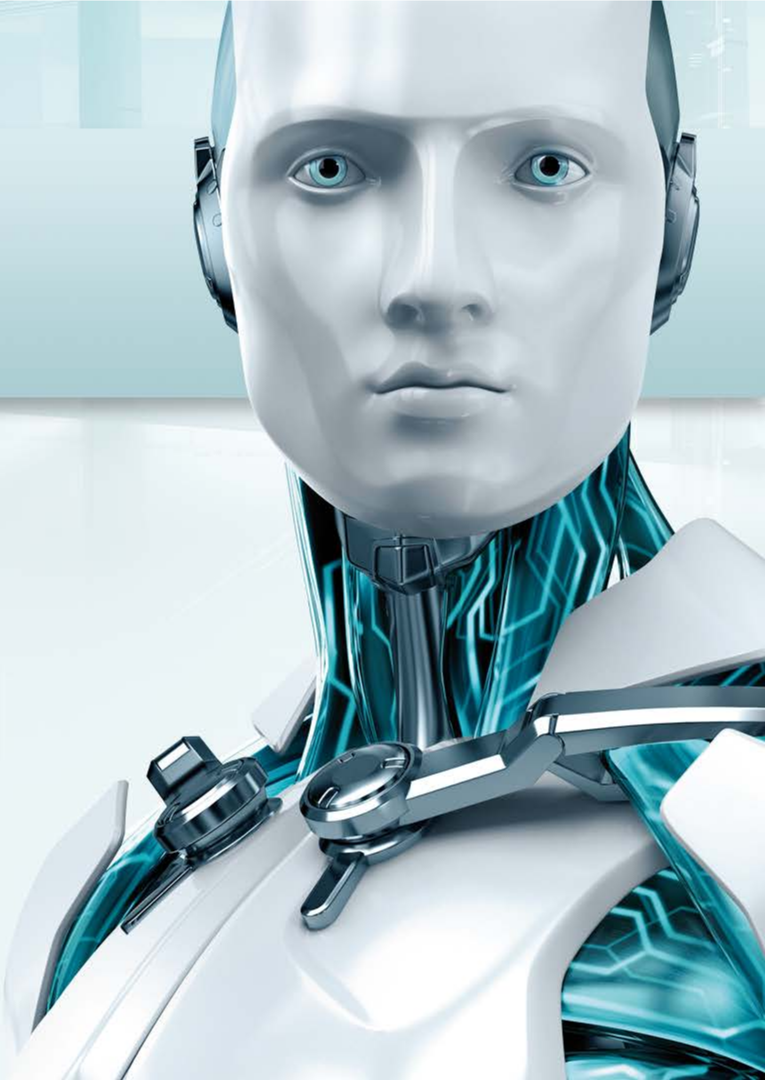
Why THEY want your digital devices

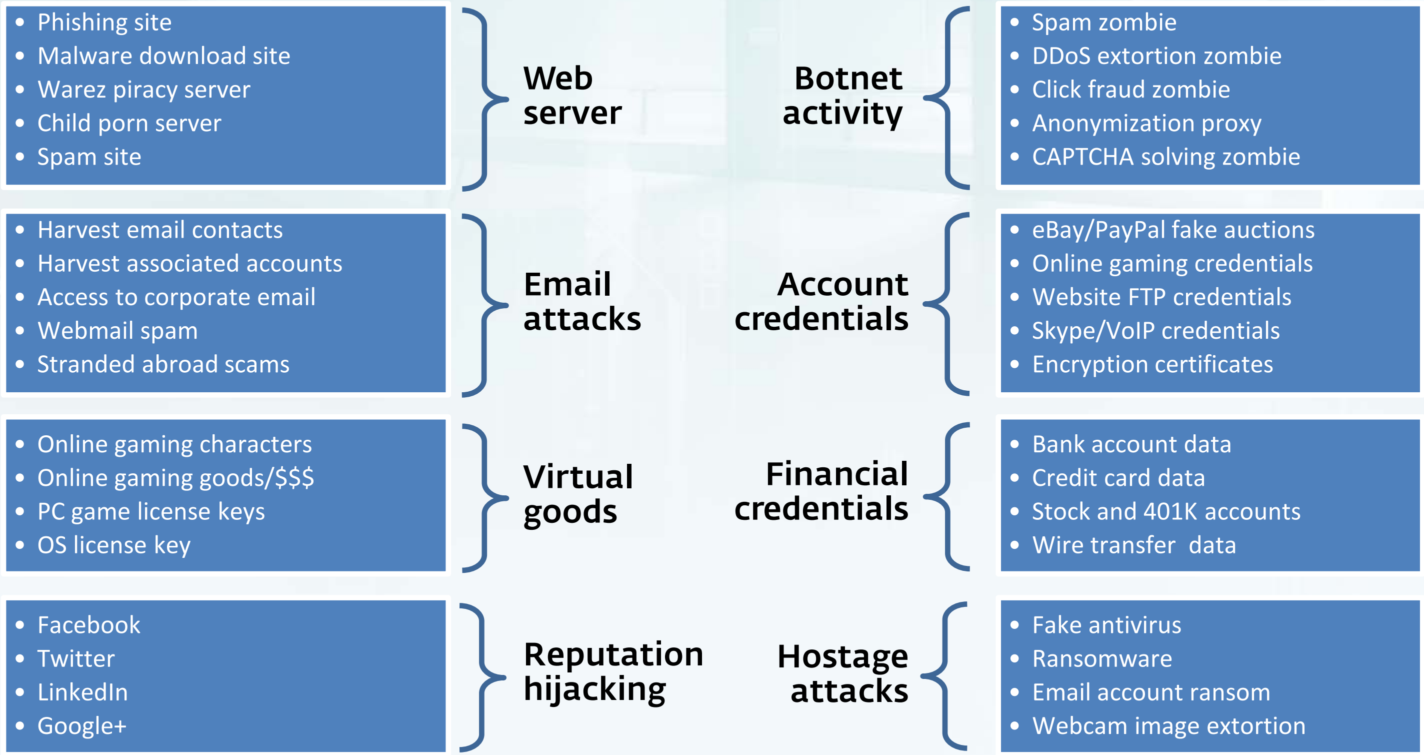


Stephen Cobb, CISSP

Security Evangelist

To own your network?

36 ways to abuse hacked devices



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

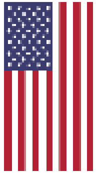
- Fake antivirus
- Ransomware
- Email account ransom
- Webcam image extortion

