WARNING! SECURITY BREACH!

BusinessConnect 2015

A New Way To Work

Stealing Millions and Hungry for More…

Mark Johnston

Executive Security Architect

IBM Security

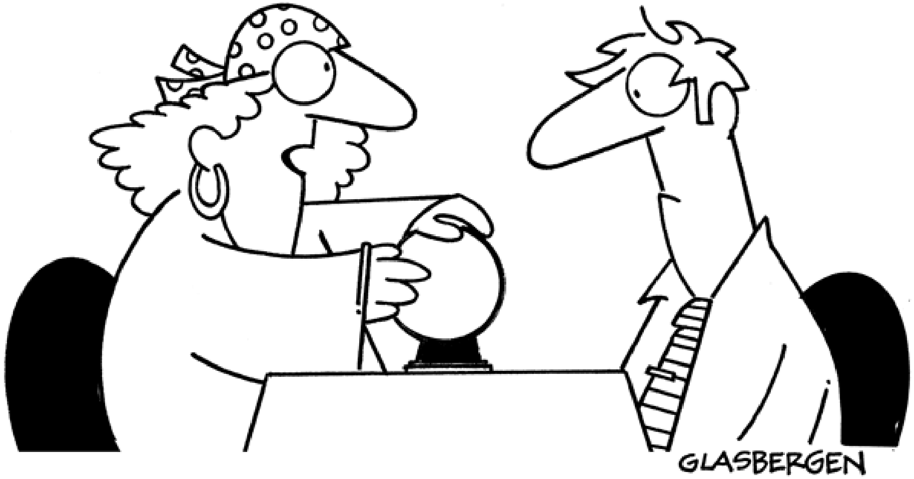
Agenda

- Recent security threats & impact

- What is the challenge we are up against?

- How we can work together to defeat Cyber Criminals?

© Randy Glasbergen
glasbergen.com



"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."

SONY

Hack Most Serious Cyberattack Yet on U.S. Interests

— REUTERS

CHASE

76M Households Compromised

— The New York Times

TARGET

Hack Costs Add
Up to $148M

— WALL STREET JOURNAL

THE HOME DEPOT

60M Credit Card Numbers Stolen

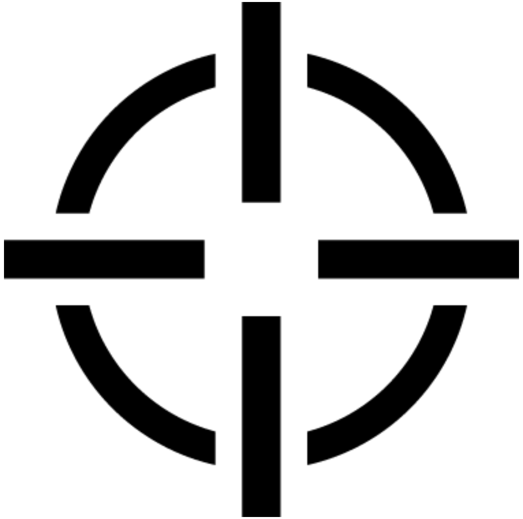
— Time Inc.

"There are only two types of companies those **that have been hacked**, and **those that will be**"

