Dell SecureWorks

Counter Threat Unit Research Team
- Elite cyber intelligence talent focuses on threat actors, tradecraft and countermeasures

Counter Threat Platform
- Next generation technology applies intelligence to protect thousands of customers worldwide

Certified Security and Compliance Experts
- 1,000+ security and compliance professionals deliver award-winning services and customer satisfaction

Global Security Operations Centers
- 7 resilient, high-security facilities provide vendor-neutral, in-region service delivery 24x7x365

We help thousands of organizations protect against cyber threats, simplify regulatory compliance and embrace innovation securely.
The Internet is “where the bad guys will go because that’s where our lives are, and our money, our secrets and our intellectual property,”

James Comey, FBI Director
Role of a managed security service provider

Increase risk
Reduce reward
Increase effort
Dell SecureWorks delivers a comprehensive suite of information security services powered by our proprietary technology, global threat visibility and deep security expertise.
Recently ranked in Gartner’s “Market Trends: Managed Security Services, Worldwide, 2013” report as the number one MSSP to watch.
Cyber Security Threatscape
SMBs targeted more than ever

- Large business are fortifying their defenses
- Easy money
- Cyber criminals aren’t choosy
- Path of least resistance
- “low-hanging fruit”
- Gateway to ultimate target
- Malware testing ground

“Cybercriminals go after the big guys”
“Our core provider provides security”
“I don’t have any valuable data or assets”
Cyber Threat Macro Trends

- **Notoriety**: Basic Intrusion & Viruses
- **Fame**: Viruses & Malware
- **Financial Theft & Damage**
- **National Interests**
  - Government Data/Networks
  - Defense Industrial Base

Timeline:
- 1990
- 1995
- 2000
- 2005
- 2007
- 2010
- 2014
The threat landscape

**Malware**
Malicious software that disrupts computer operation, gather sensitive information, or gain unauthorized access to computers

Computer viruses, worms, trojan horses, spyware, adware

**Advanced Threats**
A sophisticated and organized cyber attack to access and steal information from compromised computers

**DoS & DDoS**
Denial-of-Service
Distributed Denial-of-Service
An attempt to make a computer or network resource unavailable to its intended users

**Cyber Warfare**
Politically motivated hacking to conduct sabotage and espionage
Cyber attacks edging out terrorism as No. 1 threat to U.S.

“In the not too distant future, we anticipate that the cyberthreat will pose the No. 1 threat to our country.”

“No company is immune, from the Fortune 500 corporation to the neighborhood ‘mom and pop’ business.”

“I am convinced there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Source: FBI Director Robert Mueller Speaking at 2012 RSA Conference
## According to top cyber security experts

<table>
<thead>
<tr>
<th>Companies need to do more than just <em>react</em> to intrusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking – or the costs they may have already suffered.</td>
</tr>
<tr>
<td>He doesn’t believe there is a single secure, unclassified computer network in the U.S.</td>
</tr>
<tr>
<td>FBI agents are increasingly coming across data stolen from companies whose executives had no idea their systems had been accessed.</td>
</tr>
<tr>
<td>In cases handled by one computer security firm where intrusions were traced back to China, 94% of the targeted companies didn’t realize they had been breached until someone else told them.</td>
</tr>
</tbody>
</table>

“In many cases, the skills of the adversaries are so substantial that they just leap right over the fence and you don’t even hear an alarm go off.”

Source: “U.S. Outgunned in Hacker War”
Motivations behind cyber crime

• Gain financial advantage

• Intelligence gathering

• Gain competitive advantage

• Damage organizations’ brand, reputation and systems

• Obtain indirect access to a targeted business partner

• Prepare the field of battle for cyber warfare
Criminal to Criminal

Increase in criminal-to-criminal activity

- Exploit auction houses (WabiSabiLabi)
- Forums and IRC (#Vxers, cybermafia.cc)
- Distribution service (IFRAMES.BIZ)
- Botnet rental (5Socks.net)
- Licensing model (storm worm)
- Identity auctions (76service)
- Social networks (ranking and escrow)
## Identity Theft Market Value

<table>
<thead>
<tr>
<th>Category</th>
<th>US Based Credit Card</th>
<th>Non-US Credit Card</th>
<th>Prestige Credit Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card</td>
<td>$1 - $2</td>
<td>$2 - $10</td>
<td>$200 - $400</td>
</tr>
<tr>
<td>PayPal account, verified balance</td>
<td>$2 - $200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised Computer</td>
<td>$1 - $100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verified PayPal Account w. balance</td>
<td>$50 - $500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Premium Skype Acct.</td>
<td>$1 - $100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Game Accounts</td>
<td>$100 - $1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Med. Health Record</td>
<td>$50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Impact of Cyber Crime

---

**Fortune 500**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Company Name</th>
<th>Revenues ($b)</th>
<th>Profits ($mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wal-Mart Stores</td>
<td>469.2</td>
<td>16,999</td>
</tr>
<tr>
<td>2</td>
<td>Exxon Mobil</td>
<td>449.9</td>
<td>44,880</td>
</tr>
<tr>
<td>3</td>
<td>Chevron</td>
<td>233.9</td>
<td>26,179</td>
</tr>
<tr>
<td>4</td>
<td>Phillips 66</td>
<td>169.6</td>
<td>4,124</td>
</tr>
<tr>
<td>5</td>
<td>Berkshire Hathaway</td>
<td>162.5</td>
<td>14,824</td>
</tr>
<tr>
<td>6</td>
<td>Apple</td>
<td>156.5</td>
<td>41,733</td>
</tr>
<tr>
<td>7</td>
<td>General Motors</td>
<td>152.3</td>
<td>6,188</td>
</tr>
<tr>
<td>8</td>
<td>General Electric</td>
<td>146.9</td>
<td>13,641</td>
</tr>
<tr>
<td>9</td>
<td>Valero Energy</td>
<td>138.3</td>
<td>2,083</td>
</tr>
<tr>
<td>10</td>
<td>Ford Motor</td>
<td>134.3</td>
<td>5,665</td>
</tr>
</tbody>
</table>

#1 - Hacker’s Inc.

