Trends in Cyber Threats

Ann Marie Keim,
CISSP, CISA,CRISC
Annmarie.keim@nasa.gov

NASA
Kennedy Space Center

No target too big, no target too small, no sector immune

- Retail – from mega-online retailers(i.e. ebay) to Mom & Pop websites
- Medical/Pharmaceutical
- Banks/financial institutions
- Industry
- Government

Threats take MANY forms, so you need to understand what kind(s) you are likely to attract.

Where's your vulnerability?

- Your endpoints
- Your data center – servers (~68%)
- Your workstations/laptops (~32%)
- Your smartphone/blackberry
- Your VOIP phone(!)
- Your websites
- Your applications
- YOUR PEOPLE!




Some scary 2012 Stats

98% successful hacks involved external groups
58% involve activist groups
40% involved individuals – it's easier to buy and download automated attack tools (making hacks more repeatable.)
96% were not difficult to execute
41% of health care officials don't understand the impact of changes until AFTER implemented
75% security professionals believe hackers have the upper hand

*surveys from Black Hat and Cisco conferences, Verizon,privacyrights.org

More scary 2012 Stats

33 – against financial/insurance (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

66 – against retail/merchant (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

55 – against educational institutions (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

58 – against government (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

132 – against medical (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

9 – against nonprofits (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

Disclosed, **hack**ed, **card** fraud, **in**siders, **phys**ical loss, **port**able device, stationary device, **unkn**own.

*privacyrights.org

Byzantine Candor (Comment group) hacks

2012 – major effort amongst multiple IT Security organizations, monitoring hacking groups in China.

Calling cards known as 'comments' left in web code.

Highly organized, coordinated effort – linked to China's military.

Attacks stretch back to 2002. more than 1000 organizations. (FireEye Inc) Petabytes taken.

Byzantine Candor cont.

Many organizations affected and ID'd as part of 'Operation Shady Rat'.

1. Wiley Rein Law firm – one of the highest profile internat'l trade law firms. Handled a series of unfair trade cases against China that resulted in tariffs equaling $3B [1]

What was stolen? Entire email system & any attached documents

Hackers encrypted & compressed as they stole to make any forensics harder to identify.

(1) Riley, M. & Lawrence,D. (2012). Hackers linked to China's Army. Retrieved from bloomberg.com/news/

Byzantine Candor cont.

Many organizations affected and ID'd as part of 'Operation Shady Rat'.

More here

Byzantine Candor cont.

Common traits:

They work fast! One log file traced from user computers in Canada, to the Immigration and Refugee board to key figure in that org to exfiltration of the data....5 hours.

They are clever! They consolidate, filter, zip, encrypt and cover their tracks.

They leave backdoors! If one is found, you can safely assume there are others. Up to 6 have been found.

No one is immune! Diversity in clients from Fortune 500 Co, IT security firms to lawn sprinkler co in Oklahoma.

Oak Ridge Labs - Oh those crazy users!

So what happened? By the numbers....

530 received the spear phishing email
57 opened it
3 successfully installed it.

The result?
Multiple servers compromised,
GBs of data extracted,
Labs offline for 3 weeks.

Note: the malware was configured to remove all traces if installation was not successful! Anti-forensics and obfuscation in action.

A shift to *DIFFERENT* targets

2010 and earlier
Credit card numbers

2011 Hackers now prefer
USER CREDENTIALS

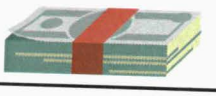
The latest? A shift to smaller targets

Boston restaurant group Briar

A small target … fewer defenses, easier pickings

DEFAULT userid/passwords on point of sale
Employees shared same userid/password
No secured wireless or remote access
Continued to accept payments AFTER the malware was discovered.

The company admitted no wrongdoing. Cheaper for them than litigation. Their defense? We're not IT – we're restauranteurs!



Why smaller targets?

- Typically fewer defenses
- Longer to discover a breach - avg is 6 months (Note: in large and defense orgs, avg is weeks)
- Limited to no logging for forensics - they can't help if they want to!
- No intrusion detection or prevention
- Systems run out-of-the-box - default settings, default credentials
- No one in charge of security
- The easiest to infiltrate… and use as a BOT to help get to YOUR NETWORK.