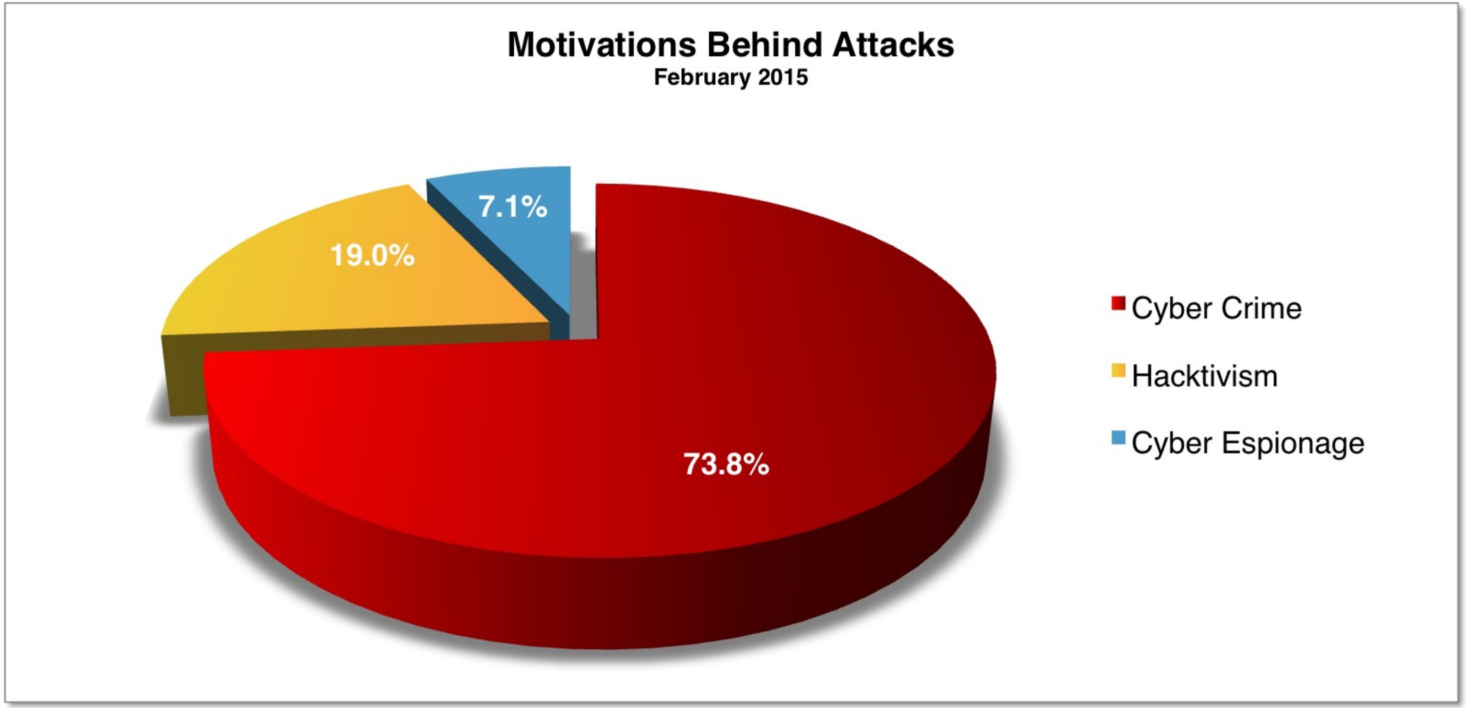
And even they are converging into one category companies that have been hacked and will be hacked again.

Robert Mueller, former Director of the FBI

EVERYONE In This Room Is A TARGET



What's The Motivation of an Attack ?

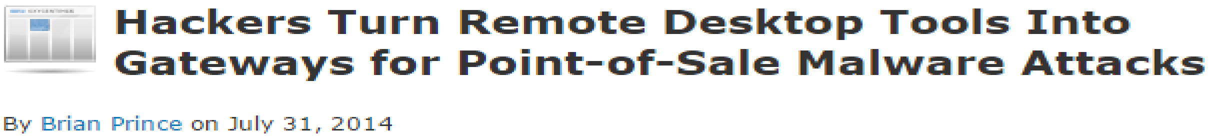


Motivations Behind Attacks
February 2015

Source: hackmageddon.com

2014 - Advanced Malware is The Weapon of Choice

- From simple RATs to advance malware – device takeover was everywhere
- PoS attacks targeted built in remote session solutions
- Citadel's persistent RDP and new targets



Hackers Turn Remote Desktop Tools Into Gateways for Point-of-Sale Malware Attacks

By Brian Prince on July 31, 2014

CITADEL MALWARE VARIANT ALLOWS ATTACKERS REMOTE ACCESS, EVEN AFTER REMOVAL

by Michael Mimoso Follow @mike_mimoso August 1, 2014 , 10:06 am

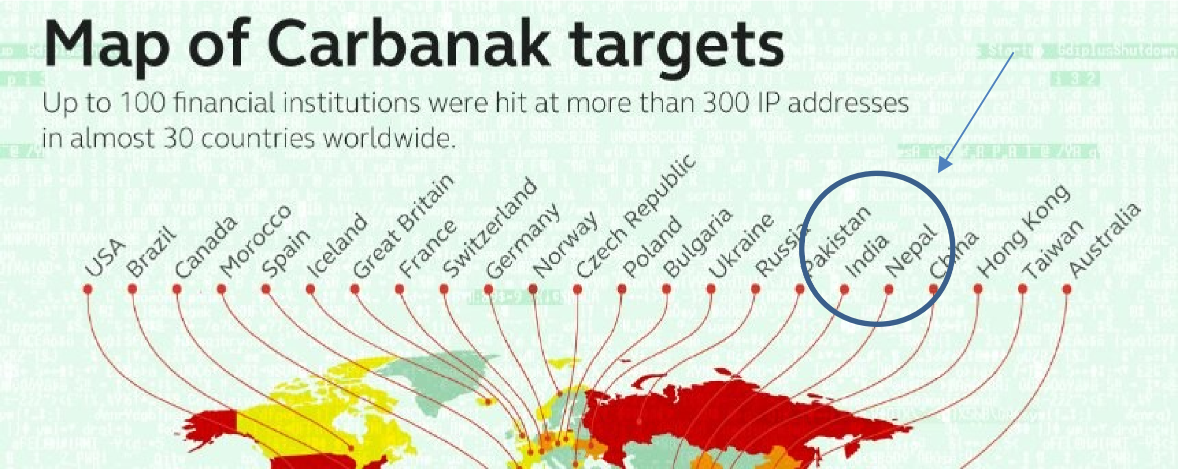
CITADEL VARIANT USED IN ATTACKS AGAINST MIDDLE EASTERN PETROCHEMICAL COMPANIES

An Example : Heard of Carbanak?

