New Trends in Cyber Threats, Recognizing and Fighting Persistent Threats

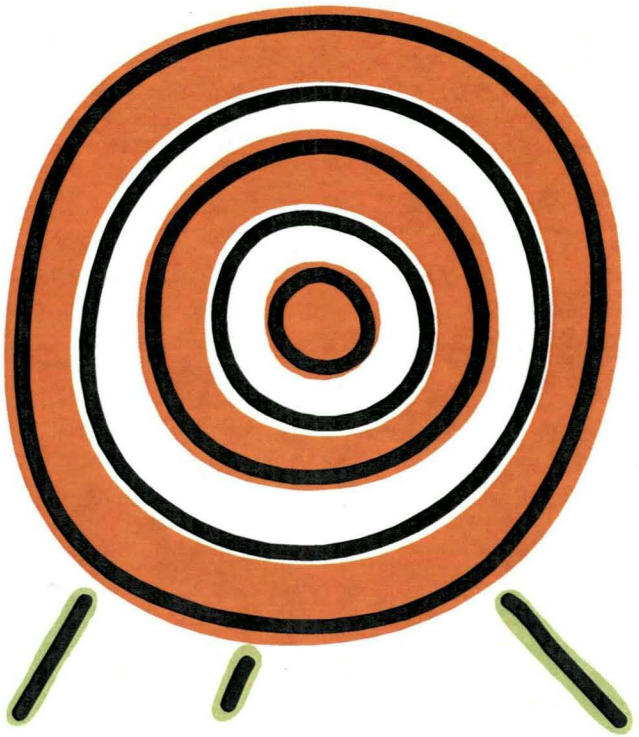
Ann Marie Keim,
CISSP, CISA,CRISC
Annmarie.keim@nasa.gov

Kennedy Space Center

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

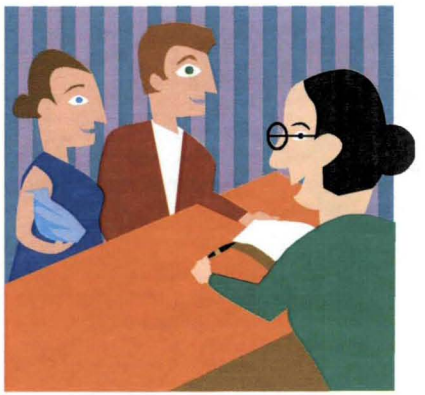
- Retail – from mega-online retailers(i.e. ebay) to Mom & Pop websites
- Medical/Pharmaceutical
- Banks/financial institutions
- Industry
- Government

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
- Your workstations/laptops
- Your smartphone/blackberry
- Your VOIP phone(!)
- Your websites
- Your applications
- YOUR PEOPLE!



Some scary 2011 Stats

58% successful hacks involved groups

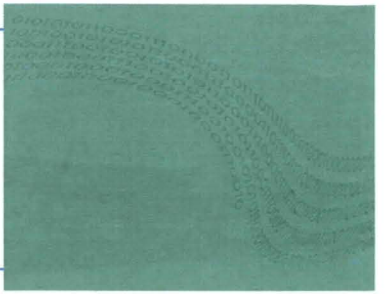
40% involved individuals - it's easier to buy automated attack tools (making hacks more repeatable)

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, privacyrights.org

More scary 2011 Stats



42 - against financial/insurance (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

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

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

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

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

6 - against nonprofits (DISC, HACK, CARD, INSD, PHYS, PORT, STAT, UNKN)

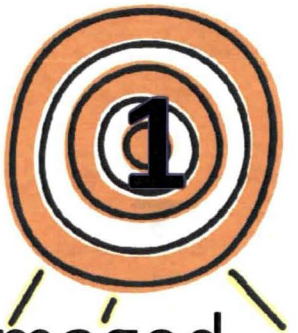
Disclosed**, hack**ed, **card** fraud, **ins**iders, **phys**ical loss, **port**able device, **stat**ionary device, **unkn**own.

