A Hacker’s Perspective

CONFIDENTIAL – PROPRIETARY AND PRE-DECISIONAL
Any use of this material without specific permission is strictly prohibited

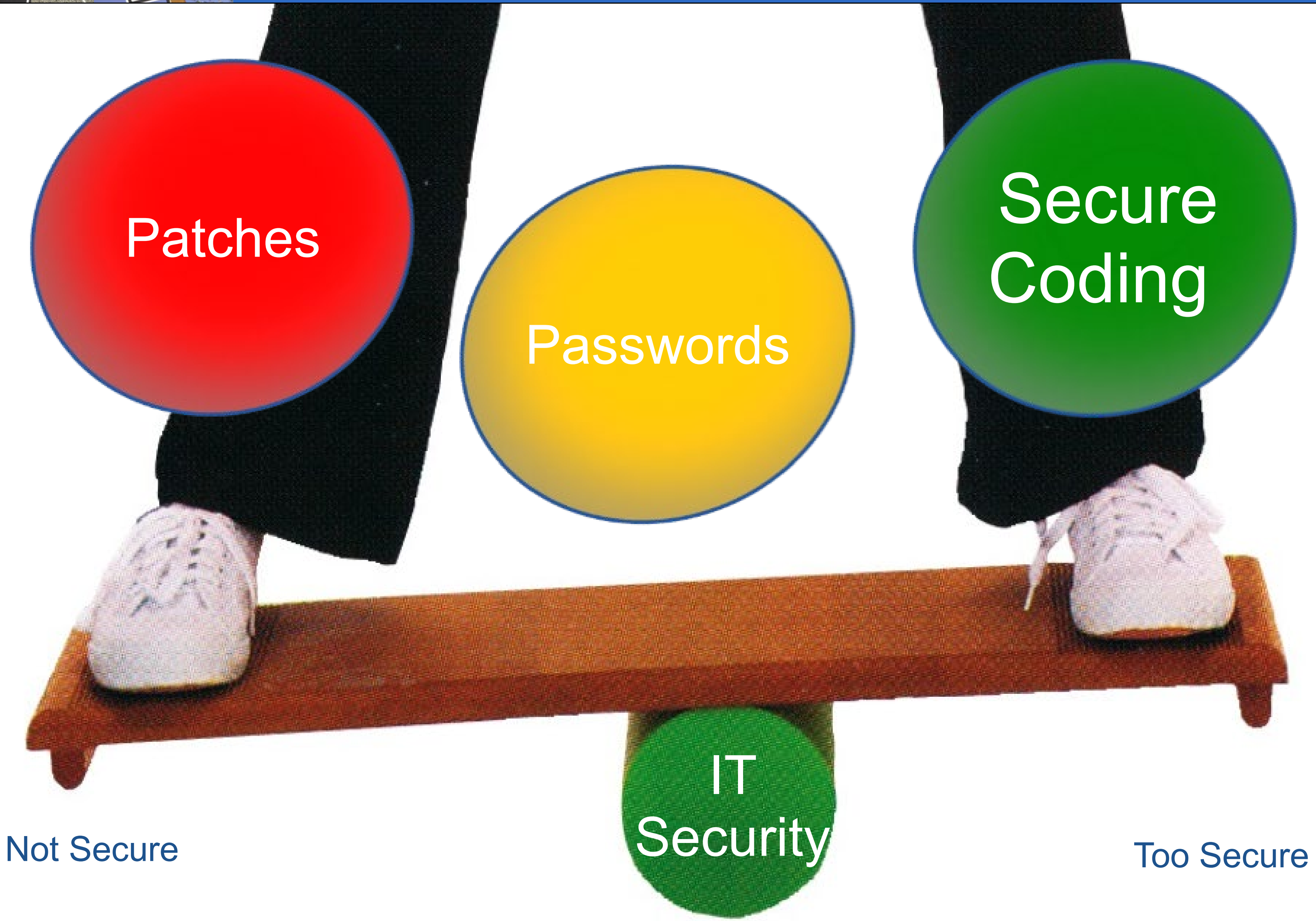
Purpose and Scope

- To present a best practice approach to auditing your servers
- To present real life examples of vulnerability assessment successes
- To present hacker techniques in plain terms

Legal Disclaimer

- Don’t try this at home
- Get written permission before trying any of these techniques
  - The main difference between a security admin and a hacker is permission

