

Cybercrime 101 – Online Fraud Made Simple

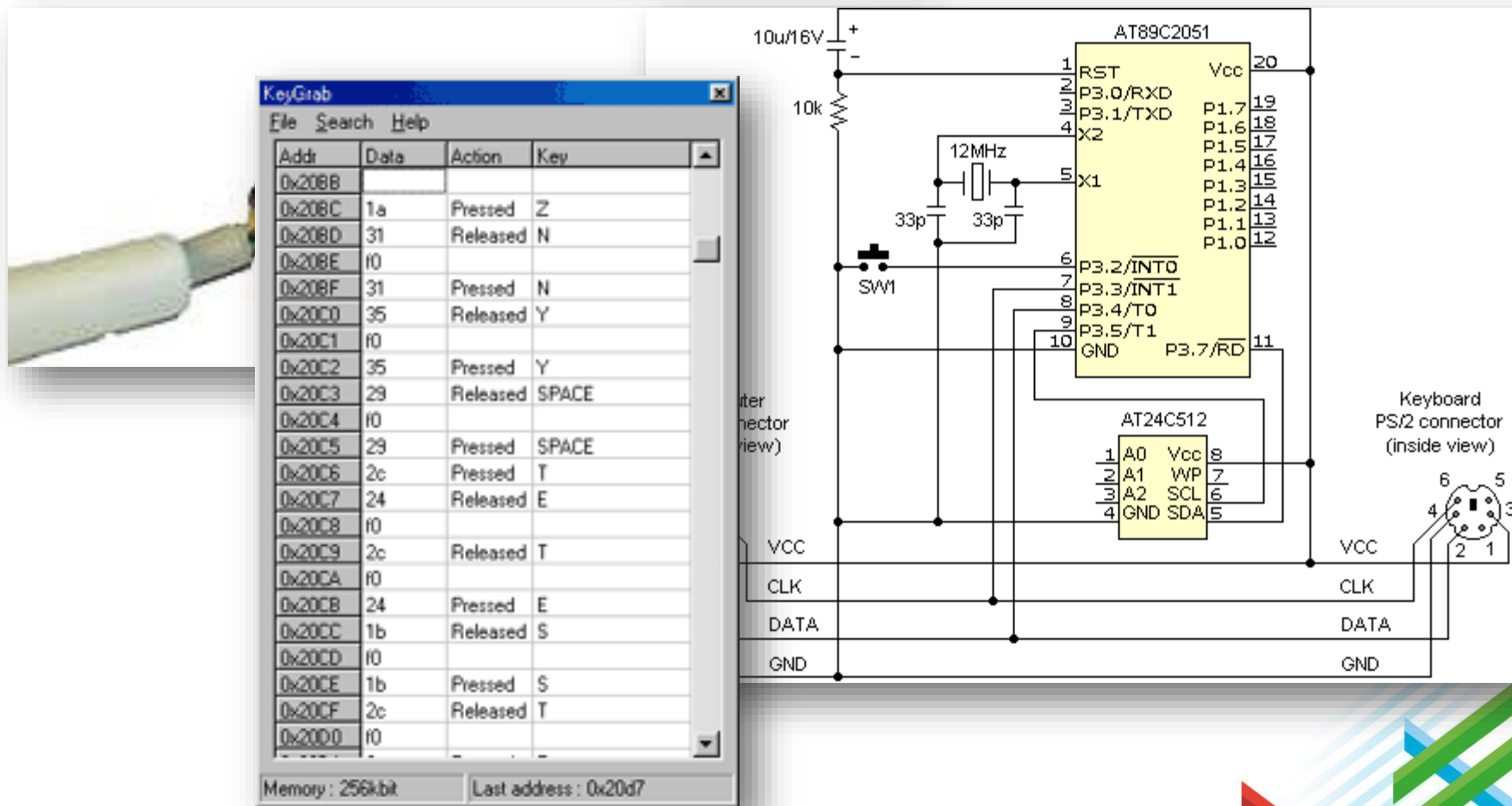
Etay Maor, Fraud Prevention Solutions Manager

Trusteer, an IBM Company

Cybercrime 1991

Or: How I Got in Trouble...

It used to be a lot of work stealing credentials



The image displays a KeyGrab application window, a physical keyboard connector, and a detailed circuit diagram of the AT89C2051 microcontroller interfaced with an AT24C512 EEPROM and a PS/2 keyboard connector.

