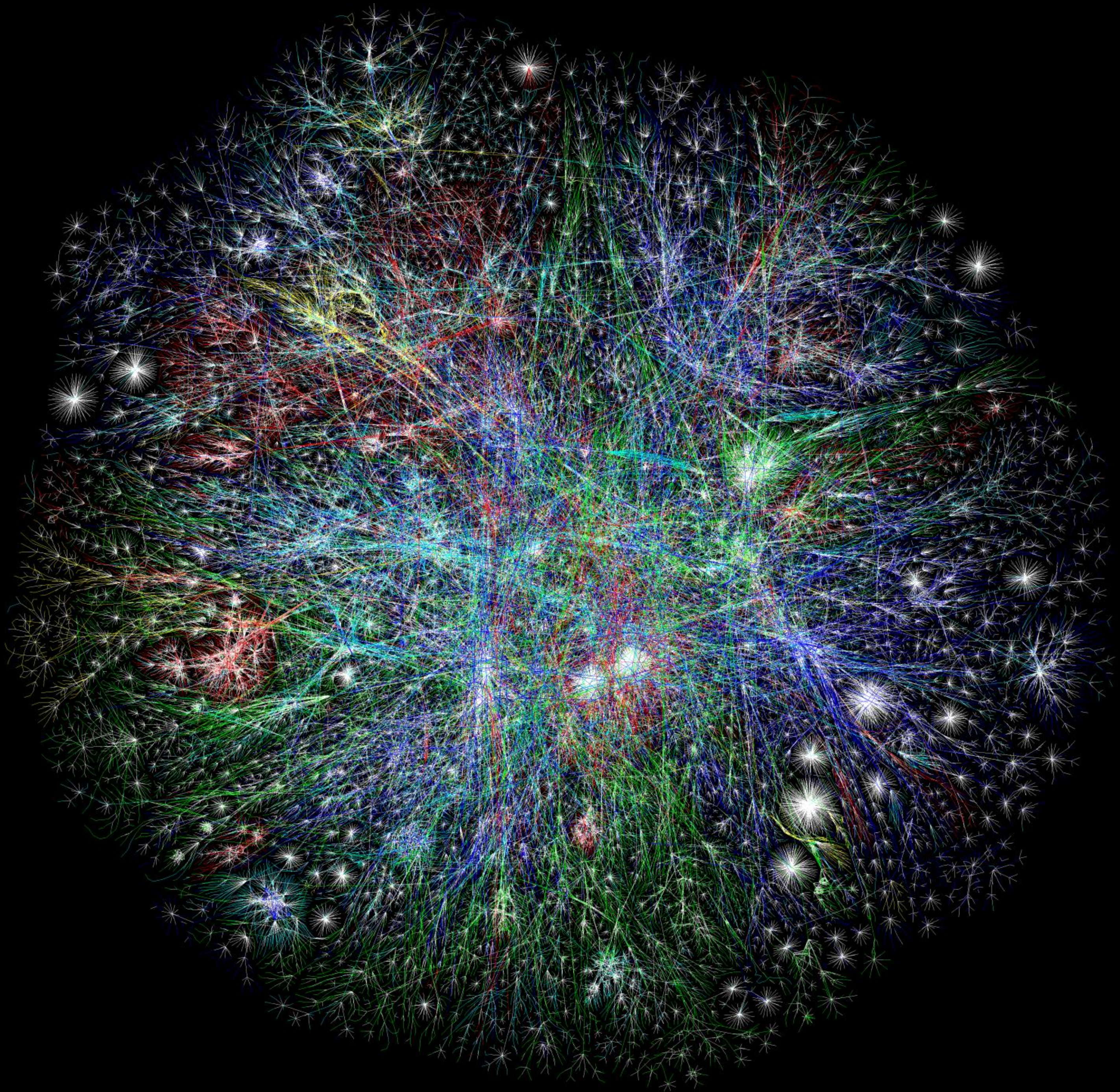
Securing Court Information

October is National Cyber Security Awareness Month!

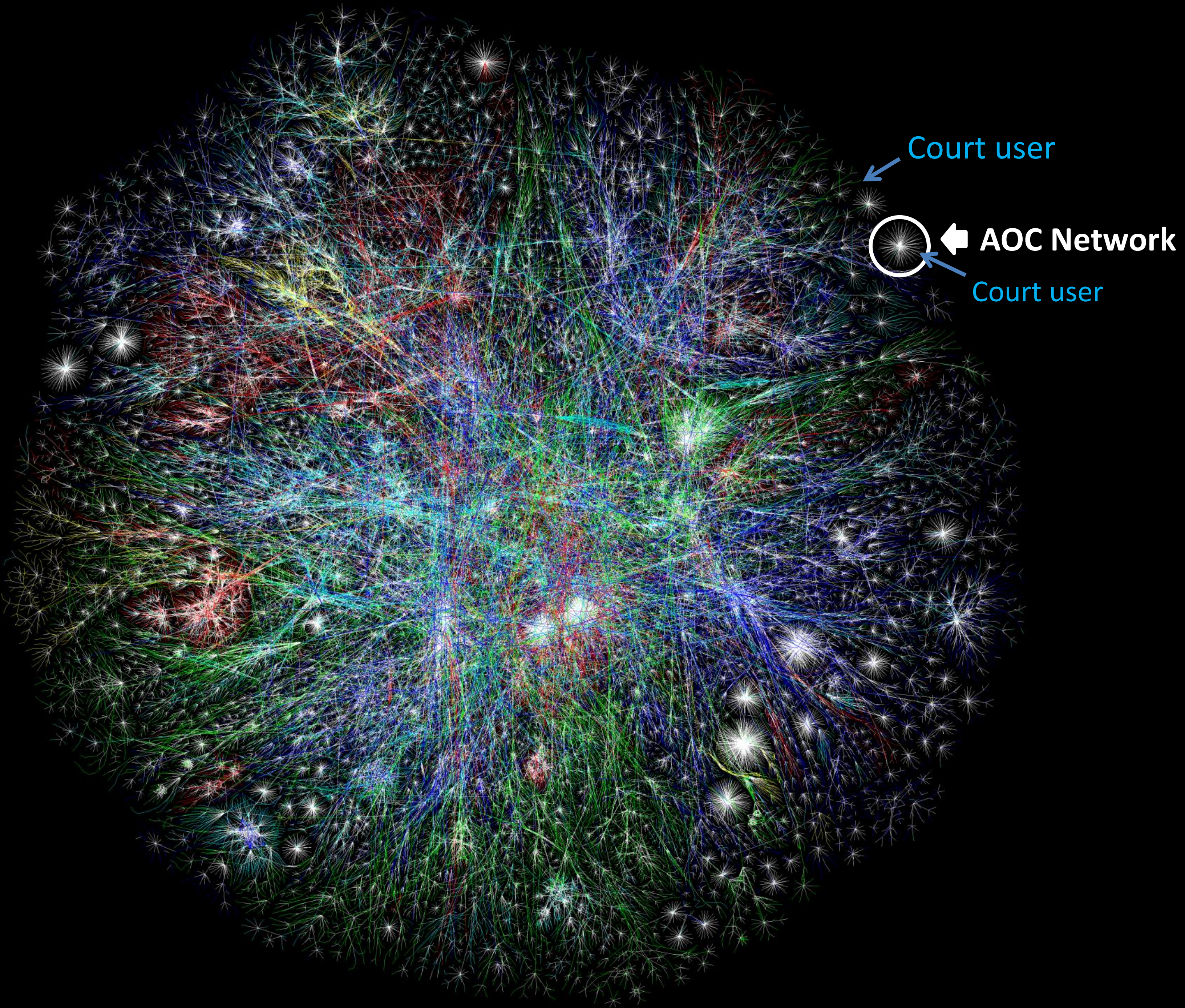
- 11th Annual
- Sponsored by the Department of Homeland Security

- How it all works
  - Computers 101
  - Hackers
  - Court Data
- Justice Building Network
  - Attacks
  - Resources
  - Defense In Depth
- Threats to Court Data
- What Can You Do?
  - Antivirus
  - Software Updates
  - Phishing
  - Passwords



Computers 101

- A computer is a machine that follows instructions
- These instructions are the software created by programmers


Court user
AOC Network
Court user

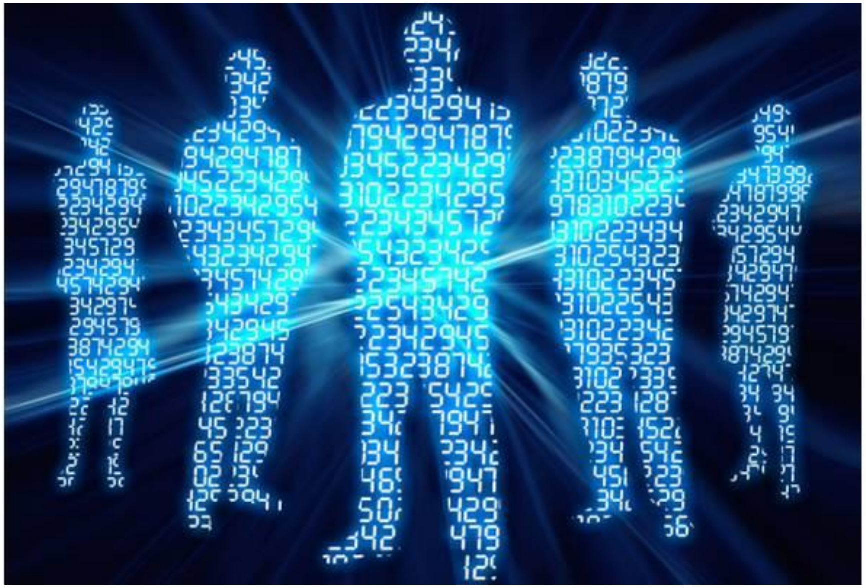
Definitions

- Hackers vs Attackers
- Malware

Hackers

- Script Kiddies
- Knowledgeable Users
- At the highest level, hackers are computer programmers and hacking is a business!
- They are smart, they do this for a living, and they just need to make other people's computers follow their instructions.