Juggling Tasks



Patches

Passwords

Secure Coding

IT Security

Not Secure

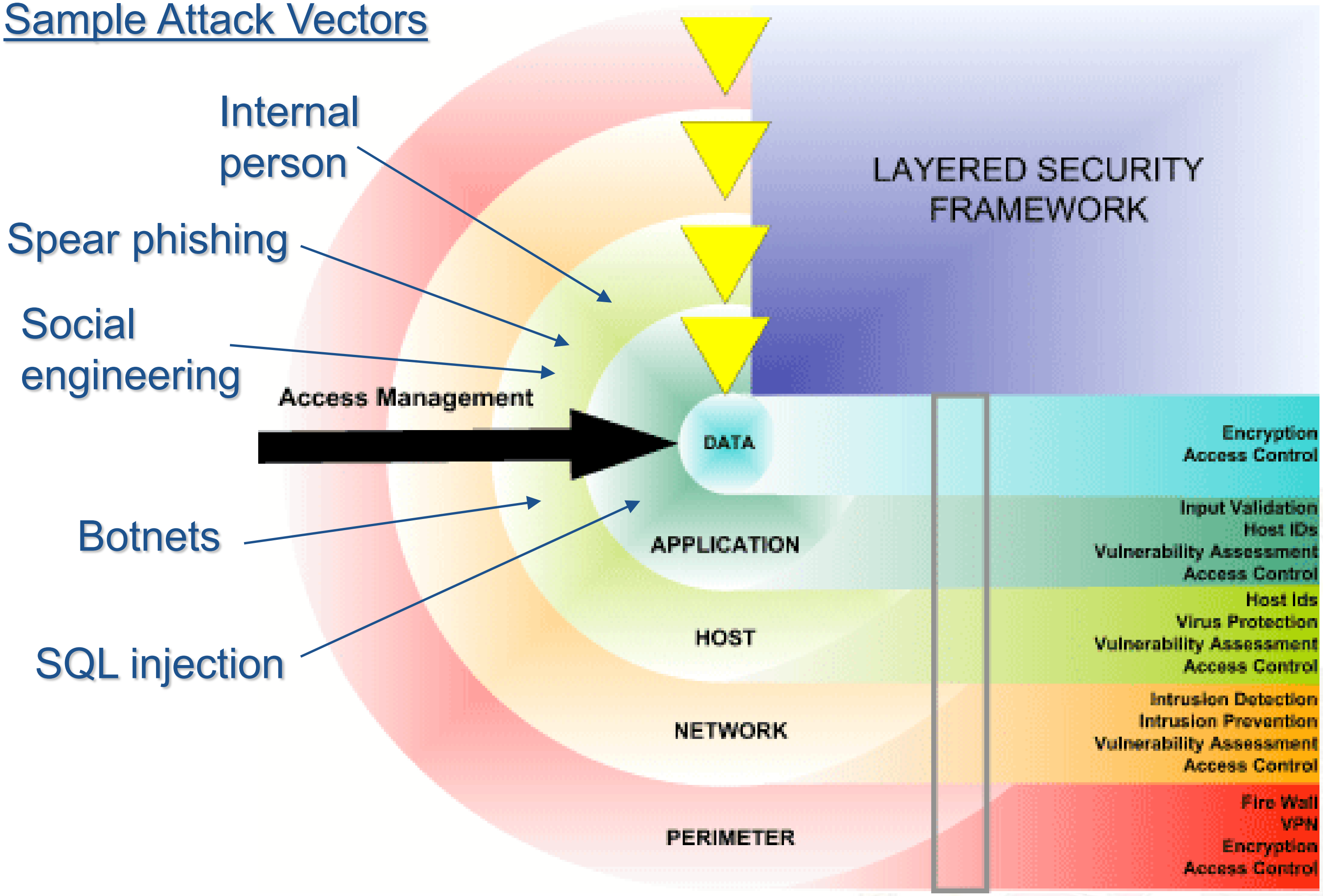
Too Secure

Owasp Top Threats 2019

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

Layered Security

Sample Attack Vectors



Internal person

Spear phishing

Social engineering

Botnets

SQL injection

Access Management

LAYERED SECURITY FRAMEWORK

DATA	Encryption Access Control
APPLICATION	Input Validation Host IDs Vulnerability Assessment Access Control
HOST	Host Ids Virus Protection Vulnerability Assessment Access Control
NETWORK	Intrusion Detection Intrusion Prevention Vulnerability Assessment Access Control
PERIMETER	Fire Wall VPN Encryption Access Control

Return on Investment

- 2006 Illinois breach notification law
- Average cost to notify per identity compromised?

