







GOOD CYBERSUCURITY IS A BUSINESS REQUIREMENT

HAVING CYBERSECURITY IS A LEGAL REQUIREMENT

The Reality of Cybercrime

- It is a business
- It is a weapon

IT IS ALSO CRIME AS USUAL!

What is different is its mass appeal,
and relative simplicity

- It is difficult to trace
 - It is delocated

Then, You Can't Escape

- You can't just disconnect
- Firms must and will adopt cloud based solutions
 - To remain competitive;
 - To remain efficient;
 - To respond to customer demands;
 - Because of legislations

Know Your Ennemy: WHO is behind cybercrime?



Evolution of Cybercrime

"Today's cybercriminals do not necessarily require considerable technical expertise to get the job done, nor, in certain cases, do they even need to own a computer.

All they need is a credit card"

Troels Oerting
Head of EC3 European
Cybercrime Centre

Cybercrime Eco-System



Categories of Services

Attack Components (insourced or outsourced)

(Research)

Crimeware

Infrastructure

Hacking-as-a-Service

Research-as-a-Service

Availability includes

- Sale of Vulnerabilities
- Personal data

Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
iOS	\$100,000–\$250,000

Research-as-a-Service

By Country

USA DOCTOR EMAIL DATABASE

PRICE LOWERED!
\$114.34 tax incl.
\$124.34 tax excl.
(price reduced by 10 %)

Quantity : 1

Availability: 999 items in stock

Add to cart

Add to my wishlist

PayPal

Click here to pay

By profession

France Email Database 1 million

PRICE LOWERED!
\$495.49

Add to cart

View





Crimeware-as-a-Service: Exploits

the user realizes it is there. If the dialog is displayed in a small enough window, the user may not realize it is being displayed, and if the right keyboard sequence is carefully followed, they can end up running a downloaded executable. Additional secure engineering steps are needed to ensure that the user presses the correct key sequence, without being able to show any relevant visual feedback, as the page cannot see that the keys are being pressed

High ☐ ☒ ☐

CVE-2012-19251 Opera 11.61 Remote download and execution vulnerability

Dialogs such as the download dialog are usually displayed on top of page content, to ensure that the user knows that the dialog is requesting attention. In some cases, this policy was not implemented correctly in Opera, allowing certain page content to overlay the dialog. In these cases, clicking the page content causes the dialog to be closed instead. While an attacker may not have much control over the experience of the overlapping content, they may be able to use it to trick the user into performing harmful actions, such as running a downloaded executable

High ☐ ☒ ☐

CVE-2012-19262 Opera 11.61 Address Bar Spoofing

The address field should always show the address of the page that is being displayed. In certain cases, if a target site responds slowly, reloading an attacking page and redirecting to the target page can cause the address field to show the target site's address, while the attacking site is still being displayed.

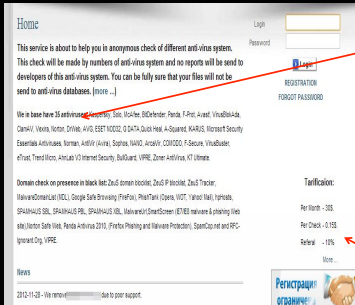
Damage = Cost

LOW = \$200

MEDIUM = \$400

HIGH = \$600

Crimeware-as-a-Service: Ancillary Services



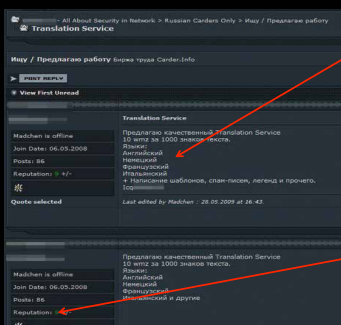
Service:

35 AV Products

Tariff:

Per month = \$30
Per Check = \$0.15

Crimeware-as-a-Service: Professional Services



Services on offer

Reputation:

+ 9 Reputation

Cybercrime Infrastructure-as-a-Service



Cybercrime Infrastructure-as-a-Service

Many products and services available

Crimeware-as-a-Service: Professional Services

Reputation:
Live Customer Service Chat

Send 30 million emails

Crimeware-as-a-Service: Botnets

Price:

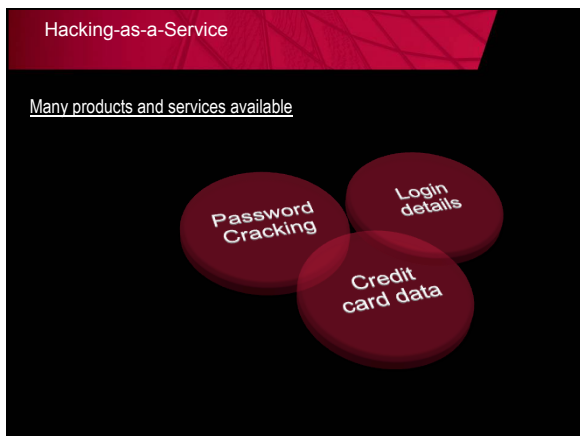
1-4 hours	\$2 per hour
5-24 hours	\$4 per hour
1 month	\$1000

