

# THE DIR CYBERSECURITY INSIGHT<sup>1</sup>

November FY2017 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

*Thankful For Cybersecurity Professionals*

## Thankful for You

It is November and time to think back on the things and people you are thankful for and hold most dear. Well the Office of the Chief Information Security Officer at DIR is thankful for you! We value all the work you have done over the past year and appreciate your commitment to keeping the state of Texas secure. This holiday season let's not limit security to our respective agencies, but share our knowledge.

The holidays offer much needed time with friends and family, although, as cybersecurity professionals, security is a topic never far from our minds. We urge you to take a few moments this Thanksgiving, reflect on the importance of your family and friends, and help keep them safe by offering them a few security tips. Here are a few ways to start the conversation:

- Update your mobile software
- Back up your information
- Keep devices locked using strong PINs and passwords
- Think before connecting to any public wireless (airplane or in an airport, hotel, bus etc.)
- Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network
- Do not broadcast your location on social media. This tells thieves you are not home.
- Talk to your kids about what is and is not appropriate to post online

We are thankful for you and your knowledge so we urge you to share it. Take time this holiday season to keep those you are thankful for safe.

## CONTENTS

### Monthly Article

Thankful for You P.1

### Interest Articles

The Mirai IoT Botnet P.2

### Program Updates

InfoSec Academy P.2-3

NSOC Update P.3

### Spotlight

Terri Duncan P.4-5

### Events

P.5

# The Mirai IoT Botnet

On October 21, several popular sites like Twitter, Netflix, Amazon, Etsy, Vox, Pinterest, PayPal, Verizon, Spotify and Reddit were affected by a massive DDoS attack on Dyn, a major DNS service provider company. This made it difficult for users to conduct business on, or request information from, these major websites that relied on Dyn for DNS service.

This DDoS attack created massive amounts of internet traffic to overload the targets' servers, and was orchestrated by hackers using the Mirai IoT botnet. Malware is used to infect computer systems and turn them into internet-controlled bots – or *botnets*. It's usually distributed by means of phishing emails, drive-by downloads or even using social engineering. Mirai is unique because of its ability to scan the internet for IoT (Internet of Things) systems protected by factory default or hard-coded usernames/passwords. The source code for Mirai, which was launched against [KrebsOnSecurity](#) in September, was publicly released on site Hackforums.net.

Hackers use Mirai to perpetrate such an extravagant DDoS by gaining control of smart technology DVRs and internet-connected cameras. Surveillance cameras and recording devices were primarily used to create a vast botnet (Tens of millions of IPs) to distribute massive amounts of internet traffic to Dyn. The Chinese electronics company, Hangzhou Xiongmai Technology (HXT), manufactured such devices that were especially vulnerable to Mirai infection. Though HXT had pushed out a patch that prompted customers to update their default passwords back in September of 2015, many of the infected devices were still running older and susceptible firmware.

Though Dyn engineers were able to restore DNS service shortly after the attack, the presence of Mirai is indicative of a new generation of malware that has long-reaching capabilities and ever-increasing scanning proficiency. The securities solutions firm, [Corero Network Security](#), predicts that this recent DDoS is "child's play," compared to what is to come. They expect that we shall soon see a new, zero-day-like DDoS attack vector that utilizes LDAP (Lightweight Directory Access Protocol) to produce "amplification attacks," which could see DDoS traffic amplified by as much as 55 times.

Read more this attack and the NSOC monitoring on page three.

## InfoSec Academy Update

A critical goal of the Texas InfoSec Academy is to encourage higher education and state security professionals to participate in security education and certification classes. We are excited to announce that participation in this program is growing. InfoSec Academy participants have completed 109 courses broken down as follows:

Texas Security Policy & Assurance (online)	53
Texas Security Policy & Assurance (instructor led)	33
<b>Online Live Courses</b>	
Certified Information System Security Professional (CISSP)	10
Certified Information Security Manager CISM	6
EC-Council Certified Ethical Hacker CEH	4
CompTIA Security+ Certification	3

In addition, close to 50 additional participants are currently taking the Texas Security Policy & Assurance online. This online version takes approximately four hours to complete and the instructor led class requires approximately seven hours. The next scheduled instructor led Texas Policy & Assurance classes are on November 21, 2016, and January 20, 2017. This class is a prerequisite for the certification prep classes.