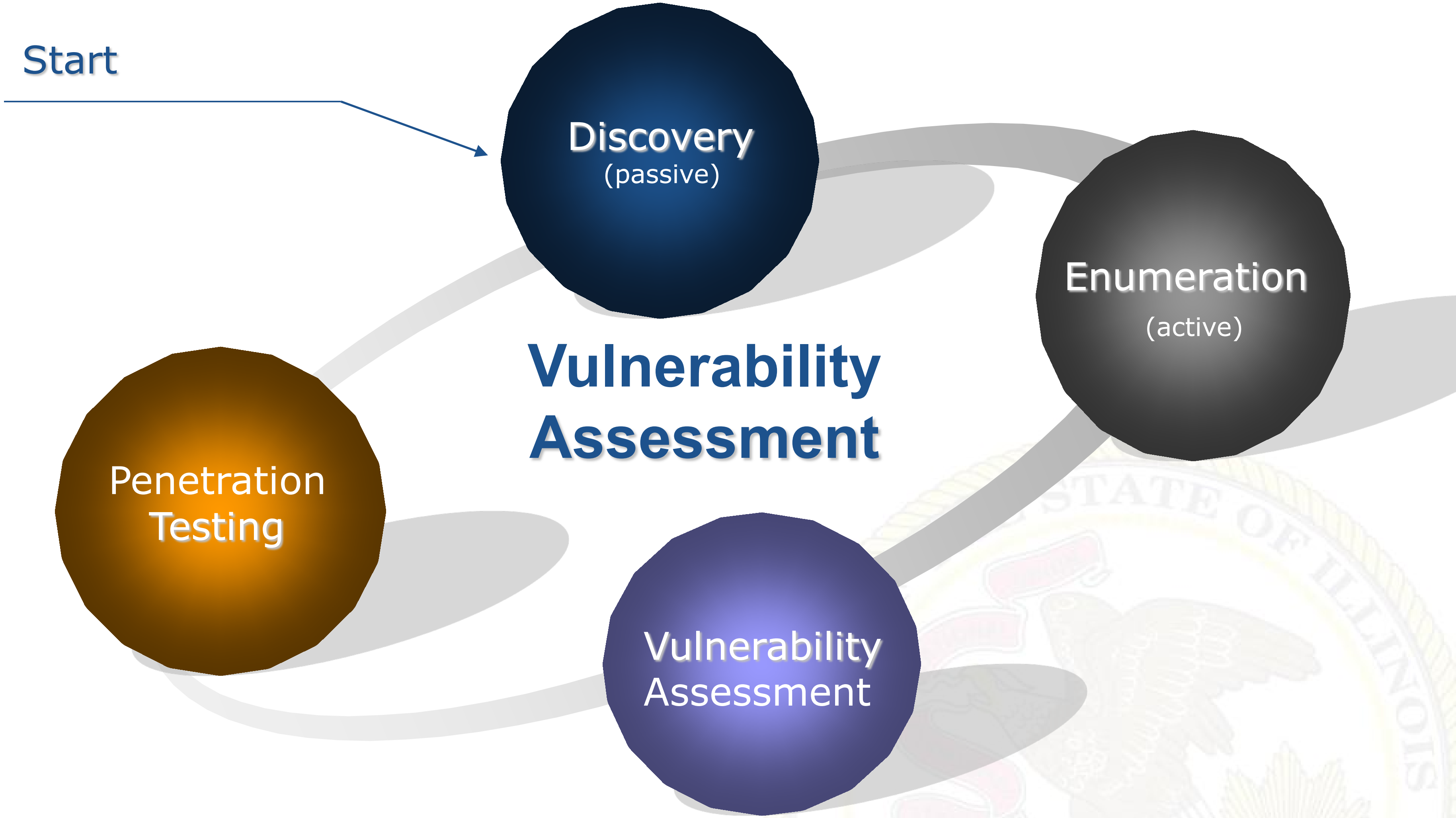
  $14 - 90

- Black market value of your identity?

  $2

- What is the return on investment for proactive security?
  - ROI spreadsheet

Testing Methodology



Vulnerability Assessment

Discovery

- Internet registrar search (http://whois.net)
- General company research (Google, etc.)
- Dumpster diving
- Archive.org
- Newsgroups
  - Techs posting questions
- Job postings
  - Specific software used

Discovery – Google hacking

- Password site:yoursite.com
- Filetype:doc site:yoursite.com classified
- Robots.txt site:yoursite.com
- Intitle:index.of “parent directory” site:yoursite.com

Enumeration

- Ping sweeps / port scanning
- Banner grabbing (telnet ip port)
- Fingerprinting
- MSN virtual hosts search (ip:address)
- Directory Structure
  - Default directories: /admin /secure /adm
  - Backup files: /.bak /backup /back /log /archive
  - Include files: /include /inc /js /global /local

Enumeration

- Common files
  - Ws_ftp.log
  - Install.txt
  - ToDo
- HTML source code
  - Password, select, insert, #include, #exec, connect, //
  - Comments
  - Mailto:

Enumeration

- Hidden fields
- Query strings
  - User ID (/login?userID=558253)
  - Session ID (/menu.asp?sid=69jt7b9329kuy)
  - Database queries (/dbsumit.php?sTitle=ms&iphone=5551212)

Video (Terminal Services)

Corrective Actions

- Investigate and disconnect unauthorized hosts
- Disable or remove unnecessary or vulnerable services

Vulnerability Assessment

- Proactive
- Validate policy compliance
- ID vulnerabilities
- Fast and easy
- MS08-067 is the current litmus test

Video (MS06-040 proof of concept)

Vulnerability Assessment Weaknesses

- False positives
- Requires high expertise in networking and OS security

Corrective Actions

- Upgrade or patch vulnerable devices
- Improve setup procedures and security baseline steps
- Assign a staff member to monitor alerts and mailing lists
- Modify the organization's security policies
- Implement and monitor Intrusion Detection

Example (DoD calls)

Passwords

- Password Cracking
  - Identify weak or default passwords
  - Verify the use of complex passwords
  - Brute force attack estimator

Video (Lock your PC)

Characters (complex)	Estimated time to crack
7	.009 hours
8	2.34 hours
14	9 hours
15	209 days

24 most-used passwords

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

Passwords

- A strong password is:
  - 8 or more characters
  - Uppercase and lowercase
  - Alpha-numeric
  - Odd character(s)
  - Non-dictionary
  - Non-pronounceable
  - 15 or more characters for admin passwords