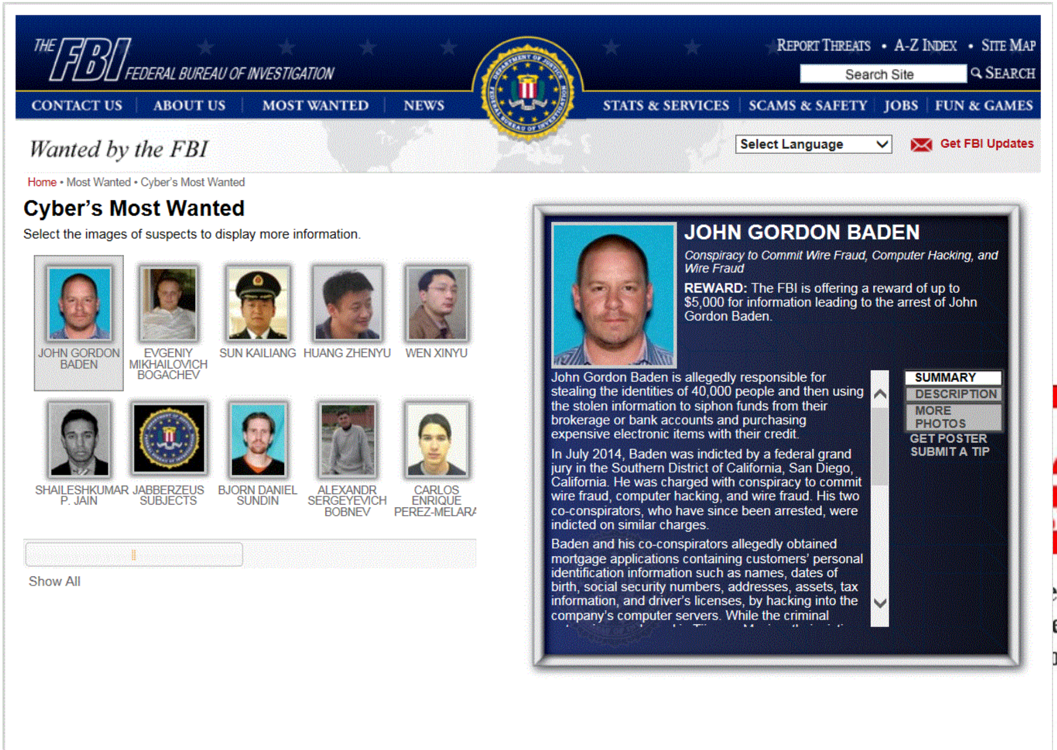
  - Organized Crime
  - Political Players (countries, hactivists)
  - Malicious



Kristoffer Von Hassel

Cyber's Most Wanted List

- 26 Individuals
  - 1 American
  - 5 Chinese military
  - Most of the rest are Russian



Cyber's Most Wanted

Select the images of suspects to display more information.

JOHN GORDON BADEN

Conspiracy to Commit Wire Fraud, Computer Hacking, and Wire Fraud

REWARD: The FBI is offering a reward of up to $5,000 for information leading to the arrest of John Gordon Baden.

John Gordon Baden is allegedly responsible for stealing the identities of 40,000 people and then using the stolen information to siphon funds from their brokerage or bank accounts and purchasing expensive electronic items with their credit.

In July 2014, Baden was indicted by a federal grand jury in the Southern District of California, San Diego, California. He was charged with conspiracy to commit wire fraud, computer hacking, and wire fraud. His two co-conspirators, who have since been arrested, were indicted on similar charges.

Baden and his co-conspirators allegedly obtained mortgage applications containing customers' personal identification information such as names, dates of birth, social security numbers, addresses, assets, tax information, and driver's licenses, by hacking into the company's computer servers. While the criminal

SUMMARY
DESCRIPTION
MORE PHOTOS
GET POSTER
SUBMIT A TIP

ANTED

Y THE FBI

r Fraud; Accessing a Computer Without Authorization for the Purpose e and Private Financial Gain; Damaging Computers Through the ommands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

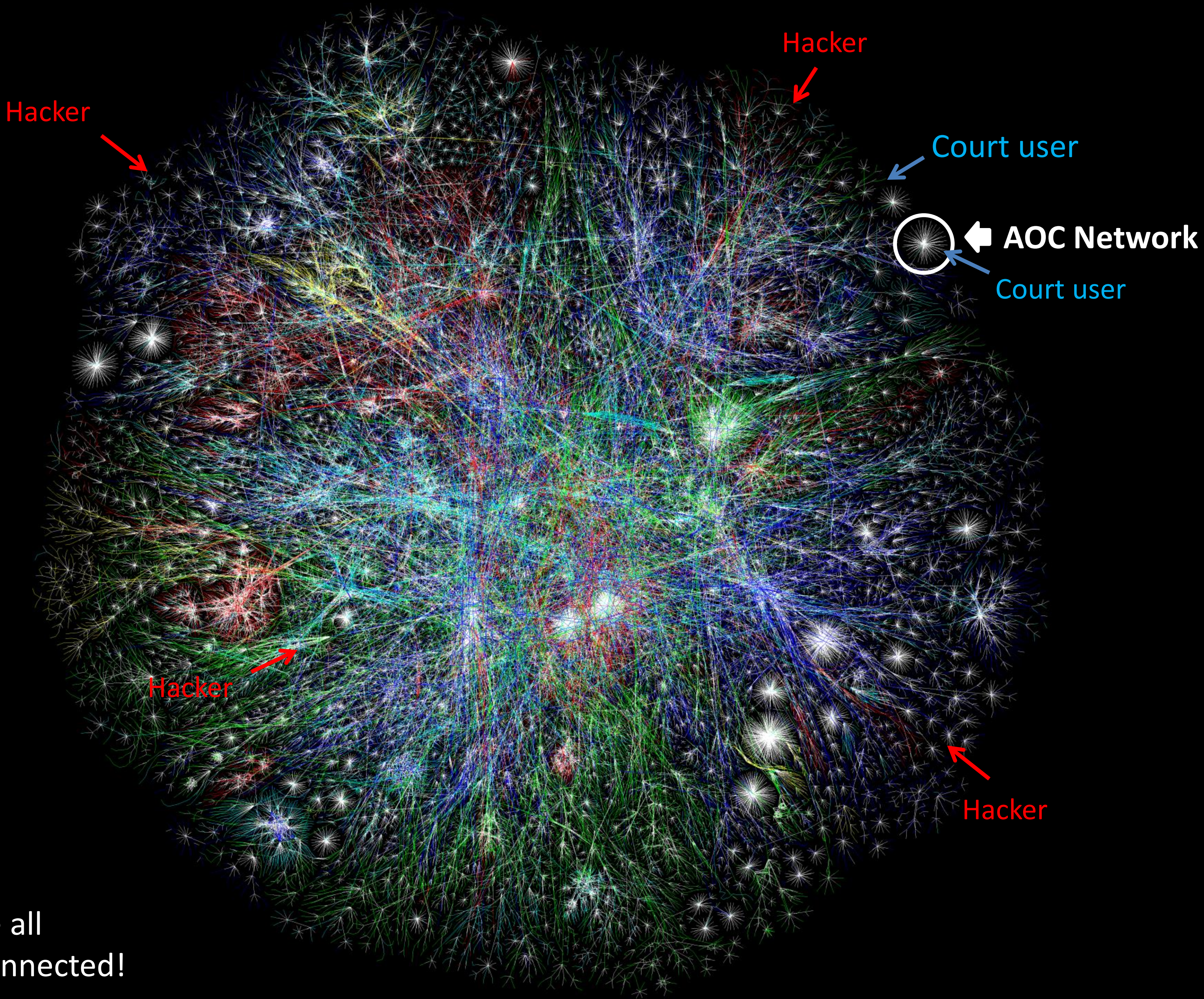
Huang Zhenyu

Wen Xinyu

Sun Kailiang

Gu Chunhui

Wang Dong



We are all
interconnected!

What does the court have of value?

- AOC Network
  - Personal info - court databases and web pages, network files
    - DL, SS#, email addresses, etc.
  - Financial info - court databases and web pages, network files
- Court Users
  - Personal info
    - DL, SS#, email addresses, etc.
  - Financial info
  - Access to court databases

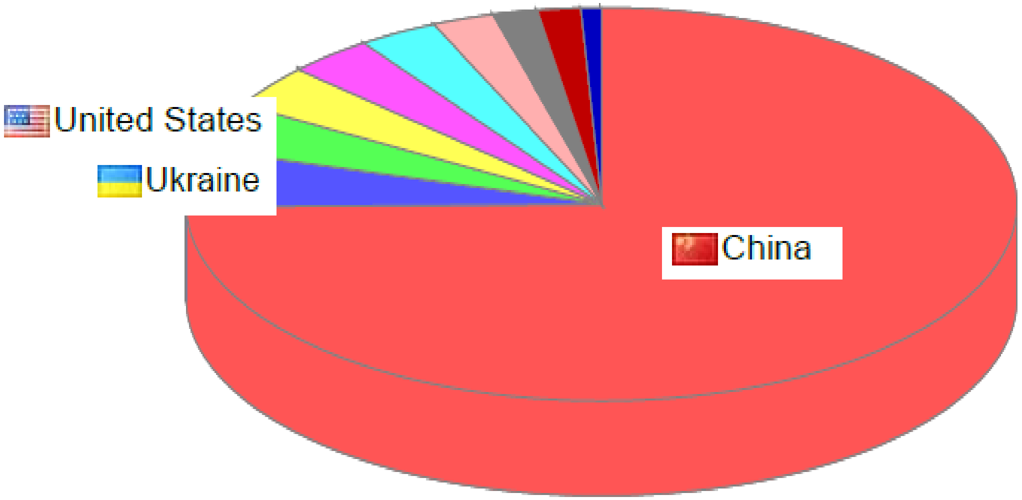
Attacks on Justice Building Network

• October Blocked Attacks	30,590
• 2014 Total Blocked Attacks	**470,665**

Blocked Attacks – Top 10 Countries

China	73%
Ukraine	5%
United States	4%
Israel	3%
Korea, Republic of	3%
Argentina	3%
Taiwan	2%
Brazil	2%
Chile	2%
France	1%

(Other 2%)



Resources within Justice Building Network

- Contexte Database
- IMIS Database
- Jury Database
- Laserfiche
- Web Servers
- User Workstations

AOC Defenses for Resources/Court Data

- Physical security of server room
- IPS
- Firewalls
- Data Backups
- Disaster Recovery
- Controlled access to databases
- Security level access within databases

Defense In Depth

Layers of protection to slow attacks and speed recovery

Physical security
IPS/IDS
Firewalls
Passwords
Policy
Antivirus
Software updates
Etc.

