



UNIVERSITÀ DEGLI STUDI
DI TRENTO



Crime Pays if You are Just an Average Hacker

Shim Woohyun, Luca Allodi, Fabio Massacci
lastname@disi.unitn.it

Cyber Security 2012 IEEE/ASE Conference
16 December 2012, Washington D.C., USA



Outline

Motivation

- Market for security doesn't really work well [1]
- “There are also the markets we don't like that work entirely too well: for example, the market for stolen goods, that encourages burglary [..]”¹
- Cost of cybercrime:
 - Herley: It's quite tricky to get black market numbers right [2]
 - Anderson: Our investments in security are 10x the gains for the attackers (i.e. we're using the wrong strategy) [3]
- However, we still do not have a model of the economically involved hacker
 - Black markets for attack tools
 - Black markets for compromised hosts
 - Black markets for credit cards

1. MicroMOTIVES and MACROBehavior – Thomas C. Schelling. *Ed. Norton*, pg 30.



Motivation

“Why does an hacker become an hacker?”

What's happening in the black markets

- Do bank robbers manufacture their own guns?

Exploitation success rate: 10-15%

Success rate highly depends on quality of traffic

Средний пробив на связке: 10-25%

* Пробив указывается приблизительный, может отличаться и зависит напрямую от

Install rates, slightly higher than usual:

* Отстук стандартный, даже чуть выше стандартного:

- > Зевс = 50-60% Zeus = 50-60%
- > Лоадер = 80-90% Loader = 80-90%

Price for latest version 1.6.x:

Цена последней версии 1.6.x:

- > Стоимость самой связки = 2000\$ Package cost = 200\$
- > Чистки от АВ = от 50\$ "Clean" from AV = from 50\$
- > Ребилд на другой домен/ИП = 50\$ Rebuild on new domain/IP=50\$
- > Апдейты = от 100\$ Update = from 100\$
- * Связка с привязкой к домену или IP . Package bounded to one domain or IP

♥ 23.03.2011, 19:44

Update for version ..

Апдейт до версии "**Eleonore Exp v1.6.5**"

The package features these exploits:

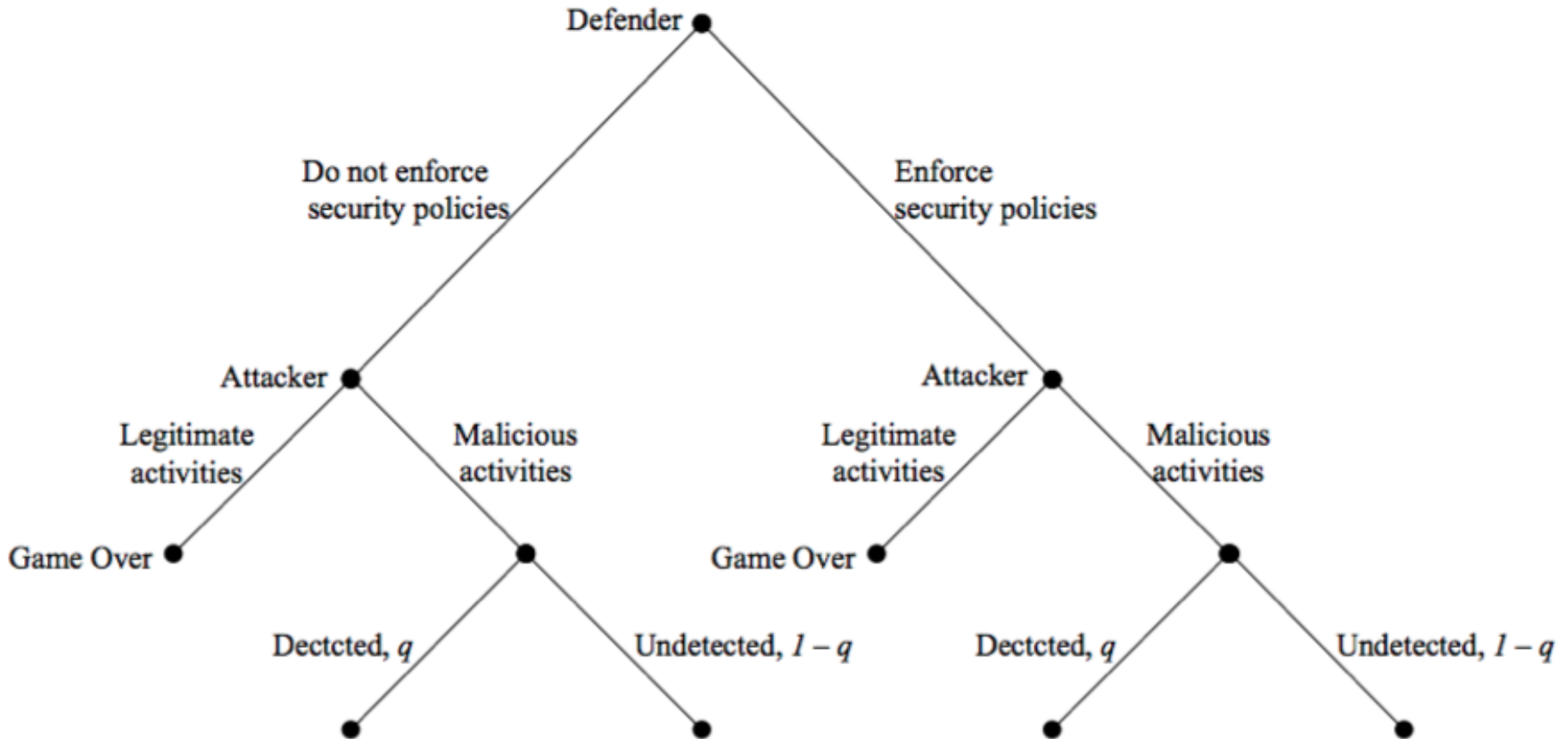
В состав связки входят следующие эксплойты:

- > CVE-2006-0003 (MDAC)
- > CVE-2006-4704 (WMI Object Broke)
- > CVE-2008-2463 (Snapshot)
- > CVE-2010-0806 (IEpeers)
- > CVE-2010-1885 (HCP)
- > CVE-2010-0188 (PDF libtiff mod v1.0)
- > CVE-2011-0558 (Flash <10.2)
- > CVE-2011-0611 (Flash <10.2.159)
- > CVE-2010-0886 (Java Invoke)
- > CVE-2010-4452 (Java trust)

*Виста и 7ка бьется

Work on Vista and Win7

The game



Preliminary Model (1/4)

- To build our model, we look at the attacker:
 - He has limited time
 - Might have a regular job
 - Other activities

T: total time

L: time dedicated to legal activities

I : time dedicated to illegal activities

$$L = (T - I)$$

Preliminary Model (3/4)

- To build our model, we look at the attacker:

T: total time

L: time dedicated to legal activities

I: time dedicated to illegal activities

$$L = (T - I)$$

B: maximum benefit from legal activities

p: probability of earning B

S: minimum benefit from legal activities

$$EU_{\text{Legal}} = L(pB + (1-p)S)$$

- ..With the effects of security policies against criminal activities, enforced by the defender..

q: probability of detection of the criminal activity

t: time to detect and disable criminal activity

Preliminary Model (4/4)

- To build our model, we look at the attacker:

T: total time

L: time dedicated to legal activities

I: time dedicated to illegal activities

$$L = (T - I)$$

B: maximum benefit from legal activities

p: probability of earning B

S: minimum benefit from legal activities

$$EU_{\text{Legal}} = L(pB + (1-p)S)$$

q: probability of detection of the criminal activity

t: time to detect and disable criminal activity

- ..and the potential return for the criminal activity

Z: maximum benefit from a criminal activity

C: cost for the hacker in perpetrating it

$$EU_{\text{Criminal}} = I(q(Zt - C) + (1-q)Z)$$

Preliminary Model (4/4)

