16900: z/OS Mainframes at Risk: The Current Threat Landscape!

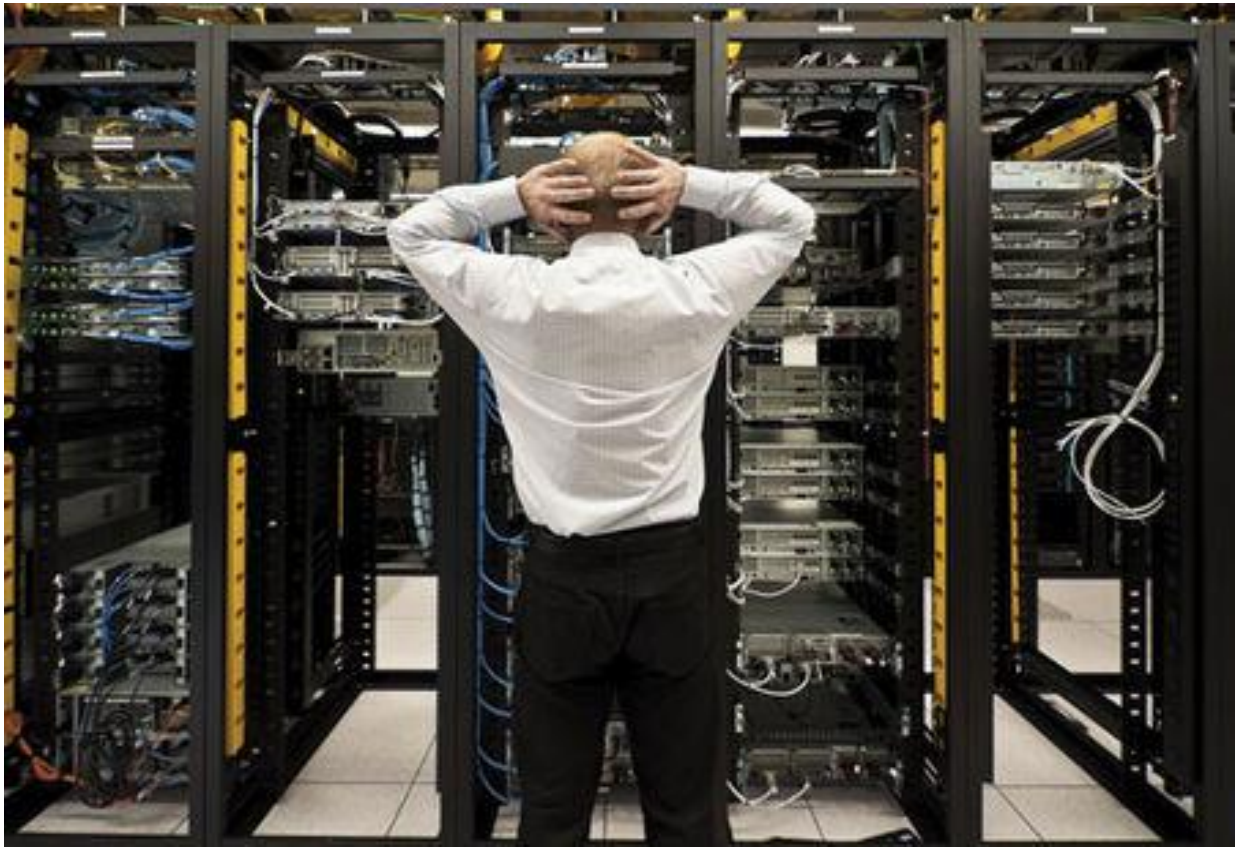
Brian Marshall
Vice President, Research and Development
Vanguard Integrity Professionals

Tuesday March 3, 2015

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

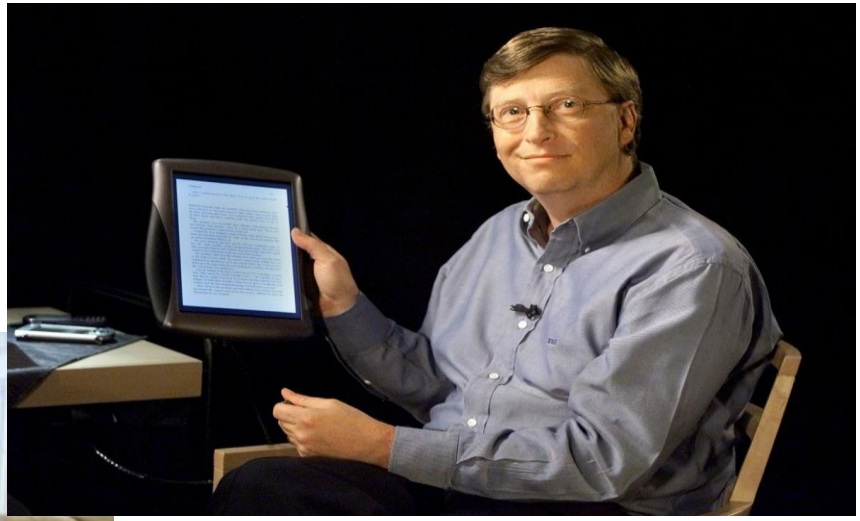
Well, today it's all about data!