How much are YOU worth?* Prices for programs in the underground

DDOS attack: $100 a day

Standard crimeware toolkit: $100 to $1,000

Single bot (purchased in bulk): 3 CENTS

Botnet with up to 10,000 bots for rent: $200 an hour

* Sources: Kaspersky Lab, Symantec, Trend Micro

How much are YOU worth?* Prices for data in the underground

Utility bill, scanned: $10

Full identity: $6 – $80

Gmail username and password: $80

Facebook (userID and password) : $300

Passport, scanned: $20 FREE with an RFID scanner!

Driver's license, scanned:$20

Bank-account credentials: $15 to $850

Credit card with $1,000 available: $25
Credit card with personal information: $80

Economies of Scale

Hackers have been able to create:

STANDARDIZED
AUTOMATED
REPEATABLE

attacks against REPEAT targets!

Can YOU say the same thing for YOUR IT Security practices?

What do you have to protect?

Money? Online Presence?

Intellectual property? Contracts? Inventions?

Technology?

Medical records (and insurance information)?

A few words about users

- 60% will insert a found thumbdrive into their desktop/laptop
- 90% if it has a company logo on it!
- More than 50% will give up their passwords in exchange for a token gift!
- 90% share password across accounts
- 41% share passwords with others
- 14% have never changed their banking password

Source: Webroot, Trend, McAfee

Assessments & Auditing

92% breaches discovered by a 3rd party!

Any number of tools are available, (some free)

- STAT (Security Threat Avoidance Technology)
  Scanner by Harris Corp. http://www.statonline.com/index.asp
- Nessus Security Scanner http://www.nessus.org/
- Retina by eEye (http://www.eeye.com/)

You can't fix what you can't see!
'That which is measured, is improved.'

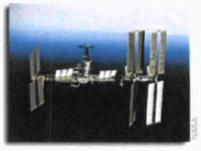
Vulnerabilities vs Remedies

- Identify main vulnerabilities
  - Endpoints (web, perimeter, remote access)
  - Servers (applications)
  - Users
- COUNTER WITH:
  - Secure configurations & monitoring
  - Patching & VERIFICATION
  - Maintaining a baseline configuration - change mgmt!
  - Account management (user accounts not business accounts)
  - User awareness training!! (again and again)

"Automating a bad process just leads to getting bad results more quickly."

Is there NOWHERE SAFE?

Kennedy Space Center



2008 - - - NASA Discovers Computer Virus Aboard the International Space Station

Source: NASA.GOV

Hacked!

Kennedy Space Center

2011 - NASA, Stanford Hacked by Software Scammers

source: Fox News

A CISO's Bad Day

Kennedy Space Center

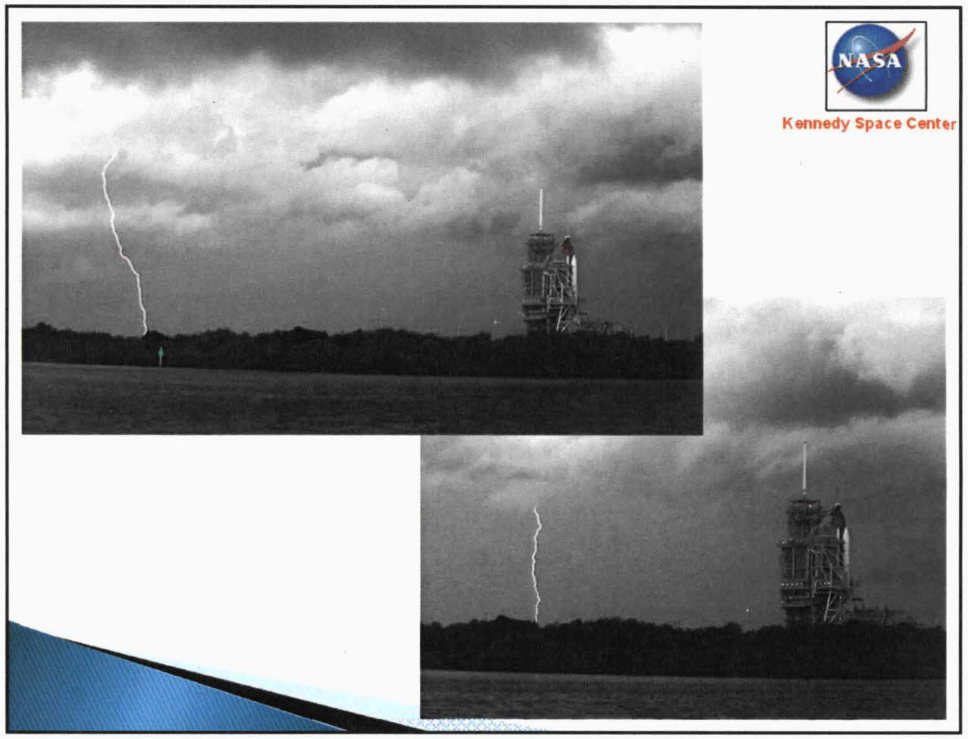
"NASA computer hacked, satellite data accessed "

