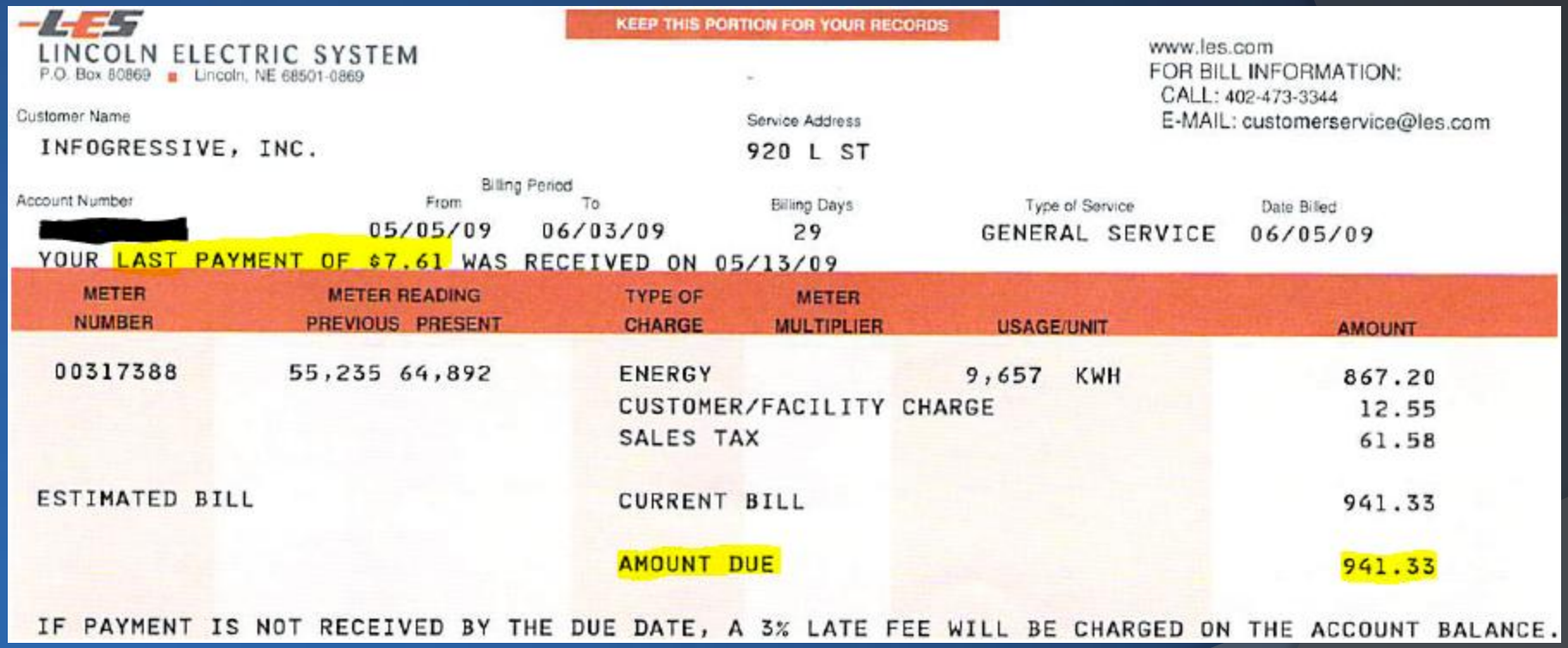

Infogressive, Inc.

# VULNERABILITY MANAGEMENT:
## A DEFENSE-IN-DEPTH APPROACH

Justin Kallhoff
CISSP, C|EH, GPCI, GCIH, GSEC, GISP, GCWN, GCFA

Tristan Lawson
CISSP, C|EH, E|CSA, GISP, GSEC, MCSA, A+, Net+, Server+, Security+

# COMPUTERS MAKE MISTAKES?



LES

LINCOLN ELECTRIC SYSTEM
P.O. Box 80869 ■ Lincoln, NE 68501-0869

KEEP THIS PORTION FOR YOUR RECORDS

www.les.com
FOR BILL INFORMATION:
CALL: 402-473-3344
E-MAIL: customerservice@les.com

Customer Name
INFOGRESSIVE, INC.

