The SMB Cyber Security Survival Guide

Stephen Cobb, CISSP

Security Evangelist

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?

Web server

- Phishing site
- Malware download site
- Warez piracy server
- Child porn server
- Spam site

Botnet activity

- Spam zombie
- DDoS extortion zombie
- Click fraud zombie
- Anonymization proxy
- CAPTCHA solving zombie

Email attacks

- Harvest email contacts
- Harvest associated accounts
- Access to corporate email
- Webmail spam
- Stranded abroad scams

Account credentials

- eBay/PayPal fake auctions
- Online gaming credentials
- Website FTP credentials
- Skype/VoIP credentials
- Encryption certificates

Virtual goods

- Online gaming characters
- Online gaming goods/$$$
- PC game license keys
- OS license key

Financial credentials

- Bank account data
- Credit card data
- Stock and 401K accounts
- Wire transfer data

Reputation hijacking

- Facebook
- Twitter
- LinkedIn
- Google+

Hostage attacks

- Fake antivirus
- Ransomware
- Email account ransom
- Webcam image extortion

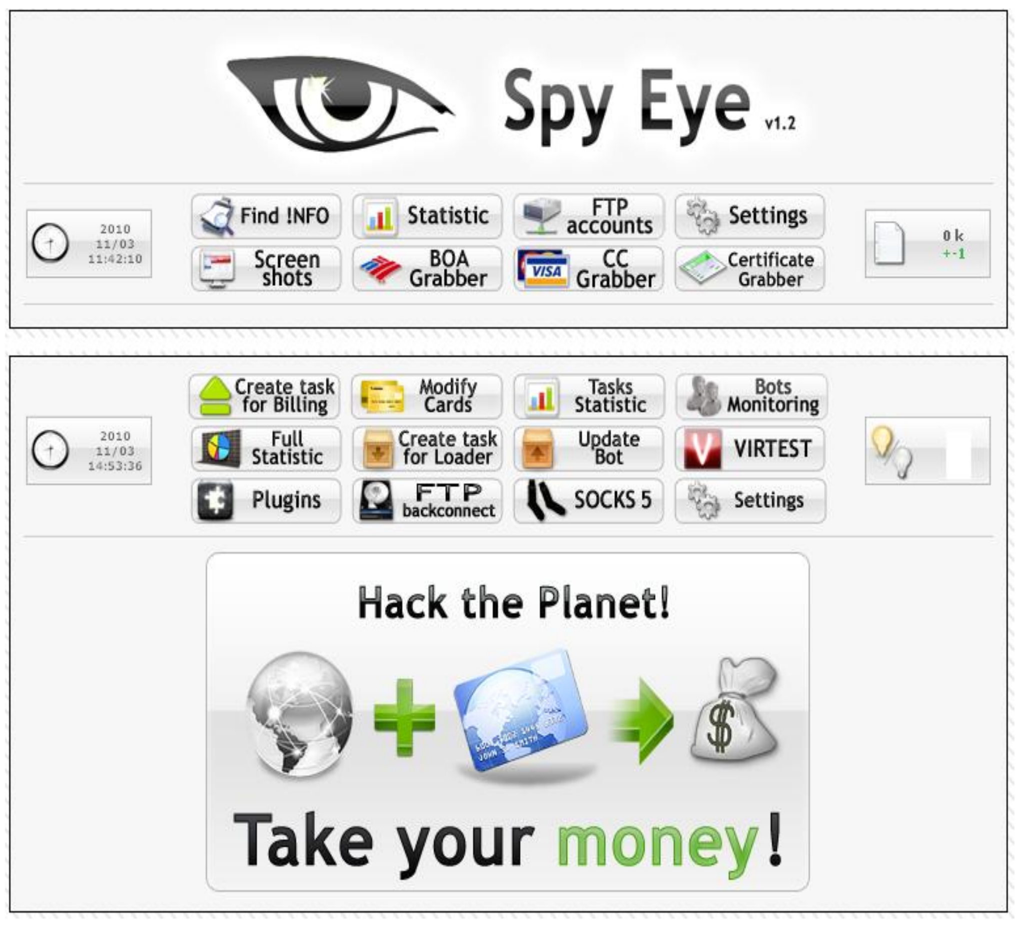
Based on original work by Brian Krebs: krebsonsecurity.com