Carbanak: How Would You Have Stopped a $1 Billion APT Attack?

Kicking off 2015 with a bang, a well-orchestrated advanced persistent...

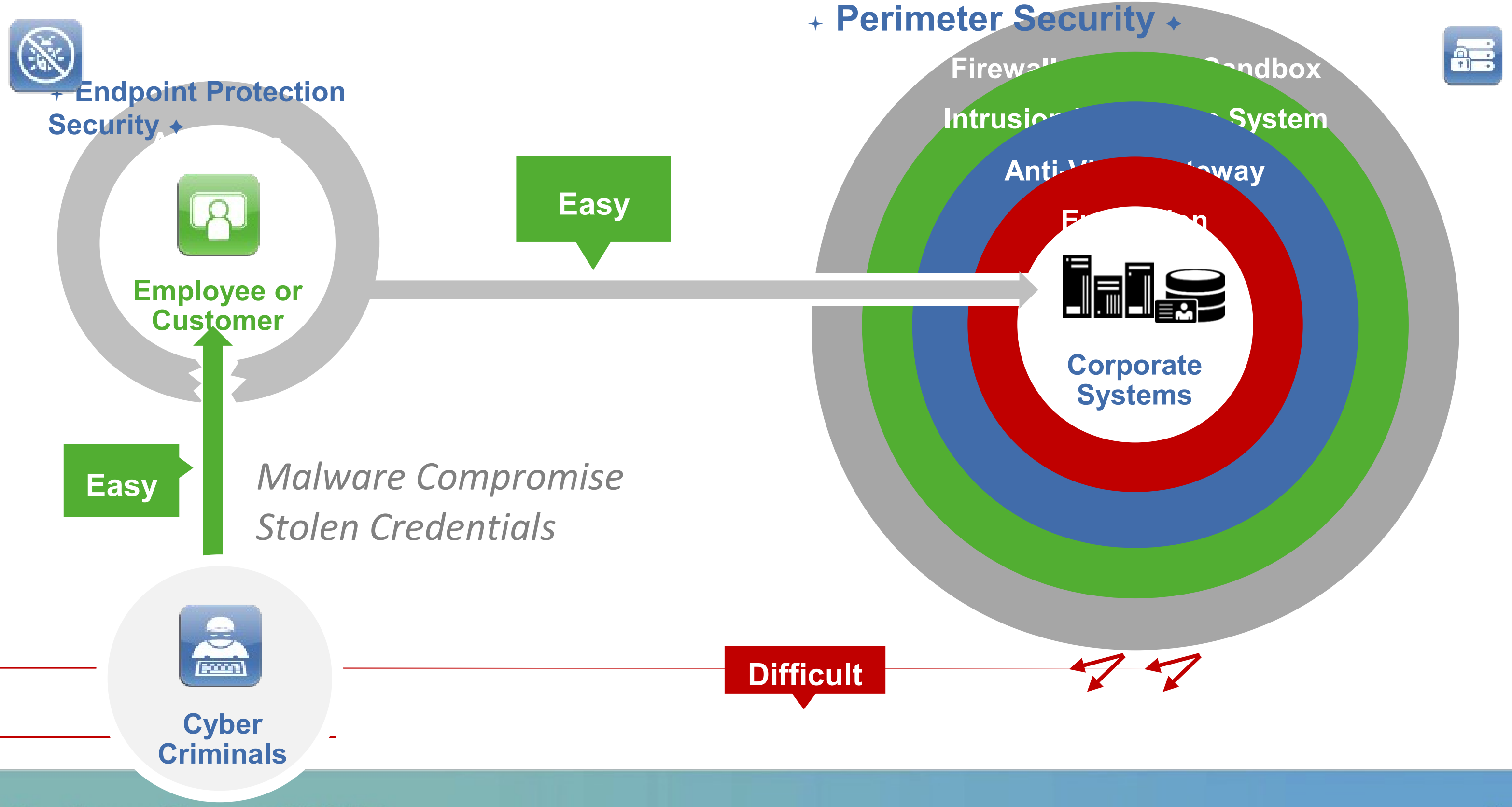
compromising individual online banking sessions with malware, the brazen Carbanak gang targeted banks' internal systems and operations, resulting in a multichannel robbery that averaged $8 million per bank.



Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.