Service Address
920 L ST

| Account Number | Billing Period From | To | Billing Days | Type of Service | Date Billed |
|---|---|---|---|---|---|
| [redacted] | 05/05/09 | 06/03/09 | 29 | GENERAL SERVICE | 06/05/09 |

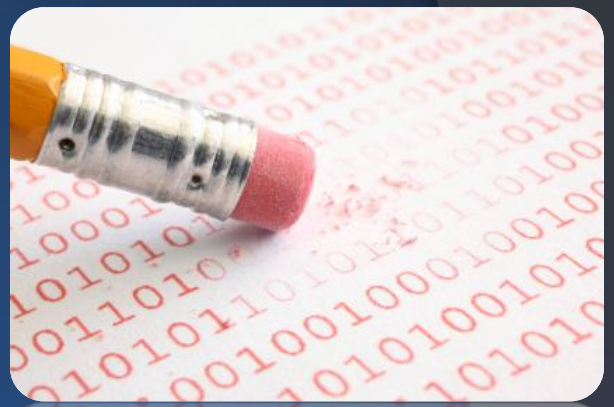
YOUR LAST PAYMENT OF $7.61 WAS RECEIVED ON 05/13/09

| METER NUMBER | METER READING PREVIOUS | PRESENT | TYPE OF CHARGE | METER MULTIPLIER | USAGE/UNIT | AMOUNT |
|---|---|---|---|---|---|---|
| 00317388 | 55,235 | 64,892 | ENERGY | | 9,657 KWH | 867.20 |
| | | | CUSTOMER/FACILITY CHARGE | | | 12.55 |
| | | | SALES TAX | | | 61.58 |
| ESTIMATED BILL | | | CURRENT BILL | | | 941.33 |
| | | | AMOUNT DUE | | | 941.33 |

IF PAYMENT IS NOT RECEIVED BY THE DUE DATE, A 3% LATE FEE WILL BE CHARGED ON THE ACCOUNT BALANCE.

# ERASING SOME MYTHS

- Internal vs. External
- In Signatures We Trust
- Defend, Defend…Pray
- Microsoft Problem?
- Damn the Insiders?
- We’re not a Target



# INTERNAL VS. EXTERNAL

## M&MS AREN'T GOOD.

- DMZs, well patched and defended
- Where is the E-mail and Internet access
- We can't just rebuild workstations
- In 2008, 95% of attacks were client-side 5% were server-side*
- Connected to the Internet vs. not.

*Source: Symantec Global Internet Security Threat Report

# IN SIGNATURES WE TRUST

## SIGNATURES = TOO LATE.

- A/V Don't set it and forget it
- A/V Perimeter and host-based
- Different vendors a good thing
- Good guys will NEVER catch up
- 2008 number of new malicious code signatures increased by 265% over 2007*

- Don't depend on anything with signatures.

<Demonstration>

*Source: Symantec Global Internet Security Threat Report

# DEFEND, DEFEND…PRAY

## WE ALL LOSE……EVENTUALLY.

- You've hardened your systems
- You've built many layers of defense
- You can't control everything, particularly users
- Months before big orgs become aware, why?
- Watch logs, learn about File Integrity

# MICROSOFT PROBLEM?

## 2008 TOP 10 RISKS

1. Browser Vulnerabilities
2. Rogue Anti-Virus/Social Engineering
3. SQL Injection
4. Malicious Web 2.0 Components
5. Adobe Flash
6. DNS Cache Poisoning/DNS Zone File Hijacking
7. Active X Vulnerabilities
8. RealPlayer Vulnerabilities
9. Apple QuickTime Vulnerabilities
10. Adobe Acrobat Reader PDF Vulnerabilities