Based on original work by Brian Krebs: krebsonsecurity.com

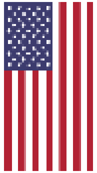
MONEY

ADVANTAGE

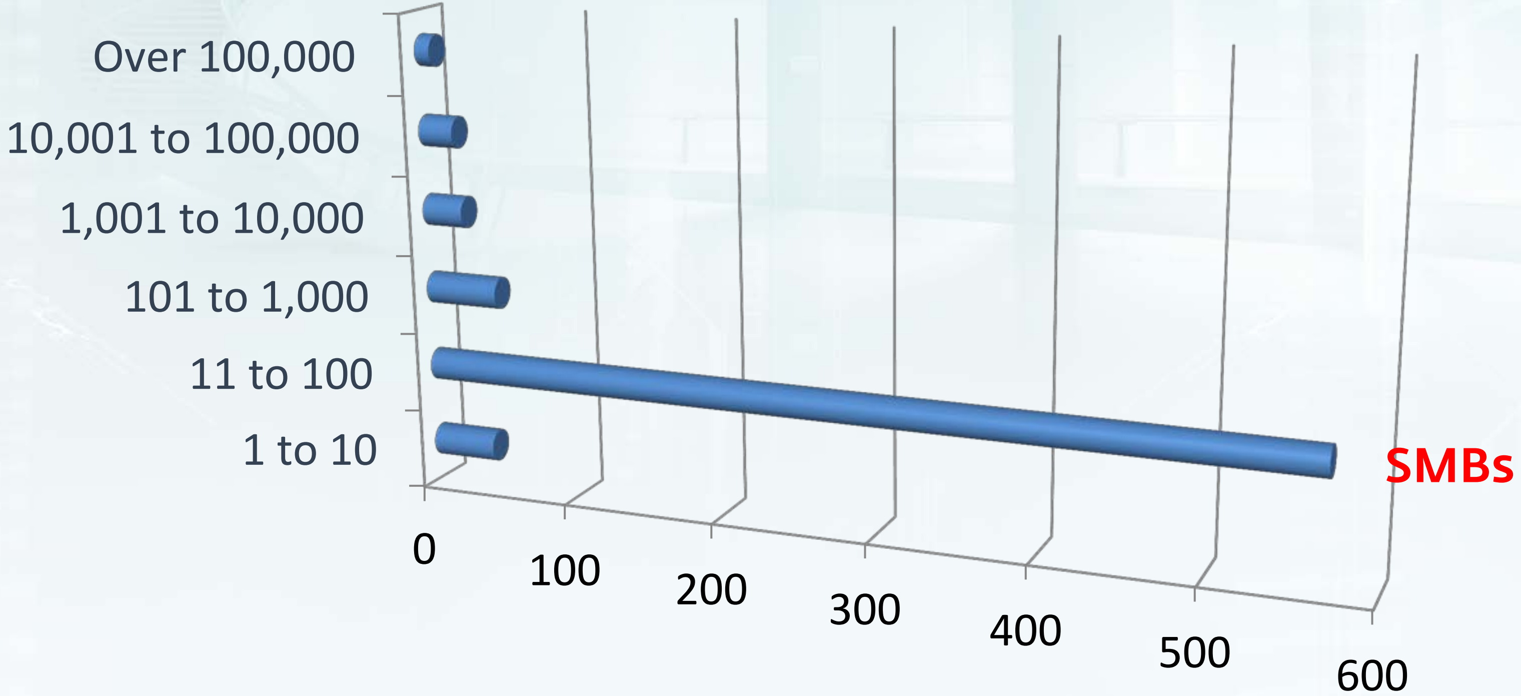
IMPACT



CREDENTIALS

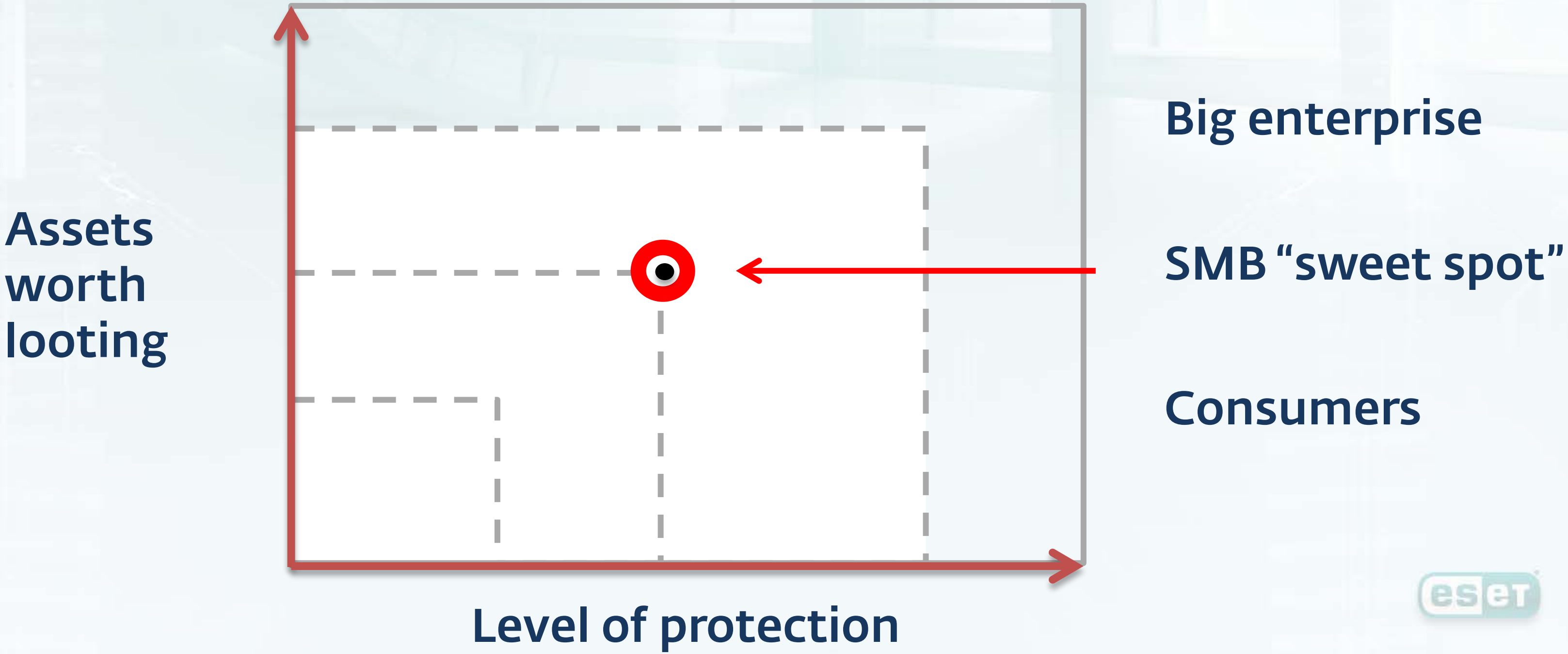


720 breaches by size of organization (employees)



Verizon 2012 Data Breach Investigations Report

