Security Newsletter: 2016 Year in Review as much as we appreciate you reading it!

End of Year Cyber Security Stats









Breaches That Rocked 2016

Some of the most impactful breaches, hacks, and attacks worth remembering.

DNC HACK

OFFICIAL JOINT ANALYSIS REPORT

Hackers allegedly working with Russia's civilian intelligence service sent e-mails with hidden malware to more than 1,000 people working for the American government and political groups. U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election. This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The U.S. Government is referring to this malicious cyber activity as GRIZZLY STEPPE.

Note: Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities.

Review the official GRIZZLY STEPPE report: Click here.

Stolen Yahoo Data Includes Government Employee Information

Bloomberg Technology, 14 Dec 2016: More than 150,000 U.S. government and military employees are among the victims of Yahoo! Inc.'s newly disclosed data breach. It's a leak that could allow foreign intelligence services to identify employees and hack their personal and work accounts, posing a threat to national security. These employees had given their official government accounts to Yahoo in case they were ever locked out of their e-mail.

Learn more: Click here.

Hackers Hold Hollywood Healthcare Hostage

Lazarus Alliance, 19 Feb 2016: Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to hackers who seized control of the hospital's computer systems holding them a healthcare hostage. The assault on Hollywood Presbyterian occurred Feb. 5, 2016, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices.

Additional information: Click here.

Answering the Call of Duty

The New Year brings opportunities and challenges. For our very own Kirk Burns this principle is holding true. After receiving information of his call to active duty, covered in last month's newsletter, I pounced on the opportunity to interview the veteran. This article is the result of our impromptu interview and as many classic 'Kirk quotes' I could scratch down.

Late last year, the Cyber Security Training Officer received news of his forthcoming 2017 military deployment. For those who do not know, Kirk currently serves as a US Army Chief Warrant Officer 4. Destined for Afghanistan, I was stunned to learn this will be his forth Middle Eastern tour.

As we talked about his previous roles in Desert Storm and Desert Shield, I smiled at the subtle ironic similarity to most super hero comic classics (Minus the cape and tights of course). By day, the DPS Cyber Security Training Officer, but by night and some weekends, he is a US ARMY Black Hawk Pilot. Kirk has over 30+ years of aviation experience. Considering the aeronautical specialty, Kirk expects his role to be relevant to airspace management, but he is "preparing for anything".

This made absolute sense to me, but I remained curious to know if he perceived any cyber security or IT work on the horizon. 'Potentially' Kirk affirmed, "My role is pretty volatile". Many details of his deployment remain up in the air, but considering his rank, I would not be surprised if he can only provide a sanitized description.

CYBER SECURITY SHAREPOINT

Cyber Security is constantly seeking new and better ways to serve our customers. With this spirit to serve, we introduce our latest initiative: The Cyber Security SharePoint site. It streamlines information sharing by centralizing resources in one location. The site went live this month, and is routinely updated.

Check it out, and tell us what you think!

He will have already crossed the ocean by the time you read this article, but Cyber Security still asks you please keep our friend in your hearts and minds.

As our interview drifted into after work hours, and the office cubicles vacantly stand at solemn attention, I asked the Security Trainer if he had a message for his readers. "Remember your training," and with a firm, yet comforting smile, the Chief Warrant Officer replied, "**Do Good Cyber**". Thank you for your service, and safe travels Kirk!

He returns to us early 2018.

Connect with us	More Interesting Links	Visit the Website
For newsletter support contact Jennifer.Carson@dps.texas.gov	Slashdot Security Week Security Now	Check out our Website for additional security information.