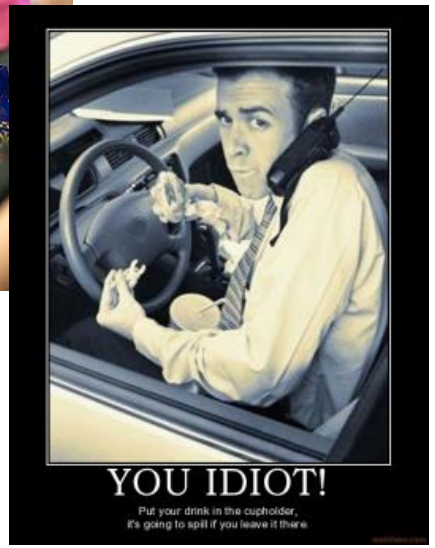
So, where is your data today?

Wherever you are…….

Your data on the move with tablets….



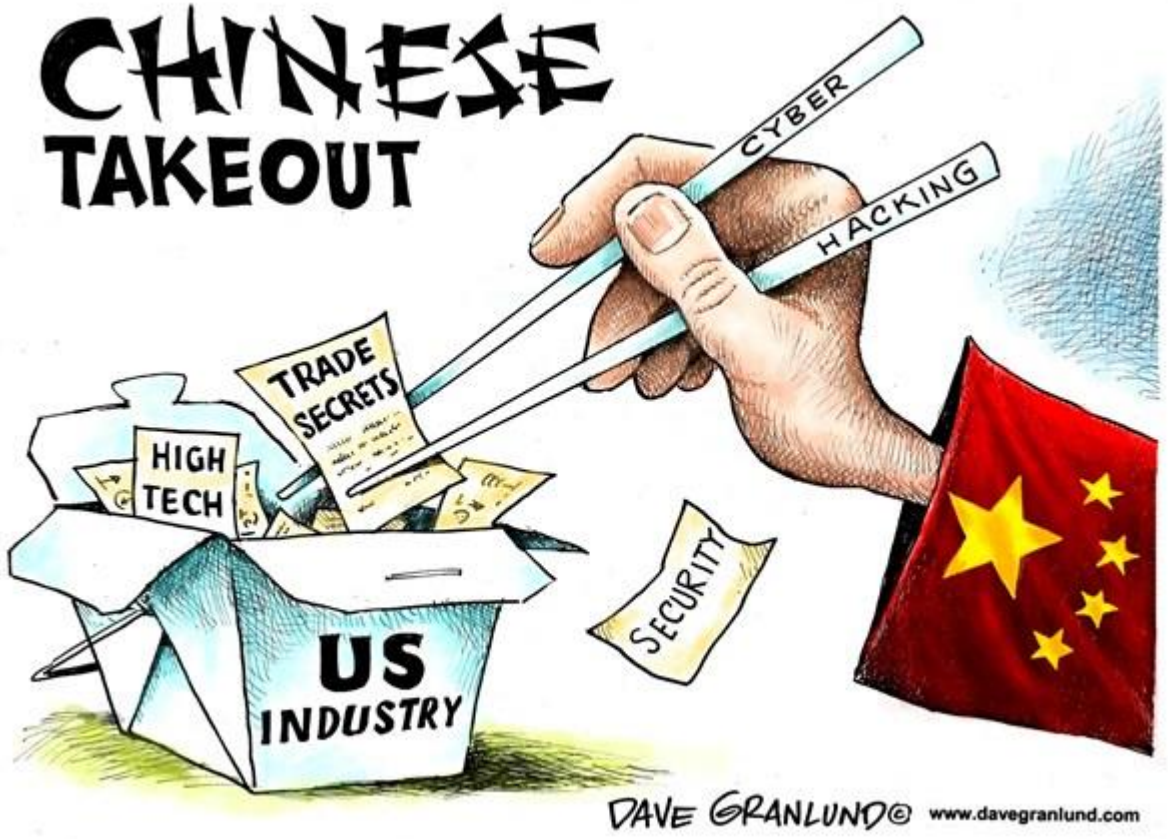
…and oh so many devices!