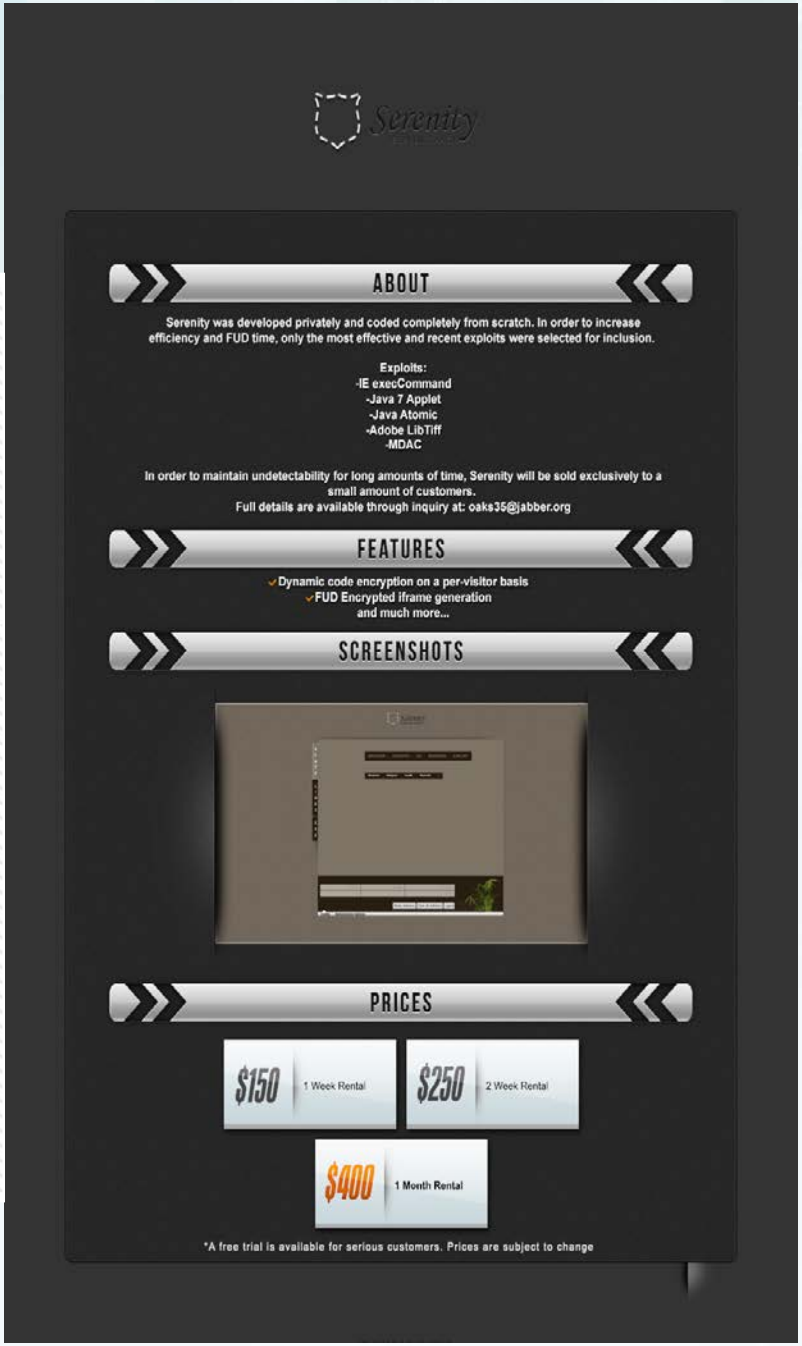
The face of cybercrime today

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

www.fbi.gov/wanted/cyber

Tools of the trade





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:
-IE execCommand
-Java 7 Applet
-Java Atomic
-Adobe LibTiff
-MDAC