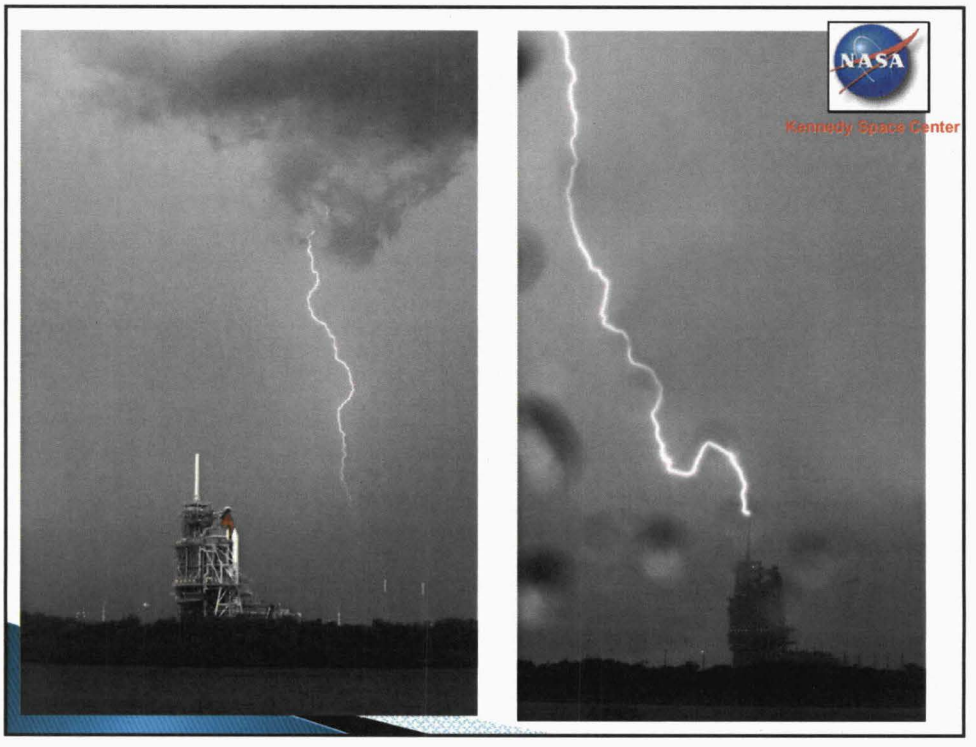
Romanian claims responsibility; space agency says 'necessary steps taken'

Goddard Space Flight Center May 2011

The hacker, who calls himself TinKode, took to Twitter shortly before noon May 17 to boast of his feat.

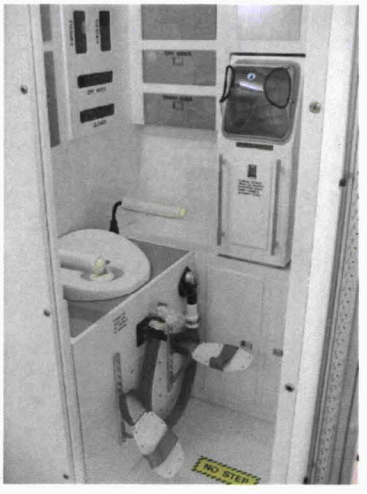
Source: MSNBC




NASA
Kennedy Space Center


NASA
Kennedy Space Center

What are people MOST interested in?



Kennedy Space Center

Defense in Depth @ KSC