*privacyrights.org

Geohot vs Sony April 2011

George Hotz, known as 'Geohot' hacked Sony PS3 and posted the jailbreaks online.

Sony answered by filing a lawsuit, citing Digital Millennium Copyright Act (DCMA) and Computer Fraud and Abuse Act.

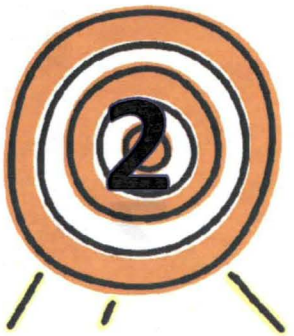


The result? MILLIONS in losses($171), damaged reputation, customer backlash, stock prices in the gutter.

HB GARY vs. Anonymous

Aaron Barr, CEO of an IT security firm HBGary, boasts he can name the scoundrels who comprise Anonymous, responsible for bringing carnage to MC/ VISA/ Paypal in the wake of Wikileaks case, and he will NAME NAMES!

He became?



HBGary vs Anonymous

So what happened?

Servers broken into, emails published, including evidence of criminal activity, website defaced and databases destroyed.

Bonus round: second site of owner Greg Hoglund taken offline and registered user accounts published.

How? The nitty gritty

A webserver with a common SQL injection vulnerability(patch available- unpatched)

A custom Content Management System (little support)

using MD5 hashes... badly (easily cracked)

Easy passwords & repeat passwords! CEO and COO - Just 6 digits, all lowercase, and 2 numbers, same passwords across multiple systems.

Nitty gritty 2

Elevated privileges via unpatched linux

Hackers free to deface website, grab data, dump emails.

Socially engineered admin to open firewall and reset password.

BOTTOM LINE? Best practice is not always standard practice! Standard advice is GOOD advice!

A shift to *DIFFERENT* targets

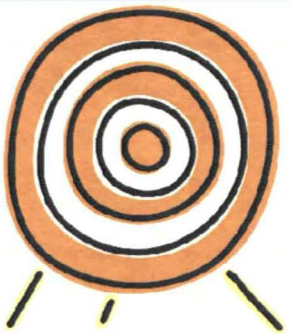
2010 and earlier

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

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!

Result? $110,000 fine and a list of actions to take.

Why smaller targets?

- Typically fewer defenses
- Longer to discover a breach – avg is 6 months
- 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
- Nearly 89% NOT in compliance with PCI/DSS at time of breach.

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

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

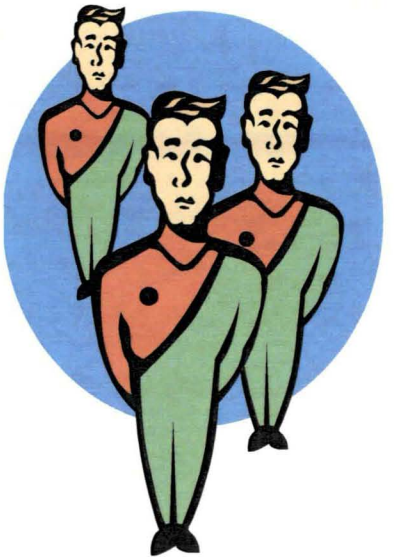
* Sources: Kaspersky Lab, Symantec, Trend Micro

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!

Vulnerability Assessments

If you don't have in-house expertise, HIRE IT.

Any number of tools available, (some free)

- STAT (Security Threat Avoidance Technology) Scanner by Harris Corp. http://www.statonline.com/index.asp
- Internet Scanner by ISS Internet Security Systems http://www.iss.net
- Nessus Security Scanner http://www.nessus.org/