The OCISO team would appreciate your feedback on the Texas InfoSec Academy. If you have taken a certification prep course, please tell us if you plan to or have already taken the certification test. Please send any feedback or questions to [infosecacademy@dir.texas.gov](mailto:infosecacademy@dir.texas.gov).

### Cancellation Policy

If are registered for a certification prep course but must cancel, you must do so 2 weeks prior to the course start date. If you do not, you can take the course at a later date, but cannot substitute a different course.

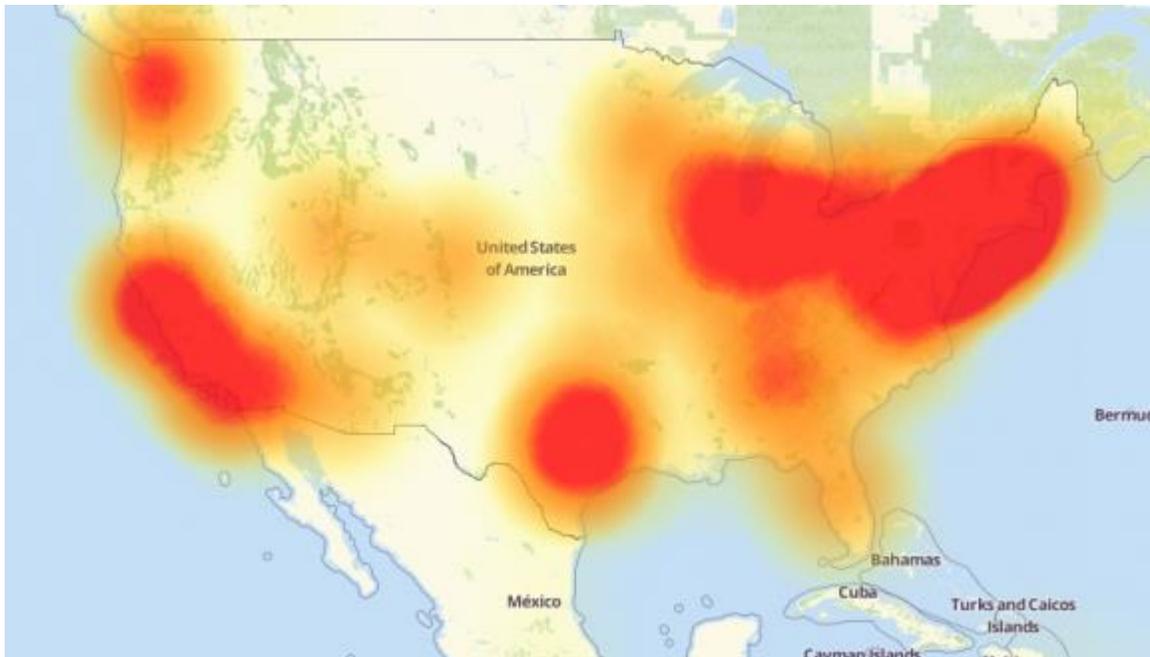
## NSOC Update

As discussed on page two, several large companies including Twitter, Amazon, Netflix and others were subject to a DDOS attack. This was an interesting attack because it used a type of malware that finds and exploits “Internet of Things” (IoT) devices such as web cameras and DVRs to attack those companies. These devices are protected by little more than factory-default usernames and passwords, and the malware enlists these IoT devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users. See a link to the article in Krebs on Security below for more information.

The DIR NSOC offers DDOS monitoring and protection for its customers. We did not see any impacts (thankfully!) during this attack timeframe. Most attacks are noticed and mitigated before there is any impact to our customers. Please remember that if you are an NSOC customer, and are concerned that you may be experiencing a DDOS attack, contact us – it might have been low level and evaded our detection baselines. If you do not receive Internet services from the NSOC, please remember to ask your provider about DDOS services, or consider evaluating tools that may help if you are targeted.