Source - WebSense Security Labs


Note: 2/10 involve services in DMZ, 8/10 client-side

# DAMN THE INSIDERS?

## 2008 Attack Statistics

74% External Sources
20% Insiders
32% Business Partners
39% Multiple Parties

Source: 2009 Verizon Data Breach Investigations Report

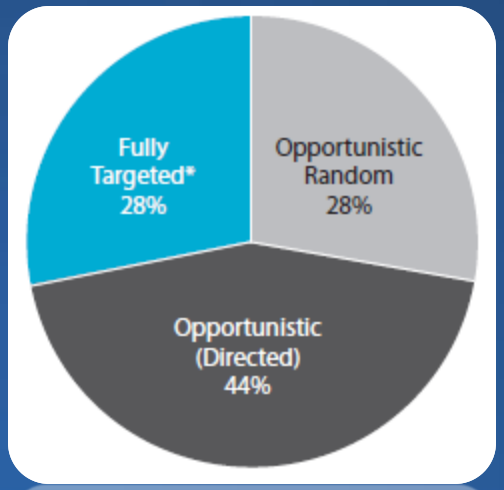
# EXTERNAL WHERE?

## 2008 Attack Statistics

| 2008 Rank | 2007 Rank | Country | 2008 Overall Percentage | 2007 Overall Percentage | Malicious Code Rank | Spam Zombies Rank | Phishing Websites Host Rank | Bot Rank | Attack Origin Rank |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | United States | 23% | 26% | 1 | 3 | 1 | 2 | 1 |
| 2 | 2 | China | 9% | 11% | 2 | 4 | 6 | 1 | 2 |
| 3 | 3 | Germany | 6% | 7% | 12 | 2 | 2 | 4 | 4 |
| 4 | 4 | United Kingdom | 5% | 4% | 4 | 10 | 5 | 9 | 3 |
| 5 | 8 | Brazil | 4% | 3% | 16 | 1 | 16 | 5 | 9 |
| 6 | 6 | Spain | 4% | 3% | 10 | 8 | 13 | 3 | 6 |
| 7 | 7 | Italy | 3% | 3% | 11 | 6 | 14 | 6 | 8 |
| 8 | 5 | France | 3% | 4% | 8 | 14 | 9 | 10 | 5 |
| 9 | 15 | Turkey | 3% | 2% | 15 | 5 | 24 | 8 | 12 |
| 10 | 12 | Poland | 3% | 2% | 23 | 9 | 8 | 7 | 17 |

**Table 2. Malicious activity by country**
*Source: Symantec*

# "WE'RE NOT A TARGET"




Source: Verizon Business Report

Random Opportunistic: Attacker(s) identified the victim while searching randomly or widely for weaknesses and then exploited the weakness.

Directed Opportunistic: Although the victim was specifically selected, it was because they were known to have a particular weakness that the attacker(s) could exploit.

Fully Targeted: The victim was first chosen as the target and then the attacker(s) determined a way to exploit them.

# STATISTICS, BLAH BLAH

## WHAT'S THE POINT?

- Include workstations in your processes and priorities
- Drop non-U.S. inbound traffic at the perimeter
  - 77% of malicious traffic dropped, ONE firewall rule
  - Extra CPU/Memory/Bandwidth for the good guys
- Don't lose track of insiders, limit access
- Restrict Internet access, including IT
- Business partners and remote workers on the rise (VPN)

  "The number of Americans working at home at least one day a month will rise from 28 million to 100 million by 2010." -WorldatWork

# THE PARADIGM SHIFT

- Client-side attacks are the most common attack vector.
- Treat workstations like servers if they have access to sensitive data
- With this shift, managing vulnerabilities becomes a larger operational problem
  - Requires more resources
  - More organized effort
  - More teamwork

# WARNING: BORING DEFINITION

Vulnerability Management:

The process of finding and fixing mistakes in software and configuration errors.