In order to maintain undetectability for long amounts of time, Serenity will be sold exclusively to a small amount of customers.
Full details are available through inquiry at: oaks35@jabber.org

FEATURES

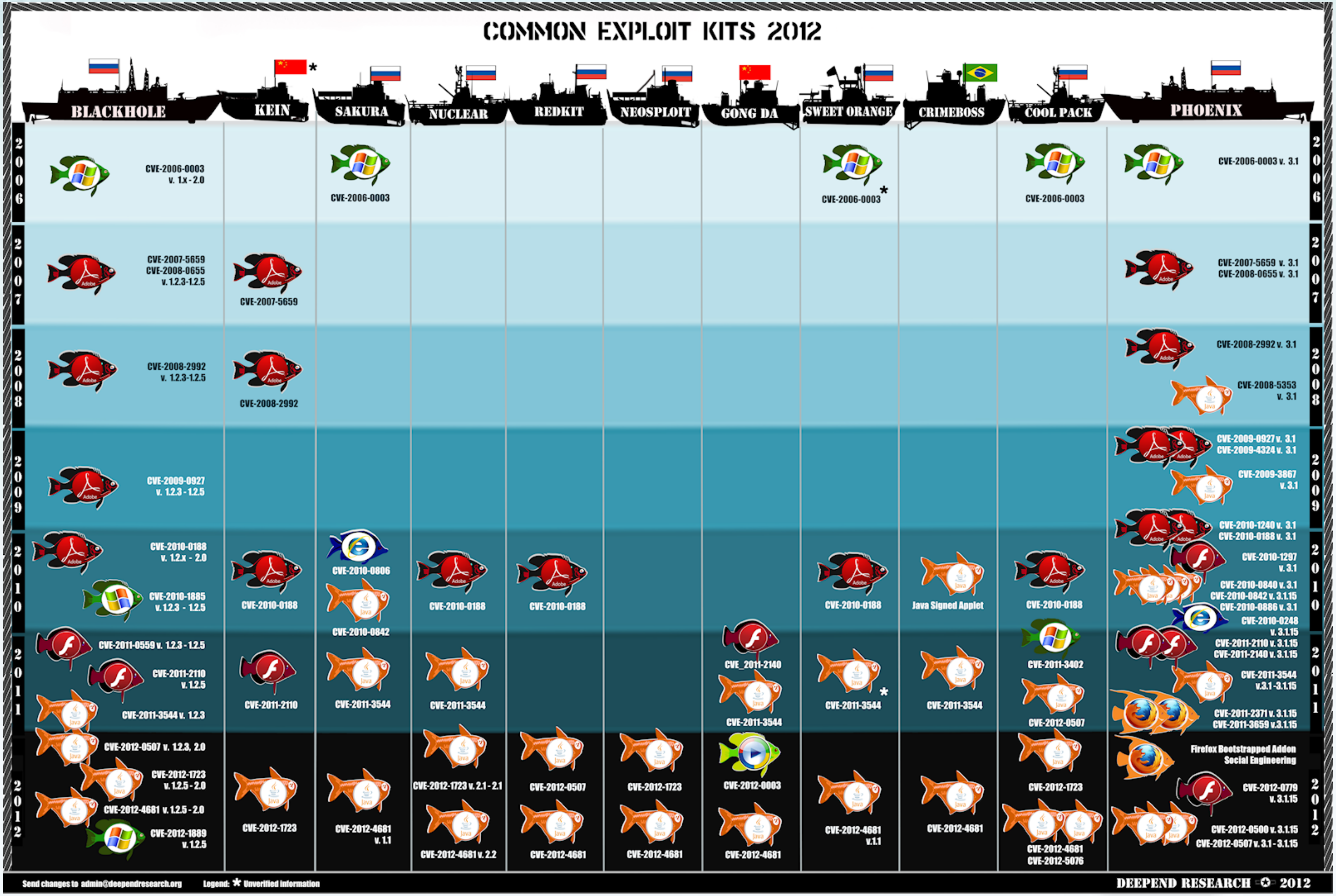
✓Dynamic code encryption on a per-visitor basis
✓FUD Encrypted iframe generation
and much more...