The SMB sweet spot for the cyber-criminally inclined

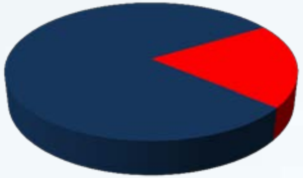


How do they get to your devices?

1. Malware involved in 69% of breaches
2. Hacking* used in 81% of breaches

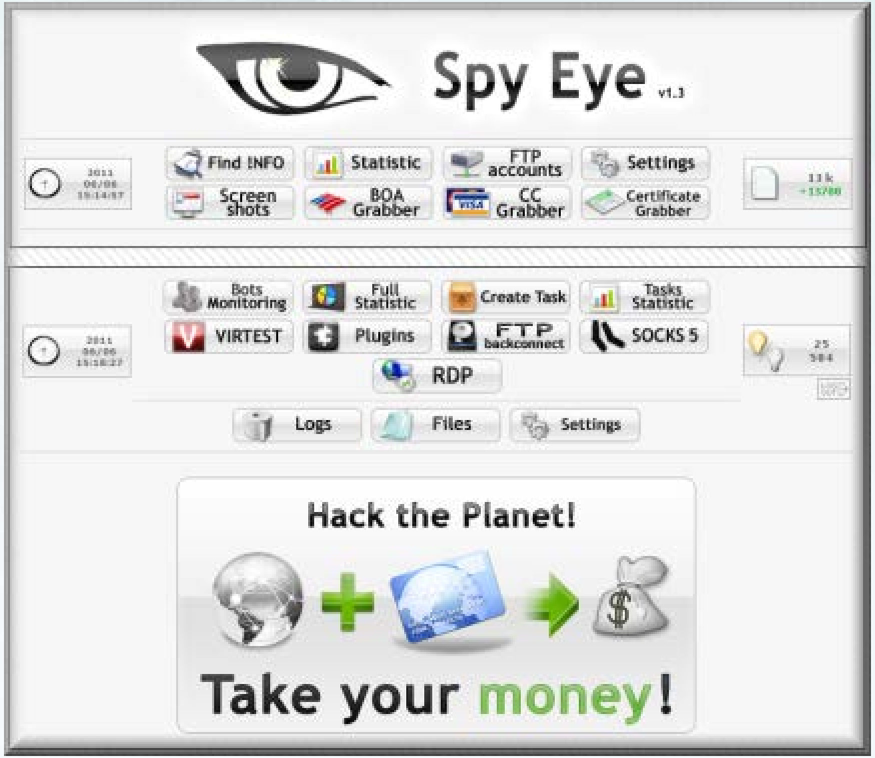
Breaches combining malware and hacking: 61%