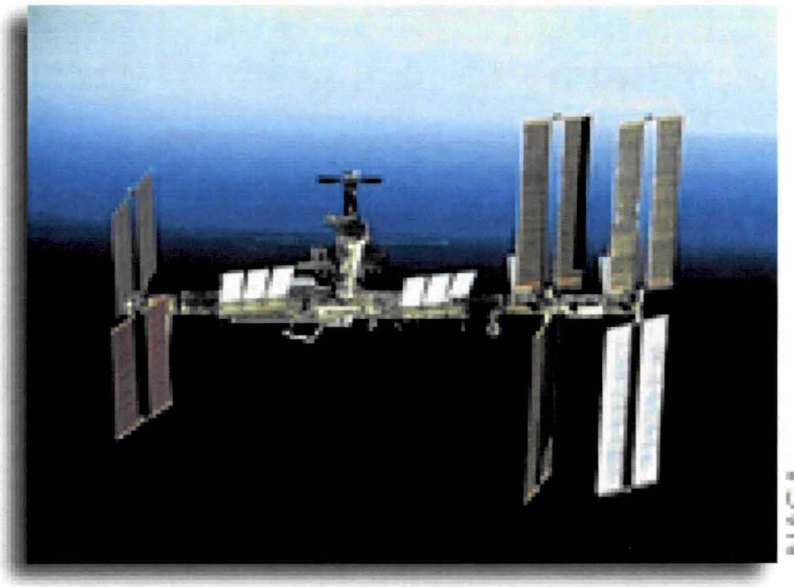
You can't fix what you can't see!

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
  - Account management (user accounts not business accounts)
  - User awareness training!! (again and again)

Is there NOWHERE SAFE?

