Society of SAME American Military Engineers

NEWSLETTER

FEBRUARY 2018

ANNOUNCEMENTS

SAME Guam Post shirts are for sale

SAVE THE DATE

18-24 FEB
Engineers Week

22 FEB
Joint GSPE/AIA/GCA/SAME meeting

07-08 MAR
Guam Industry Forum at Dusit Thani

09 MAR
Charlie Corn Golf Tournament
(SAME scholarship fundraiser)

John Robertson, PE, SAME Guam Post President and Special Agent David Anderson (FBI)

CYBER THREATS & AWARENESS

Main Presentation
by
Special Agent David Anderson
Federal Bureau of Investigation

The FBI (IC3) received **298,728** cyber crime and fraud complaints in 2016 with reported losses in excess of $1.4 Billion.

Business Email Compromise (BEC) was the No. 1 cause of loss.

BEC Global *Exposure*	Over $5 Billion (since 2013)
BEC Reports	All 50 States & 131+ countries

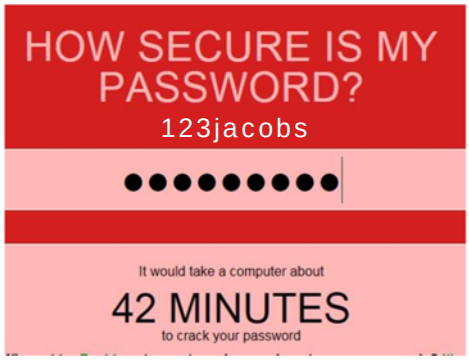
BEC From January 2016 - June 2017:

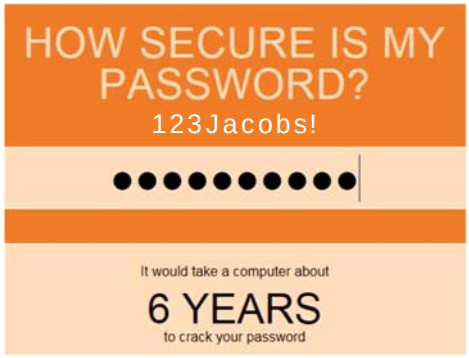
-	Attempted	$222,890,660
-	Returned/Frozen	$74,831,206 (34%)
-	**Unrecovered**	**$148,059,454 (66%)**

Having an understanding of what information your organization possesses that is of value to an attacker is critical to determining where to spend the most security resources.

Read more on the following page.

Find us on: facebook **SAME Guam Post** or log on to SAME.org & click on *"Membership"* at the top of the Home Page





WHAT TO DO IF YOU ARE A VICTIM

Immediately contact your bank and initiate a recall.

Call you local FBI Office.

SA David Anderson
(671) 645-1814

Information and graphics courtesy of
Federal Bureau of Investigation

CYBER THREATS & AWARENESS

WHAT ARE THEY AFTER?

Attacks typically target **data**, **people**, or **infrastructure**.

INTELLECTUAL PROPERTY

Intellectual property is the lifeblood of many organizations. Theft of such information can affect the long-term survival of the organization.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

A leak of this information can cause damage to customers and civil liability exposure.

MONEY

Monetary losses can result from denial of service to critical business systems. Critical assets should be identified and more resources should be spent on protecting them over less critical corporate assets.

BUSINESS EMAIL COMPROMISE

How does it start? It starts with an infection of the system (usually through malware delivered by email) and/or the purchase of user credentials on the Dark Web. An infected email can be sent from a domain very similar to the target to create the appearance that the email came from within the company; an example of this might be "accounting@IBM.com" vs "accounting@1BM.com".

Credentials sold online are used to – among other things - log in to customer accounts, read emails, and access any documents stored or transferred there. In cases where malware is used and the actor is more sophisticated, key-loggers can collect passwords and spyware can allow the intruder to change settings, forward telephone lines, and access microphones, cameras, and location data (etc..)

WHAT CAN YOU DO?

REVISIT POLICIES & PROCEDURES

- Make sure policies provide for verification of any changes to existing invoices, bank deposit information and/or contact information.
- Contact requestors by phone before complying with email requests for payments or personnel records transfers.
- Consider requiring two parties to sign off on payments.

PASSWORD DISCIPLINE

- Use long passwords and consider changing them frequently.
- Don't re-use passwords for more than one account.
- Consider using a Password Manager.

SOCIAL MEDIA

- Posting business or vacation travel of company staff could let BEC scammers know when executive are out of reach.
- Social Media can also provide scammers with information about friends, family and business deals.