Pick The Best Password

password

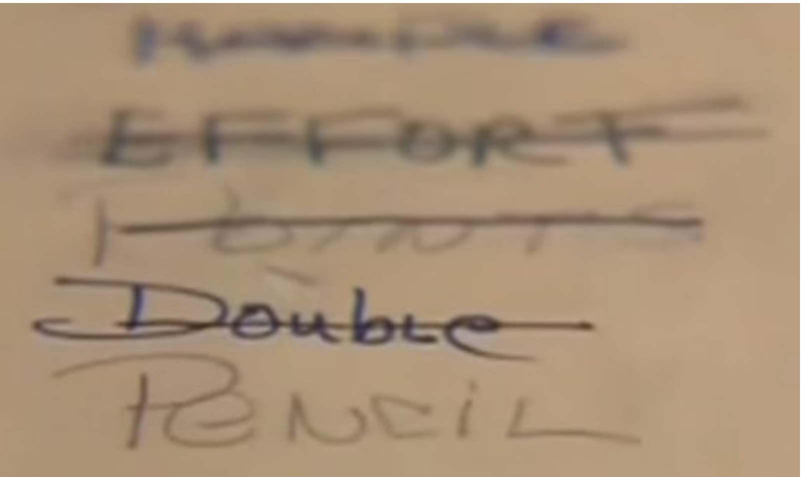
Summer13

P@swordCompl3x

juggle13 google

Password tips

- Don’t let the browser remember your password
- Logout of sites before shutting down the browser
- Password safe / LastPass (to store passwords)
- No sticky notes with passwords
- Password group policies that enforce complexity / length
- Don’t let a student administer a website or server



Passwords

- Prevention
  - Set minimum length and complexity through group policies
  - Disable LM hashing
  - Don’t store passwords in plain text
    - Password Safe,etc
    - Educate the users
  - Change defaults

Example (Router and password)

Post Testing Actions

- Remediate vulnerabilities
- Update policies
- Security awareness
- Legal notice
- Patch, patch, patch
- Change passwords

Demo’s

- Video (Client side scripting)
- Video (Path traversal attack)
- Video (SQL injection)
- Video (Cross-site scripting)
- Video (Information Security)

Penetration Testing

- Identify methods of gaining access to a system by using common tools and techniques used by attackers
- Should be performed after careful consideration, notification, and planning
- Perform during off hours to prevent unplanned outages

Penetration Testing

- Rules of engagement
  - Specific IP addresses/ranges to be tested
  - Any restricted hosts
  - A list of acceptable testing techniques
  - Times when testing is to be conducted
  - Identify period for testing
  - IP addresses of the tester’s machines
  - Points of contact for the penetration testing team, the targeted systems, and the networks

(Example) (Example)

Penetration Testing

- Blue teaming
  - Testing *with* the knowledge and consent of the organization's IT staff
  - Least expensive and most frequently used

Penetration Testing

- Red teaming
  - Testing *without* the knowledge of the organization's IT staff but with full permission of upper management
  - Useful for testing the IT staff's response to perceived security incidents
  - May be conducted with or without warning
  - More expensive and time consuming
  - Better indication of everyday security

Penetration Testing

- Outside attack
  - Usually performed first
  - Usually limited by firewall
  - Focus on commonly used ports
  - Done with very little inside information
  - Testers are not provided with any real information about the target environment
  - Leverages minimal access to gain greater access