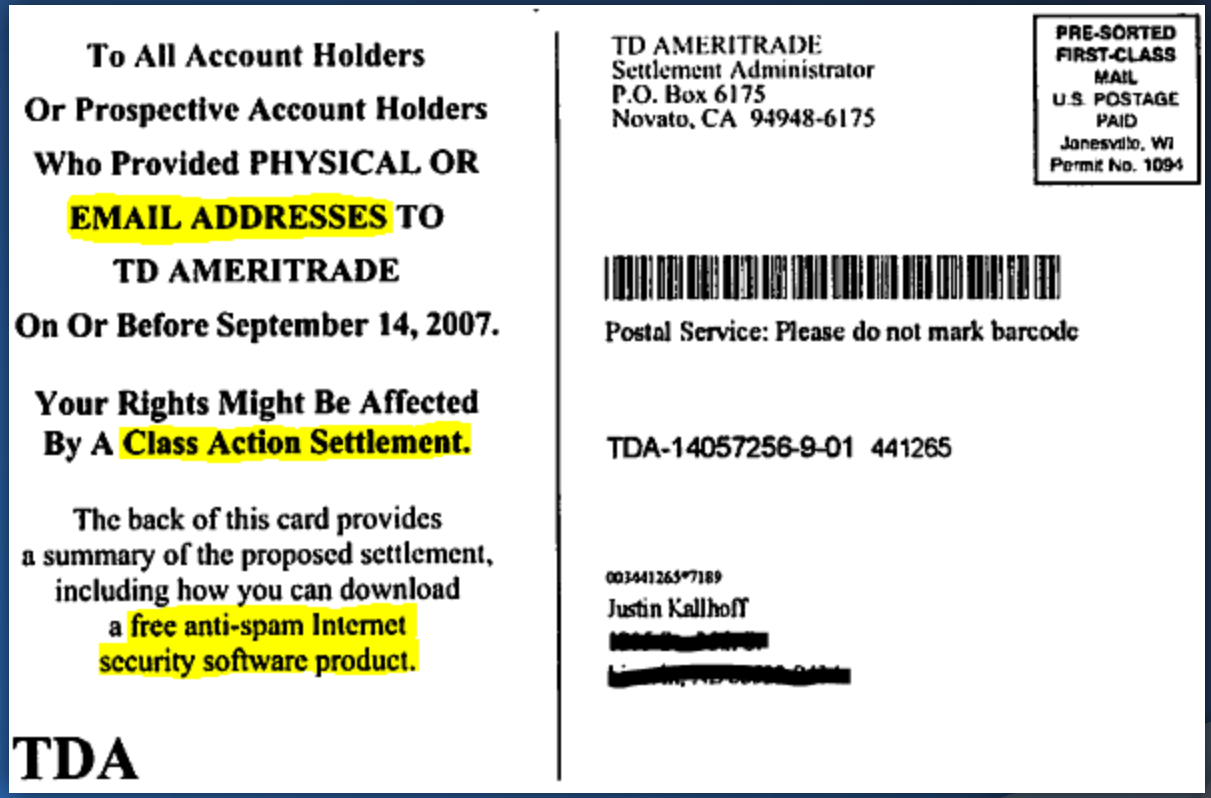
The standard assumption by computer scientists is 5 to 20 bugs in every thousand lines of software code.

# WHY DO I CARE?

The Risks:

- Money
- Reputation
- Customers
- Compliance
- Productivity and Time

# JUST CC#S, SSNS AND PII?



To All Account Holders
Or Prospective Account Holders
Who Provided PHYSICAL OR
EMAIL ADDRESSES TO
TD AMERITRADE
On Or Before September 14, 2007.

Your Rights Might Be Affected
By A Class Action Settlement.

The back of this card provides
a summary of the proposed settlement,
including how you can download
a free anti-spam Internet
security software product.