YOU are one of the most important defenses!

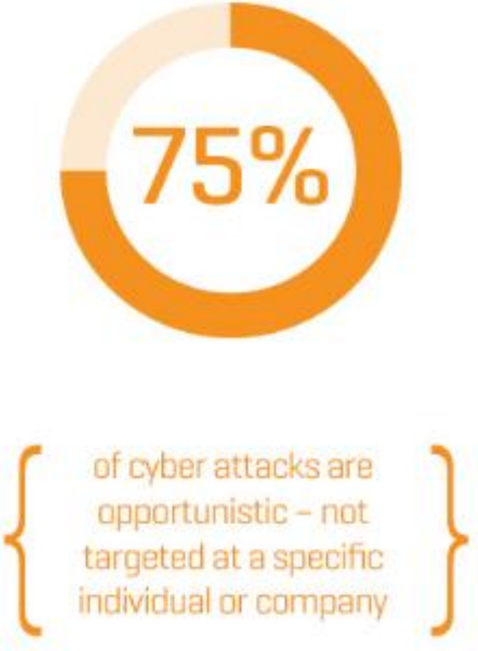
Threats

- Social Engineering – Phishing
- Breaching Systems – Software Updates, Antivirus, Weak Passwords

- Intercepting Data – Not generally your concern, https
- Disruption
- Hactivism – case outcomes

*Jan 24, 2014 – uscourts.gov hacked?
e-filing affected

Keep in mind….



{ of cyber attacks are opportunistic – not targeted at a specific individual or company }

….there doesn't even need to be a reason.

Target Breach

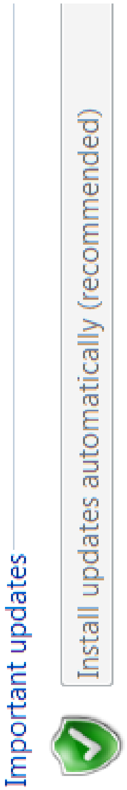
- Started with a phishing email to contractor with about 125 employees
- 40 million cards stolen
- 70 million personal information records stolen (name, address, email, and phone number)

What can you do to protect court data?

- Antivirus*
- Software Updates*
- Phishing
- Passwords

Updating Antivirus and Software

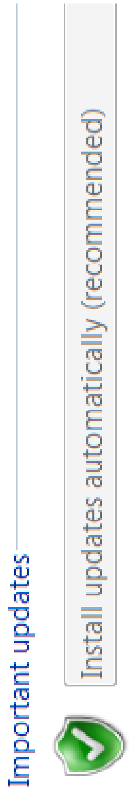
- Justice Building Network
  - AOC CIS
- Courts with IT support
  - IT Staff
- Courts without IT support
  - ?



Important updates

Install updates automatically (recommended)

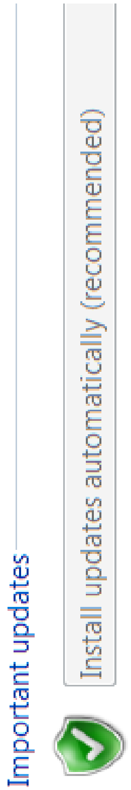
Definitions



Important updates

Install updates automatically (recommended)

- Antivirus software blocks <u>known</u> malware.
  - Symantec, McAfee, AVG, Kaspersky, etc.
- Software Updates (Patches) fix flaws in programming, including security flaws
  - Microsoft Windows, Internet Explorer, Google Chrome (twice), Firefox, Java, Adobe Flash Player… have all had critical security patches released in October



Important updates

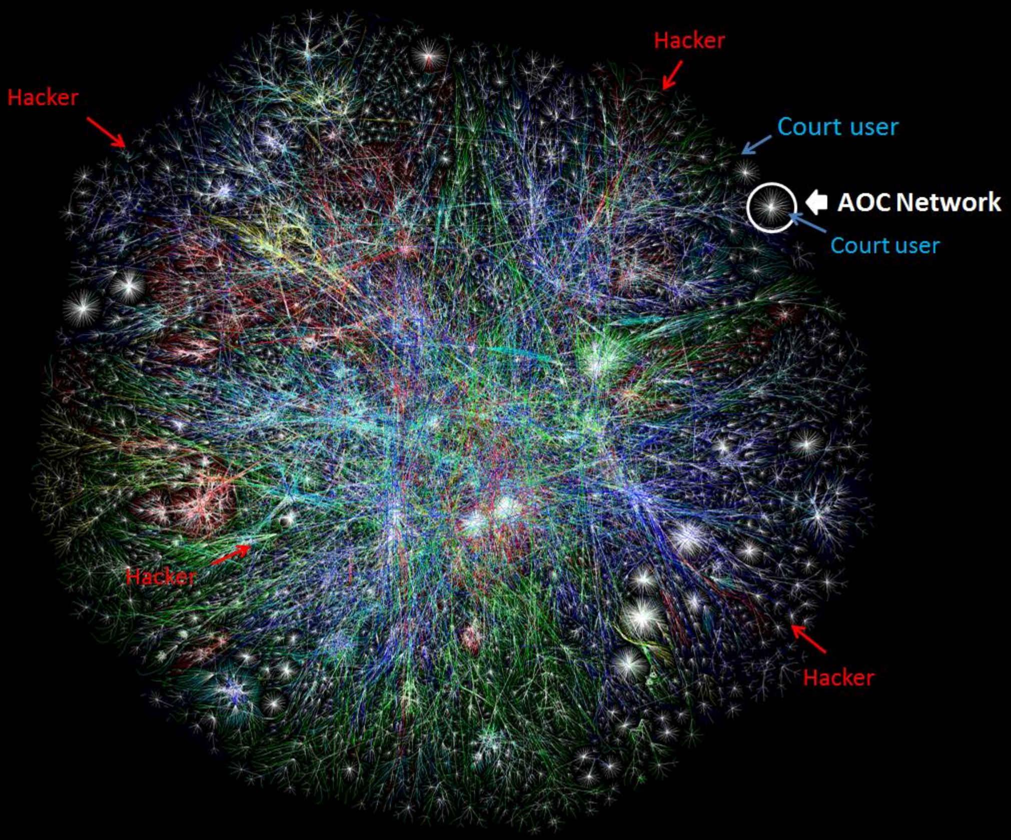
Install updates automatically (recommended)

90% of successful exploits are made against unpatched computers!

Antivirus and patched software work hand-in-hand.

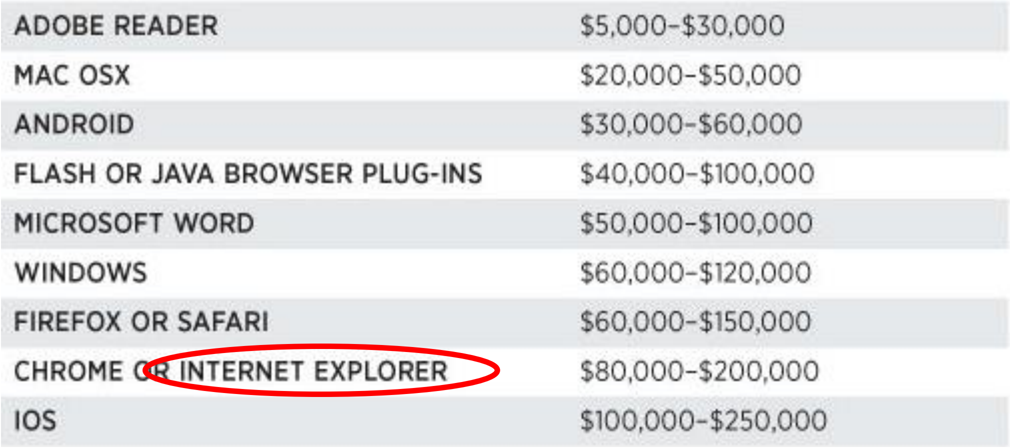
Internet Explorer

Vulnerability X



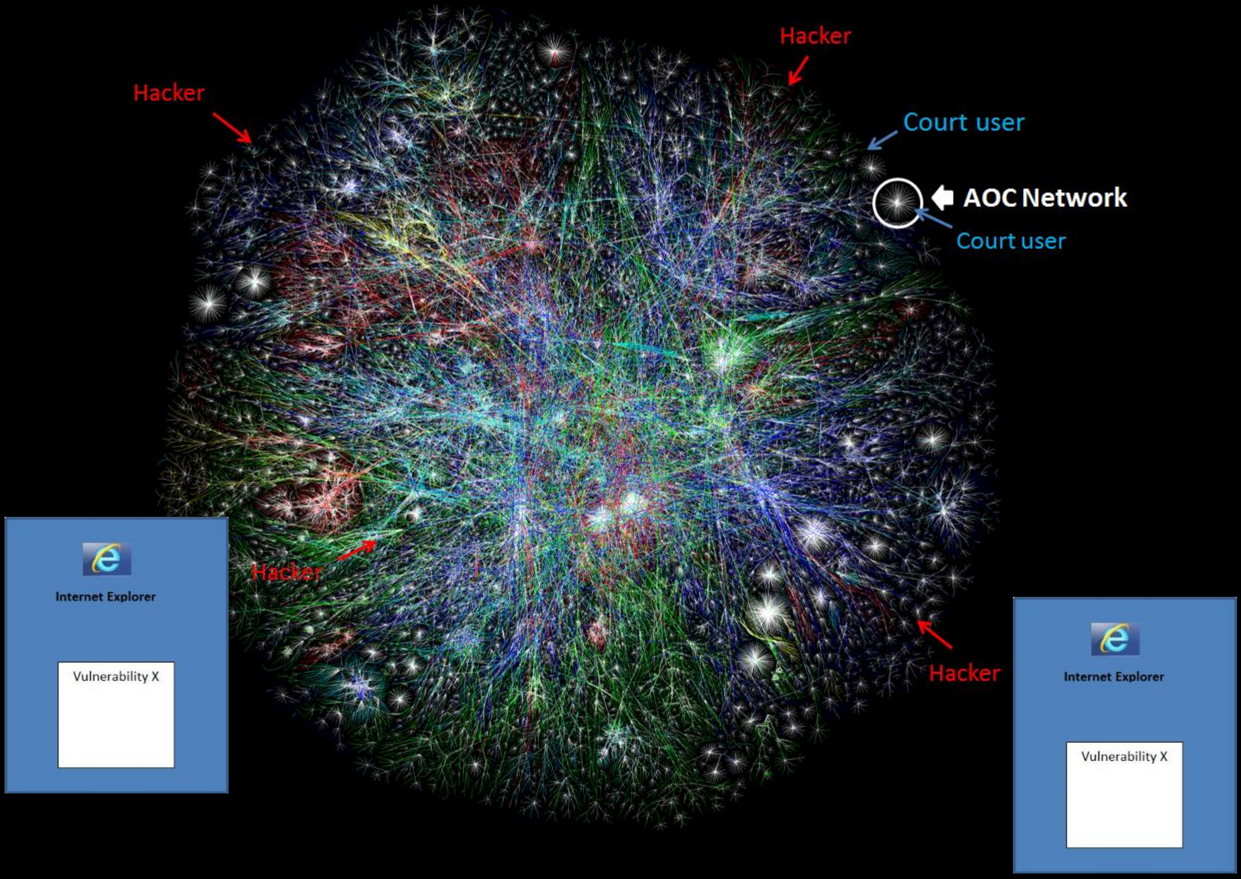
Zero-Day Market

Rough market value assembled by Forbes reporter in 2012:

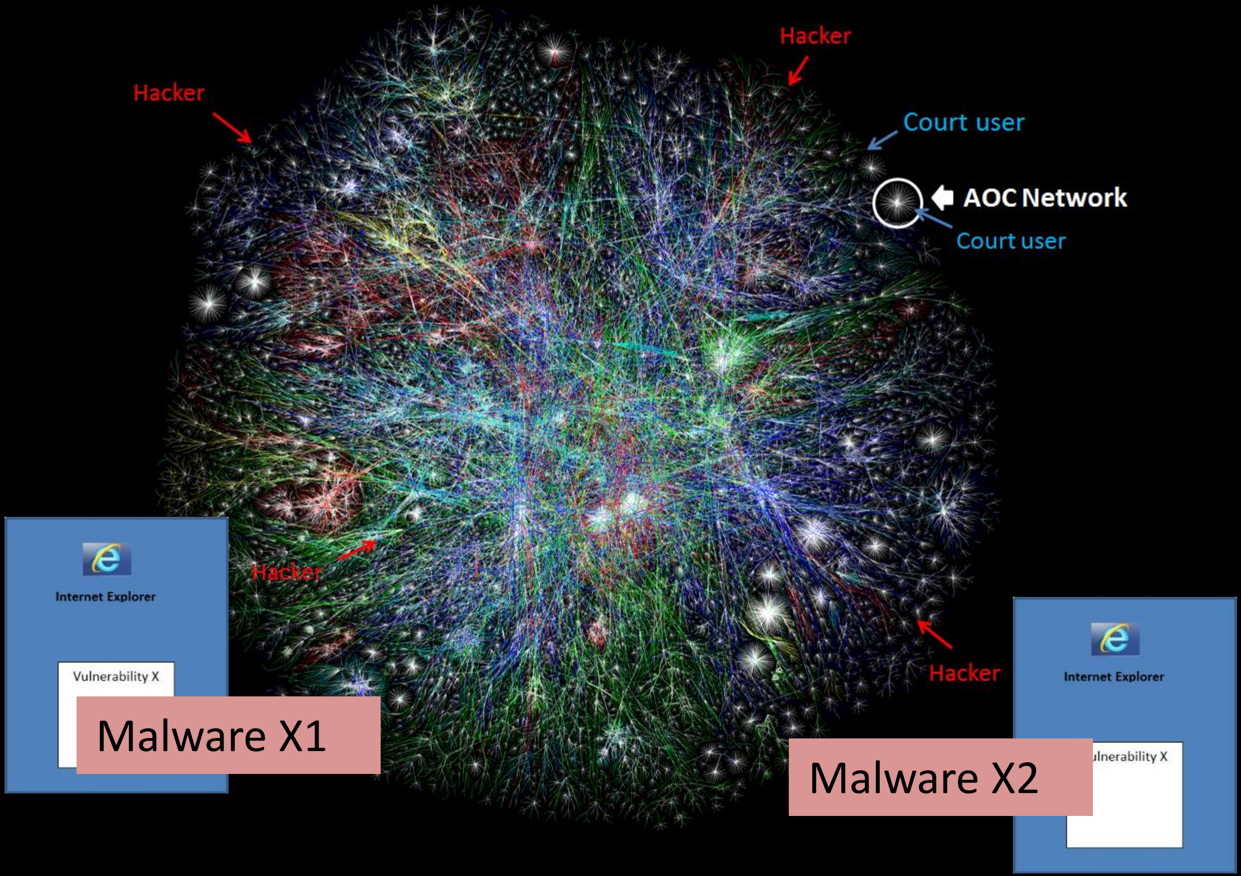


ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

*from Forbes.com, March 2012



Hacker
Hacker
Court user
AOC Network
Court user
Internet Explorer
Vulnerability X
Hacker
Hacker
Internet Explorer
Vulnerability X