SCREENSHOTS

PRICES

$150	1 Week Rental
$250	2 Week Rental
$400	1 Month Rental

*A free trial is available for serious customers. Prices are subject to change



COMMON EXPLOIT KITS 2012

	BLACKHOLE	KEIN *	SAKURA	NUCLEAR	REDKIT	NEOSPLOIT	GONG DA	SWEET ORANGE	CRIMEBOSS	COOL PACK	PHOENIX
2006	CVE-2006-0003 v. 1.x - 2.0		CVE-2006-0003					CVE-2006-0003 *		CVE-2006-0003	CVE-2006-0003 v. 3.1
2007	CVE-2007-5659 CVE-2008-0655 v. 1.2.3-1.2.5	CVE-2007-5659									CVE-2007-5659 v. 3.1 CVE-2008-0655 v. 3.1
2008	CVE-2008-2992 v. 1.2.3-1.2.5	CVE-2008-2992									CVE-2008-2992 v. 3.1 CVE-2008-5353 v. 3.1
2009	CVE-2009-0927 v. 1.2.3 - 1.2.5										CVE-2009-0927 v. 3.1 CVE-2009-4324 v. 3.1 CVE-2009-3867 v. 3.1
2010	CVE-2010-0188 v. 1.2.x - 2.0 CVE-2010-1885 v. 1.2.3 - 1.2.5	CVE-2010-0188	CVE-2010-0806 CVE-2010-0842	CVE-2010-0188	CVE-2010-0188			CVE-2010-0188	Java Signed Applet	CVE-2010-0188	CVE-2010-1240 v. 3.1 CVE-2010-0188 v. 3.1 CVE-2010-1297 v. 3.1 CVE-2010-0840 v. 3.1 CVE-2010-0842 v. 3.1.15 CVE-2010-0886 v. 3.1 CVE-2010-0248 v. 3.1.15
2011	CVE-2011-0559 v. 1.2.3 - 1.2.5 CVE-2011-2110 v. 1.2.5 CVE-2011-3544 v. 1.2.3	CVE-2011-2110	CVE-2011-3544	CVE-2011-3544			CVE_2011-2140 CVE-2011-3544	CVE-2011-3544 *	CVE-2011-3544	CVE-2011-3402 CVE-2012-0507	CVE-2011-2110 v. 3.1.15 CVE-2011-2140 v. 3.1.15 CVE-2011-3544 v.3.1 -3.1.15 CVE-2011-2371 v. 3.1.15 CVE-2011-3659 v.3.1.15
2012	CVE-2012-0507 v. 1.2.3, 2.0 CVE-2012-1723 v. 1.2.5 - 2.0 CVE-2012-4681 v. 1.2.5 - 2.0 CVE-2012-1889 v. 1.2.5	CVE-2012-1723	CVE-2012-4681 v. 1.1	CVE-2012-1723 v. 2.1 - 2.1 CVE-2012-4681 v. 2.2	CVE-2012-0507 CVE-2012-4681	CVE-2012-1723 CVE-2012-4681	CVE-2012-0003 CVE-2012-4681	CVE-2012-4681 v.1.1	CVE-2012-4681	CVE-2012-1723 CVE-2012-4681 CVE-2012-5076	Firefox Bootstrapped Addon Social Engineering CVE-2012-0779 v. 3.1.15 CVE-2012-0500 v. 3.1.15 CVE-2012-0507 v. 3.1 - 3.1.15