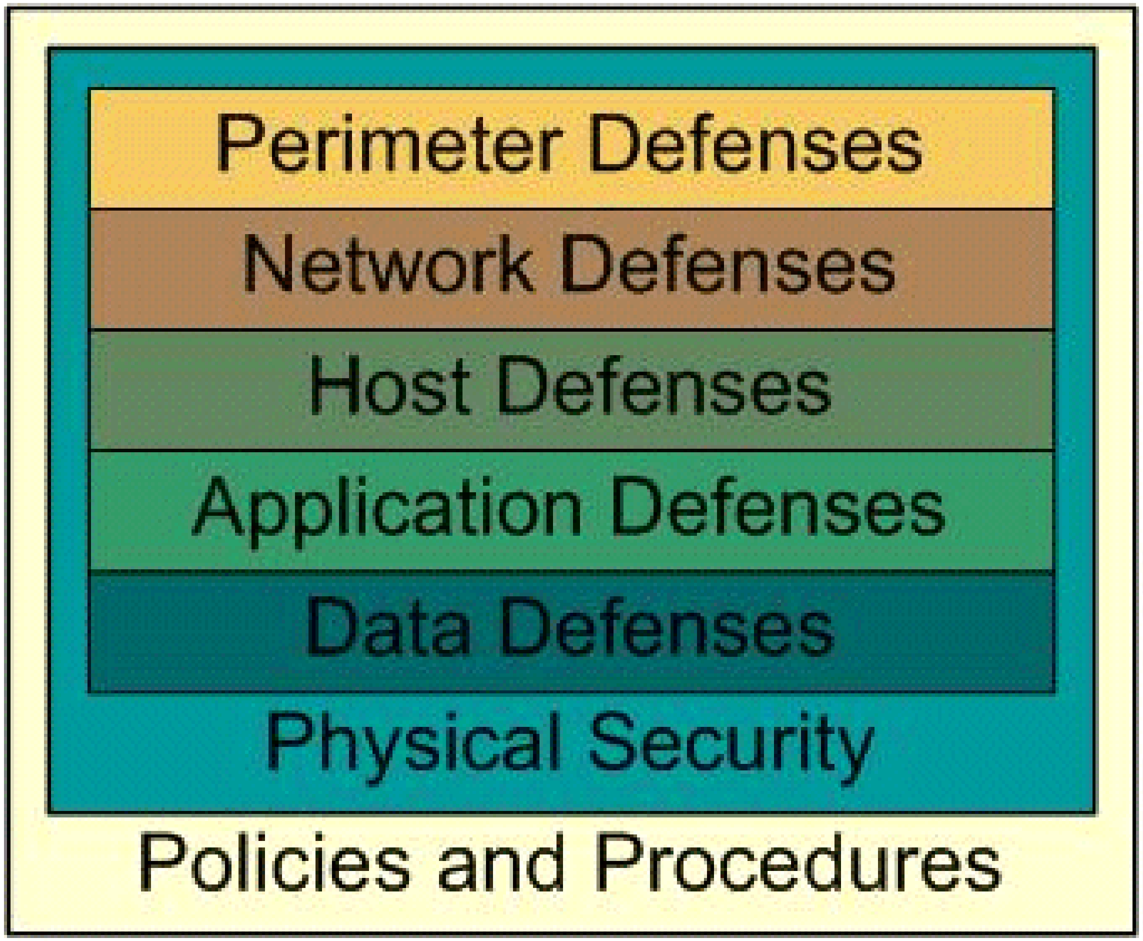
Penetration Testing

- Inside attack
  - Testers are on the internal network
  - Granted some level of access to the network (generally a user)
  - Attempts privilege escalation
  - Provided with commonly known network information

Roles and Responsibilities

- Only designated individuals should conduct the tests
- Alert appropriate staff that network mapping is taking place