Hacker

Hacker

Court user

AOC Network

Court user

Internet Explorer

Vulnerability X

Malware X1

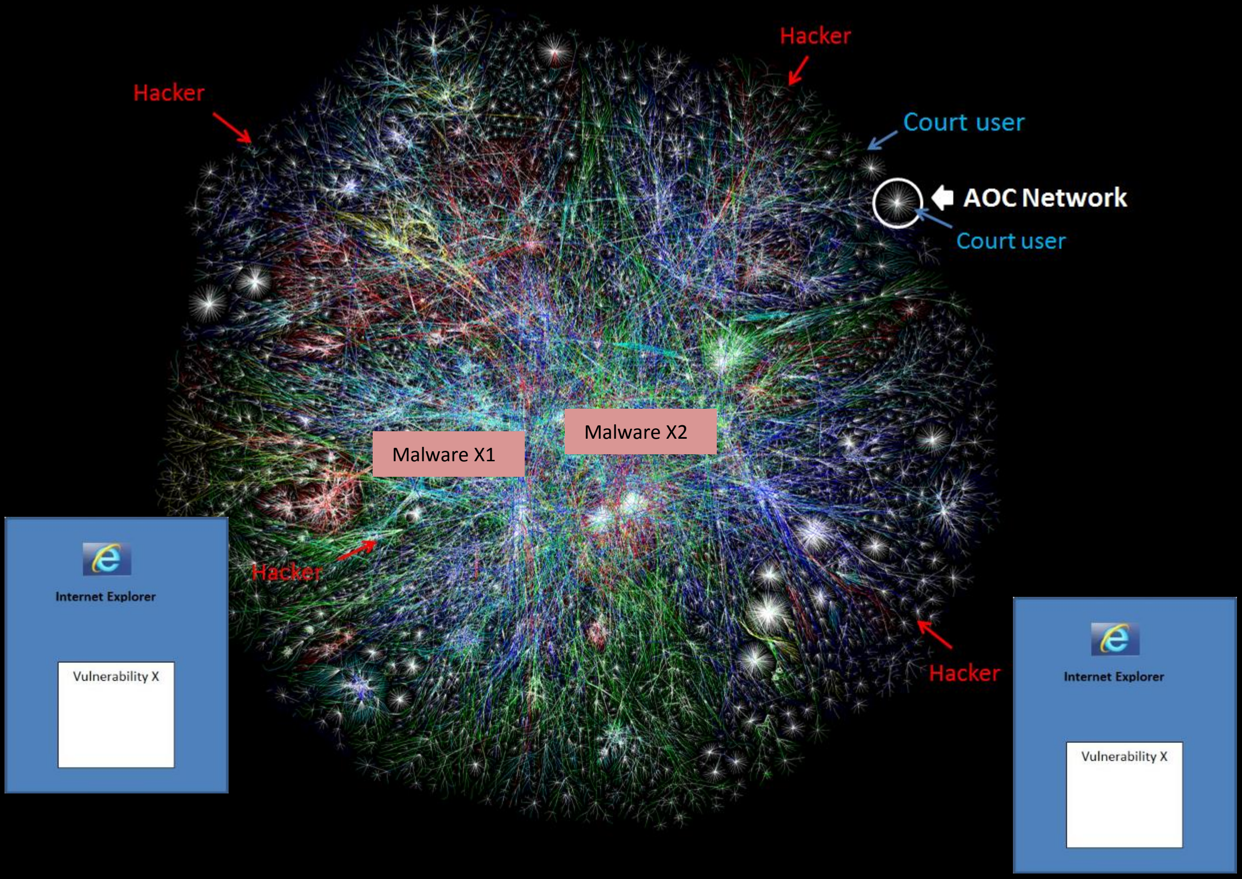
Hacker

Hacker

Internet Explorer

ulnerability X

Malware X2



Hacker

Hacker

Court user

AOC Network

Court user

Malware X2

Malware X1

Internet Explorer

Vulnerability X

Hacker

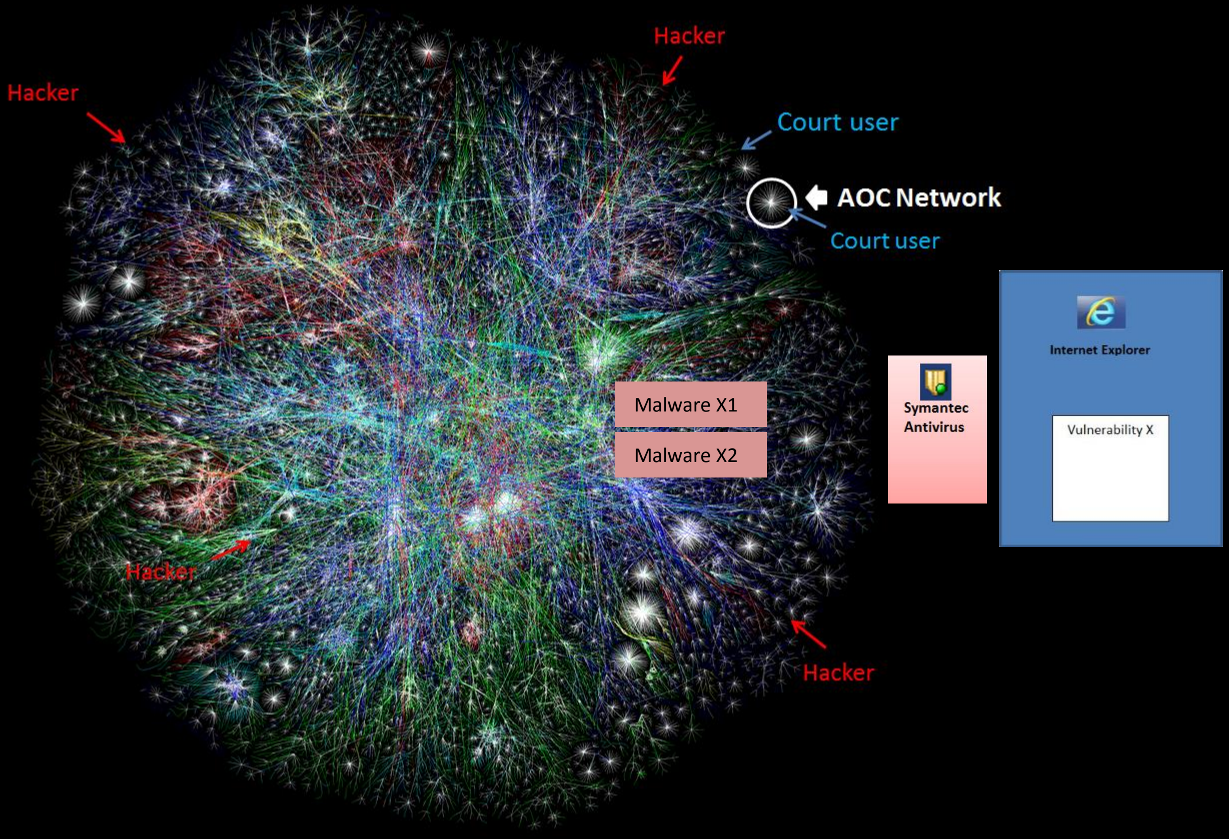
Hacker

Internet Explorer

Vulnerability X

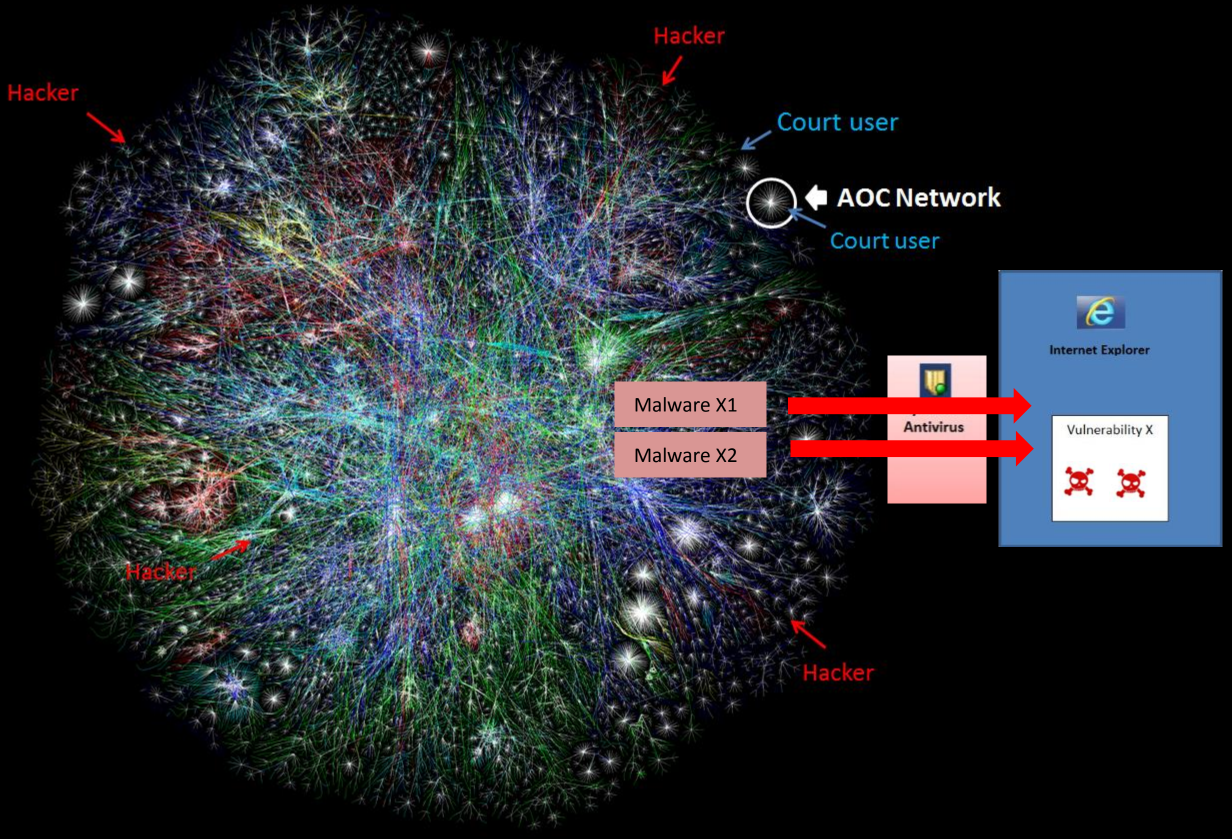
How Malware Spreads

- Phishing
- Websites
- Botnet



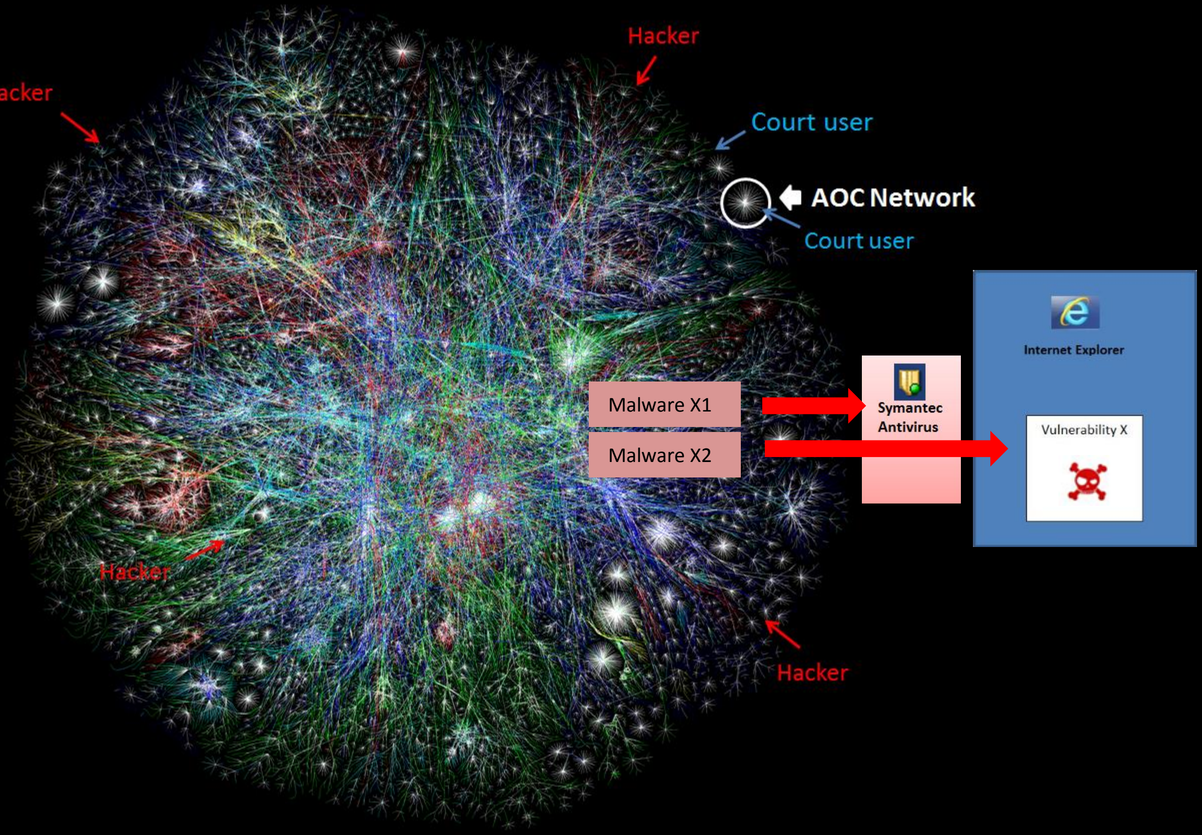
Three scenarios follow for this user coming into contact with Malware X1 and X2…