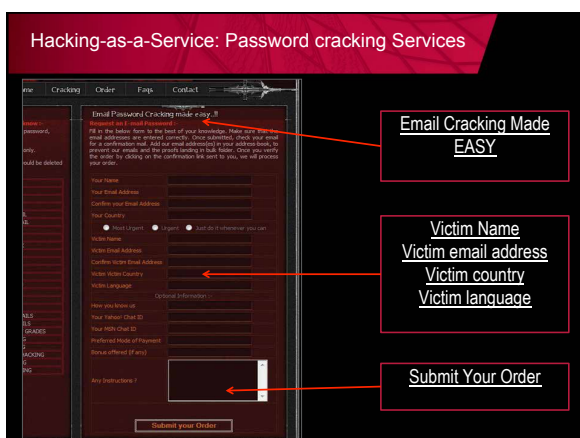
Guarantee

We can hit most large websites.

No Refunds!







Hacking-as-a-Service: Password cracking Services

Table 2. Prices for stolen credit card numbers.

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)											
	US			EU			CA, AU			Asia		
Visa Classic	\$15	\$80		\$40	\$150		\$25	\$150		\$50	\$150	
Master Card Standard		\$90			\$140			\$150			\$140	
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160		\$55	\$150	
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170		\$60	\$170	
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175		\$70	\$170	
Purchasing/Signature	\$50	\$120			\$70		\$55			\$80		
Infinite				\$130	\$190		\$60	\$200			\$190	
Master Card World		\$140										
AMEX	\$40			\$60			\$45			\$70		
AMEX Gold	\$70			\$90			\$95			\$100		
AMEX Platinum	\$50											

Without PIN

\$25

With PIN

\$100

With PIN + balance

\$200

You Are Particularly Exposed

According to the most recent DBIS(UK)/PWC *Information Security Breaches Survey* (2013):

- 76% increase with the number of breaches in small and medium size firms;
- 63% were attacked by outsiders in the last year;
- 23% were hit by denial-of-service attacks;
- 15% confirmed unauthorised incursions;
- 9% admit that intellectual property was stolen.

You Operate Under a Stringent Regulatory Regime

- Sox; Data Protection;
- Statutory and professional compliance; Confidentiality;
- Criminal and civil liabilities

Obligations to deliver in the cloud:

- Filings; case submission; discovery.

YOUR BUSINESS IS ALL ABOUT INFORMATION!

YOUR REPUTATION

YOUR LIABILITIES

YOUR SURVIVAL AS A BUSINESS

THIS IS NOT AN IT PROBLEM

RISK MANAGEMENT

One Approach

1. Collate every bit of legislation, regulation, guidelines, best practices; compliance requirements for every territory you operate in;
2. Make sense of that:
THERE IS NO HOMOGENEOUS CYBER"stuff"
LAW!
3. Dump that stuff onto your IT folks;
4. Hope for the best ...

Much Better To Do

1. Appoint a real operational risk manager (law firms: the compliance officer for legal practice?)
2. Categorise and assess risk:
 1. Business continuity
 2. IP protection
 3. Confidentiality
 4. Sector specific compliance requirements
3. Maintain a risk assessment schedule
4. Identify gaps and mitigating actions:
IMPLEMENT
5. EDUCATE; EDUCATE; EDUCATE

A Good Start:

The American Bar Association (USA) and its Cybersecurity Legal Task Force
(also note the evolution of ABA Model rules, like Model Rule 1.6 on Confidentiality, or Model Rule 4.4 on Professional Conduct)

The Law Society (UK) Information Security Guidelines

Bundesamt für Sicherheit in der Informationstechnik: guideline for IS audits

IFAC guidelines

TRAIN
EDUCATE
ADVOCATE

It is a PEOPLE PROBLEM!
My passwords; My encryption; My funny clicking

Keeping Safe Online – do the basics well

Create strong passwords

Don't give out personal information

Be careful when using IM & Email

Only shop from secure sites

Watch out for 'Phishing' sites

Keep safe whilst gaming

Monitor children's online activities

Looks too good to be true – it will be

YOUR REPUTATION
YOUR BUSINESS
YOUR PERSONAL LIFE

THANK YOU FOR LISTENING!

Examples
