

THE DIR CYBERSECURITY INSIGHT

December FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

OCISO WISHES YOU



SANS Holiday Hack Challenge

It's the holidays, and along with family time and gifts usually comes game time. SANS is heading up a Holiday Hack Challenge. So hone your hacking talents and check out the information below:

It is the most wonderful time, when Ed Skoudis & Josh Wright and their team of challenge creators unleash months of creativity and technical prowess into one of the most anticipated moments of the year - the SANS Holiday Hack Challenge!

www.holidayhackchallenge.com

This year, Ed & Josh and their team have developed something they've never done before. The challenge starts off in an easy to learn and maneuver online RPG (Role Playing Game) where you'll go on a quest to discover all the pieces you'll need (plus hints and tips) to hack your way through the rest of the challenge. The quest is filled with tons of Easter eggs, some of your favorite SANS instructors, and lots of fun for the whole family!

These challenges are designed to build upon your skills or give you the opportunity to learn new and interesting tools and techniques. Open to all novice to advanced information security professionals who are looking for a progressively challenging game this Holiday Season.

Will you be able to discover "Who the Villain" is in this year's storyline? Oh yes, there is a storyline, and so much more to unwrap at www.holidayhackchallenge.com - including how to earn a free online SANS training course.

The SANS Holiday Hack Challenge is totally free and is a labor of love for all who contribute to it. We hope you enjoy!

Learn more about this year's SANS Holiday Hack Challenge and ring in the New Year with some new InfoSec skills! www.holidayhackchallenge.com

Wishing you Happy Holidays and an amazing 2016!

CONTENTS

Monthly Article

SANS Holiday Hack Challenge **P.1**

NSOC Update

Infostealers **P.2**

Our State ISO

Spotlight

Joshua Kuntz **P.3**

OCISO Corner

Paul Casey **P.4**

From our State

CISO **p.5**

Events **p.6**

Network Security Operations Center (NSOC)

“Malware by any other name would be just as evil.” Okay, that’s not the *exact* quote, but malware comes in many forms with countless variants. Infostealer is one of these malware variants that can do serious damage to networks and wallets.

What are infostealers?

Infostealers are fraudulent applications that use a trojan horse delivery system to collect sensitive information about users. As soon as an infostealer is installed on a compromised computer, it begins to record all keystrokes and gathers detailed, Personally Identifiable Information (PII) including user bank, email, and credit card accounts as well as other information which could then be sold. Scammers can profit in the range of \$0.10- \$1000 for each credential. Infostealers attempt to collect as many details as possible while silently working in your computer’s background for months or longer. If you have a suspicion that your computer could be infected with an infostealer, you should immediately move to remediate the machine and any associated accounts.

Infostealers are nothing new to security professionals. They are a known threat to user credentials. What is slightly different about infostealers in the modern landscape is that they have not only been used as a standalone tactic to harvest user credentials, but they are also now being used in conjunction with ransomware. There are constantly new types of infostealers being developed because infostealers and ransomware have been monetized. Whether stolen credentials are used to facilitate a ransomware compromise or are sold on the black market for other nefarious purposes, the result is the same: the bad guys get money. For example, Symantec reported that some of the most popular items of information sold in the underground economy changed hands for the following prices:

Credit card information - between US\$0.06 - \$30 each.

Bank accounts - between US\$10 - \$1000 each depending on the balance.

Email accounts - between US\$0.10 - \$100 each

How can I remove it?

There may not be any tell-tale signs you’ve been infected with an infostealer. Trojan malware is designed to stay hidden and to run behind the scenes. However, if you think you may be infected with an infostealer, you should scan your PC with reputable anti-spyware, anti-virus and/or anti-malware programs to remove this trojan from your computer. Depending on where the infection is, for example the registry or root drive, a re-image may also be required to remove the infection. It is also a good idea to change all of your passwords across all platforms and programs.

What does the NSOC do about it?