Scenario 1 – no antivirus update, no software update



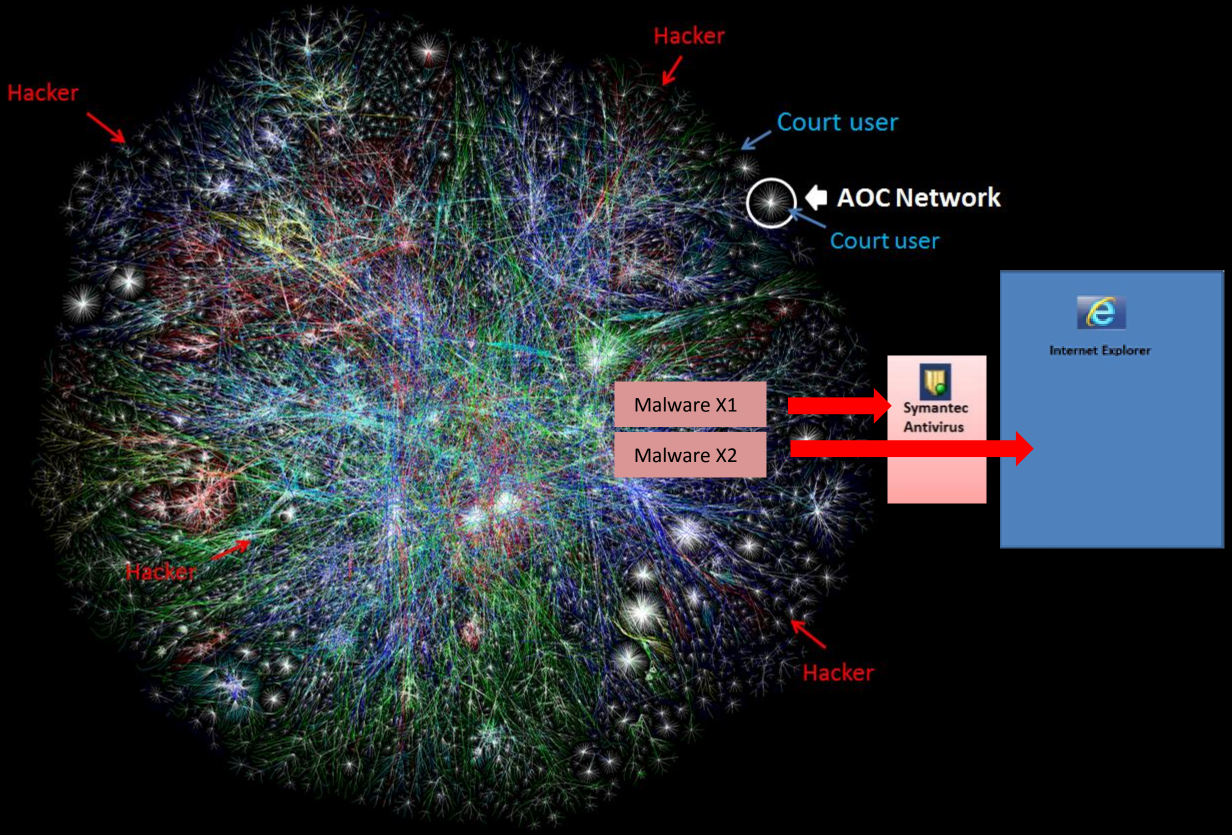
Result – infection by Malware X1 and Malware X2

Scenario 2 – antivirus update for Malware X1, no software update



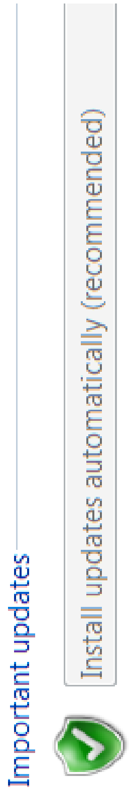
Result – Malware X1 blocked, infection by Malware X2

Scenario 3 – antivirus update for Malware X1, software update



Result – no infection

Software Update Notes

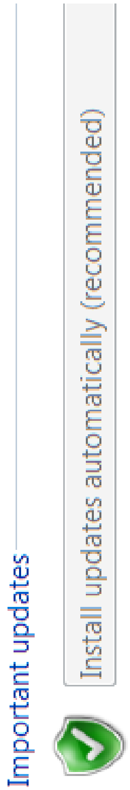


Important updates

Install updates automatically (recommended)

- Automatic Updates
- Java
  - Contexte/Xerox
  - Do not update without notification from AOC
- Windows XP and other unsupported software

What you can do



Important updates

Install updates automatically (recommended)

- Justice Building Network
  - Let Desktop Support (Wade, Jimmy Don, Shadrick) know if you notice something out of date
- Courts with IT support
  - Ask IT staff if they are updating software
  - Let IT staff know if you notice something out of date
- Courts without IT support
  - Keep your software updated
  - Need guidance?

Phishing

- Phishing is an attempt through email to solicit personal information . Often malicious code is also involved.

more than

{2/3}

of cyber incidents reported to the federal government are phishing attempts

over

90%

success rate

{ of a user clicking on a link or attachment for phishing campaigns of only **10** emails }

Phishing

- Reputable companies/entities will not ask you for personal information through email.
- If in doubt, contact the company/entity directly.

Suspicious Emails

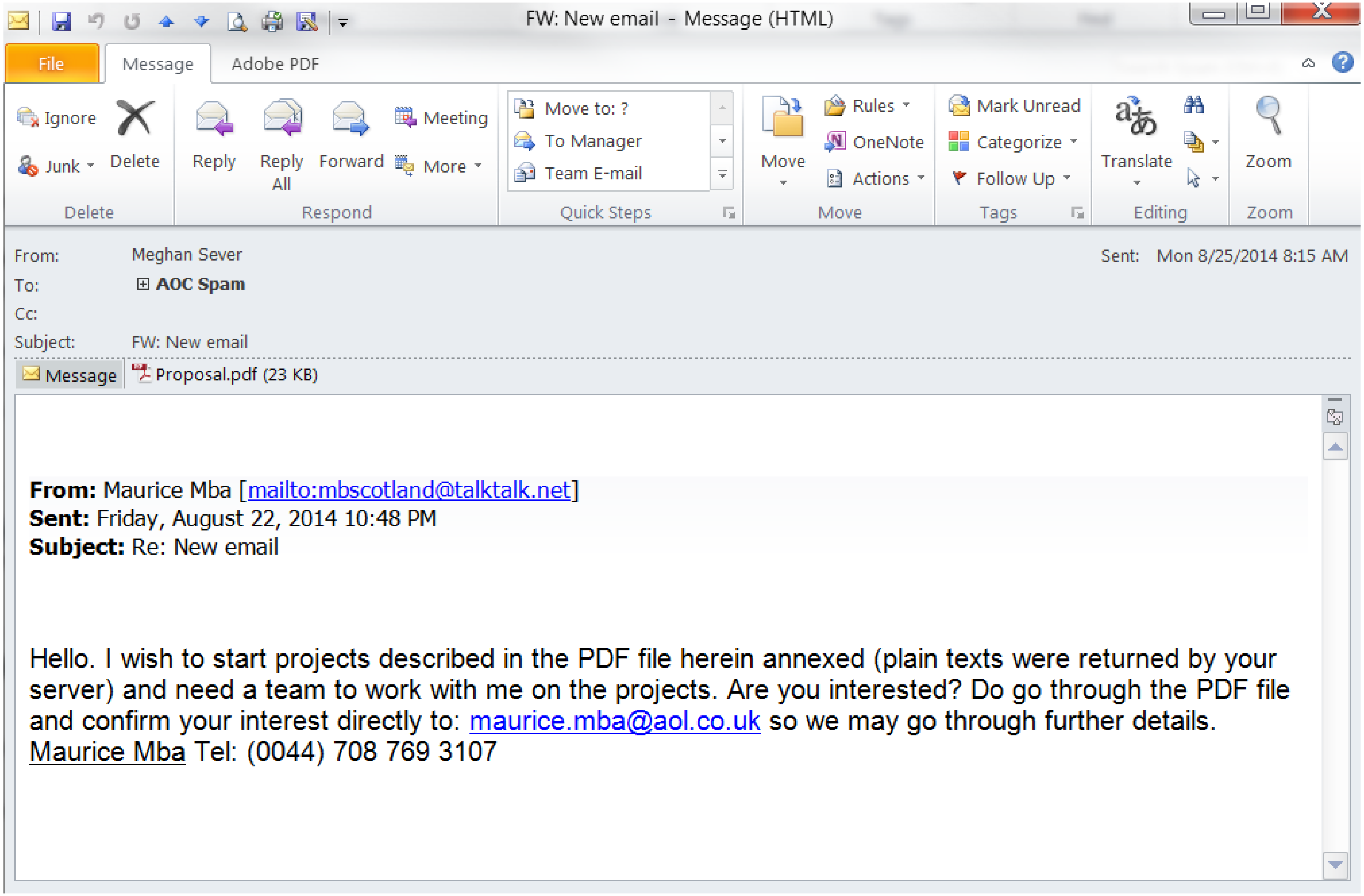
- Try to convince you to click on a link or attachment.
- You do not know the sender and/or the email address is long/convoluted/strange.
- Word usage/grammar/punctuation errors.
- Email details that do not apply to you (package tracking, airline ticket, court/legal proceedings, etc.).

What to do

- Do not click on any links or attachments.
- Delete the email (Inbox, Sent Items, Deleted Items).

Phishing Example

(Malicious Attachment)



From: Meghan Sever

Sent: Mon 8/25/2014 8:15 AM

To: AOC Spam

Cc:

Subject: FW: New email

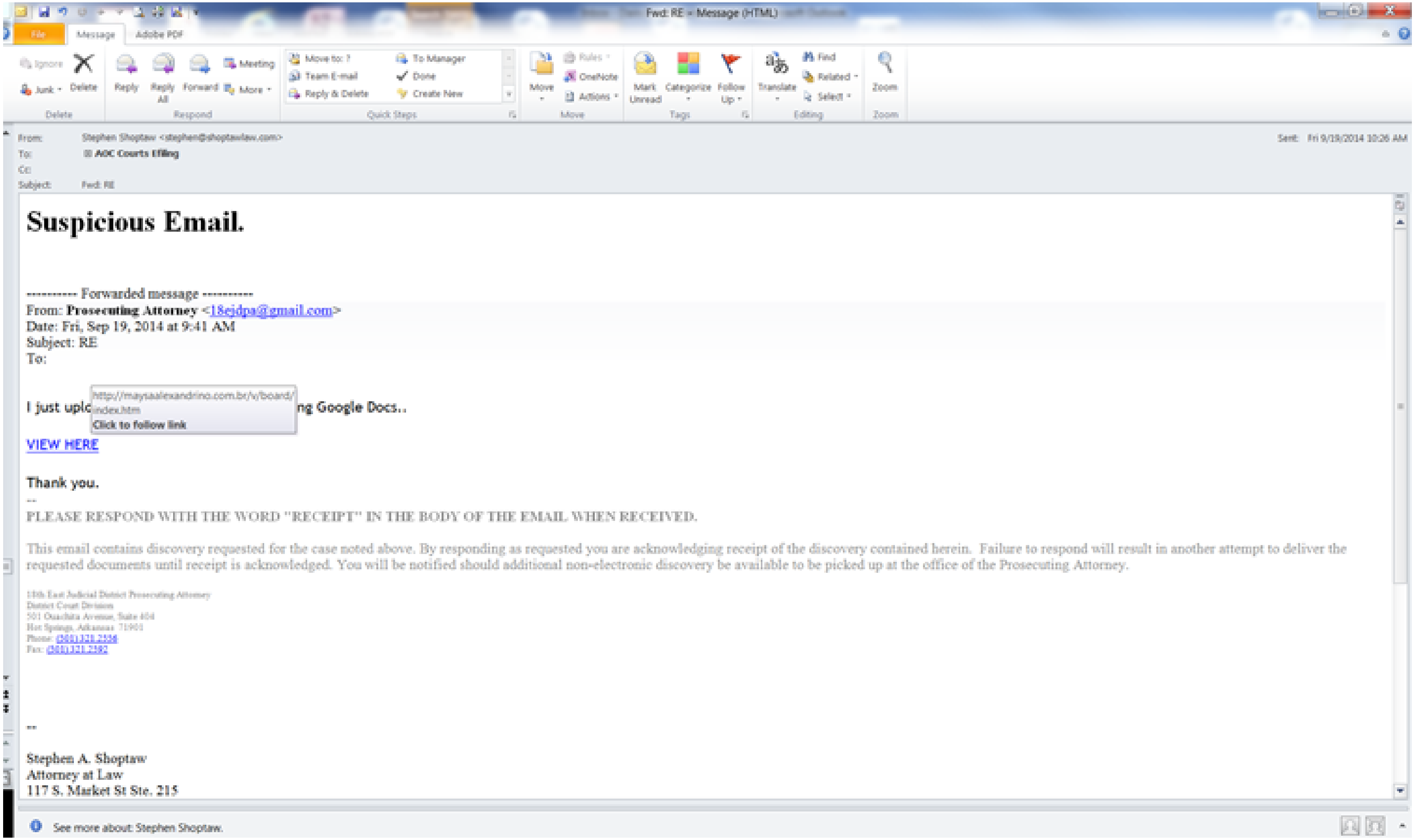
Message | Proposal.pdf (23 KB)