- To build our model, we look at the attacker:

T: total time

L: time dedicated to legal activities

I: time dedicated to illegal activities

$$L = (T - I)$$

B: maximum benefit from legal activities

p: probability of earning B

S: minimum benefit from legal activities

$$EU_{\text{Legal}} = L(pB + (1-p)S)$$

q: probability of detection of the criminal activity

t: time to detect and disable criminal activity

Z: maximum benefit from a criminal activity

C: cost for the hacker in perpetrating it

$$EU_{\text{Criminal}} = I(q(Zt - C) + (1-q)Z)$$

Preliminary Model (putting it together)

LEGAL

T: total time
L: time dedicated to legal activities
I: time dedicated to illegal activities
 $L = (T - I)$

B: maximum benefit from legal activities
p: probability of earning B
S: minimum benefit from legal activities

$$EU_{\text{Legal}} = L(pB + (1-p)S)$$

CRIMINAL

q: probability of detection of the criminal activity
t: time to detect and disable criminal activity

Z: maximum benefit from a criminal activity
C: cost for the hacker in perpetrating it

$$EU_{\text{Criminal}} = I(q(Zt - C) + (1-q)Z)$$

Preliminary Model (putting it together)

$$EU_{\text{Legal}} = L(pB + (1-p)S)$$

$$EU_{\text{Criminal}} = l(q(Zt - C) + (1-q)Z)$$



$$EU_M = q[(T-L)(Zt-C) + L(pB + (1-p)S)] + (1-q)[(T-L)Z + L(pB + (1-p)S)].$$

Our approach with the model [4]

- We use a simulation approach
- We fix a “standard value” for each parameter according to our direct observations
- ... briefly describe Krebs et al. [4]
- $p = 0.3$
- $S = 0.5$
- ... and briefly explain why 0.3. and 0.5

Parameters estimation (q)

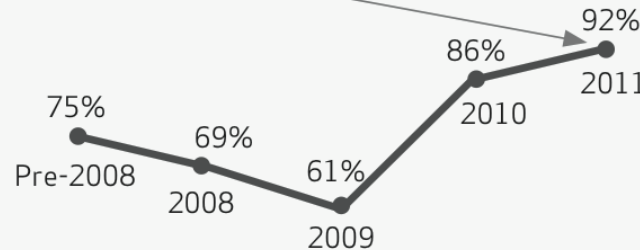
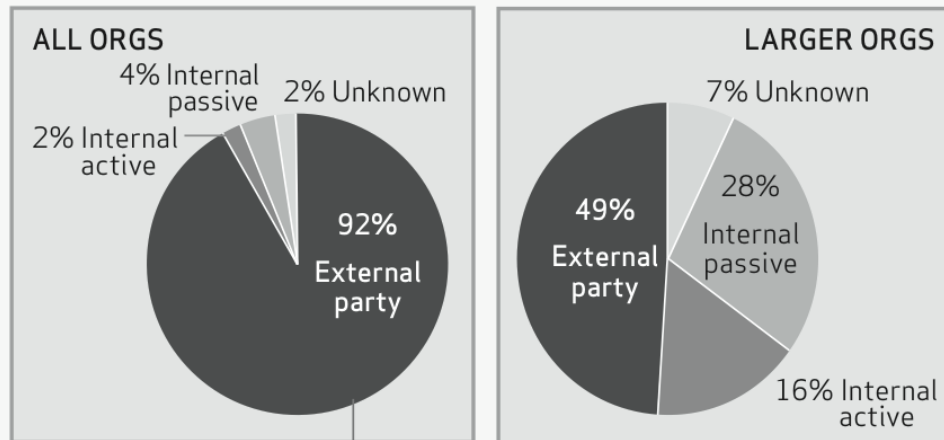
- q =Probability of neutralization by defenders
- Verizon 2012 Incident report

Unfortunately, as our research has shown for the last several years, third parties discover data breaches much more frequently than do the victim organizations themselves.