Carbanak - The Path of Least Resistance



+ Perimeter Security +

Firewal andbox

Intrusio System

Anti-V teway

E n

Corporate Systems

+ Endpoint Protection Security +

Employee or Customer

Easy

Easy

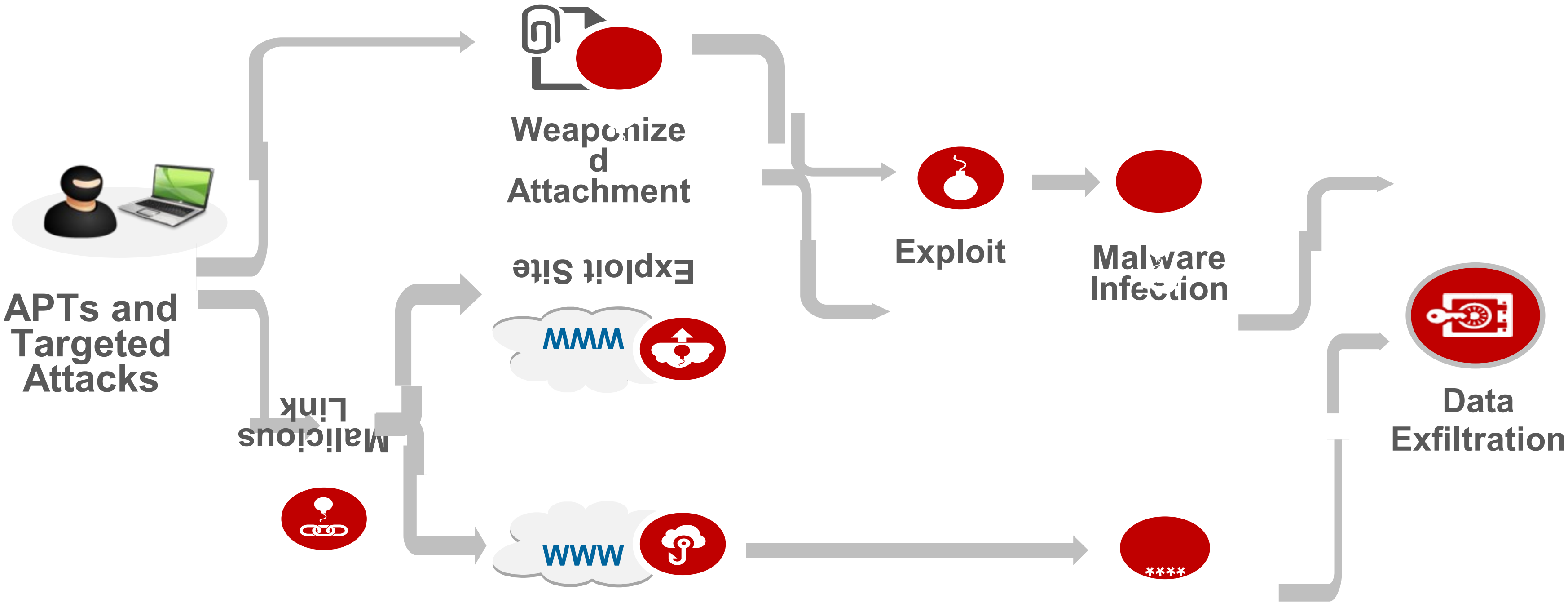
Malware Compromise

Stolen Credentials

Difficult

Cyber Criminals

How does Malware get on my devices?



