The challenge

• A data security breach can put a business out of business or create serious unbudgeted costs

• To survive in today’s hostile environment SMBs must
  – Hold the line against older threats like physical theft and corrupt insiders, while addressing more recent concerns like spear-phishing, online scams, fraud and company data on mobile devices (which may not belong to the company)
The survival guide

- Build a road map and checklist
- Help SMBs navigate the current security landscape
- Stay one step ahead of the bad guys
  - What do “they” want?
  - How do they go after it?
What's the value of a hacked or stolen PC, Mac, smartphone, tablet or server?

<table>
<thead>
<tr>
<th>Web server</th>
<th>Botnet activity</th>
</tr>
</thead>
</table>
| • Phishing site  
  • Malware download site  
  • Warez piracy server  
  • Child porn server  
  • Spam site | • Spam zombie  
  • DDoS extortion zombie  
  • Click fraud zombie  
  • Anonymization proxy  
  • CAPTCHA solving zombie |

<table>
<thead>
<tr>
<th>Email attacks</th>
<th>Account credentials</th>
</tr>
</thead>
</table>
| • Harvest email contacts  
  • Harvest associated accounts  
  • Access to corporate email  
  • Webmail spam  
  • Stranded abroad scams | • eBay/PayPal fake auctions  
  • Online gaming credentials  
  • Website FTP credentials  
  • Skype/VoIP credentials  
  • Encryption certificates |

<table>
<thead>
<tr>
<th>Virtual goods</th>
<th>Financial credentials</th>
</tr>
</thead>
</table>
| • Online gaming characters  
  • Online gaming goods/$$$  
  • PC game license keys  
  • OS license key | • Bank account data  
  • Credit card data  
  • Stock and 401K accounts  
  • Wire transfer data |

<table>
<thead>
<tr>
<th>Reputation hijacking</th>
<th>Hostage attacks</th>
</tr>
</thead>
</table>
| • Facebook  
  • Twitter  
  • LinkedIn  
  • Google+ | • Fake antivirus  
  • Ransomware  
  • Email account ransom  
  • Webcam image extortion |

Based on original work by Brian Krebs: krebsonsecurity.com
The face of cybercrime today

- Well-funded
- Organized
- Efficient
- Skilled
- Global
- Relentless
- Expanding

www.fbi.gov/wanted/cyber
Tools of the trade

Spy Eye v1.2

Find INFO  Statistic  FTP accounts  Settings
Screen shots  BOA Grabber  CC Grabber  Certificate Grabber

Create task for Billing  Modify Cards  Tasks Statistic  Bots Monitoring
Full Statistic  Create task for Loader  Update Bot  VIRTEST
Plugins  FTP backconnect  SOCKS 5  Settings

Hack the Planet!

Take your money!

ABOUT
Serenity was developed privately and coded completely from scratch. In order to increase efficiency and FUD time, only the most effective and recent exploits were selected for inclusion.

Exploits:
- RFI
- OS Command
- Java 7 Applet
- Java Atomic
- Adobe 5.0/7.0/9.0
- MDAC

In order to maintain an irreplaceability for long amounts of time, Serenity will be sold exclusively to a small amount of customers. Full details are available through inquiry at: saka23@sabber.org

FEATURES
- Dynamic code encryption on a per-cluster basis
- FUD Encrypted iframe generation
- and much more...

SCREENSHOTS

PRICES

<table>
<thead>
<tr>
<th>Price</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>$150</td>
<td>1 Week Rental</td>
</tr>
<tr>
<td>$250</td>
<td>2 Week Rental</td>
</tr>
<tr>
<td>$400</td>
<td>1 Month Rental</td>
</tr>
</tbody>
</table>

* A free trial is available for serious customers. Prices are subject to change.
Sophisticated, profit-seeking, market-based economy

- Specialization
- Modularity
- Division of labor
- Standards

Markets
The SMB sweet spot for the cyber-criminally inclined

- Assets worth looting
- Level of protection

Big enterprise
SMB "sweet spot"
Consumers
720 security breaches analyzed by size of organization (employees)

Verizon 2012 Data Breach Investigations Report
The road map goes A B C D E F

Assess your assets, risks, resources
Build your policy
Choose your controls
Deploy controls
Educate employees, execs, vendors
Further assess, audit, test
Assess your assets, risks, resources

• **Assets**: digital, physical
  – If you don't know what you've got
  – You can’t protect it!

• **Risks**
  – Who or what is the threat?

• **Resources**
  – In house, hired, partners, trade groups, associations
Build your policy

• Security begins with policy
• Policy begins with C-level buy-in
• High-level commitment to protecting the privacy and security of data
• Then simple rules for how to control access
Choose the controls you will use to enforce your policies

For example:

– Only authorized employees can access certain data
– Control: Require identification and authentication of all employees via unique user name and password
– Limit access through application(s) by requiring authentication
– Log all access
Deploy controls and make sure they work

• Put control in place; for example, antivirus (anti-malware, anti-phishing, anti-spam)

• Test control
  – Does it work technically?
  – Does it “work” with your work?
  – Can employees work it?
Educate employees, execs, vendors, partners

• Everyone needs to know
  – What the security policies are, and
  – How to comply with them through proper use of controls
• Pay attention to any information-sharing relationships
  – Vendors, partners, even clients
• Clearly state consequences of failure to comply
Further assess, audit, test...
This is a process, not a project

- Lay out a plan to assess security on a periodic basis
- Plan to stay up-to-date on emerging threats
- Be vigilant around change
  - New vendor relationships
  - Employees departing
  - Hiring practices
Checklist

• Do you know what data you are handling?
• Do your employees understand their duty to protect the data?
• Have you given them the tools to work with?
• Can you tie all data access to specific people, times and devices?
Checklist (continued)

• Have you off-loaded security to someone else?
  – Managed service provider
  – Privacy cloud provider
  – Public cloud provider

• Be sure you understand the contract
  – You can’t off-load your liability
  – Ask how security is handled, what assurances are given
Checklist (continued)

• Firewalls, AV scanners, encryption
  – Not perfect, but they do the heavy lifting

• Physical security
  – Premises
  – Devices (password protected?)
  – Services

• Beyond passwords
  – Two-factor authentication (2FA)
  – Soft or hard tokens, biometrics
If you could only check 2 things?

How do data breaches occur?
1. Malware involved in 69% of breaches
2. Hacking* used in 81% of breaches
   Breaches combining malware and hacking: 61%

*80% of hacking is passwords: default, missing, guessed, stolen, cracked

Verizon 2012 Data Breach Investigations Report
The Top 2 Things?

Two main attacks: Malware, Hacking

...and defenses: Scanning, Authentication
Scanning requires proper implementation

AV use at a sample of 80 healthcare facilities

- Require AV on mobile devices
- Scan devices prior to connection
- Scan devices while connected

Ponemon Institute Third Annual Benchmark Study on Patient Privacy & Data Security
Authentication requires more than passwords

Passwords exposed in 2012: **75,000,000**
And those are just the ones we know about
Need to add a second factor to authentication
The Top 2 Things

Malware → SMART Scanning

Hacking → STRONG Authentication

Plus policies and training to implement effectively
THANK YOU ★ STEPHEN COBB
stephen.cobb@eset.com ★ WeLiveSecurity.com