KeyGrab Application Window:

Addr	Data	Action	Key
0x208B			
0x208C	1a	Pressed	Z
0x208D	31	Released	N
0x208E	10		
0x208F	31	Pressed	N
0x20C0	35	Released	Y
0x20C1	10		
0x20C2	35	Pressed	Y
0x20C3	29	Released	SPACE
0x20C4	10		
0x20C5	29	Pressed	SPACE
0x20C6	2c	Pressed	T
0x20C7	24	Released	E
0x20C8	10		
0x20C9	2c	Released	T
0x20CA	10		
0x20CB	24	Pressed	E
0x20CC	1b	Released	S
0x20CD	10		
0x20CE	1b	Pressed	S
0x20CF	2c	Released	T
0x20D0	10		

Memory : 256kbit Last address : 0x20d7

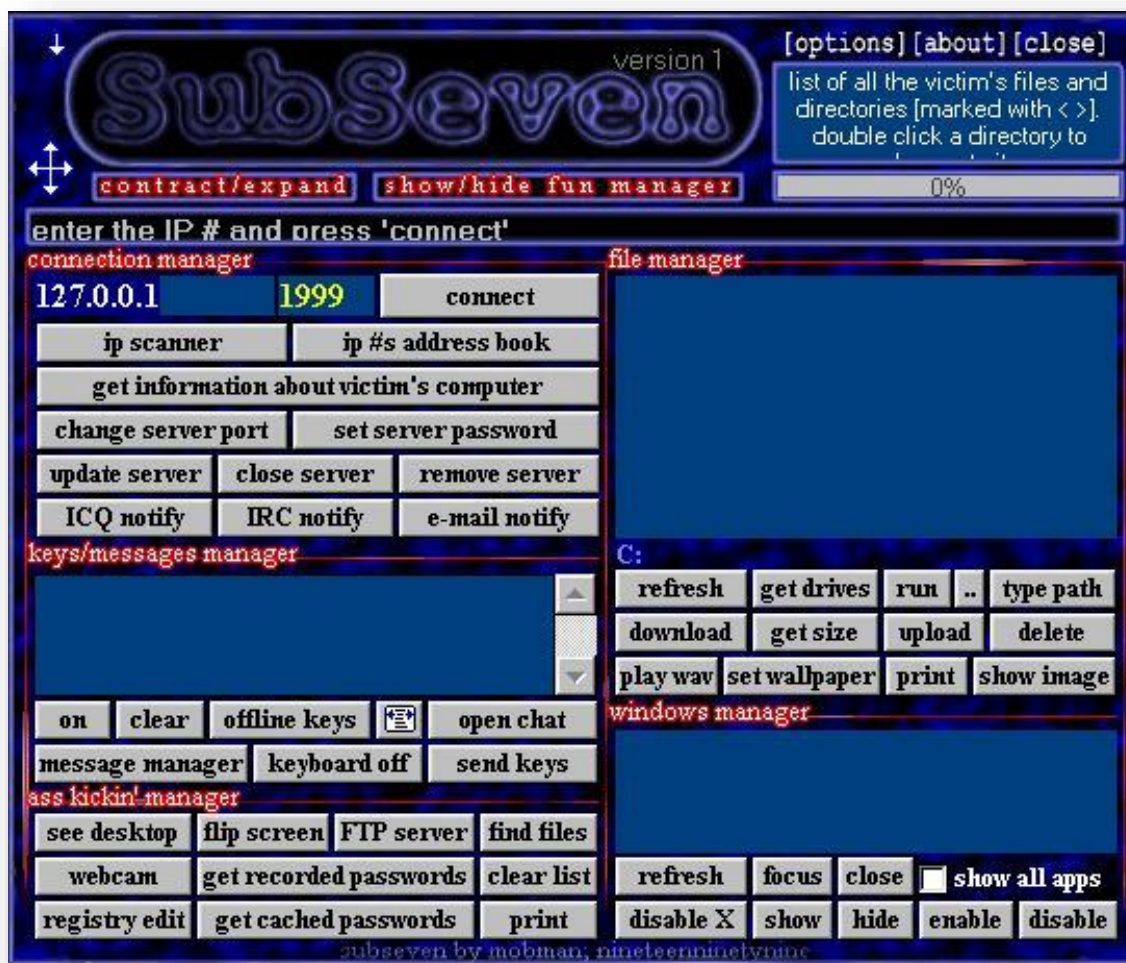
Circuit Diagram:

The circuit diagram shows the AT89C2051 microcontroller (AT89C2051) interfaced with an AT24C512 EEPROM and a Keyboard PS/2 connector (inside view). The AT89C2051 is connected to a 10u/16V power source through a 10k resistor. A 12MHz crystal oscillator is connected to pins 4 (X2) and 5 (X1) of the AT89C2051, with 33pF capacitors on each side. A switch (SW1) is connected to pin 6 (P3.2/INT0) and ground. The AT24C512 EEPROM is connected to the AT89C2051 via I2C: A0 (pin 1) to GND, A1 (pin 2) to VCC, A2 (pin 3) to SCL (pin 6 of AT89C2051), and SDA (pin 4) to INT1 (pin 7 of AT89C2051). The Keyboard PS/2 connector (inside view) is connected to the AT89C2051: Pin 1 (VCC) to VCC, Pin 2 (CLK) to CLK (pin 10 of AT89C2051), Pin 3 (DATA) to DATA (pin 9 of AT89C2051), and Pin 4 (GND) to GND. The AT89C2051 is also connected to a 10u/16V power source through a 10k resistor. The AT89C2051 is connected to a 10u/16V power source through a 10k resistor. The AT89C2051 is connected to a 10u/16V power source through a 10k resistor.

Cybercrime 2000

Or: How I Got in Trouble...AGAIN

Things got easier – GUIs and functionality greatly improved



2000 - Today

Malware is the cybercriminals' tool of choice. What can you do with it?

- Steal credentials
- Take screenshots
- Inject HTML
- Much more...

Sounds difficult? Let's see






2013, UK, Cybercriminals Are Looking at Big Numbers



UK organizations are a major target for cybercriminals:

Iceto
Newcomer



Join Date: Mar 2010
Posts: 160

Vouchers:

(8) UK партнер ищущий на Большие суммы.

Accounts sometimes have enormous balances:
100k -200k,
<BANK NAMES>
All come with full info.

I need a pro who can transfer large amounts and cash them out using his own plans. Forum deposit is a must, feedbacks from other fraudsters too.





2013, UK, Cybercriminals Have New Tricks

The 5 ½ steps for committing online fraud successfully:

1. Gather intelligence
2. Analyze, adapt and develop new counter measures
- 2.5 If you are too lazy – someone will do it for you! (If the price is right)
3. Protect your investment
4. Learn new tricks

Professional tip: LOCATION LOCATION LOCATION





2013, UK, Cybercriminals Have New Tricks

The 5 ½ steps for committing online fraud successfully:

1. Gather intelligence

UK Case Study

Large UK bank

3 weeks worth of data

1.5M accounts reviewed

10M login attempts

Criminals are acting awkward – they are not cashing out! Why?



2013, UK, Cybercriminals Have New Tricks

The 5 ½ steps for committing online fraud successfully:

2. Analyze, adapt and develop new counter measures (mobile usage)

UK Case Study

Large UK bank

3 weeks worth of data

1.5M accounts reviewed

10M login attempts

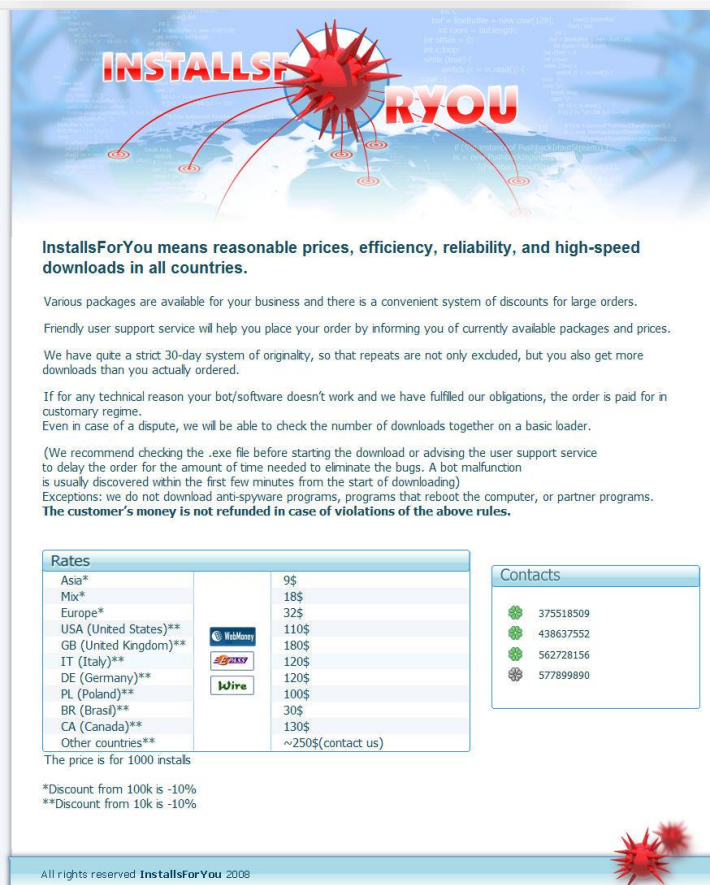
30% of OLB access is coming from mobile. Confirmed online fraud from this channel! HOW?