APTs and Targeted Attacks

Weaponize
d
Attachment

Exploit Site

Malicious Link

Phishing Site

Exploit

Malware Infection

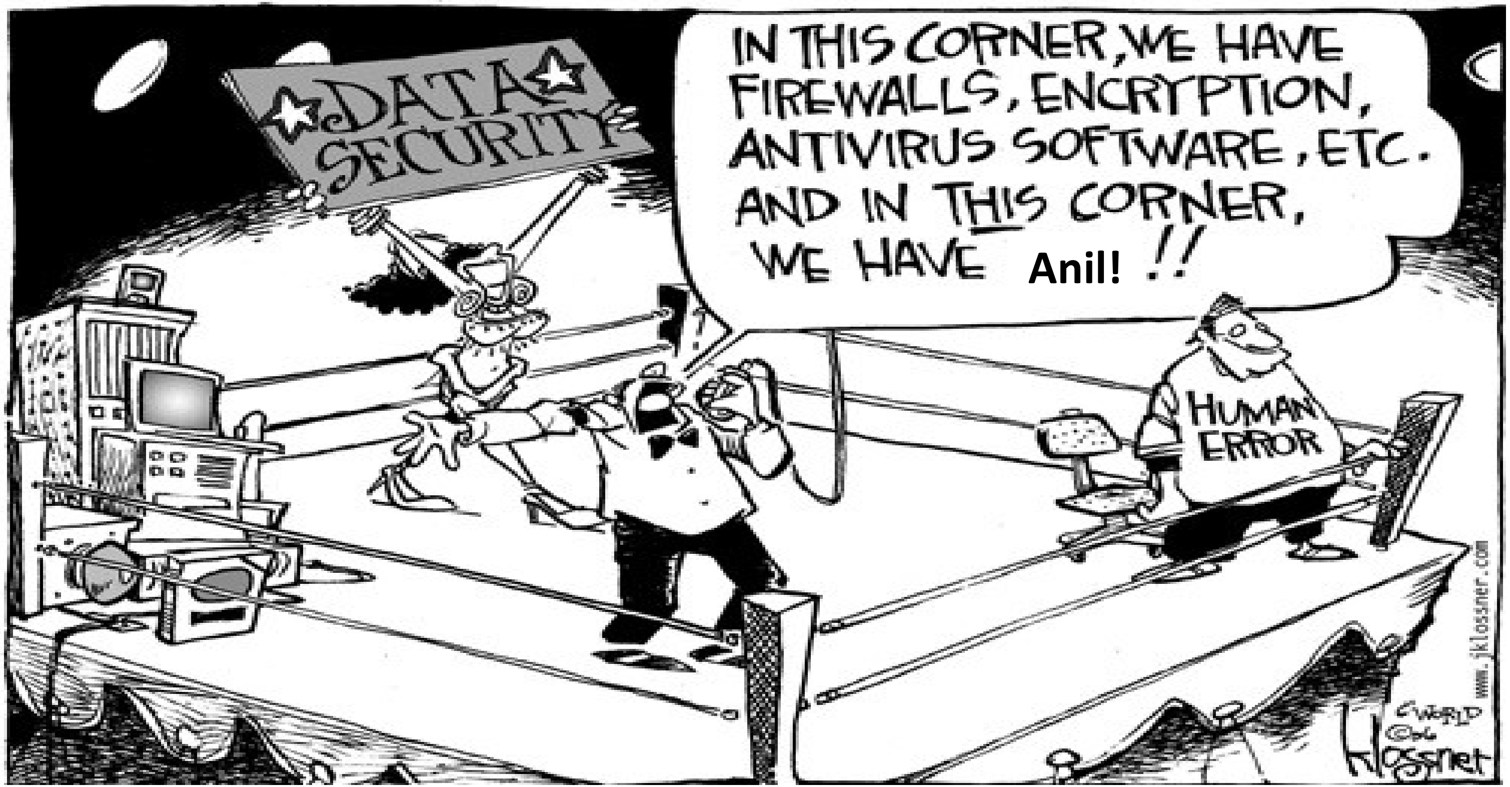
Credential Theft

Data Exfiltration

1:500 PCs infected with Advanced Evasive APT malware!

IBM Trusteer Research

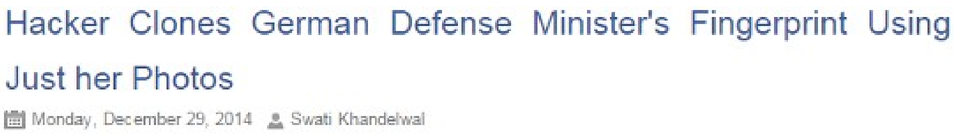
Users will alwavs make mistakes !


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE Anil! !!
HUMAN ERROR
www.jklossner.com
©WORLD ©06
Klossner

Defenses have always been and will always be bypassed

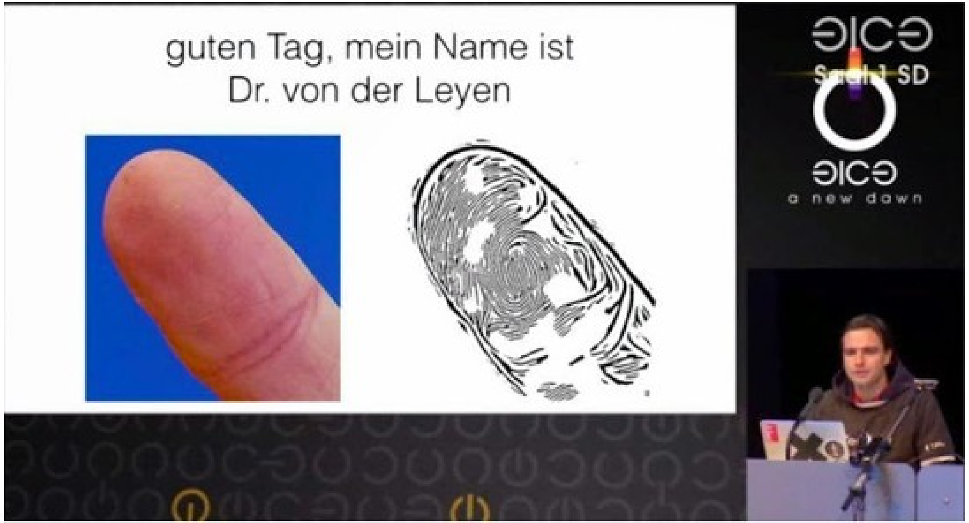
It can be easy to breach biometric authentication as shown in late 2014 by a Hacker

Whatever we use to protect our systems will eventually be attacked.