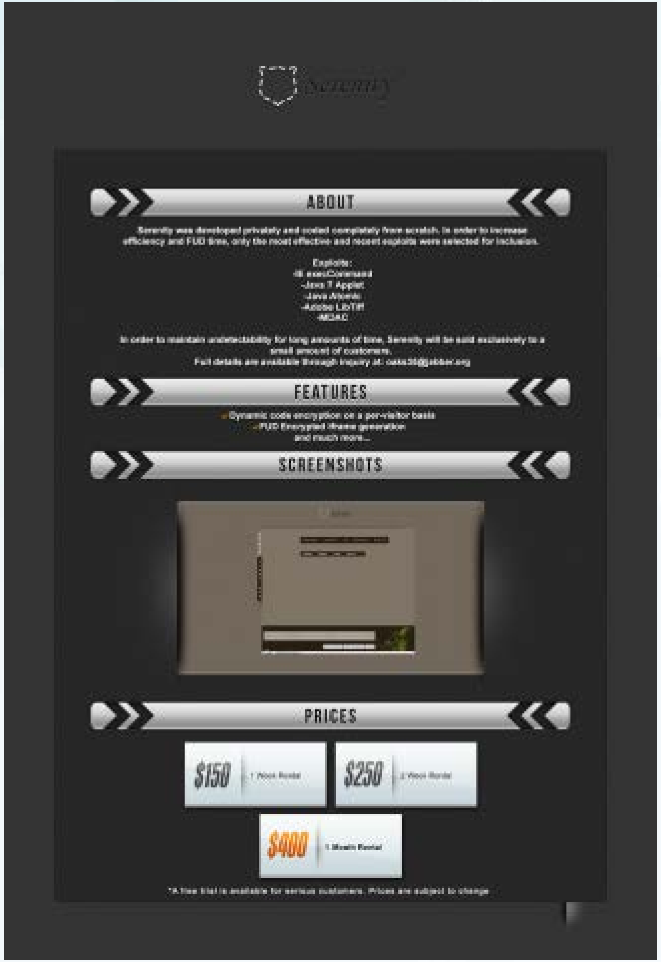
*80% of hacking is passwords: default, missing, guessed, stolen, cracked



Verizon 2012 Data Breach Investigations Report

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: [illegible]@jabber.org

FEATURES

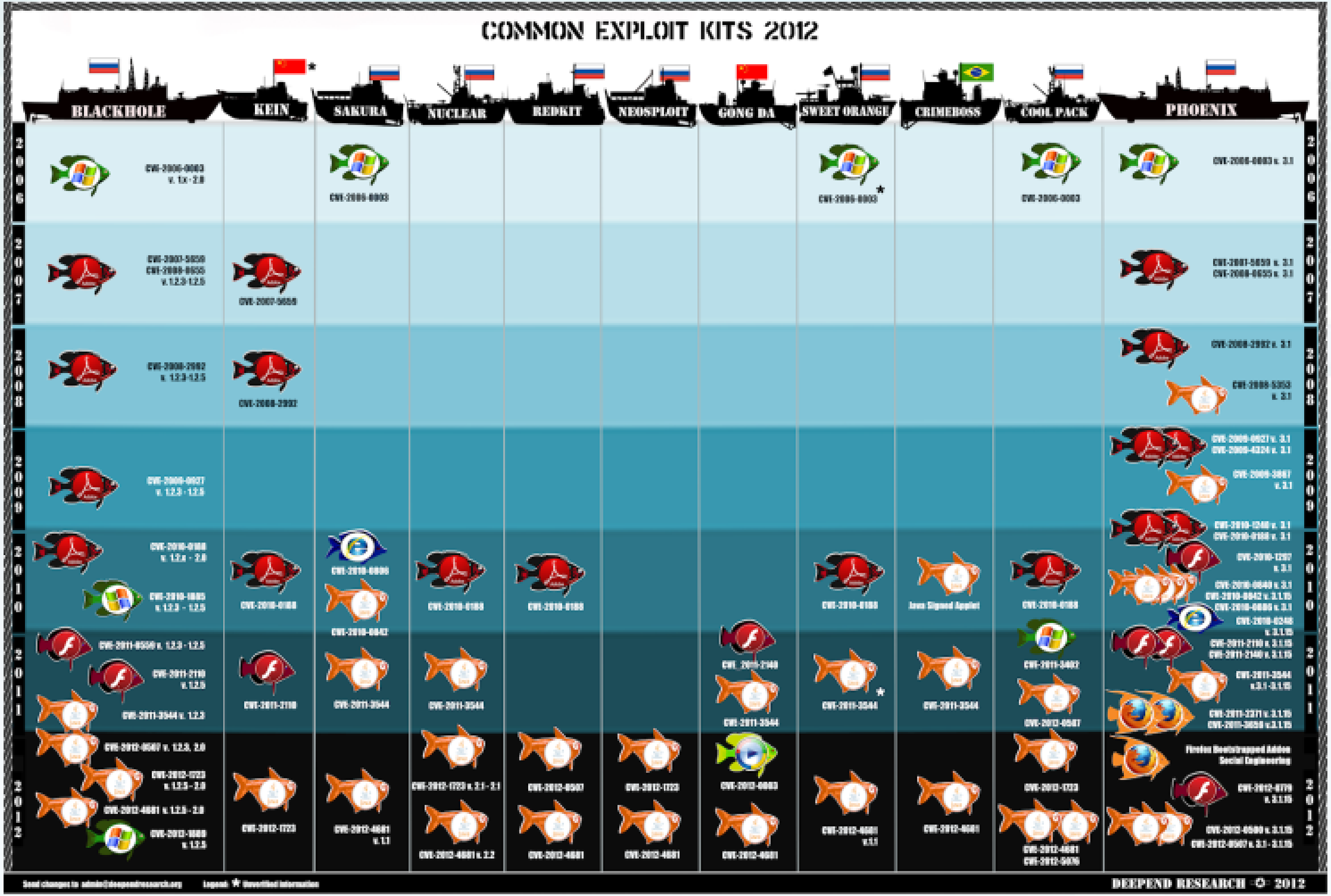
- Dynamic code encryption on a per-visitor basis
- FUD Encrypted iframe generation
- and much more...