Send changes to admin@deependresearch.org   Legend: ★ Unverified information

DEEPEND RESEARCH ✪ 2012

Sophisticated, profit-seeking, market-based economy

Specialization

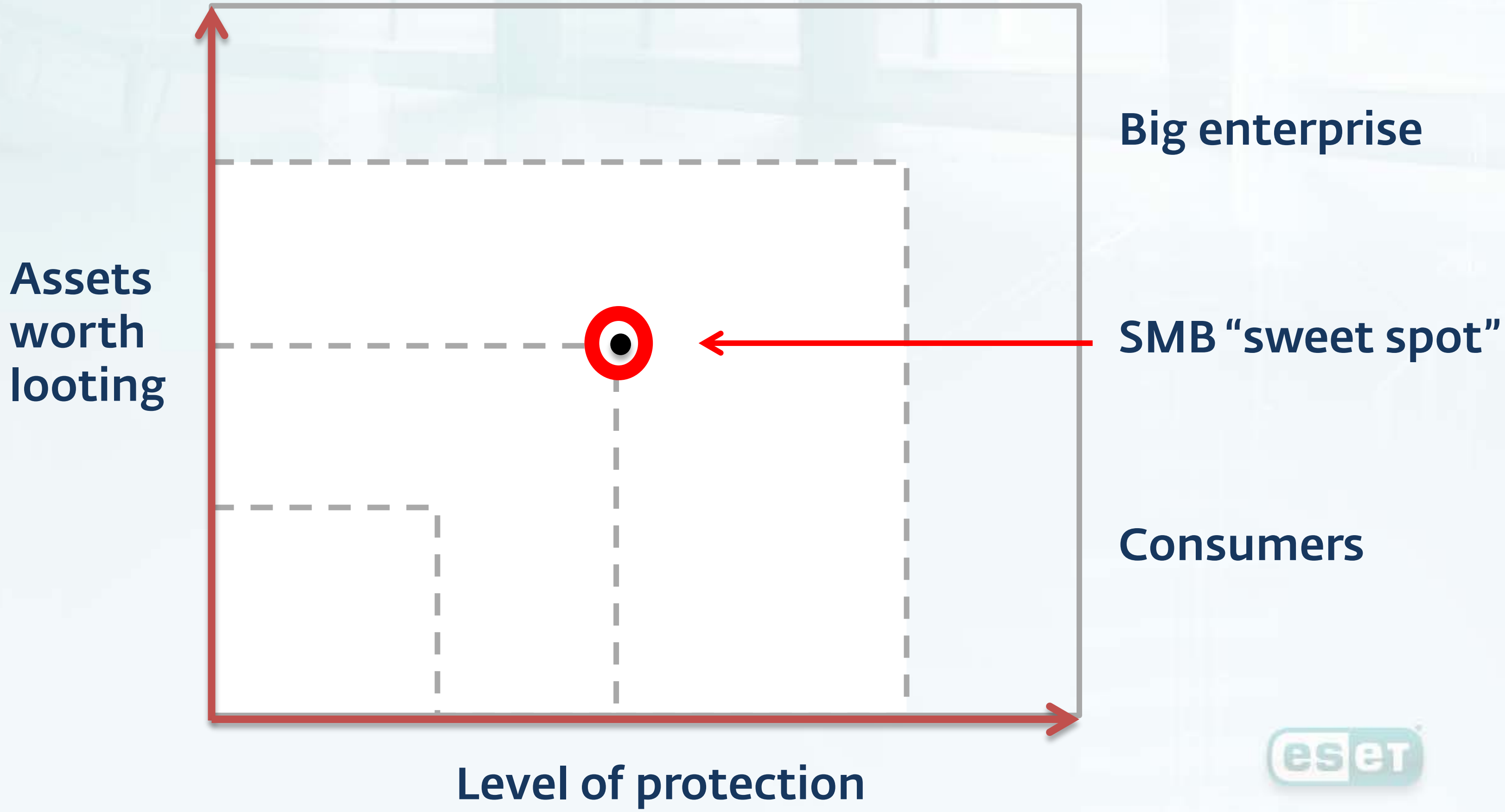