The NSOC adds any IP addresses and domains associated with either infostealer Command & Control servers or communicating with infected machines to the blacklist. The NSOC also has multiple toolsets that are constantly being updated with new signatures and filters to monitor and (when possible) block these types of communications. With that being said, there are always new infostealer variants being used and new IP’s and domains being compromised. Because of this, we are never going to be 100% safe from this type of threat at any given point in time.

What can you do about it?

As always, the best defense to avoid infection is to run an effective user awareness program for security. Our users are the first line of defense. In addition, continuous monitoring of your assets (both accounts and hosts) will help to reveal if you have been infected.

As always, feel free to reach out to me direct at Jeremy.wilson@dir.texas.gov or the rest of the security team at the NSOC at security-alerts@nsoc.dir.texas.gov or at security.alerts@dir.texas.gov with questions about this article or NSOC Security operations in general. Thanks and stay safe out there!

Information Security Officer Spotlight



Joshua Kuntz
Information Security Officer, CISSP
Texas Department of Motor Vehicles

From 1995 – 2001 I was an electronics technician in the United States Marine Corps. From 2001 – 2009 I lead the satellite team at TxDPSS which provided the secure network for the Texas Law Enforcement Telecommunications System (TLETS).

From 2009 – 2012 I developed and operated the Information Security Program as the ISO at the Texas Juvenile Justice Department

From 2012 – Present I've been the ISO of TxDMV. However, at TxDMV I've been asked and agreed to fulfil the interim position of CIO (IRM) from Feb-April of and then as the Enterprise Project Management Office Director from August 2013 – April 2014.

How did you come to the security field?

Like many in our profession, I moved into the security field laterally. I was essentially a network technician that understood the importance of securing the data that we transmitted, and developed the awareness of how those security controls could be applied universally to differing disciplines. I was given a chance to prove myself at the Texas Youth Commission in developing their security program after they had an audit finding for not employing a full time ISO. From there I gained my certification and participated in as many interagency initiatives as I could.

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

I think the biggest change in Information Security has been awareness. When I first started as the ISO of TYC, it was difficult to get management to understand the importance of information security's role in the overall business context. However, each high profile data breach that hits the news media has sharpened the focus of business leaders and

legislators on the possible impact of not dedicating enough resources, time, or attention to information security.

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

TxDMV has 16 Regional Service Centers and supports 512 county Tax Assessor Collector offices, who conduct the frontline business of titling and registration. The TACs are local elected officials who advocate for their constituency quite vocally. Trying to support their individual business needs while protecting the security of the enterprise wide network that interconnects them all can be quite a challenge.

What do you like best about your job?

Problem solving and educating... I'm often faced with questions, not always directly on security, about how the section/project/division/agency should approach an issue or deal with a concern. I like to help the requester work through the logical problem solving steps to help them deal with problems that come up later.

Top 3 life highlights?

The birth of my daughter
Marine Corps graduation
Fishing with my Father

What are your hobbies?

Hunting, fishing, camping, gardening, hiking, shooting... pretty much anything outdoors.

People would be surprised to know that you...

I reenact the pre-1840 Fur Trade Era Rendezvous... We wear period correct clothing, live in canvas tents, cook over open fires, and have competitions; muzzleloader rifle, pistols, & smoothbore shoots, primitive archery, tomahawk & knife throwing, primitive fire starting.

OCISO Corner – Getting to Know the Team



Paul Casey
Information Security Analyst
Department of Information Recourses

What is your responsibility in DIR and with the State?

My job duties center around the RSA Archer GRC platform. I work to transform the business requirements of agencies and its users into solutions enabling them to gain value from the Archer tool in the form of automated workflows and business processes.

When and where did you start your career?

After attending school at The University of Texas at Austin, I found that I didn't want to leave this wonderful city. I worked at UT in the Information Technology department before moving in to the information security field at U.T. System. Assisting a new CISO, in building a new information security program from the ground up, gave me a lot of insight into this complex, fast moving field. I really enjoy being a resource for agencies as they work to secure their environments.