Kennedy Space Center



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

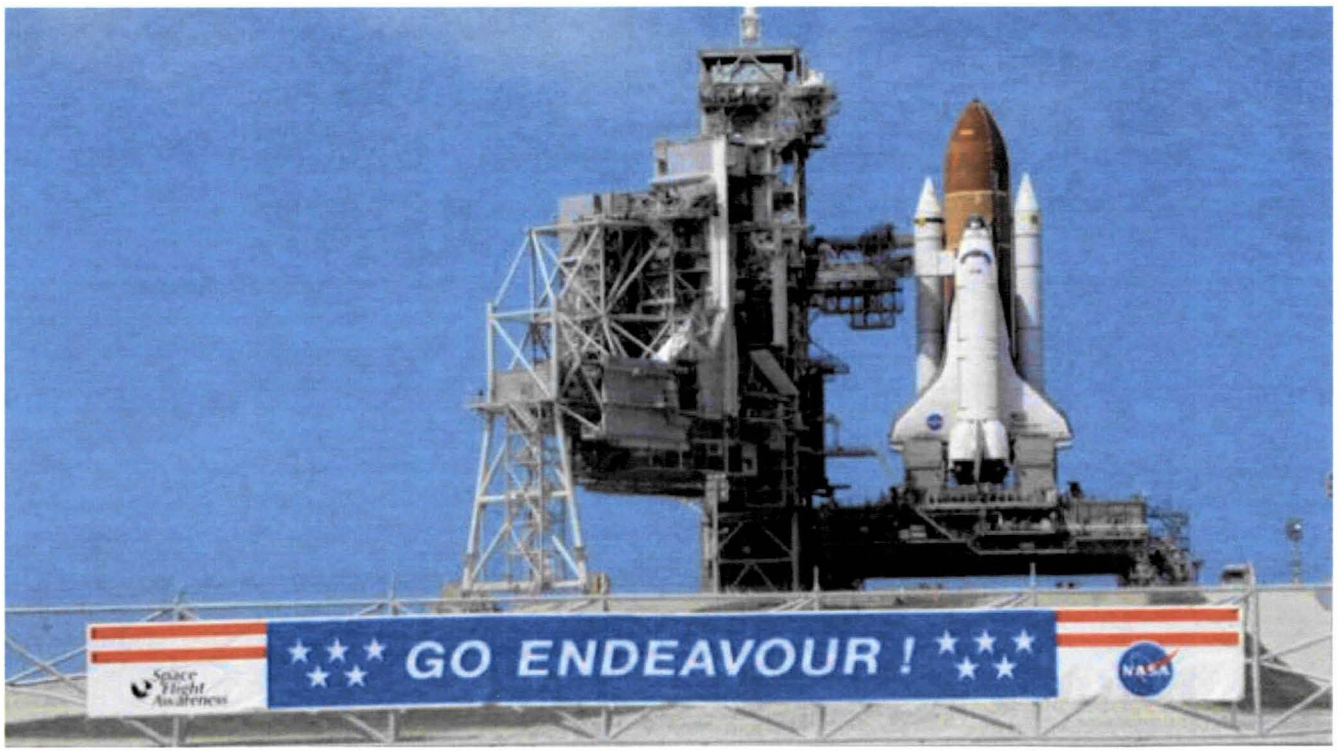
Source: NASA.GOV

Hacked!

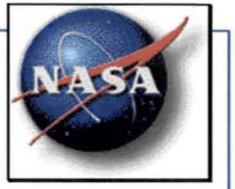
Kennedy Space Center

2011 - NASA, Stanford Hacked by Software Scammers

source: Fox News



A CISO's Bad Day



Kennedy Space Center

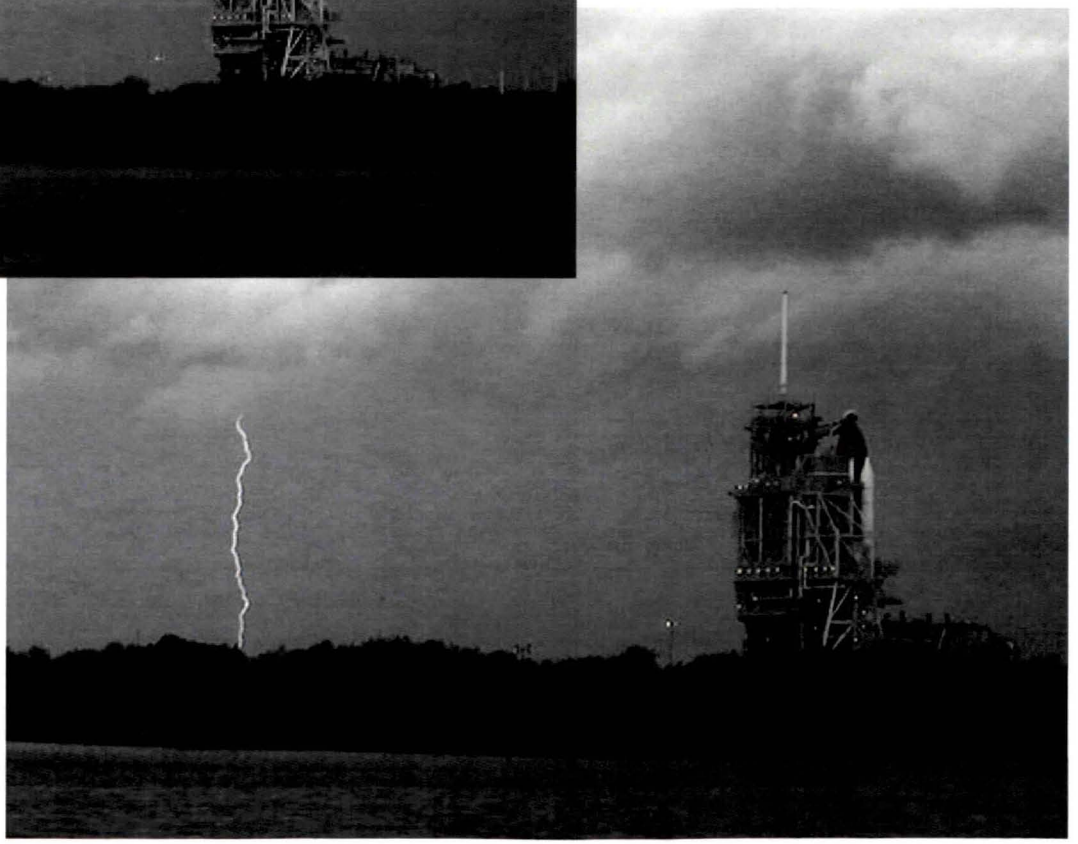
"NASA computer hacked, satellite data accessed "