Modularity

Markets

Division of labor

Standards

The SMB sweet spot for the cyber-criminally inclined



Assets worth looting

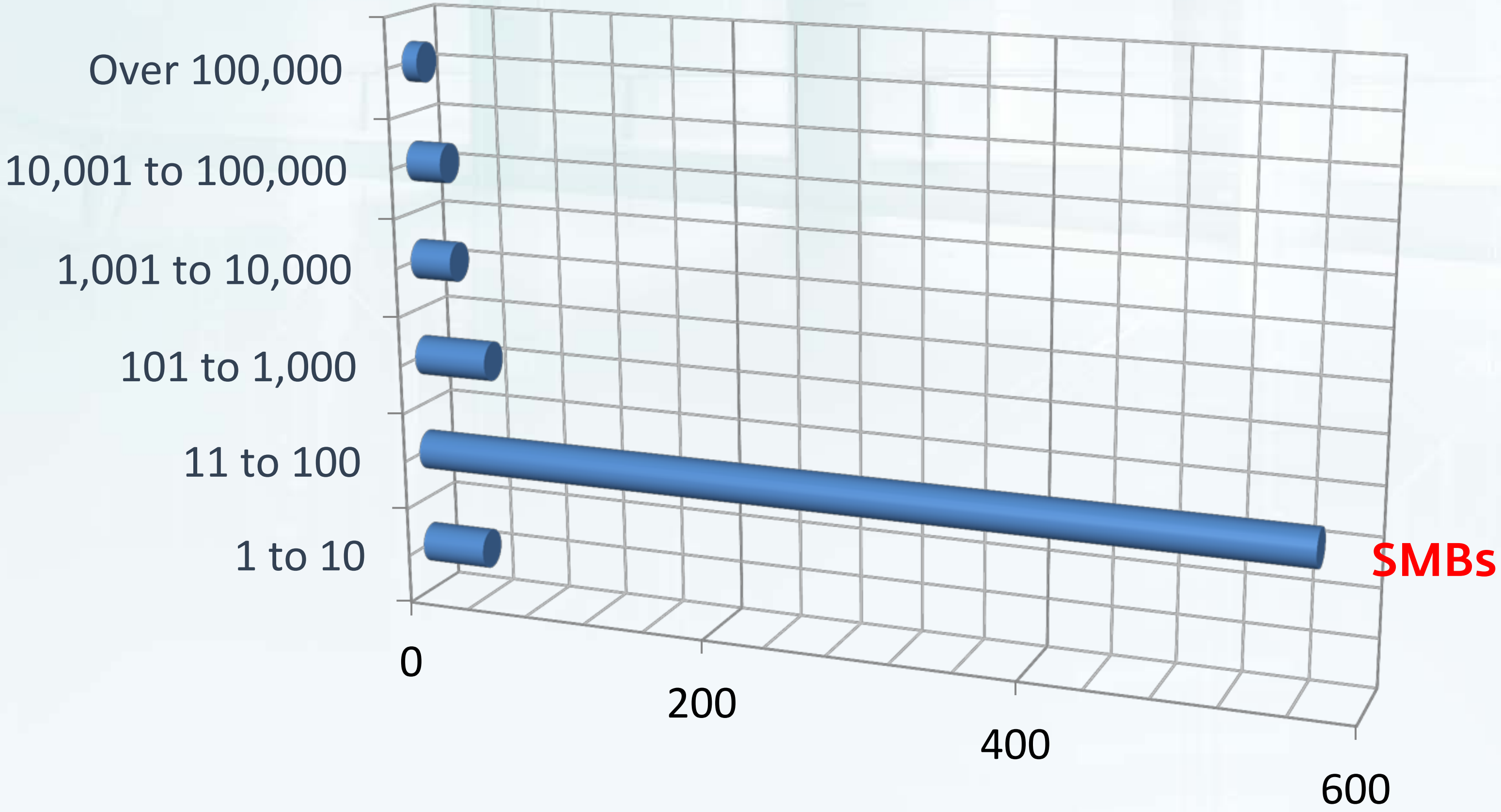
Big enterprise

SMB “sweet spot”