Hacker Clones German Defense Minister's Fingerprint Using Just her Photos

Monday, December 29, 2014 Swati Khandelwal

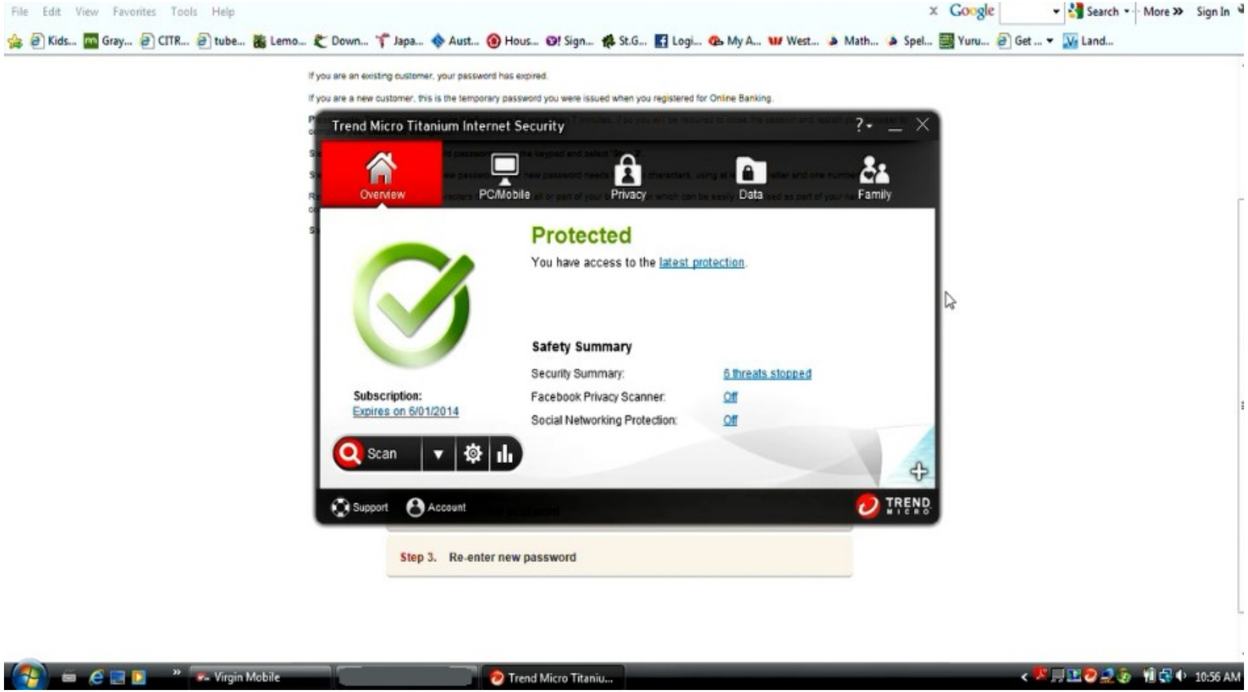


guten Tag, mein Name ist
Dr. von der Leyen

Can we really fight this ?

Advanced Malware DEFEATS

- Anti-Virus
- Multi-factor Authentication
- Sandbox Technologies
- Behavioral Anomaly engines
- Humans



If you are an existing customer, your password has expired.

If you are a new customer, this is the temporary password you were issued when you registered for Online Banking.

Trend Micro Titanium Internet Security

Protected

You have access to the latest protection.

Safety Summary

Security Summary: 6 threats stopped

Facebook Privacy Scanner: Off

Social Networking Protection: Off

Subscription:
Expires on 6/01/2014

Step 3. Re-enter new password

What can we do?