From: Maurice Mba [mailto:mbscotland@talktalk.net]
Sent: Friday, August 22, 2014 10:48 PM
Subject: Re: New email

Hello. I wish to start projects described in the PDF file herein annexed (plain texts were returned by your server) and need a team to work with me on the projects. Are you interested? Do go through the PDF file and confirm your interest directly to: maurice.mba@aol.co.uk so we may go through further details.
Maurice Mba Tel: (0044) 708 769 3107

Phishing Example

(Link is to a website with .br)



From: Stephen Shoptaw <stephen@shoptawlaw.com>
To: AOC Courts Efiling
Cc:
Subject: Fwd: RE

Sent: Fri 9/19/2014 10:26 AM

Suspicious Email.

---------- Forwarded message ----------
From: **Prosecuting Attorney** <18ejdpa@gmail.com>
Date: Fri, Sep 19, 2014 at 9:41 AM
Subject: RE
To:

I just uplo[http://maysaalexandrino.com.br/v/board/index.htm
Click to follow link]ng Google Docs..

VIEW HERE

Thank you.

--

PLEASE RESPOND WITH THE WORD "RECEIPT" IN THE BODY OF THE EMAIL WHEN RECEIVED.

This email contains discovery requested for the case noted above. By responding as requested you are acknowledging receipt of the discovery contained herein. Failure to respond will result in another attempt to deliver the requested documents until receipt is acknowledged. You will be notified should additional non-electronic discovery be available to be picked up at the office of the Prosecuting Attorney.

18th East Judicial District Prosecuting Attorney
District Court Division
501 Ouachita Avenue, Suite 404
Hot Springs, Arkansas 71901
Phone: (501)321.2556
Fax: (501)321.2582

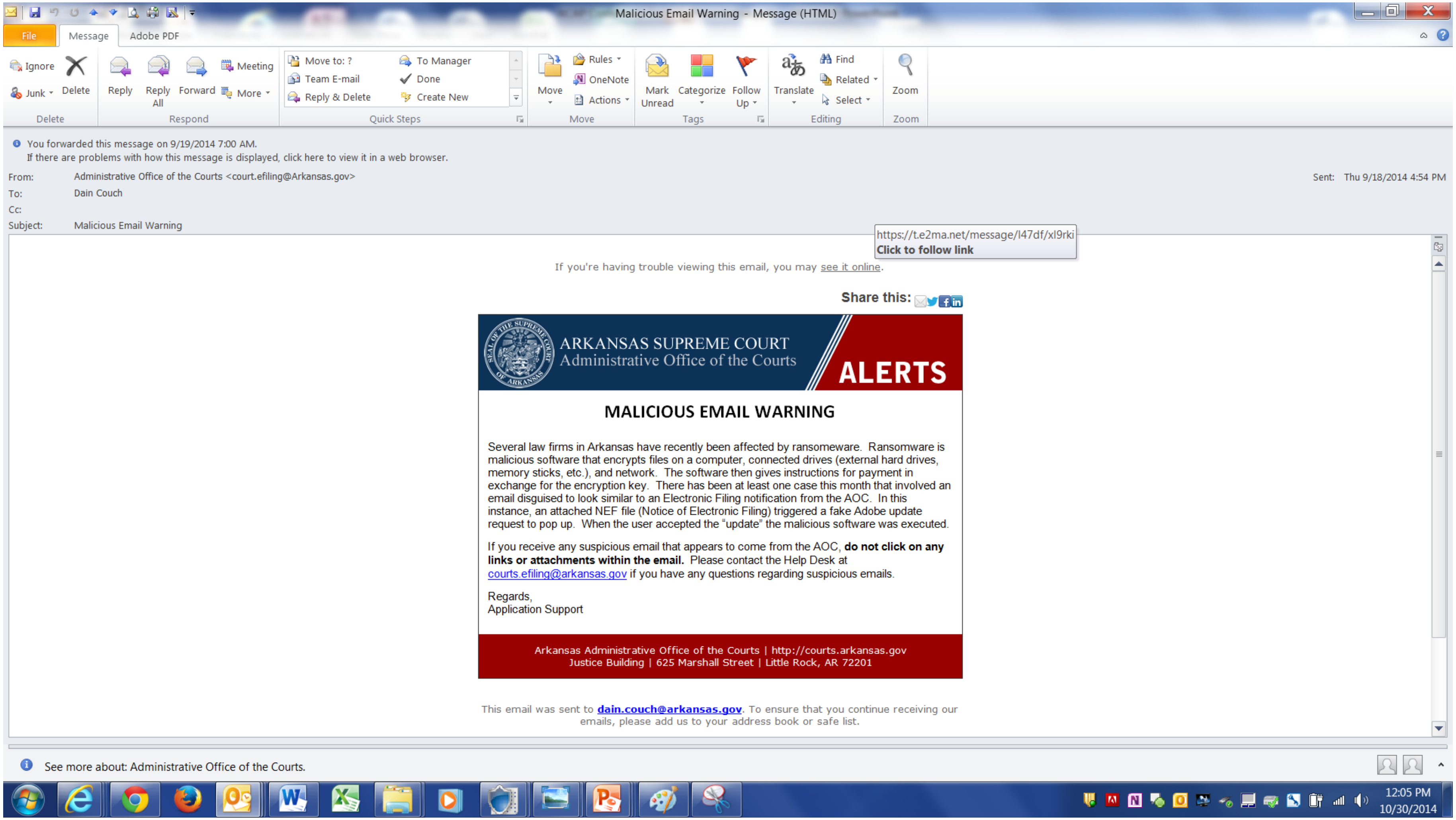
--

Stephen A. Shoptaw
Attorney at Law
117 S. Market St Ste. 215

See more about: Stephen Shoptaw.

NOT a Phishing Example

(Emma Notice – link “https://t.e2ma.net/message/l47df/xl9rki”)



You forwarded this message on 9/19/2014 7:00 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.

From: Administrative Office of the Courts <court.efiling@Arkansas.gov>
To: Dain Couch
Cc:
Subject: Malicious Email Warning
Sent: Thu 9/18/2014 4:54 PM

https://t.e2ma.net/message/l47df/xl9rki
Click to follow link

If you're having trouble viewing this email, you may see it online.

Share this:

ARKANSAS SUPREME COURT
Administrative Office of the Courts
ALERTS

MALICIOUS EMAIL WARNING

Several law firms in Arkansas have recently been affected by ransomeware. Ransomware is malicious software that encrypts files on a computer, connected drives (external hard drives, memory sticks, etc.), and network. The software then gives instructions for payment in exchange for the encryption key. There has been at least one case this month that involved an email disguised to look similar to an Electronic Filing notification from the AOC. In this instance, an attached NEF file (Notice of Electronic Filing) triggered a fake Adobe update request to pop up. When the user accepted the “update” the malicious software was executed.

If you receive any suspicious email that appears to come from the AOC, **do not click on any links or attachments within the email.** Please contact the Help Desk at courts.efiling@arkansas.gov if you have any questions regarding suspicious emails.