Consumers

Level of protection

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

A B C D E F
F E D C B A

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

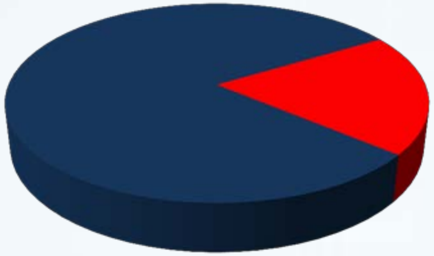
If you could only check 2 things?

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%

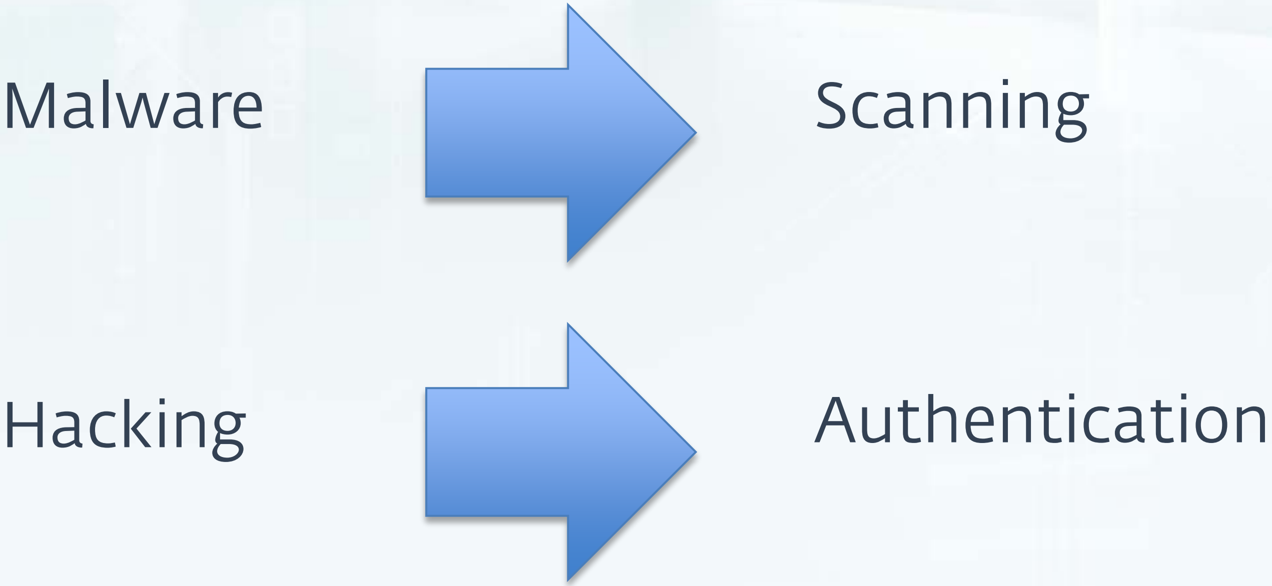
*80% of hacking is passwords: default, missing, guessed, stolen, cracked



Verizon 2012 Data Breach Investigations Report

The Top 2 Things?