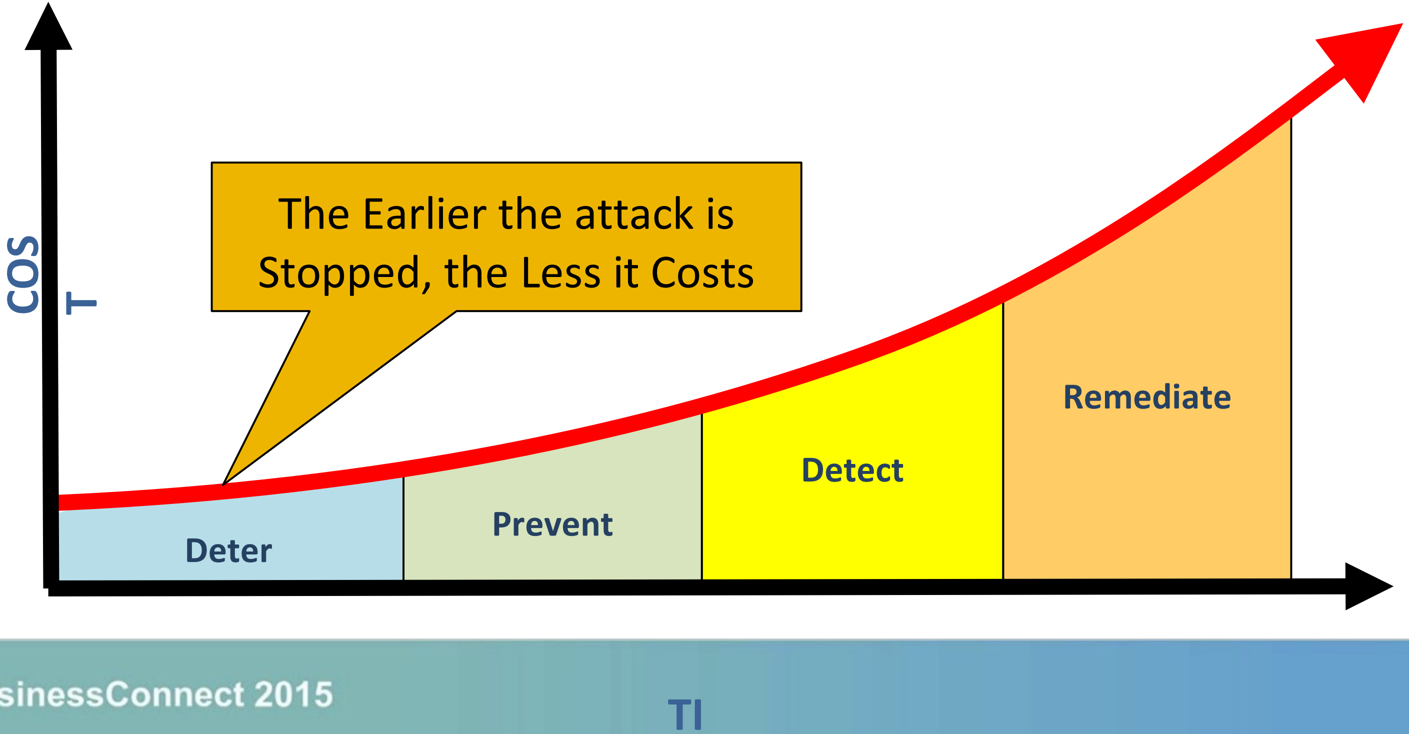
Be prepared

Take action

Know your Critical Business Assets

Why you need to act NOW!

"An ounce of prevention is worth a pound of cure."
Benjamin Franklin



IBM X-Force Threat Exchange …

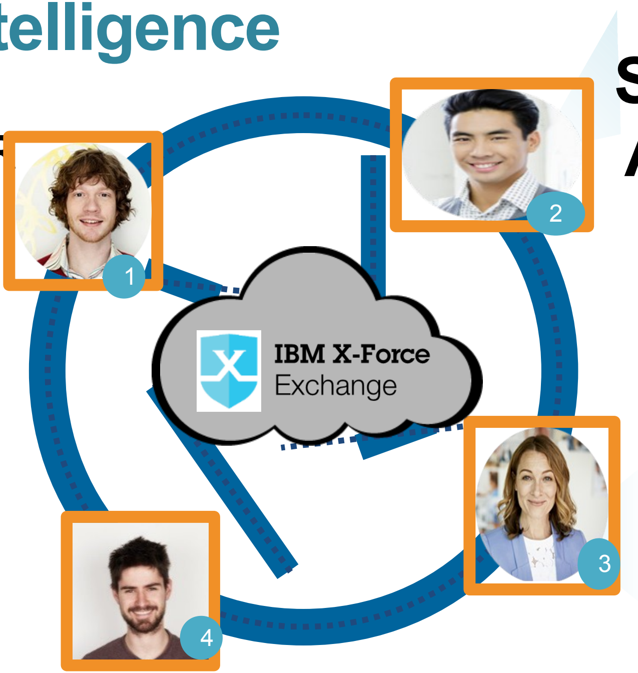
You are part of the

SOLUTION

IBM X Force Threat Exchange : A collaborative platform for sharing threat intelligence

Add context to threats via peer collaboration

- **<u>Connect</u>** with industry peers to validate findings
- **<u>Share</u>** a collection of Indicators of Compromise (IOCs) to aid in forensic investigations