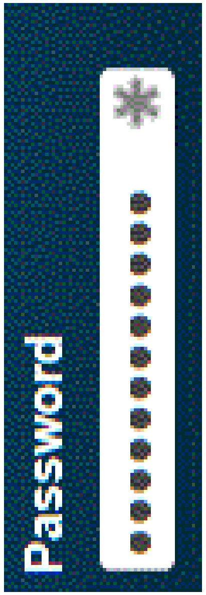
Regards,
Application Support

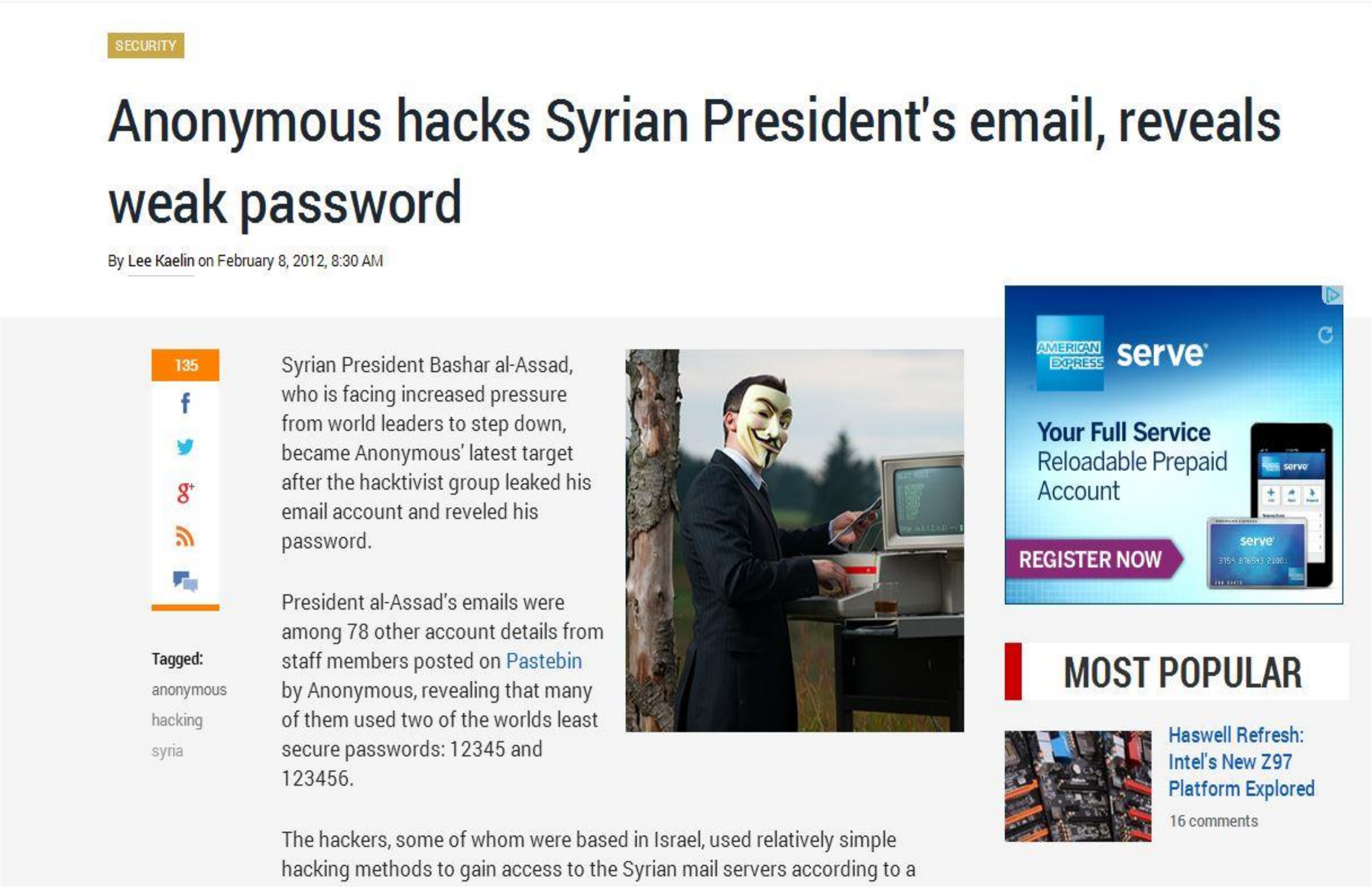
Arkansas Administrative Office of the Courts | http://courts.arkansas.gov
Justice Building | 625 Marshall Street | Little Rock, AR 72201

This email was sent to **dain.couch@arkansas.gov**. To ensure that you continue receiving our emails, please add us to your address book or safe list.

See more about: Administrative Office of the Courts.

Spaceballs (1987)





SECURITY

Anonymous hacks Syrian President's email, reveals weak password

By Lee Kaelin on February 8, 2012, 8:30 AM

Syrian President Bashar al-Assad, who is facing increased pressure from world leaders to step down, became Anonymous' latest target after the hacktivist group leaked his email account and reveled his password.

President al-Assad's emails were among 78 other account details from staff members posted on Pastebin by Anonymous, revealing that many of them used two of the worlds least secure passwords: 12345 and 123456.

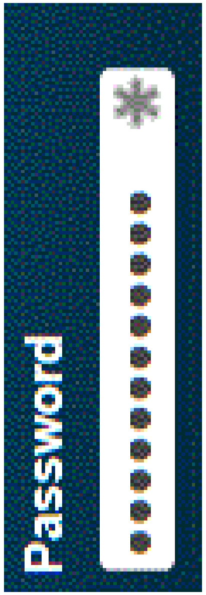
The hackers, some of whom were based in Israel, used relatively simple hacking methods to gain access to the Syrian mail servers according to a

Tagged:
anonymous
hacking
syria

MOST POPULAR

Haswell Refresh: Intel's New Z97 Platform Explored
16 comments

25 Most Used Passwords of 2013

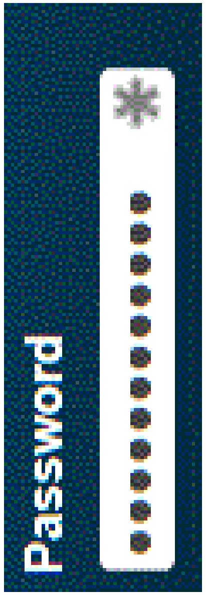


1. **123456**
2. **password**
3. **12345678**
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. admin
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. **12345**
21. password1
22. princess
23. azerty
24. trustno1
25. 000000

*from annual splashdata list

A Little Math

For an 8 character password:



- Numbers:

  10*10*10*10*10*10*10*10= **100,000,000**

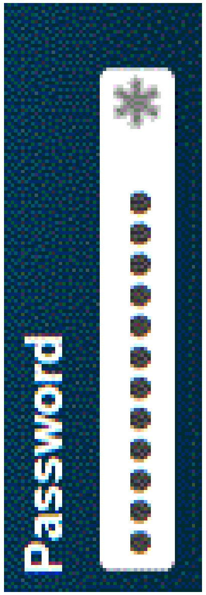
  (100 million)

- #s, lowercase, uppercase, and special:

  95*95*95*95*95*95*95*95 = **6,704,780,954,517,120**

  (6 quadrillion, 704 trillion, 780 billion, 954 million, 517 thousand, 120)

Password Tips

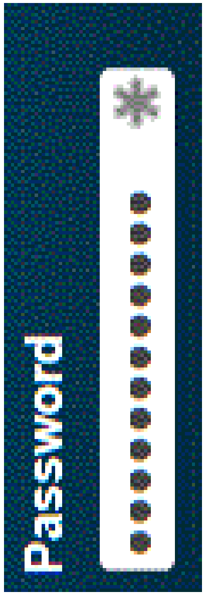


- The longer, the better.
- Use all 4 character types.
- Don’t use the same password for multiple accounts.
- Don’t share your password with anyone.

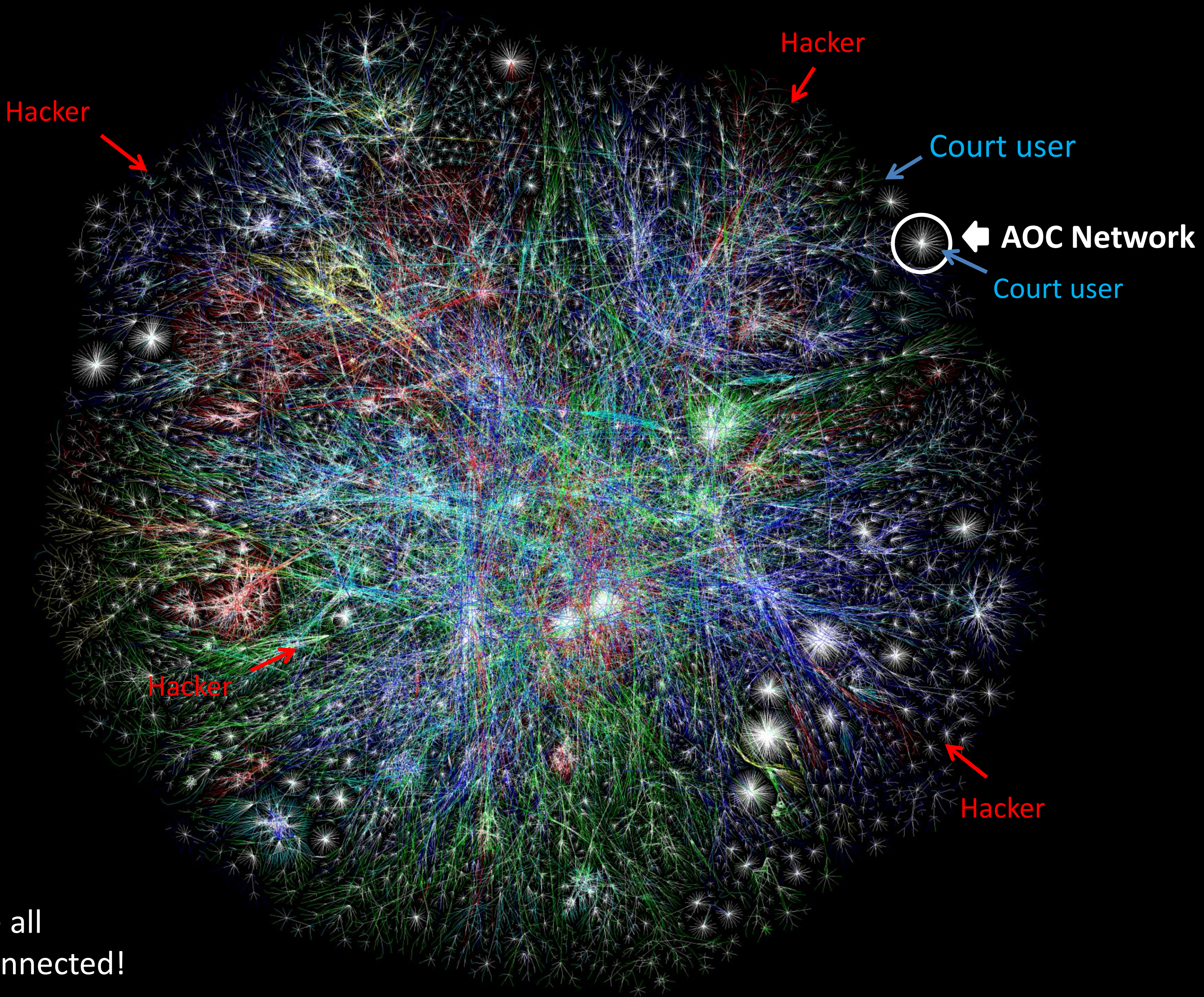
Ex: Amy lost her tooth yesterday.

Amy lost her toof yesterday.

aMYlosthert00fyesterday>>



Friends of the Court



We are all interconnected!

End