As always I can be reached at [Jeremy.wilson@dir.texas.gov](mailto:Jeremy.wilson@dir.texas.gov) for any questions you may have, stay safe out there!

<https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>



A depiction of the outages caused by today’s attacks on Dyn, an Internet infrastructure company. Source: Downtdetector.com.

# Information Security Officer Spotlight



**Terri Duncan**  
**Information Security Officer**  
**Texas Department of Transportation**

I began my career in the Air Force as a mechanic and found I was not fond of smelling like jet fuel and grease. This presented an opportunity to find cleaner work and led me to electronics school. I've loved my work ever since and am so appreciative of being able to do something that I love. I spent 11 years with the Department of Energy (DOE) performing physical and cybersecurity engineering for our nuclear weapons and I sure had fun doing it. I also spent seven years designing and integrating industrial automation solutions. I then spent six years with the nuclear power industry performing cyber assessments, designing solutions and testing to meet federal regulations. I have a BS in Engineering (SDSU) and Masters in Public Administration (OU). I now work for TxDOT and have been with the agency about 17 months. I am the first ISO and appreciate the many peers in other agencies that have been welcoming, affirming and collaborative. TxDOT has approximately 13,000 laptops and 5,000 mobile devices to support. We have accomplished many updates to our network that allow us to give more mobility to our end users to use in the field to accomplish their work.

**Tell us how information security has changed since you started in your role.**

I remember working through college building clone PC's with 256K RAM, 10MB hard drives and TTL monitors. Physical security was the only form of security. I've seen cybersecurity develop as we've progressed to digital processes and mobile uses. Originally, we thought an isolated network was secure. Then we thought firewalls protected them, then software and monitoring systems became available. Data analytics and automated responses were something we saw on Star Trek.

**Who are your users/customers, and what is one of the most challenging areas for you?**

Our customers are every employee and contractor with TxDOT. We are currently expanding mobility

and it brings unique challenges with it. Our goal is to leverage technology so our end users can access everything they need to do their job from any location.

**What do you like best of your job?**

I enjoy it and the Texas Legislature has invested heavily in securing access to our data. I think the best thing I like is the people I work with.

**Have you ever changed career paths?**

I have not had an absolute change in career paths. Part of being an engineer is constantly keeping up with the changes in technology. I did not begin my career in cybersecurity, but it was a natural progression and I am very happy with it.

**What has been the greatest challenge that you have faced, and how did you resolved it?**

I had a motorcycle accident six years ago that should have taken my life. I spent months in the hospital and at home rehabilitating. I learned how much I took for granted, like rolling over in bed by myself, going to the bathroom and walking. I did it one step at a time and I credit my strength, perseverance and success to my faith.

**Tell us about your most proud accomplishment.**

My proudest accomplishment is my three children and two granddaughters. They have taught me so much and it's been a heck of a ride sometimes, but I'd do it all over again.

**Top 3 life highlights:**

- Attending bomb school
- Leading a national security program
- My children

**What are your hobbies?**

- Reading
- Volunteering
- Cooking

**Favorite line from a movie?**

I have many. One of the top is Monty Python's Holy Grail, it's "just a flesh wound."

**What books are at your bedside?**

- We Were Wrong, Keith Stewart
- Hacking Essentials
- It Worked for Me – Colin Powell
- The Kindness of Strangers – Mike McIntyre

**If you could interview one person (dead or alive) who would it be?**

Jesus

**If given a chance, who would you like to be for a day?**

My mother

**What is one thing you couldn't live without?**

Hope

**What is the best advice you have received and that you have used?**

Be kind. Your words and action can harm and hurt. No matter what you need to say or do, there is a kind way to do it.

**What would be your advice for a new security professional?**

Hang on, this is quite a ride!

# Events

---

## 2016 Save the Dates

- Innotech Austin: November 17, 2016, Austin, TX
- TASSCC State of the State: December 16, 2016, Austin, TX
- Information Security Forum: April 11-12, 2017, Palmer Events Center, Austin, TX

THE DIR CYBERSECURITY INSIGHT




---

Feedback, comments, stories, etc. | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

---