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



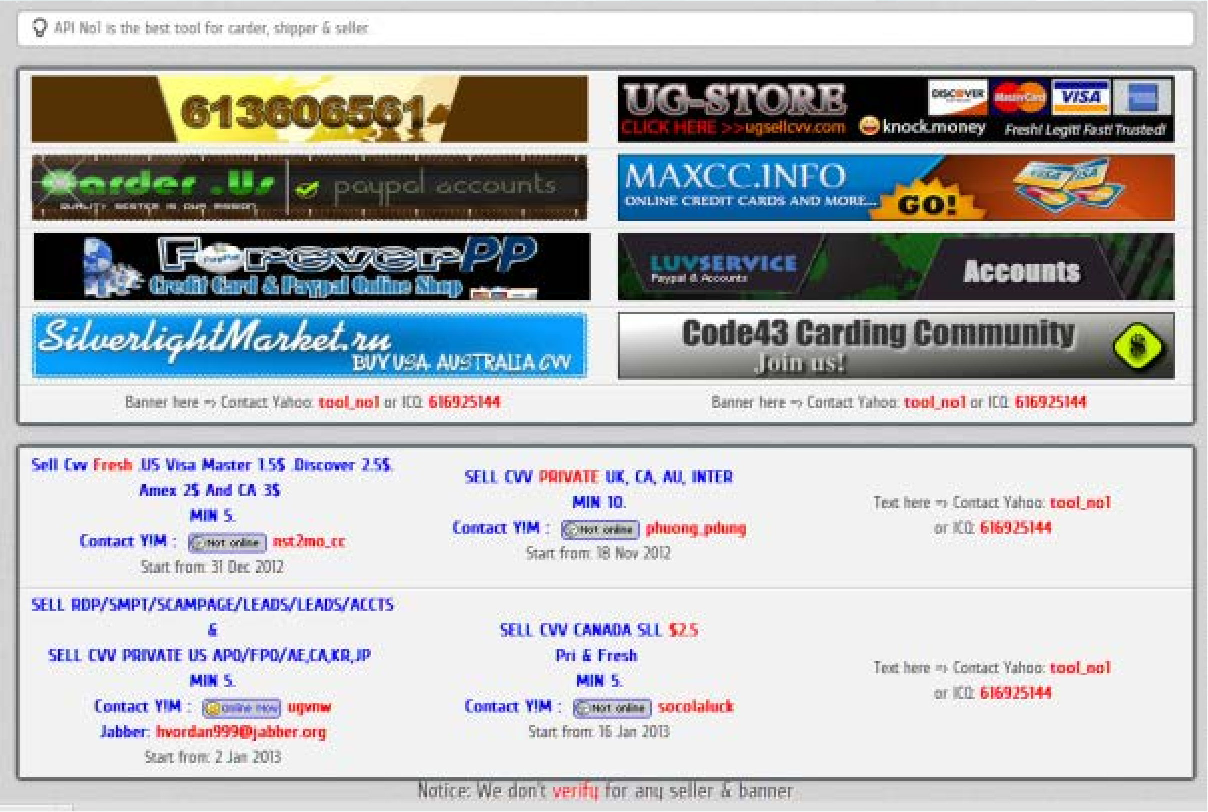
COMMON EXPLOIT KITS 2012

	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. 1.2.3 - 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

Thriving markets for credentials



API No1 is the best tool for carder, shipper & seller

Banner here => Contact Yahoo: tool_no1 or ICQ: 616925144

Banner here => Contact Yahoo: tool_no1 or ICQ: 616925144

Sell Cvv Fresh .US Visa Master 1.5$ .Discover 2.5$.
Amex 2$ And CA 3$
MIN 5.
Contact Y!M : Not online nst2mo_cc
Start from: 31 Dec 2012

SELL CVV PRIVATE UK, CA, AU, INTER
MIN 10.
Contact Y!M : Not online phuong_pdung
Start from: 18 Nov 2012

Text here => Contact Yahoo: tool_no1
or ICQ: 616925144

