Cyber Security Threats
Are you an easy target?

Vint Cerf: "My thought at the time, thirty-five years ago, was not to build an ultra-secure system, because I could not tell if even the basic ideas would work. We never got to do the production engineering. Unfortunately, the bad guys know this full well, and are exploiting it to the limit".
Cyber crime: average company loss in selected countries 2016

Average costs of cyber crime in selected countries as of August 2016
(in million U.S. dollars)

- United States: 17,36
- Japan: 8,39
- Germany: 7,84
- United Kingdom: 7,21
- Brazil: 5,27
- Australia: 4,3

Evolution average costs US
(in million U.S. dollars)

- FY 2013: 11,56
- FY 2014: 12,69
- FY 2015: 15,42
- FY 2016: 17,36

Source: Ponemon Institute - HP Enterprise Security (August 2016)

The Industrialization of Hacking

Attackers and defenders drive each other to innovate...
...resulting in distinct threat cycles
Hacking Generations

Generation Five

- Formation of an active underground economy
- Cybercrime has recently been developing at a much faster rate
- All the tools of the trade are now for sale
- Cybercrime has its own social networks with escrow services
- Malware can be licensed and receive tech support
- You can rent botnets by the hour, for your own crime spree
- Pay-for-play malware infection services have appeared that quickly create botnets. Lively market for zero-day exploits has been established
Congressional Testimony given by Ed Amoroso, Chief Security Officer from AT&T, and General Alexander, the former Director of the NSA.
Cybercriminal pyramid

FBI: The Zeus Fraud Scheme

Cyber Theft Ring

Malware exploiters purchase malware and use it to launch attacks on victims’ computers. They construct networks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.

Money mule networks are comprised of individuals who are paid for the transfer of stolen funds. They receive a percentage for their services.

Victims include individuals, businesses, and financial institutions.

1. Malware coder writes malware, which is sold on the black market.
2. Money mule is approached by fraudsters.
3. Money mule agrees to transfer money.
4. Malware exploiters manipulate victim’s computer.
5. Money mule transfers money to victim’s bank account.
6. Money mule logs into victim’s online bank account.

How the Fraud Works

Victims are both individuals and owners of compromised machines.

Malware exploiters

Money mule

Victims

mule organization

malware coder/exploiters

Global Reach

Law Enforcement Response To Date:

- Total FBI cases: 390
- Attempted fraud: $2.7 million
- Actual loss: $70 million

United States: 92 charged and 39 arrested
United Kingdom: 29 arrested and eight search warrants
Ukraine: Five detained and eight search warrants
Global domination: locations where the GOZ/CryptoLocker virus has struck computers

Layers of the Internet

SURFACE WEB
Indexed content
Can be found with traditional search engines like Google and accessed with traditional browsers.

DEEP WEB
Indexed and unindexed content
Cannot be found with traditional search engines. Might require password or network permissions.

DARK WEB
Intentionally hidden content
Can be accessed with special software like Tor. Might require password or network permissions.
How TOR Works

Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.
Criminal & popular topics in the Dark Web
Silk Road
We only seeing the tip of the Iceberg

Headline Grabbing Attacks

Tens of Thousands More Below the Surface

APT Attacks
Zero-Day Attacks
Polymorphic Attacks
Targeted Attacks
Shadow Brokers VS. Equation Group

CyberWarfare begins
Attacks (http://www.speedguide.net/ports.php)
Number of newly added ransomware families, 1H 2016

- During the first three months of the year, the FBI revealed that ransomware caused enterprises a total of US$209 million in monetary losses.
- Australia is the most targeted country on earth for mobile banking trojans and is also a juicy target for ransomware attacks.
- Australia experience 1.42 per cent of all infections in the world.
- The percentage of ransomware attacks out of all recognised attacks globally almost doubled in the second half of 2016, from 5.5 per cent to 10.5 per cent (Checkpoint).
- Aside from ransomware helping cybercriminals to extort money from businesses, they had also caused businesses to shut down temporarily.
- According to a white paper from Osterman Research, it is at “epidemic” levels, with nearly 50 percent of U.S. companies experiencing a ransomware attack.
- During the past year Ransomware became one of the most dangerous cyberthreats.
- Global losses now likely running to hundreds of millions of dollars.
Ransomware strikes Australia