2013, UK, Cybercriminals Have New Tricks

The 5 ½ steps for committing online fraud successfully:

2.5 If you are too lazy – someone will do it for you! (If the price is right)

INSTALLS FOR YOU

InstallsForYou means reasonable prices, efficiency, reliability, and high-speed downloads in all countries.

Various packages are available for your business and there is a convenient system of discounts for large orders.

Friendly user support service will help you place your order by informing you of currently available packages and prices.

We have quite a strict 30-day system of originality, so that repeats are not only excluded, but you also get more downloads than you actually ordered.

If for any technical reason your bot/software doesn't work and we have fulfilled our obligations, the order is paid for in customary regime.

Even in case of a dispute, we will be able to check the number of downloads together on a basic loader.

(We recommend checking the .exe file before starting the download or advising the user support service to delay the order for the amount of time needed to eliminate the bugs. A bot malfunction is usually discovered within the first few minutes from the start of downloading.)

Exceptions: we do not download anti-spyware programs, programs that reboot the computer, or partner programs.





The customer's money is not refunded in case of violations of the above rules.

Rates	
Asia*	9\$
Mix*	18\$
Europe*	32\$
USA (United States)**	110\$
GB (United Kingdom)**	180\$
IT (Italy)**	120\$
DE (Germany)**	120\$
PL (Poland)**	100\$
BR (Brasil)**	30\$
CA (Canada)**	130\$
Other countries**	~250\$(contact us)

The price is for 1000 installs

*Discount from 100k is -10%

**Discount from 10k is -10%

Contacts	
	375518509
	438637552
	562728156
	577899890

All rights reserved InstallsForYou 2008

2013, UK, Cybercriminals Have New Tricks



The 5 ½ steps for committing online fraud successfully:
3. Protect your investment

The image shows a composite of two screenshots. On the left is the Zeus crypter interface, featuring a dark background with glowing red lines and a list of tools: Anti-Debugger, Virtual-PC, VMWare, OllyDBG, Virtual-Box, and RegShot. On the right is a video player showing a scan report from a 'Multi-Engine Antivirus Scanner'. The report details file information for a 'crypted.exe' file, including its size (145604 bytes), MD5 hash, and SHA1 hash. A table below lists the results of various antivirus engines, all showing a 'CLEAN' status.

Antivirus	Database	Engine	Result
Avira	01/02/2011	5.0.0.20	
Avast	01/02/2011	5.0	
AVG	01/02/2011	9.0.0.725	
Avira AntiVir	01/02/2011	7.6.0.59	
BitDefender	01/02/2011	7.0.0.2555	
ClamAV	01/02/2011	0.96.2.1	
Comodo	01/02/2011	4.0	
Dr.Web	01/02/2011	5.00.0	
F-PROT	01/02/2011	4.6.1.107	
Ikarus T3	01/02/2011	1001084	
Kaspersky	01/02/2011	9.0.0.736	
NOD32	01/02/2011	4.2.42.0	
Panda	01/02/2011	10.0.3.0	

Video title: Zeus Crypter November 2012 Crypter ! 0_33 ! VB6 ! Bypass All Anti Virus
Channel: Randy J. Miller · 14 videos
Views: 557 views
Buttons: Subscribe, 9, 1, 2



2013, UK, Cybercriminals Have New Tricks



The 5 ½ steps for committing online fraud successfully:

4. Learn new tricks

A screenshot of a private message or advertisement for 'Private Carding Lessons'. The header shows a profile picture of a cartoon character and a redacted name. The text describes an 'Academy of Carding' and lists various services offered, including online carding, instore carding, botnet lessons, and cashout services. It also mentions the price and contact information.

Private Carding Lessons

I m glad to present the [REDACTED] Academy of Carding , where all new carders can learn the best way to made money on carding world .

- * Online Carding (how card item , ticketsetc)
- * Instore Carding (how card safe , bins , technicetc)
- * Botnet Lessons (what is botnet trojan , how that worketc)

ALL lessons are given throught ICQ & JABBER with encryption logs !!