Why security field?

I find the complexity of the information security field to be both challenging and exciting. There are so many specialties and concepts wrapped in to one field that you can have many interests and deal with them all in one day.

What is your personal back ground (born/raised/school/family?)

I was born and raised in the oldest town in Texas, Nacogdoches. Of course, that may also help to explain why I got to a city like Austin and never wanted to leave. I am technically an only child but have four half-brothers and three half-sisters. I met my wife in college and have two

overscheduled children, a 13 year old girl and an 8 year old boy.

What did you think you were going to be when you grew up?

I played a lot of sports as a kid, so I really wanted to be a baseball player. Over time, and curveballs that I couldn't hit, I set my goal to become an athletic trainer for professional sports. That lasted until I found out they had to go to school for more than four years as I wasn't quite a motivated learner in those days.

What is the greatest lesson you have learned?

It's a quote from Gandhi that I still struggle to implement, "Live as if you were to die tomorrow. Learn as if you were to live forever." The world overwhelms us with instant access to information and tasks that sometimes I frantically race around all day and forget to enjoy the experiences.

What do you want your legacy to be?

Quite simply, to always positively impact any path I cross.

Do you have a favorite hobby or pastime?

I like to play most sports and to compete with friends on the field or court. I enjoy being outside in nature through hiking or fishing. I also like mentoring children, so I coach soccer teams and volunteer in local soccer organizations. I like reading about people's motivations, psychology, and sports statistics.

What do you like best about working at DIR?

I love the State of Texas and supporting the mission of our agencies. Our State Agencies do a lot of great, important work and I want to have a part in making their mission easier to accomplish.

Insight from our Texas CISO

Holidays

As a security professional I have mixed feelings about the holiday season. Spending time with family, food, faith, and football is great. There is nothing better than sitting with my sons, watching football, on a day it's "just too cold" to go out (yes, I live in Austin. I know it's never really too cold to go out, but I can suspend disbelief).

I also know this time of year is filled with phishing and financial crimes. So while I'm visiting with family, I'm the "Debbie downer" reminding them to watch their credit card statements... Maybe don't click on "e-cards" you get in email... shred everything.

Yeah, I'm really fun at parties.

I think it is important to warn those we care about to look out for these types of threats. What steps can the average person take to protect themselves from electronic crime? We can educate them on things like:

- Verifying secure connections in web browsers used for online shopping
- Being wary of "free" Wi-Fi in public locations
- Investigating credit monitoring and identity protection services
- Using 2-factor authentication on ecommerce sites (Amazon now has 2-factor for general use. See <https://www.amazon.com/gp/help/customer/display.html?nodeId=201596330>)

Who, besides us, is in a better position to let our loved ones know of emerging threats and the significant damage that identity theft can have on their lives?

Did I mention how fun I am at parties?

As KHOU in Houston reported¹ it isn't just electronic crimes that spike during the holidays. Old fashioned smash-and-grab crimes also surge during this time of year. While we are helping our families and friends understand phishing, we can't forget that criminals will always find the weakest target. Sometimes that is a car window.

So, Happy Holidays and a Good New Year to everyone. I wish you all a safe, happy, and peaceful transition to the New Year.

P.S. I'm also available for parties, my calendar seems a bit light this year...?



Eddie Block
CISO, State of Texas

Eddie Block
CISO, State of Texas

¹ <http://www.khou.com/story/news/crime/2015/11/25/why-criminals-love-the-christmas-shopping-season/76395218/>

Events

2015 Save the Dates

- Information Security Forum: April 14-15

OCISO Participation Around the State

- Eddie Block, Claudia Escobar and Jeff Rogers attended TASSCC State of the State held December 11.
- Eddie Block and Claudia Escobar participated in the Arizona Statewide Cybersecurity Exercise held December 8-9.