Factor Detections Increased

October 15 | November 15 | December 15 | January 16 | February 16 | March 16
---|---|---|---|---|---
1 | 5 | 9 | 11 | 12 | 153

Series 1
Ransomware: nine best security practices to apply now

1. Backup regularly and keep a recent backup copy off-line and off-site. Encrypt your backup
2. Enable file extensions
3. Open JavaScript (.JS) files in Notepad
4. Don’t enable macros in document attachments received via email
5. Be cautious about unsolicited attachments
6. Don’t give yourself more login power than needed
7. Consider installing the Microsoft Office viewers
8. Patch early, patch often
9. Stay up-to-date with new security features in your business applications
Internet of Things (IoT)
The Social Engineering Attack Cycle

1 - Information Gathering
2 - Development of Relationship
3 - Exploitation of Relationship
4 - Execution to Achieve the Objective

2002 Gartner G2
Social Engineering Attack

“Amateurs hack systems, professionals hack people” - Bruce Schneier

Diagram with nodes labeled as:
- Social Engineer
- Target
- Compliance Principles
- Medium
- Goal
- Techniques

Connections:
- Individual
- Group of Individuals
- E-mail
- Face to Face
- Telephone
- SMS
- Paper Mail
- Storage Media
- Webpage
- Pamphlets
- Friendship or Liking
- Commitment or Consistency
- Scarcity
- Reciprocity
- Social Validation
- Authority
- Direct Communication
- Bidirectional Communication
- Unidirectional Communication
- Indirect Communication
- Financial Gain
- Unauthorised Access
- Service Disruption
- Phishing
- Pretexting
- Baiting
- Quid Pro Quo
Apparently, the criminals behind BackDoor.BlackEnergy.36 are the same people who used earlier versions of programs in this malicious family. This assumption is supported by the fact that BackDoor.BlackEnergy.36 utilizes the same encryption key that was used by some bots controlled from servers brought down in summer 2012.

Recall that BackDoor.BlackEnergy BlackEnergy is a complex multi-component malware primarily used for spamming. It enabled criminals to create one of the largest spam botnets, capable of sending as many as 18 billion messages per day at its peak period of activity. BackDoor.BlackEnergy programs download their modules and the xml configuration file from a control server.
The Silver Bullet Does Not Exist…

- "Block or Allow"
- "It matches the pattern"
- "No key, no access"
- "No false positives, no false negatives"
- "Self Defending Network"
- "Fix the Firewall"
- "Detect the Unknown"
- Sandboxing
- Application Control
- IDS / IPS
- UTM
- PKI
- AV
- FW / VPN
Cyber Economics

Lower Cost to Attack then Defend

Attack surface growing:

- Cyber Hacktivists Organize & Target Focused Attacks;
- Fully Funded Organized Crime – Focused Attacks;
- Nation State Sponsored/Rouge Attacks

Cost to attack

Policy Effectiveness

Cost to defend

Cyber Warfare Symmetry

Cyber Resilience

info@intecracy.com.au
General approach to information security and cybersecurity

- ISO/IEC 27032 Information technology — Security techniques — Guidelines for cybersecurity

Additional:
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
Practical Application

1. Implementation and monitoring of laws and regulations
2. Business continuity plan & risk management
3. Disaster recovery planning
4. Implementation and monitoring physical security
5. Implementation and monitoring virtual security
6. Incident response plans (Selecting team members, Define roles, responsibilities and lines of authority, Define a security incident, Define a reportable incident, Training, Detection, Classification, Escalation, Containment, Eradication, Documentation)
Thank you for your attention

intecracy.com.au
alexkis@intecracy.com.au

info@intecracy.com.au