Security In-Depth



Perimeter Defenses

Network Defenses

Host Defenses

Application Defenses

Data Defenses

Physical Security

Policies and Procedures

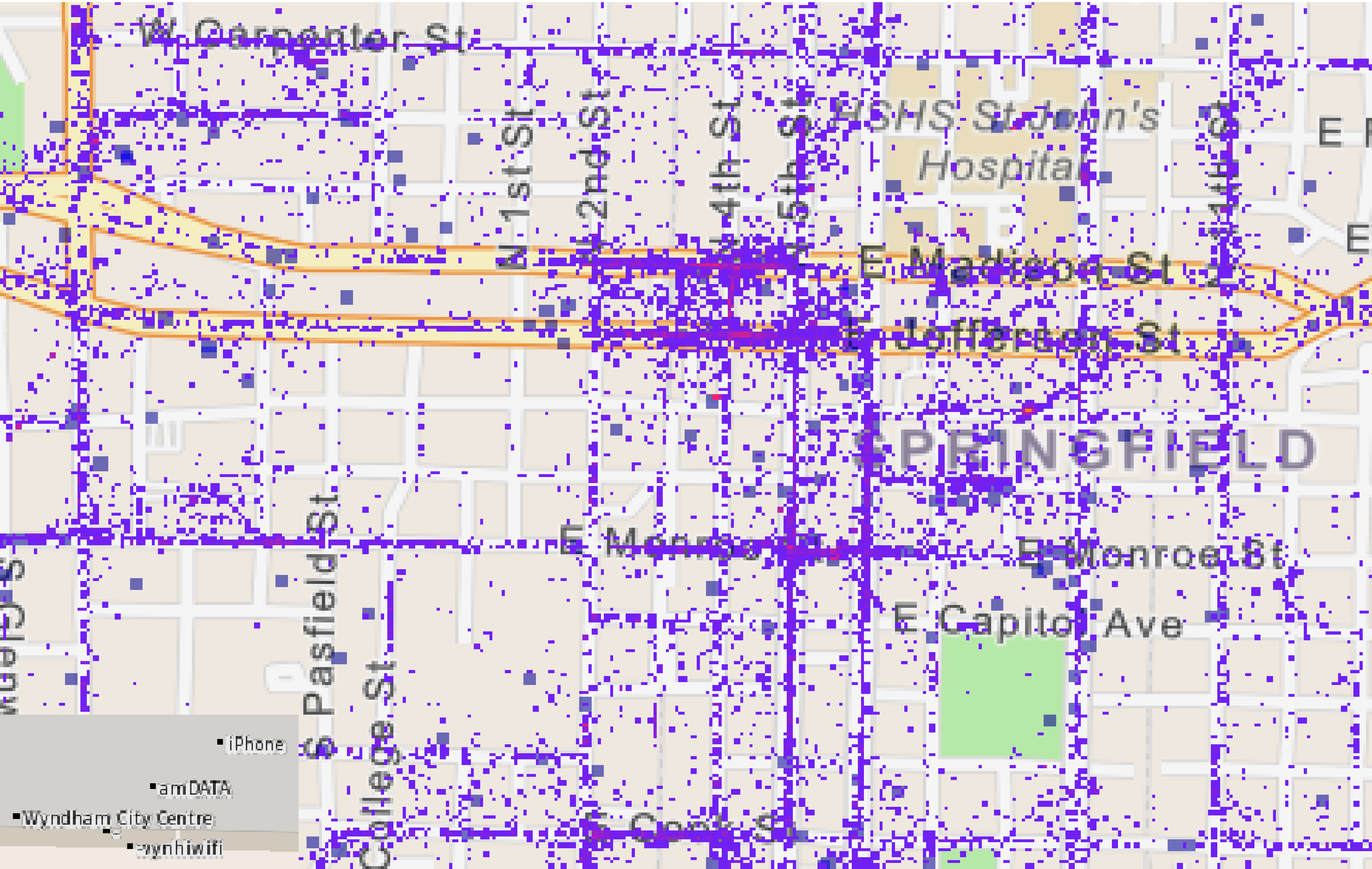
Wireless Security

- 802.11b has serious flaws in its current implementation of WEP
- AP's often set to default configuration
- 300-600 feet range (more with an antenna)
- WPA 2 or above for encryption
  - WEP 128 bit encryption can be cracked in 1 to 6 minutes

Wireless Security

- Don’t use hotel or coffee shop wireless for anything requiring authentication or confidentiality (treat them like a postcard)
- Don’t jump on “free_internet”
- Avoid theft of service

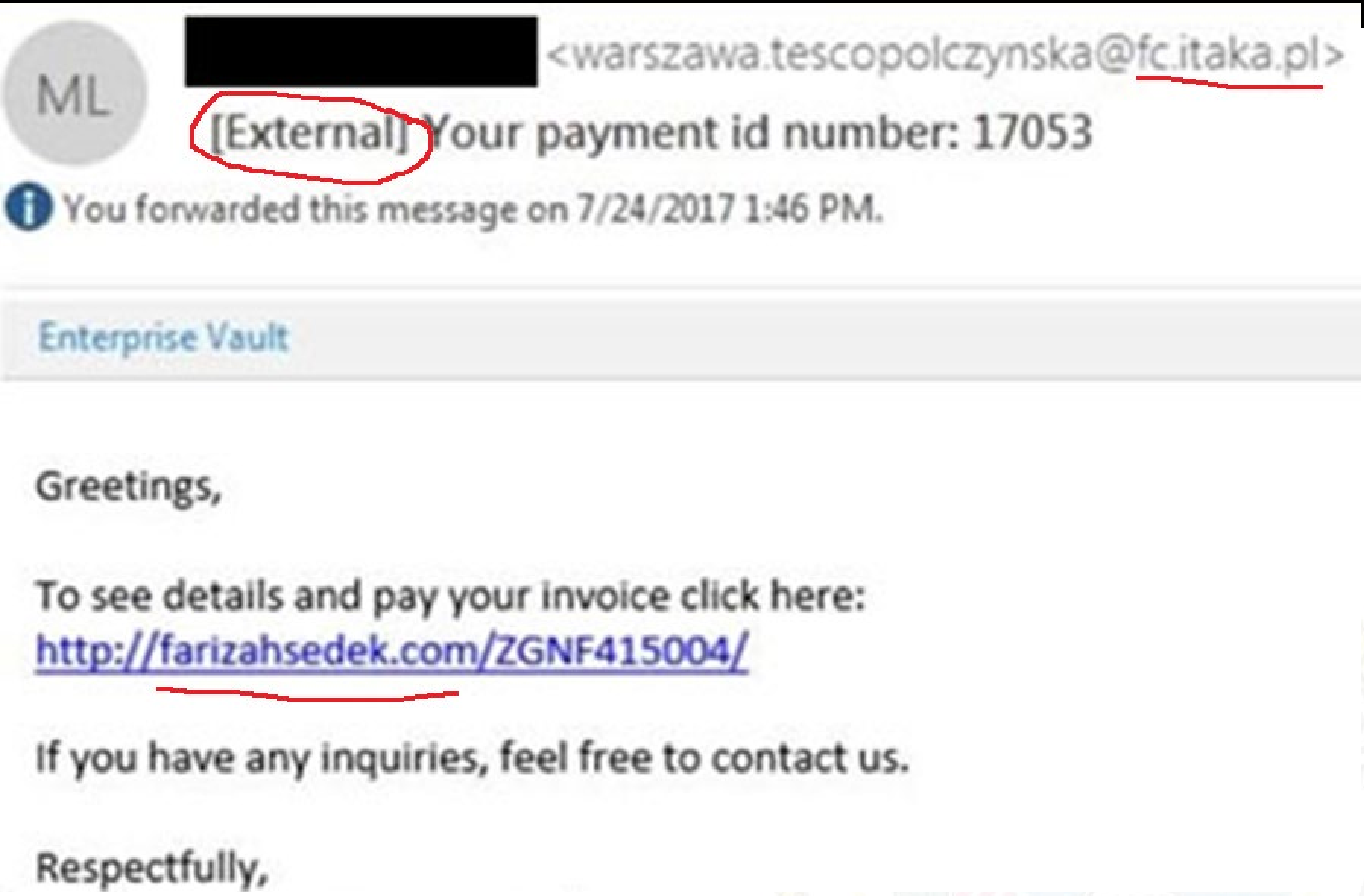
War Driving (wiggle.net)



Corrective Actions

- Create and communicate a wireless policy
- Search for (and remove) rogue AP’s and misconfigured wireless LANs

Phishing – Fake Invoices



ML

[redacted] <warszawa.tescopolczynska@fc.itaka.pl>

[External] Your payment id number: 17053

You forwarded this message on 7/24/2017 1:46 PM.

