Hawaiian Telcom University 2014

Don’t be a target!

Stephan Tallent, CISSP, FCNSP
Director, MSSP - Americas

March 17, 2014
1. Threat Landscape
2. Security Trends
3. Recent Exploits
4. What can you do?
Data breach root causes

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=277)

- Malicious or criminal attack: 37%
- System glitch: 35%
- Human factor: 29%

Ponemon Institute, 2013 Cost of Data Breach Study
Cost per root cause

Figure 7. Per capita cost for three root causes of the data breach
Consolidated view (n=277). Measured in US$

- Malicious or criminal attack: $157
- System glitch: $122
- Human factor: $117

Ponemon Institute, 2013 Cost of Data Breach Study
Who is doing the hacking & why

- **Organized Crime – 57%**
  - Financially motivated – Eastern Europe – Romania 28%
  - Finance, Retail, Hospitality

- **State Affiliated – 21%**
  - Espionage motivated – China 30%
  - Manufacturing, Pro Services, Transportation

- **Hacktivists – 2%**
  - PR motivated – North America 18%
  - Public informational
How are they doing it

• **40% of Breaches - Malware**
  - #1 malware attack method – **Key logger**
  - 84% of malware was direct install
  - 95% of malware evaded Anti-virus

• **34% email attachments**
  - Downloaded through malicious email
  - Phishing attacks, CryptoLocker

• **26% Brute Force attacks**
  - Guessed or stolen credentials

*Verizon Business, 2013 Data Breach Investigation Report*
Who are the victims

- **Retail** – 21%
  - Financially motivated – Eastern Europe

- **Manufacturing** – 12.2%
  - Espionage motivated – China 30%

- **Information Services** – 10.4%
  - PR motivated – North America 18%

*Verizon Business, 2013 Data Breach Investigation Report*
Cost per record breached

Figure 4. Per capita cost by industry classification
Consolidated view (n=277). Measured in US$

- Healthcare: 233
- Financial: 215
- Pharmaceuticals: 207
- Transportation: 169
- Communications: 150
- Services: 134
- Technology: 129
- Research: 125
- Energy: 125
- Hospitality: 114
- Consumer: 113
- Education: 111
- Media: 103
- Industrial: 103
- Public services: 81
- Retail: 78
Customers lost following breach

Figure 14. Abnormal churn rates by country sample

Ponemon Institute, 2013 Cost of Data Breach Study
1. Threat Landscape
2. Security Trends
3. Recent Exploits
4. What can you do?
Security Trends

- **Security becoming a utility**
  - Too complex and subtle for most in-house IT
  - More strategic and economical to outsource

- **Cloud migration across verticals**
  - Security is an inhibitor and opportunity
  - Customers weighing cost benefits vs. potential risk

- **Firewall and AV no longer sufficient**
  - Unified Threat Management leads demand
  - Adaptive threat protection needed against ATPs
Traditional Defenses Don’t Work

• **Blended Threats increasing**
  - Web based threats increased by 30%
  - Social networking sites spoofing increased 125%

• **Advanced Persistent Threats**
  - 42% increase in targeted attacks
  - Crypto Locker, BlackPOS

• **All verticals under attack**
  - 31% of all targeted attacks aimed at businesses with less than 250 employees

MSS Market Demand

- **MSS market to reach $15B by 2015**
  - 14.7% CAGR from 2012 to 2017**
  - Global MSS market $9B in 2013*(Frost & Sullivan)
  - North America share = $3.06B*

- **Market Segment Dynamics**
  - SME MSS double to near 50% of the market in 2013/14
  - Enterprises adoption expands to $6.8B by 2017***

- **MSS Market Evolution**
  - Cloud MSS grows to 69% of market over next 5 years
  - CPE MSS dropping to 50%(from 57%) of market by 2017***

*Frost & Sullivan, **Gartner, ***Infonetics*
Agenda

1. Threat Landscape
2. Security Trends
3. Recent Exploits
4. What can you do?
2013 Threat Landscape Developments
2013 Threat Landscape Developments

- **IPMI Vulnerabilities Found**
  - Weak Authentication

- **BadBios**
  - Airgap Theory

- **TIFF Zero-Day**
  - Hangover Botnet

- **CryptoLocker**
  - US-CERT, CCIRC

- **Fokirtor**
  - Advanced Linux Worm

**Events:**
- **April:**
  - 700,000 SIM Cards Vulnerable
  - Trojanised Weapons

- **July:**
  - MobileRAT

- **Oct 20:**
  - 7 Zero-Day IPMI Vulnerabilities
  - Publicly Disclosed
  - SuperMicro