Is your data in the cloud?

In the hands of criminals?

In the hands of other nations?



In the hands of some government agency?

We hear it every day!

So, what's new?

- IT's criticality has never been higher!
- It can be the differentiation of your business, it can be the intimacy with your customer, and it can be the public delivery of what you're doing ... you name it, it's now critical
- You just can't live without your network, your systems, your data center, etc., because you're fully reliant upon them to run a business

Know Thy Enemy – Understand the Threats

Because the truth is….

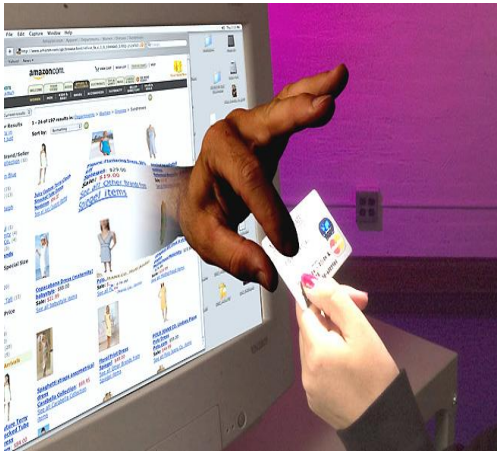
You are about to be compromised

OR

You have already been compromised

Or will you???

The web became significantly more malicious, both as an attack vector and as the primary support element of other attack trajectories (e.g., social, mobile, email).



Maybe you have better security……

The web became significantly more malicious, both as an attack vector and as the primary support element of other trajectories (i.e. social, mobile, e-mail, etc.).

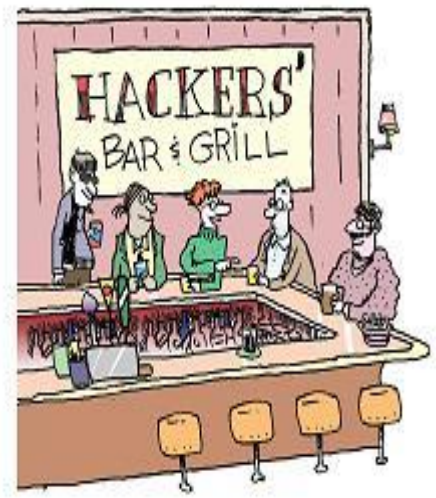
Biggest IT Myths

- Hey, it won't happen to us!
- Buy this tool <insert tool here> and it will solve all of your problems.
- Let's get the policy in place and we are good to go.
- I passed my IT audit, I must be secure.

So, where do we focus ?

We have seen an emergence of several criminal factions…

- Nation States
- Collectives
- Hacktivists



Cyber warfare: Characteristics and Challenges

- The specter of cyber warfare isn't just a problem for governments — many types of organizations are already in the line of fire
- Knowing the types of attacks and their probability will help you prepare

We're all looking for help

- Many IT managers believe the government should do more
- While there are things the federal government can do, each organization is responsible for implementing basic prevention, detection, and response controls to deal with inevitable breach attempts

Hackers get help as well

- Many tools, used by both white hat and black hat hackers, are free (e.g., Live Hacking)
- Others, like Metasploit, are intended for the professional cybercriminal and penetration tester
- Finally, nation-sponsored intrusions often make use of proprietary tools and techniques designed for a planned or ongoing attack

You've Got Mail– Do not open that email…

NYT Chief Security Officer Michael Higgins said, "Attackers no longer go after our firewall. **They go after individuals.** They send a malicious piece of code to your e-mail account and you're opening it and letting them in."

Chinese hackers use compromised university computers to attack us.

To run a NY Times campaign, attackers used a number of compromised computer systems registered to universities in North Carolina, Arizona, Wisconsin and New Mexico, as well as smaller companies and Internet service providers across the United States

Their M.O.

The cyber spies typically enter targeted computer networks through “spearfishing” attaches, in which company official receives a creatively disguised email and it tricked into clicking on a link or attachment that then opens a secret door for hackers.

How Facebook Got Hacked

- Does this sound familiar?
- Facebook says it fell victim to a sophisticated attack discovered in January 2103 in which an exploit allowed malware to be installed on employees laptops

Anti-virus? I have it installed, I am protected.