Enterprise Vault

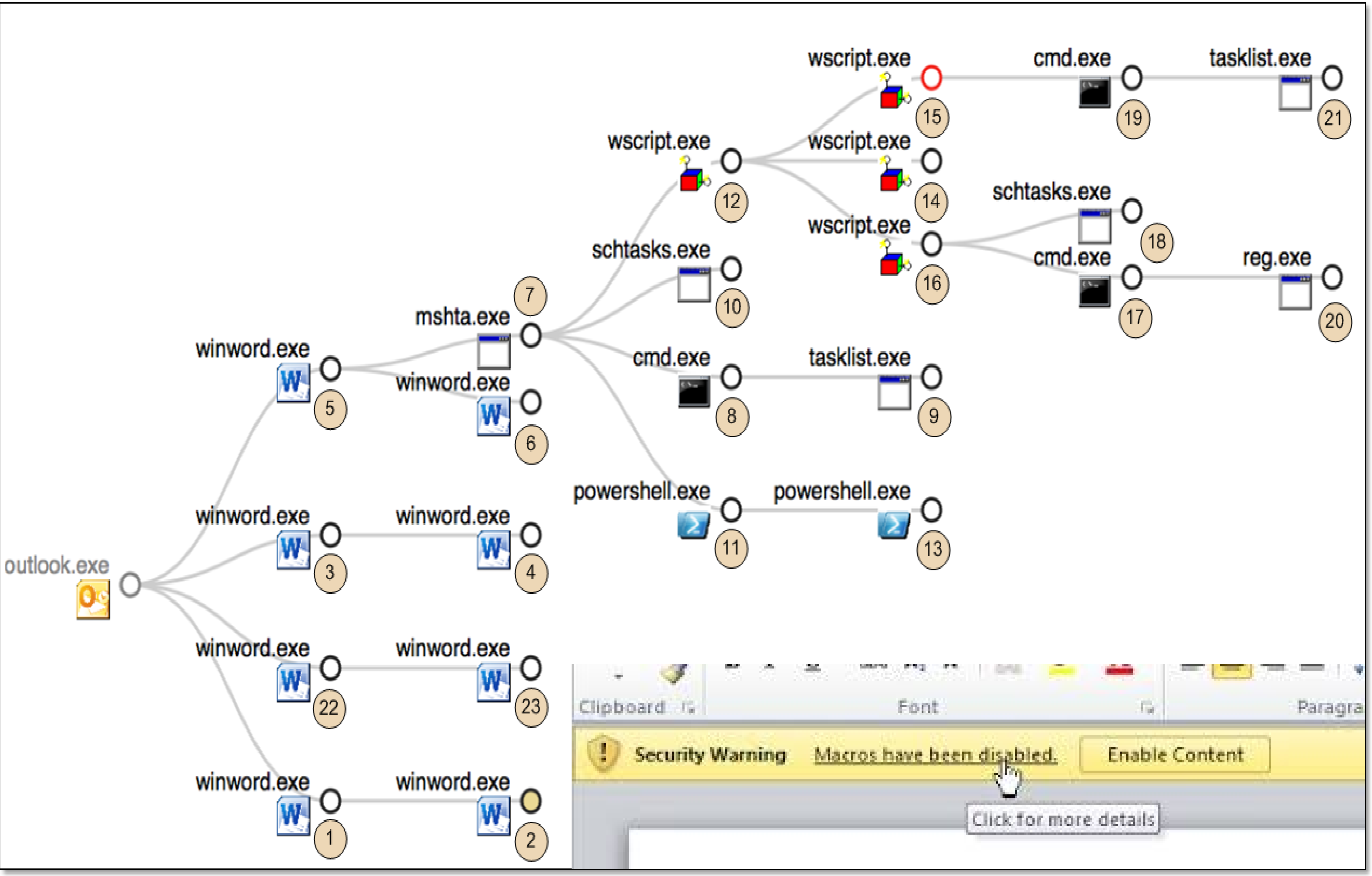
Greetings,

To see details and pay your invoice click here:
http://farizahsedek.com/ZGNF415004/

If you have any inquiries, feel free to contact us.