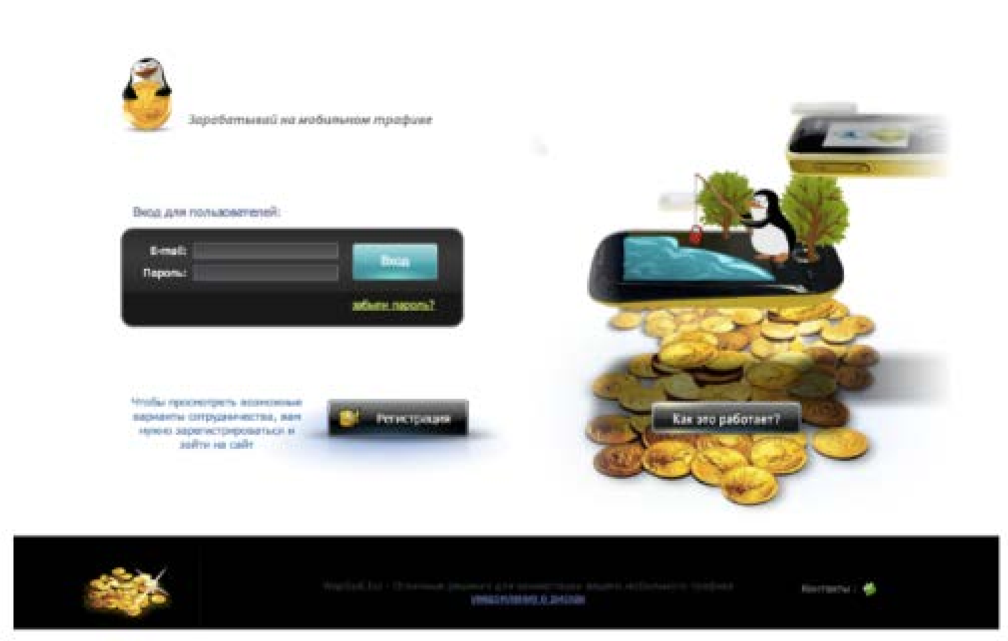
SELL RDP/SMPT/SCAMPAGE/LEADS/LEADS/ACCTS
&
SELL CVV PRIVATE US APO/FPO/AE,CA,KR,JP
MIN 5.
Contact Y!M : online now ugvnw
Jabber: hvordan999@jabber.org
Start from: 2 Jan 2013

SELL CVV CANADA SLL $2.5
Pri & Fresh
MIN 5.
Contact Y!M : Not online socolaluck
Start from: 16 Jan 2013

Text here => Contact Yahoo: tool_no1
or ICQ: 616925144

Notice: We don't verify for any seller & banner

Hot markets for hacked devices



Зарабатывай на мобильном трафике

Вход для пользователей:

Чтобы просмотреть возможные варианты сотрудничества, вам нужно зарегистрироваться и зайти на сайт

[illegible]

All driven by proven business strategies

Specialization

Modularity

Markets

Division of labor

Standards

So how do you defend your devices?