TDA

TD AMERITRADE
Settlement Administrator
P.O. Box 6175
Novato, CA 94948-6175

PRE-SORTED
FIRST-CLASS
MAIL
U.S. POSTAGE
PAID
Janesville, WI
Permit No. 1094

Postal Service: Please do not mark barcode

TDA-14057256-9-01 441265

0034412657189
Justin Kallhoff
[redacted]

# AVOID INFORMATION OVERLOAD

Scenario: You've just completed vulnerability scanning on your environment. You have 29,856 high severity vulnerabilities.

Question: Where the heck do you start?

Answer:
Vulnerability Management

# VULNERABILITY MANAGEMENT

## A PROCESS, NOT A TOOL

- Asset Discovery
- Risk Analysis
- Scanning
- Prioritize
- Assign
- Remediate
- Report
- Repeat

# ASSET DISCOVERY

- Quickly Identify Rogue Hosts/Services
- Network Awareness
- Network Inventory

# RISK ANALYSIS

If this host were to be compromised, what impact would it have on my business?

- Business Impact
  - Revenue Generation
  - Operational Impact
  - Reputation
  - Compliance

**Business Risk**

| Security Risk | Business Impact | | | | |
|---|---|---|---|---|---|
| Title: | Critical | High | Medium | Minor | Low |
| **5** | 100 | 64 | 36 | 16 | 9 |
| **4** | 64 | 36 | 16 | 9 | 4 |
| **3** | 36 | 16 | 9 | 4 | 2 |
| **2** | 16 | 9 | 4 | 2 | 1 |
| **1** | 9 | 4 | 2 | 1 | 1 |

# SCANNING AND ASSESSMENT

- Operating System/Resident Apps
- Network Services
- Web App Scans
- Policy Compliance Scans
- Authenticated Scanning!

# PRIORITIZE DISCOVERED VULNERABILITIES

Not always an obvious order of priority

Variables to Consider:

- Vulnerability Severity Level
- Risk Analysis Results
- Ease of Remediation/Automation

# ASSIGN & TRACK

- Assign vulnerabilities to individuals or groups responsible for the affected system(s).
- Track to ensure that the applied fix has resolved the vulnerability.
- Monitor to ensure the vulnerability does not return

# REMEDIATION
## THE HARD PART

- System hardening will reduce quantity
- Imaging reduces diversity and complexity
- Don’t allow users to install software
- If you fear breaking systems, create a test environment
- Manual remediation not an option for most organizations
  - Patch Management – Developing market, automate!

# REPORTING

- Demonstrate Progress
- Justify additional human resources
- Justify additional budget
- Compliance/Auditors
- Which boxes are running X or are vulnerable to Y exploit?

# REPEAT

FACT: There were ~150 Updates to Qualys' Vulnerability Database on 6/14-6/15 alone.

The vulnerability landscape changes daily. VM is a process that requires constant awareness.

Scheduled, automated, and regular scans

If scans break things, fix those problems.

Setting a goal of having all vulnerabilities eliminated at any given time is unattainable for most organizations.

So what do we do then to prevent compromise?

# DEFENSE IN DEPTH

| Easy and/or Low Cost | Moderate | High Cost and/or Difficult |
| --- | --- | --- |
| Hardening | Firewall +Egress | Physical |
| Patching | A/V Host/Perimeter | File Integrity |
| Audit Logs | Wireless | Penetration Testing |
| Centralized Logging | Education | NAC |
| Encryption | Vulnerability Mgmt | WAF |
| Fault Monitoring | | IPS |
| Trending | | Web Security |
| VPN | | |
| Proxy | | |
| Segmentation | | |
| Policy | | |

# EXECUTIVES:

Do they understand?
Answer: Nope.
Do they care?
Answer: Nope, until you get pwned.
Is it their fault?
Answer: Nope, it's yours.

