

“SOLUTIONS ARE OUR BUSINESS”

FEBRUARY 2016

## 3 New Malware to Look Out For in 2016

Cybercriminals continue to be relentless when it comes to breaking the law and getting what they want. They definitely take to heart the saying, “if at first you don’t succeed, try, try again”. These new tactics require diligence and extreme patience, and these criminals are proving they have both in abundance. Many researchers have warned for years that these new attacks will slowly come down the pipeline and it now looks like that time has arrived.

Last week, Kaspersky Lab held their annual Security Analyst Summit. What they discovered were three new attacks that were launched against Russian banks in 2015 and were successful in stealing millions of dollars. Below are the three new and improved attacks:

**Metel also known as Corkow-** This malware uses phishing emails to gain access. How it works: Attackers send the emails to employees of the banks and wait until someone takes the bait. Once the attackers are in the bank’s network, they locate the systems that control transactions. The attackers then reverse ATM transactions for specific debit cards,

then they drive around making withdrawals from different ATM machines. This scam is hard to detect because they have manipulated the system so the account balance never change.

**GCMAN-** Like other malware, this one also uses spear phishing emails to get into the network. How it works: The attackers are able to gain access by attaching malicious documents to the spear phishing email. They target the devices of HR and accounting specialists and then wait until the system administrator logs into the system. Sometimes they crash Microsoft Word program or the software used for accounting, requiring the user to call their helpdesk for assistance. Once the system administrator logs in to solve the problem, the attackers steal the admin’s password.

**Carbanak-** This malware is one of many advanced persistent threats (APT) and is not new but is improved. This particular malware is also done through phishing emails. The attackers are not trying to gain access to data, but to money. How it works: The attackers manipulate their access to the bank’s network and steal money in multiple ways. One way that has been reported is by gaining access to the systems that house shareholders’ information, changing the ownership of a company, then naming the criminal as a shareholder.

Financial organizations have to remain vigilant. Phishing scams are constantly evolving and that is more than clear based on the



### INSIDE THIS ISSUE:

**3 NEW MALWARE TO  
LOOK OUT FOR IN 2016**

**RECOGNIZING THE TEAM**

**COME JOIN US FOR THE  
ISO PEER GROUP MEET-  
ING IN TN AND WV**

above malwares. Phishing has been extremely profitable for many cybercriminals. You do not want to fall victim and one day accidentally invite cybercriminals into your office. Be sure to take a thorough look at links and emails received before opening. If something looks amiss, shut down your computer and Internet connection immediately. And always update your antivirus software, operating system and browser on a regular basis.

# Recognizing The Team



Angel and his wife Cristina!

AaSys recognizes that our success relies on our extraordinary team. We take pride in acknowledging each team member's contributions, and each year, we highlight an employee that has exceeded expectations and who has gone beyond the call of duty. The 2015 recipient of the **AaSys Employee of the Year Award** was granted to **Angel Gonzalez**.

Angel started his career with AaSys seven years ago. He always had a love for computers and the intricacies of how they worked and knew a career in engineering was the right fit for him.

Angel is based in Miami, FL and started as a Network Engineer and worked his way up to a Sr. Network Engineer. His job requires him to establish and maintain network performances for our customers by building net configurations, connections and troubleshooting network problems. Every day is different and every day presents new challenges; but Angel is up for it. He has been known to resolve and handle difficult situations with remarkable patience and admirable tact. His dependability, relatability and can-do attitude make him the go-to person, not only for our customers, but for his peers as well.

Outside of his love for computers, Angel enjoys the ocean and tries to make time for fishing, scuba diving and snorkeling.

We are honored and grateful to have Angel as part of the AaSys Team and commend him for a job well done. Congratulations Angel!



**Congratulations on being Employee of the Year 2015!**

**"The strength of the team is each individual member. The strength of each member is the team."**

**Phil Jackson.**



## Come Join Us for our ISO Peer Group Meeting In Tennessee and West Virginia!

AaSys Group is holding an Information Security Officer Peer Group Meeting in Tennessee and West Virginia. Both meetings will address the same topic. These meetings gives those responsible for the ever-increasing demands of Information Security a resource to share issues, concerns & compare best-practices to improve the overall security structure of their financial institution.

**Topic of Discussion: FFIEC IT Examination Handbook; Management Booklet**

***A Breakdown of the Revised Rules and Examiner Work Program***

**Save  
the  
Date**



### **Knoxville, TN**

Date: Thursday April 7, 2016

Time: 10:30 AM – 2:30 PM

Location: Hampton Inn Knoxville West - Cedar Bluff

9182 Executive Park Drive

Knoxville, TN 37923

### **Charleston, WV**

Date: Friday April 8, 2016

Time: 10:30 AM – 2:30 PM

Location: Hampton Inn Charleston

1 Preferred Place

Charleston, WV 25309