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

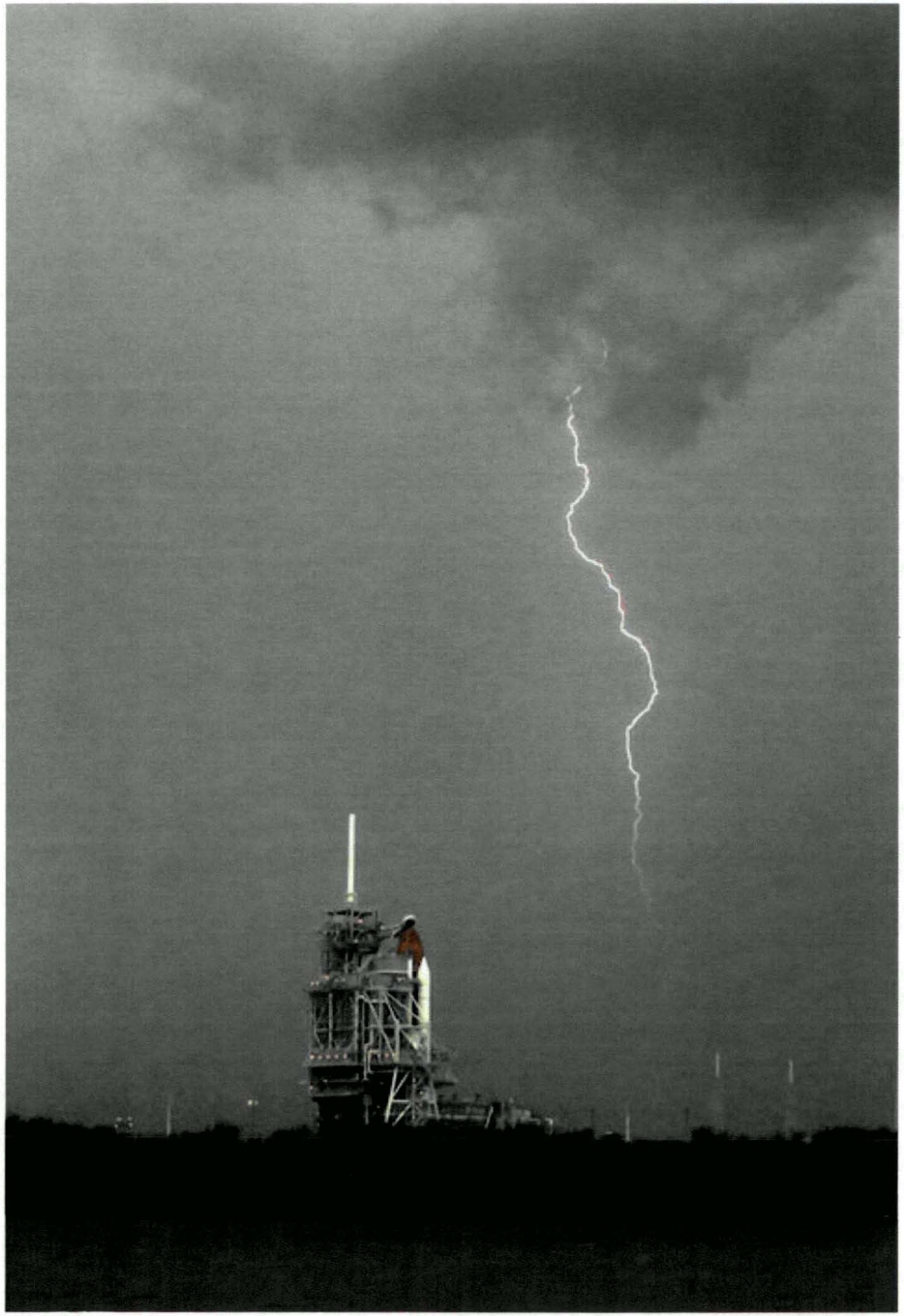
Goddard Space Flight Center May 2011

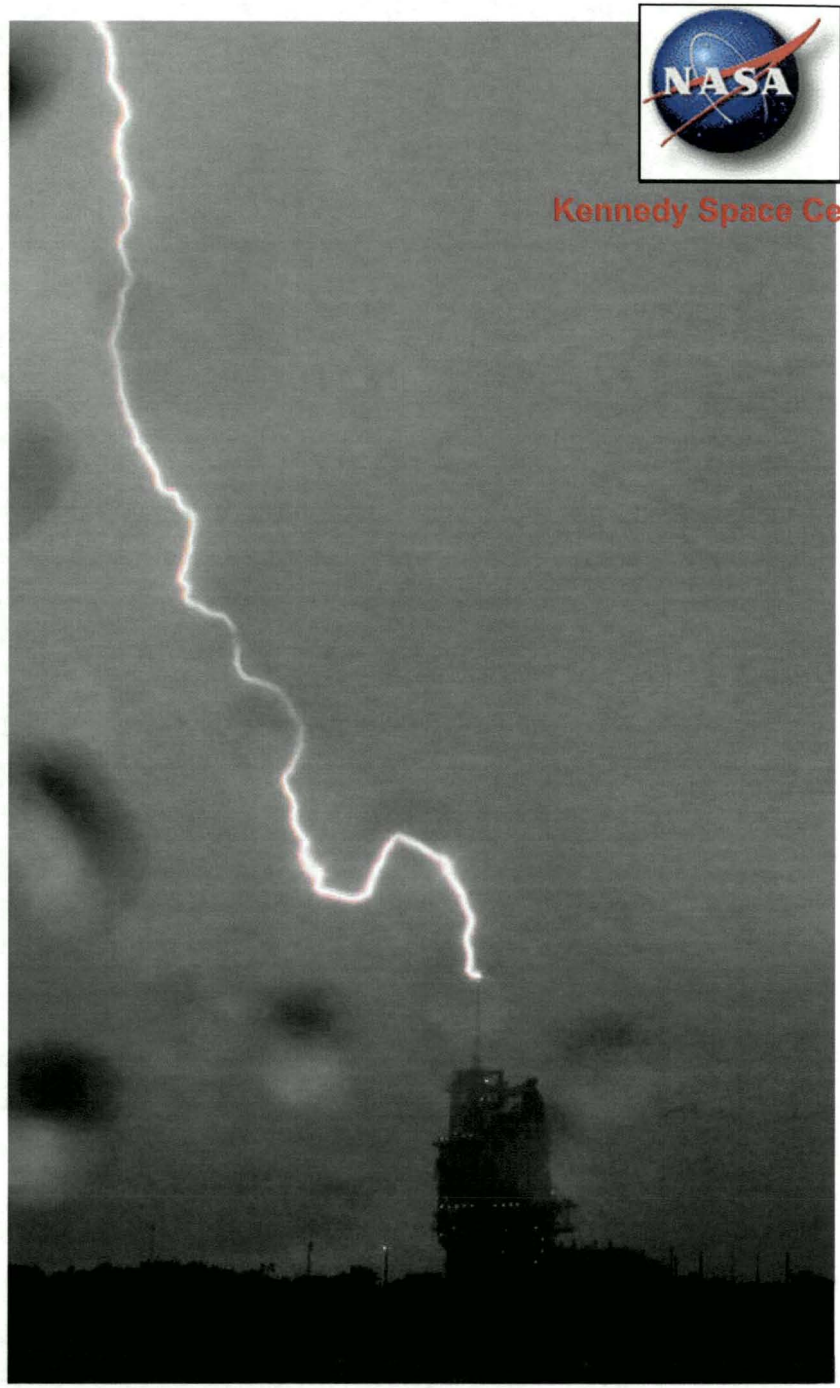
The hacker, who calls himself TinKode, took to Twitter shortly before noon May 17 to boast of his feat.

Source: MSNBC



Kennedy Space Center





Kennedy Space Center

Kennedy Space Center

Kennedy Space Center


Defense in Depth @ KSC