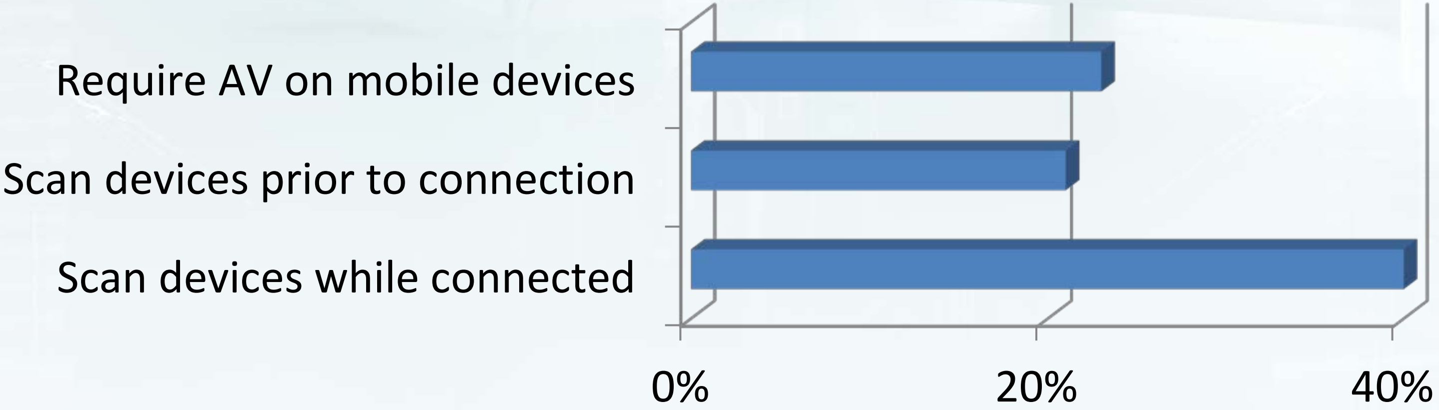
Two main attacks.... ...and defenses

Malware → Scanning

Hacking → Authentication

Scanning requires proper implementation

Measures in use at a sample of healthcare facilities



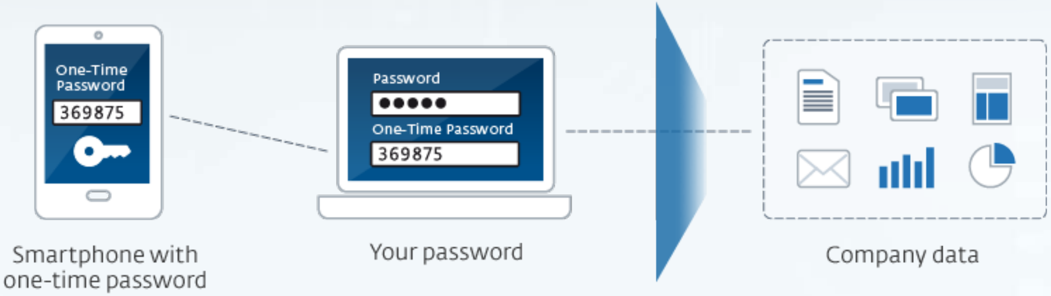
Ponemon Institute Third Annual Benchmark Study on Patient Privacy & Data Security

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 defenses you need

Malware → **SMART** Scanning

Hacking → **STRONG** Authentication

Plus polices and training to implement effectively

Thank you!

news, views and insight from the ESET security community

Welcome to the new ESET blog

BYOD risks mitigated by CYOD approach

5 physical security tips for protecting your digital devices

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

Five top tips to stay safer on public Wi-Fi

Telephone scams: it's not all about PC support

What hackers want

Stephen Cobb ★ stephen.cobb@eset.com

WeLiveSecurity.com