Respectfully,

Phishing – Kill Chain

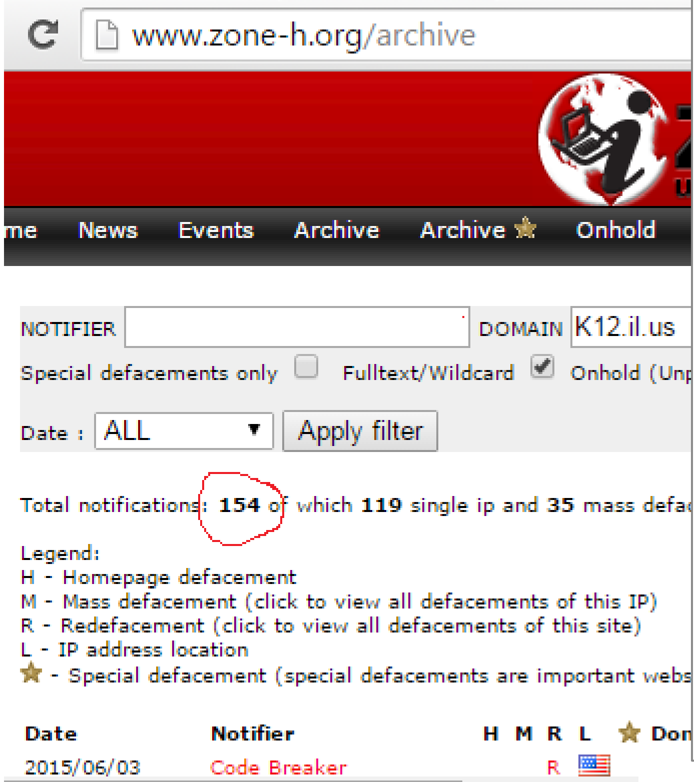


Security Warning Macros have been disabled. Enable Content

Click for more details

Defacements

- Defacement sites are a good place to start



NOTIFIER DOMAIN K12.il.us

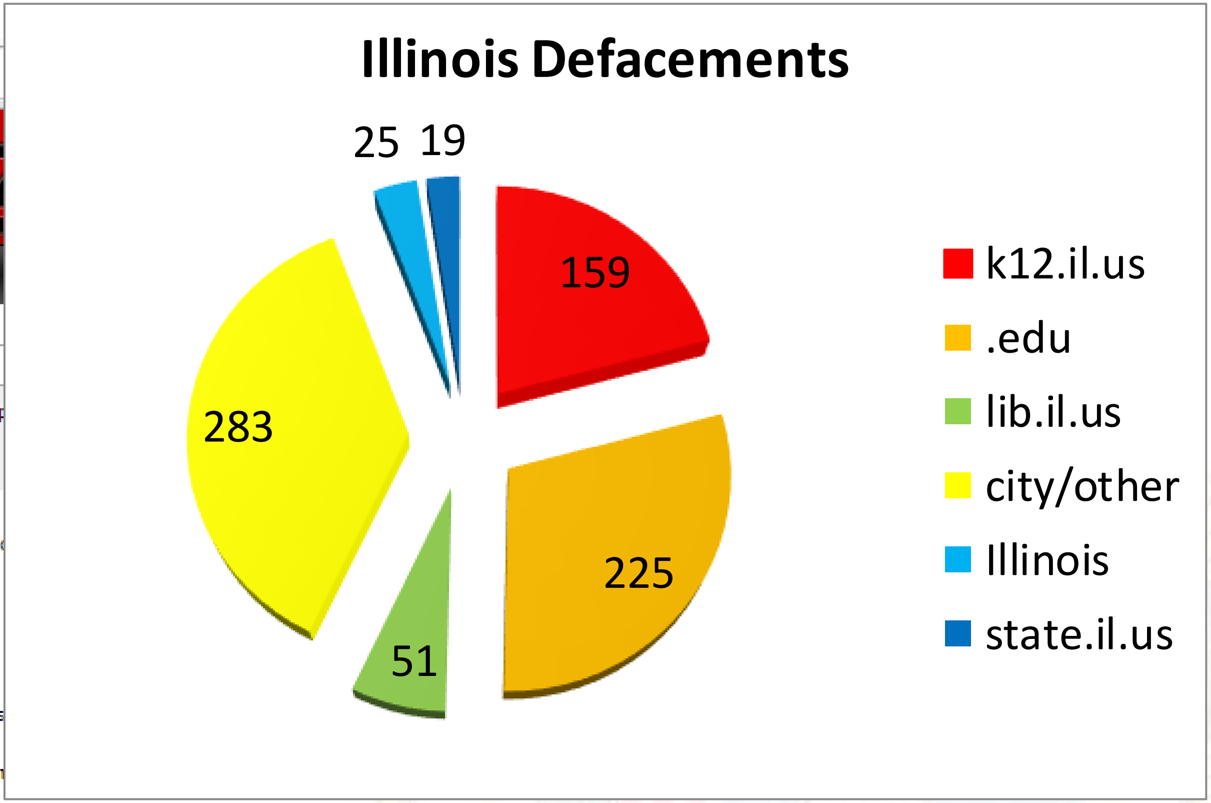
Special defacements only □ Fulltext/Wildcard ☑ Onhold (Unp

Date : ALL ▾ Apply filter

Total notifications: 154 of which 119 single ip and 35 mass defa

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important webs

Date	Notifier	H	M	R	L	★	Dom
2015/06/03	Code Breaker			R			



Conclusion

- Security is a journey, not a destination.
- Keep informed
  - Newsgroups
  - Constant research
  - Books, etc.
- Request access to your agencies audits

Resources

- Security e-mail notifications
  - www.securiteam.com
- US-CERT bulletins
  - www.us-cert.gov/cas/bulletins/
- National Vulnerability Database
  - http://nvd.nist.gov/

Physical Security

- Locks keep honest people honest

(720 ILCS 5/19-2) (from Ch. 38, par. 19-2)

If You Remember Nothing Else …

- Promptly apply patches
- Run anti-virus software configured to update daily, use on-access/on-demand scanning, and perform a full scan at least weekly
- Select uniq, complex passwords and use them everywhere
- Think BEFORE you click!!
  - www.dhs.gov/stopthinkconnect