Two main attacks…. …and defenses

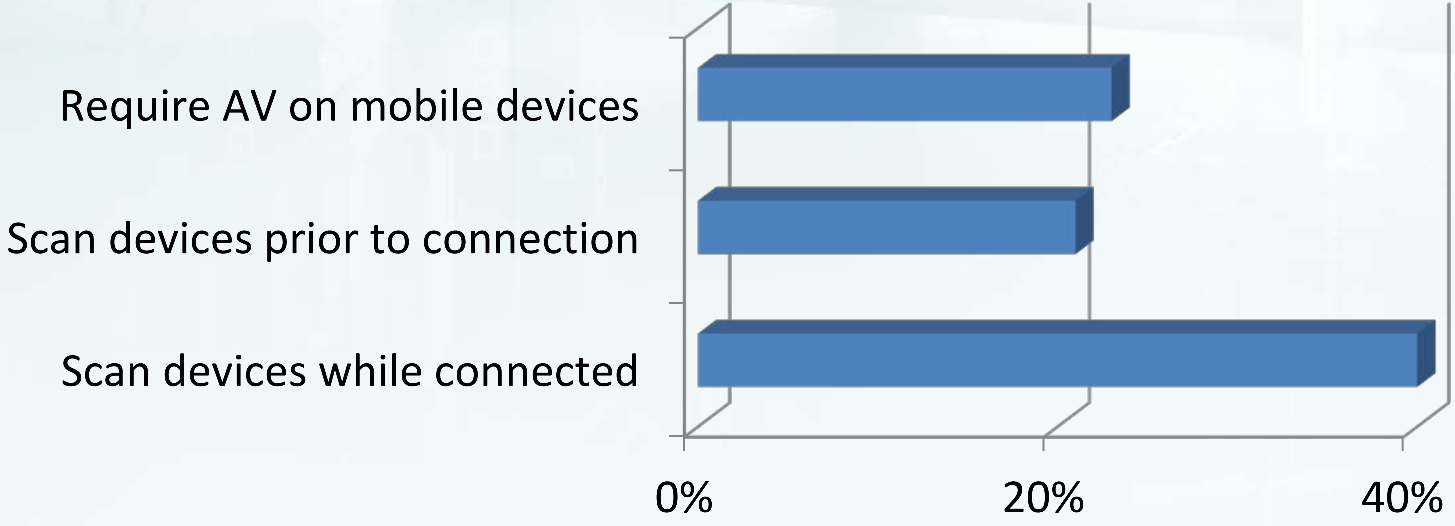


Malware → Scanning

Hacking → Authentication

Scanning requires proper implementation

AV use at a sample of 80 healthcare facilities



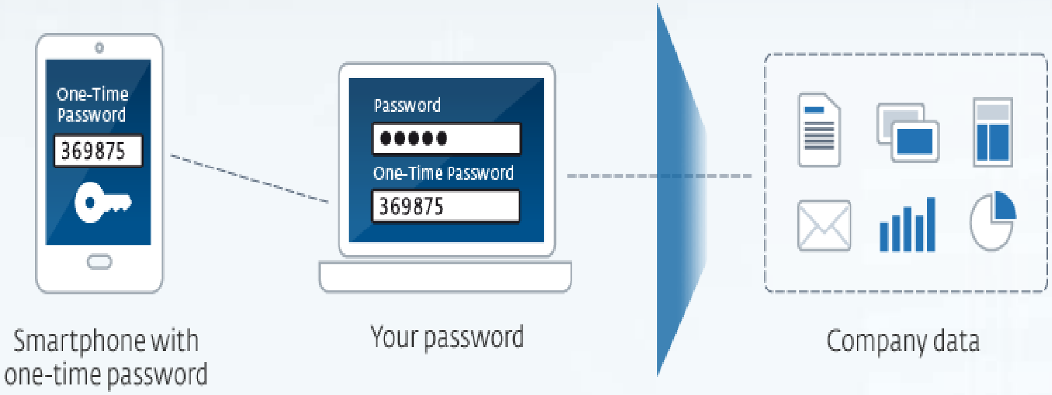
Ponemon Institute Third Annual Benchmark Study on Patient Privacy & Data Security

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

ESET
Welcome to the new ESET blog

THREATS
BYOD risks mitigated by CYOD approach

HOW TO
5 physical security tips for protecting your digital devices

EXPERT OPINION
How's your cyber security awareness...
by Stephen Cobb

HOW TO
Five top tips to stay safer on public Wi-Fi

FRAUD
Telephone scams: it's not all about PC support

PODCASTS
What hackers want