- Would be the largest company in the world
- Translate costs into "hacker revenue"
- Global costs of cyber crime is $500B

* - Center for Strategic and International Studies (CSIS) 2013
Losses due to “traditional” crimes

Cybercrime vs. traditional crime

Bank Robbery, etc.  ZeuS Group A

Recovered  Net Loss
Incident by Breach Type – May 2014

52% of breaches are hacker activity

Source: OSF DataLossDB
Incidents by Source – May 2014

63% of incidents originate outside your 4 walls

Source: OSF DataLossDB
Vulnerability trend – year over year

Source: Dell SecureWorks Counter Threat Unit Intelligence
Top Ten Hacking Countries

“There are no safe neighborhoods... All of us are next-door neighbors on the Internet in the blink of an eye.”

FBI Director James Comey

1. China
2. Turkey
3. Russia
4. Taiwan
5. Brazil
6. Romania
7. India
8. Italy
9. Hungary
10. South Korea
2013 Midsize Data Breaches - A sampling

- Vendini 56,000
- SnapChat 4,700,000
- Sun and Sight Eyeworks 9,000

- PlaySpan 100,000
- Kirkwood Community College 110,000
- Evernote 50,000,000

- High Tech Crime Solutions 32,000
- Hickory Grove Gas Station 100
- Network Solutions 500,000+
Theat Intelligence
The Counter Threat Unit

**Top security talent in the industry**
- Former CERT, Army Global NOSC, USCYBERCOM, DoD, Natl. Labs, CISOs and SANS instructors

**Highly regarded in the security community**
- Black Hat, DEFCON, ShmooCon, ToorCon, DeepSec, U.S. DoD Cyber Crime Conference, CERT-EE, AusCERT, Hacker Halted, RECON, APWG

**1,000+ security and compliance experts**
- CISSP
- INFOSEC
- CISA
- GIAC GCIA
- GIAC GSEC
- GIAC GCFW
- GIAC GCIAH
- GIAC GCFA
- GIAC GCWN
- GIAC GPEN
- CCDP
- CCNA
- CCSE
- CSPFA
- CSVN
- CSIDS
- CCSP
- CCIE
- CCSA
- CCDA
- CCNP
- INFOSEC
- MCSA
- MCSE
- MCP+I
- MCSE+I
- PMP
- NCSA
- CFE
- CCSI
- CEH
- NOP

Highly regarded in the security community
- Black Hat, DEFCON, ShmooCon, ToorCon, DeepSec, U.S. DoD Cyber Crime Conference, CERT-EE, AusCERT, Hacker Halted, RECON, APWG
CTU’s strategic focus

Focused on “who” and “how”
- Threat actors and their missions
- Tradecraft used in attacks
- “Kill chain” – how to disrupt attack process

Elite cyber-intelligence experts
- Current and historical rich attack data
- World-class intelligence platform and tools
- Industry and law enforcement relationships

CTU

- Hactivists
- AV Vendors
- Organized Cybercrime
- IPS Vendors
- Script Kiddies

Commodity

Targeted

Advanced
Global Threat Visibility

- 70+ Countries
- 3K+ Customers
- 1K+ Security Pros
- 200+ Software Engineers
- 100K+ Devices
- ~70B Daily Cyber Events
- 3000+ Daily Escalations

24 x 7 x 365

Locations:
- Chicago, IL
- Plano, TX
- Myrtle Beach, SC
- Providence, RI
- Atlanta, GA
- Edinburgh, Scotland
- London
- Bucharest, Romania
- Noida, India
- Bangalore, India
- Hyderabad, India
- Bucharest, Romania
- Kiev, Ukraine
- Guadalajara, Mexico
- Round Rock, TX
- Kawasaki, Japan
- London
- Sydney
Risk-based approach

Direct loss risk

Risk to reputation

Lost revenue, data

Lose market share

Litigation, civil damages

Fines, penalties

Liability risk

Compliance risk
Real-time monitoring and analysis

Technology

3 Firewalls
3 IDS / IPS
50 Servers / Other

510,618,423 events
506,813,197
Counter Threat Appliance and CTP Agent
3,803,598
3,805,226
207,499
207,499
Anomaly Filter
1,628

Event Consolidation
Logic/Correlation Engines

People & Process

Incident Handling Process: Aggregate, Correlate, Categorize, Assess Threat, and Respond

Security Event Benign
5,532 Events

Low Threat
Incident is logged for future correlation and reporting, but no further action required.

Medium Threat
Security Event Worm - Client Not Vulnerable
1 Incident (21 Events)
Security Event Suspicious Activity
3 Incidents (32 Events)

Security Event System / Application
1 Incident 48 Events

High Threat
Incident requires immediate intervention by Dell SecureWorks and the customer to prevent and/or remediate availability or security issue.

Information from Intelligence, Scanning, Trending & Auditing

Classification: //Dell SecureWorks/Confidential - Limited External Distribution:
The 50/30/20 Security Rule – Layered Security

50%
- Firewall
- First line of defense

30%
- Intrusion Prevention
- Identifies, examines and investigates

20%
- Servers, routers, switches, AND endpoints
- Securely direct traffic
Be proactive

• Test and assess
• Invest in prevention
• The 50/30/20 Security Rule
• Enable compliance
• Security awareness training
• Documented and tested incident response plan