- Several Facebook employees visited a mobile developer website that was compromised
- The compromised website hosted an exploit that then allowed malware to be installed on these employees' laptops
- The laptops were fully-patched and running up-to-date anti-virus software

Target Attack

- **Nov 27 – Dec 15, 2013:** Personal information, including names, mailing addresses, and phone numbers of 40 million customers who used credit and debit cards at U.S. stores are exposed to fraud.
- **Dec. 18, 2013:** Data and security blog KrebsOnSecurity first reports the data breach. The Secret Service investigates.
- **Dec. 19, 2013:** Target publicly acknowledges the breach.
- **Jan. 10, 2014:** Target says an additional 70 million customers had personal information stolen during the breach, including emails. The company lowered its forecast for its fourth quarter, saying sales were meaningfully weaker than expected after news of the breach.
- **Feb. 18, 2014:** Costs associated with the data breach topped $200 million.
- **May 5, 2014:** Target CEO Gregg Steinhafel resigns.

The How

- Target gave network access to a third-party vendor, Fazio Mechanical, and penetrated that organization two months before the Target data breach began.

- Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.

- Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.

OOOOOOPPPPPPPSSSS

On Saturday, Nov. 30, 2013 the hackers had set their traps and had just one thing to do before starting the attack: plan the data's escape route. As they uploaded exfiltration malware to move stolen credit card numbers—first to staging points spread around the U.S. to cover their tracks, then into their computers in Russia—FireEye spotted them. Bangalore got an alert and flagged the security team in Minneapolis.

And then …

OOOOOOPPPPPPPSSSS

On Saturday, Nov. 30, 2013 the hackers had set their traps and had just one thing to do before starting the attack: plan the data's escape route. As they uploaded exfiltration malware to move stolen credit card numbers—first to staging points spread around the U.S. to cover their tracks, then into their computers in Russia—FireEye spotted them. Bangalore got an alert and flagged the security team in Minneapolis.

And then …

Nothing happened.

http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

A Similar but Frightening Example to Target

- In a frightening example from 2009, China purportedly wanted access to Lockheed Martin but could not breach the company's firewalls.
- However, by penetrating a smaller defense contractor, they were able to make their way in and steal blueprints for the joint strike fighter planes F-35 and F-22 worth more than $1 trillion.
- Thanks SMBs!

Every Second

- According to TrendMicro, cybercriminals unleash a new threat targeting SMBs every second.
- Another attraction to cybercriminals is the sheer number of targets.
- In the U.S., there are about 23 million SMBs.

South Carolina D.O.R.

- The hack took over 2 months
- They pilfered the tax returns of 3.8 million state residents and 700,000 businesses going back to 1998, gaining access to the social security numbers and bank accounts of the taxpayers and 1.9 million of their dependents.

The How

- The hacking began in late August 2012 after an unidentified South Carolina Department of Revenue employee clicked on a link in an email, which installed malware.
- The data thieves used the malware to obtain the employee's login and password for accessing electronic tax returns, and then downloaded the returns over the next seven weeks and none of the data was encrypted.

How do you not notice?

Likewise, the state failed to spot the follow-up compromise of 44 different systems, the installation of backdoor software, multiple instances of password hashes being dumped, the running of Windows batch scripts, or the attacker executing numerous arbitrary commands against databases.

Reconnaissance

- As a result, a few weeks after the first successful malware infection, the attacker was still using the stolen credentials to conduct recon on 21 different state servers, although he or she hadn't yet been able to access sensitive data.
- But with more work, by Sept. 12, 2012, the attacker had successfully located and begun copying 23 database backup files, containing 74.7 GB of data, to another directory.

At least someone found it! RIGHT!!!!

The breach remained undiscovered until about a month later, on Oct. 10, 2012 when the Secret Service informed state officials that information on three residents appeared to have been stolen.

The Pain of Learning

- The bill for the data breach at SC DOR now exceeds $20 million
- The NYT data breach cost millions
- The Target attack will be in the hundreds of millions
- The loss of fighter jet plans to the Chinese is incalculable.

The 7 Phases of the Intrusion Kill Chain

1. Reconnaissance	The hacker studies his target
2. Weaponization	Attacker prepares payload for delivery
3. Delivery	Attacker sends payload to victim
4. Exploitation	The weaponized code it triggered
5. Installation	The weapon installs a back door
6. Command & Control	Outside servers get command and control
7. Actions on Objective	The attackers work to achieve their objective (usually exfiltration of data)

The Eight Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Lax patching procedures
5. Lax logging, monitoring
6. Spurning the K.I.S.S.
7. Too much access for too many
8. Failing to respond to your own internal warning systems!!!!

We are still very vulnerable.