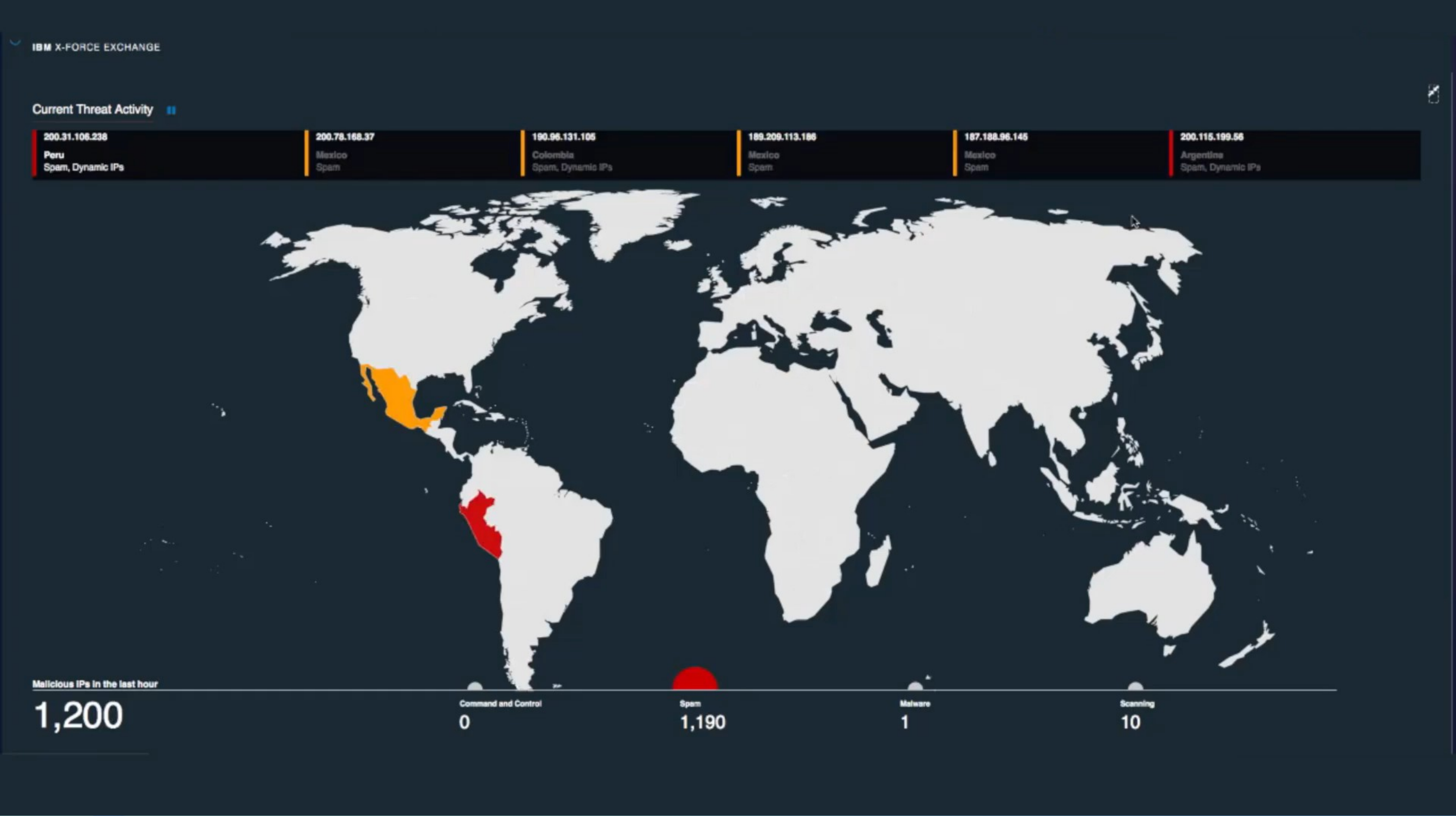


INCIDENT RESPONDER

SECURITY ANALYST

CISO

IBM X-FORCE



IBM X-FORCE EXCHANGE

Current Threat Activity

200.31.106.238
Peru
Spam, Dynamic IPs

200.78.168.37
Mexico
Spam

190.96.131.105
Colombia
Spam, Dynamic IPs

189.209.113.186
Mexico
Spam

187.188.96.145
Mexico
Spam

200.115.199.56
Argentina
Spam, Dynamic IPs

Malicious IPs in the last hour
1,200

Command and Control
0

Spam
1,190

Malware
1

Scanning
10

LEVEL THE PLAYING FIELD

With IBM threat research and X-Force Threat Exchange

Monitoring of more than…

23B web pages and images

83K vulnerabilities

8M spam and phishing attacks

860K malicious IP addresses

1,000 malware samples collected

xforce.ibmcloud.com

securityintelligence.com