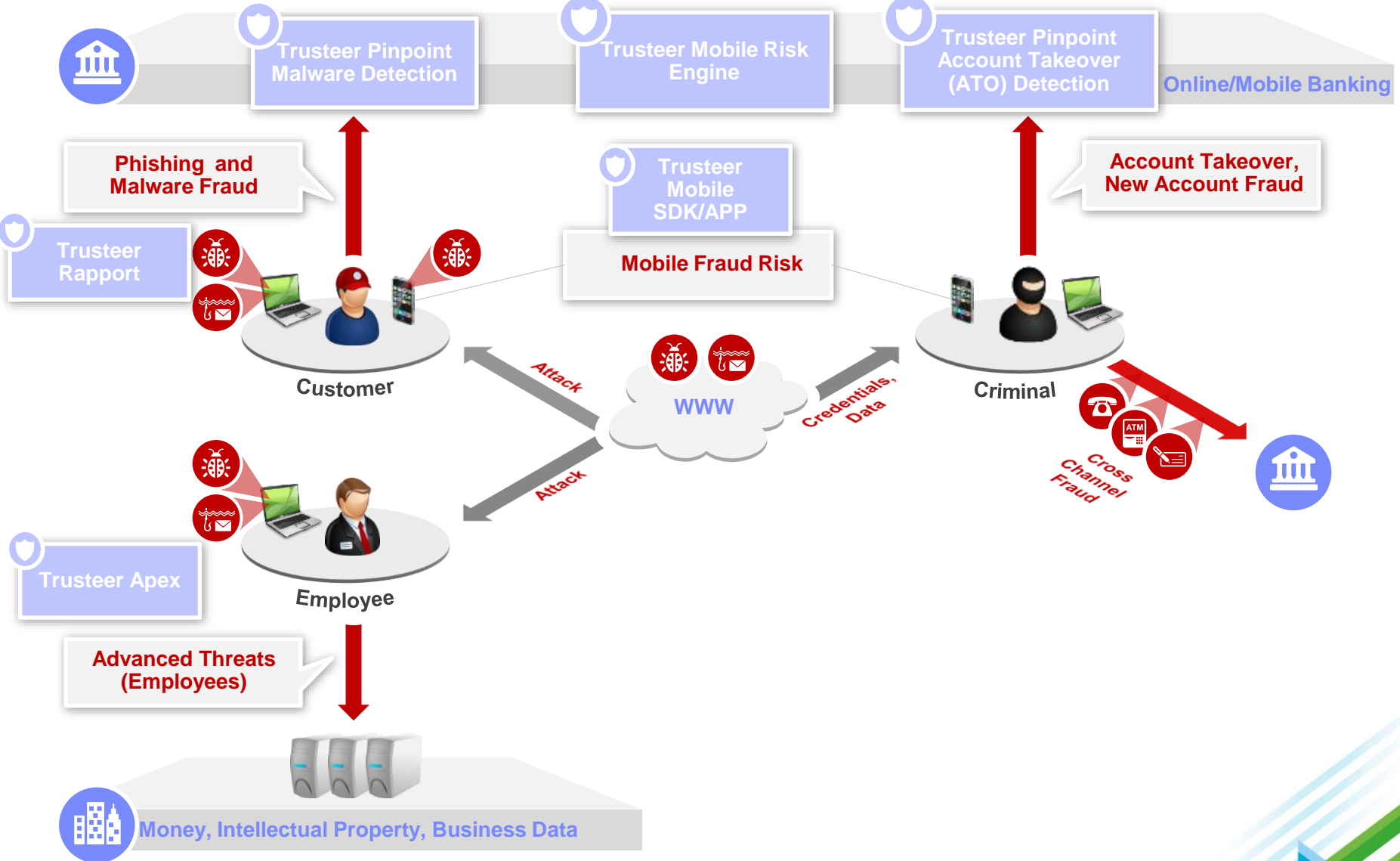
Price : 100\$/1H 150\$/1.30H

- Carding with Ebay & paypal
- Carding with CC & fullz online
- Instore carding (how be safe)
- How Cashout Bank transfer
- How Open Offshore account easy
- How card on Famous Shop (LV,prada ..etc)
- What are botnet ? zeus , spyeye ..etc
- Hacking Method
- Scam method

Contact : ICQ [REDACTED]



This is a Multi-headed BEAST



Security - On a Personal Note...





© IBM Corporation 2013. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>



Thank You!