- And yet in the face of this very clear danger, we continue to have a lot of open windows and open doors.
- Mandiant's latest threat landscape assessment indicates that the median number of days that advanced hackers are on the network before being detected is *243 days.*

Make the effort! Secure it…

Systems that are unpatched, privileged accounts that are inadequately protected, a reliance on anti-virus alone for security — these are all examples of open windows and doors that allow an attacker to easily 'walk' into our network and take way all that is dear to the business

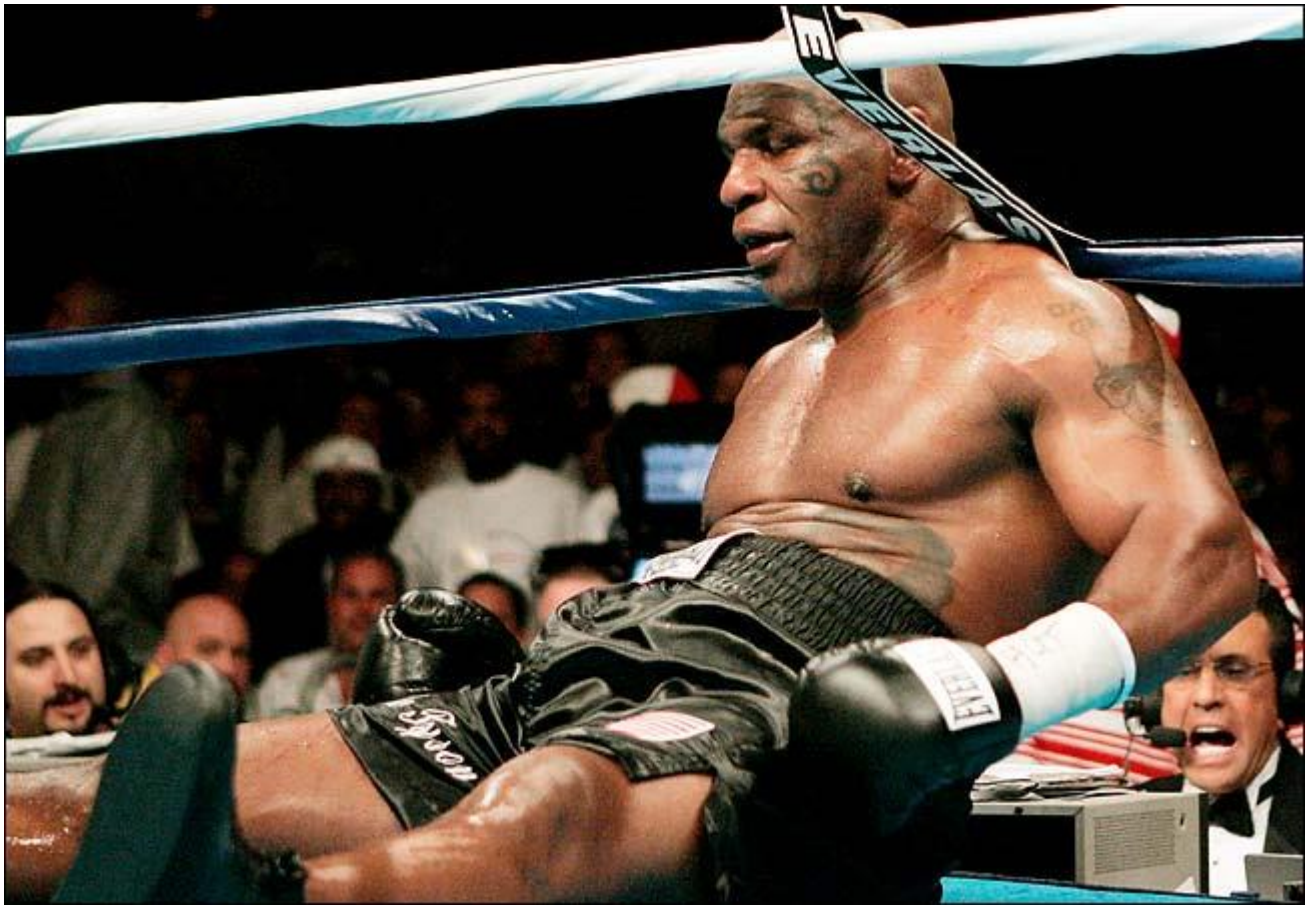
Collaborate

- The only way we can move forward safely and securely is through information sharing
- We don't have time in the day research all that is going on in the criminal world
- Think awareness

You can’t afford to give up your data, so be prepared and be alert.

How true!

"Every man has a plan, until he gets hit!"



Know who to call…and when!

Watch your network and your systems, closely…Call Vanguard!

You are the last line of Defense! Step Up!

- Understand
- Educate
- Collaborate
- Prepare

Thank You

Stop by and visit us at Booth 607!