- **Oct 31:**
  - Android 81% Market Share

- **Nov 07:**
  - Q3 2013 (IDC):
  - 81M PC Shipments
  - 258.4M Smart Phone

- **Nov 12:**
- **Nov 27:**
Target

- **Russian Hacker writes and distributes**
  - Wrote Point of Sale malware – BlackPOS - $1,800

- **Scrapes card info from POS machines**
  - Downloaded through malicious email

- **40M credit and debit cards compromised**
  - Over 70 million customers affected

- **$30M in costs to credit unions & banks**
  - Card reissue, staffing customer service
CryptoLocker

• Ransomware Trojan
  ▪ Encrypts your data and holds hostage with deadline

• 25 million machines infected
  ▪ 70% in the US

• Email attachment – ‘UPS tracking notification’
  ▪ User prompted to open a zip file

• Completely evaded Anti-virus defenses
CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
http://...\..exe

Approximate destruction time of your private key:
10/19/2013 6:09 PM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.
1. Threat Landscape
2. Security Trends
3. Recent Exploits
4. What can you do?
Why common attacks succeed…

Bad guys are changing tactics;
Very rarely do we see direct attacks on the perimeter
Interaction of security services MUST happen to be effective
FortiGuard Minute

- 52,000 Spam e-mails intercepted
- 43,000 Network intrusion attempts resisted
- 20,000 Malware programs neutralized
- 3,100 Application control signatures
- 75 Terabytes Of Threat Samples
- 47,000 Attempts to access malicious websites blocked
- 65,000 Botnet command and control attempts thwarted
- 12,500 Vulnerability management signatures
- 70 Intrusion prevention signatures
- 75 Million Rated websites in 78 categories
- 8,000 Hours of research in labs around the globe
- 1000 Web application firewall attack signatures
- 235,000 New and updated antivirus definitions
- 250 Million New and updated antispyware signatures
- 725,000 URL ratings for web filtering
- 14 Million Website categorization requests
How do you defend your org?

- **Managed Security Services**
  - Reduce security TCO & leave it to the experts
  - Avoid security obsolescence

- **Unified Threat Management**
  - Security ‘swiss-army knife’
  - Advanced Threat Protection

- **Authentication**
  - Dual Factor Authentication

- **Education**
  - Internet Common Sense training
Unified Threat Management

TRADITIONAL SOLUTIONS
Cumbersome and costly

THE FORTINET SOLUTION
Simple and cost-effective
UTM Market Leader

A Leader in UTM for a 5th Consecutive Year
Fortinet Positioned as a Leader in Gartner’s UTM Magic Quadrant

- Position Magic Quadrant
  - Enterprise Firewall
  - Wired & Wireless Infrastructure
  - Security E-Mail Gateway
  - Application Delivery Controller

Gartner

2006–2013

2010–2013

2012–2013

2005–2013

Source: Gartner (July 2013)
# Features & Certifications

<table>
<thead>
<tr>
<th>Certification</th>
<th>Fortinet</th>
<th>Check Point</th>
<th>Cisco ASA</th>
<th>Juniper SRX</th>
<th>Palo Alto</th>
<th>SonicWALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS Labs FW</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>NSS Labs NGFW</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>NSS Labs IPS</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA NGFW Evaluation</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>BreakingPoint Resiliency Score</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA Firewall</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA IPSec</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA SSL VPN</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA IPS</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA Antivirus</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ICSA WAF</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Common Criteria</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>FIPS 140</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>DoD UC APL</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IPv6 Ready</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>VB100 Virus</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>AV Comparative</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>VB Verified Spam</td>
<td>•</td>
<td>•</td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
Security Market Leadership

Worldwide Security Appliance Market Share Q2 2013 (1)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Company</th>
<th>Market Share (%)</th>
<th>Growth Y/Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco</td>
<td>16.2</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>Check Point</td>
<td>12.5</td>
<td>4%</td>
</tr>
<tr>
<td>3</td>
<td>FORTINET</td>
<td>6.2</td>
<td>13%</td>
</tr>
<tr>
<td>4</td>
<td>Juniper</td>
<td>5.5</td>
<td>(19%)</td>
</tr>
<tr>
<td>5</td>
<td>Blue Coat</td>
<td>5.1</td>
<td>61%</td>
</tr>
<tr>
<td>6</td>
<td>McAfee</td>
<td>5.0</td>
<td>10%</td>
</tr>
<tr>
<td>7</td>
<td>Market Size</td>
<td>$8.5 Bil.</td>
<td></td>
</tr>
</tbody>
</table>

Notes
(1) IDC Worldwide Security Appliances Tracker, September 2013 (market share based on factory revenue)
Global Customers

Top 5 Global Carriers

Top 10 Fortune 500

Top 10 Global 500 Banks
Recap

1. Threat Landscape
2. Security Trends
3. Recent Exploits
4. What can you do?
Thank You