Getting buy-in from the top is vital.
- Restrict access to the web
- Resource allocation to VM
- Pen tests can illustrate reality
- If you can't get buy-in, call me, I will.

# HOW TO DEPLOY MALWARE

## THE WEB 2.0 SHIFT

Step 1: Create a big FREE online network of humans
Step 2: Create a model of complete anonymous trust
Step 3: Allow anyone to post content anywhere
Step 4: Allow anyone to create and distribute applications
Step 5: Allow external advertising sources
Step 6: Name it Facebook, MySpace, Linkedin, or Twitter

HINT: Block all of them. You will get whine, be prepared with statistics and examples.

# TIGHT BUDGET?

Solutions:

1. Vulnerability Scanning (OpenVAS)
2. File Integrity Monitoring (Osiris)
3. Central Logging and Correlation (Splunk/SyslogNG)
4. Patching (WSUS,  Purgos)
5. VPN (OpenVPN)
6. Proxy (Squid)
7. Disk Imaging/Standardization (FOG)

Best Practices:

1. Egress (outbound) Firewall Rules
   - Not just about blocking your people
2. Servers NO Internet access
3. Hardening (NIST and Microsoft Templates)
4. Workstations ONLY 80, 443
5. Block executable content Web & Mail
6. Host File

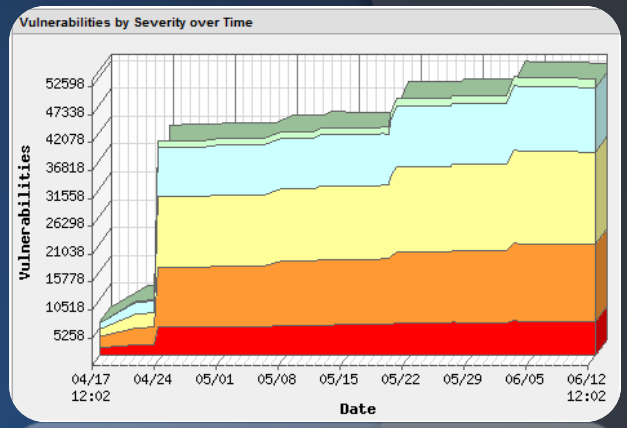
# COMMERCIAL SOLUTIONS ARE AFFORDABLE (SMB INCLUDED)

"Enterprises that implement a vulnerability management process will experience 90% fewer success attacks…" Source: Gartner

- Buffet
  - Entry Level Pricing ~$3,000/year
  - Unlimited scanning
  - 32 Internal, 4 External
- Ala Carte
  - Pay Per Scans
  - Approx. $20 per IP
  - Schedule Monthly, Quarterly, as often as possible

# TELL ME WHAT TO LOOK FOR!

- Authenticated scanning!
- Automation
- Rate and categorize risks
- Remediation tracking & ticketing
- Frequent updates
- Compliance
- Reporting, trending, historical




The Bottom Line:

Find, Confirm, Prioritize, Remediate, Rinse and Repeat

# MARKET FRESH

**STRONG POSITIVE**

QUALYS®

nCircle

POSITIVE

eEye Digital Security®

McAfee®

RAPID7
UNIFIED VULNERABILITY MANAGEMENT

PROMISING

IBM

StillSecure

TENABLE
Network Security®

CAUTION

Beyond Security

Critical Watch
VISIBILITY. MEASURABILITY. CONTROL

criston

Lumension®
IT Secured. Success Optimized.™

SAINT®

Source: Gartner (May 2008)

# PATCH MANAGEMENT SOLUTIONS


- BigFix


- Shavlik NetChk


- IBM Tivoli


- Altiris and Hercules


- Patch Authority/Desktop Authority


- Microsoft's SCCM


- Lumension (Patchlink)

# MISSING SOMETHING?

## MAJOR AREA OF VULNERABILITY NOT DISCUSSED?

HINT:

HUMANS! Security awareness training please!


Infogressive, Inc.