Parameters estimation (q)

- q = Probability of neutralization by defenders
- Verizon 2012 Incident report

Figure 44. Simplified breach discovery methods by percent of breaches



Parameters estimation (q)

- q =Probability of neutralization by defenders
- Verizon 2012 Incident report
- Grier et. all, CCS 2012 [5]
 - Exploit kits change domain monthly/weekly, meaning that neutralizing them as a threat is extremely difficult (and resource-consuming)

Parameters estimation (q)

- q =Probability of neutralization by defenders
- Verizon 2012 Incident report
- Grier et. all, CCS 2012 [5]
 - Exploit kits change domain monthly/weekly, meaning that neutralizing them as a threat is extremely difficult (and resource-consuming)
- Difficult cooperation between law forces

nakedsecurity

Award-winning news, opinion, advice and research from **SOPHOS**

Meanwhile, Russia's anti-cybercrime unit has claimed that there's a very good reason that it hasn't investigated the Koobface gang - it hasn't been asked to.

Parameters estimation ($q=0.1$)

- q =Probability of neutralization by defenders
- Verizon 2012 Incident report
- Grier et. all, CCS 2012 [5]
 - Exploit kits change domain monthly/weekly, meaning that neutralizing them as a threat is extremely difficult (and resource-consuming)
- Difficult cooperation between law forces

nakedsecurity

Award-winning news, opinion, advice and research from **SOPHOS**

Meanwhile, Russia's anti-cybercrime unit has claimed that there's a very good reason that it hasn't investigated the Koobface gang - it hasn't been asked to.

Parameters estimation (C)

- C =Cost for the attacker
- Exploit kits do not require particular technology (inexpensive)

Parameters estimation (C)

- C=Cost for the attacker
- Exploit kits do not require particular technology (inexpensive)
- Van Eeten OECD Tech Report [6]: criminals are often out of jurisdiction
- Arrest rate is very low, penalties unclear

For example, Yevgeniy Anikin and Viktor Pleschuk, who hacked the WorldPay system of The Royal Bank of Scotland and stole \$10 million from its accounts, were found guilty by a Russian court, yet only received suspended sentences, while those convicted of ordinary

Parameters estimation ($c=0.2$)

- C =Cost for the attacker
- Exploit kits do not require particular technology (inexpensive)
- Van Eeten OECD Tech Report [6]: criminals are often out of jurisdiction
- Arrest rate is very low, penalties unclear

For example, Yevgeniy Anikin and Viktor Pleschuk, who hacked the WorldPay system of The Royal Bank of Scotland and stole \$10 million from its accounts, were found guilty by a Russian court, yet only received suspended sentences, while those convicted of ordinary

Parameters estimation (B,Z)

- B=maximum return from legal activities
- Z=maximum return from criminal activities
- Returns are not only economical, but also related to personal realization (in many forms)

Parameters estimation (B,Z)

- B=maximum return from legal activities
- Z=maximum return from criminal activities
- Returns are not only economical, but also related to personal realization (in many forms)
- We distinguish two cases:
 - $Z > B$
 - Hacker values thrill, fun from hacking, sense of superiority more than lawful returns
 - $B > Z$
 - Hacker values legality and moral self-esteem more than criminal returns

Parameters estimation (B,Z)

- B =maximum return from legal activities
- Z =maximum return from criminal activities
- Returns are not only economical, but also related to personal realization (in many forms)
- We distinguish two cases:
 - $Z=1 > B=0.8$
 - Hacker values thrill, fun from hacking, sense of superiority more than lawful returns
 - $B=1 > Z=0.8$
 - Hacker values legality and moral self-esteem more than criminal returns

Parameters estimation (L)

- L=time dedicated to legal activities
- Hackers are usually young and well educated
 - Meaning they spend time studying and working

novich, Sverdlovsk region, Russia. Education: Professional Pedagogical University of Russia (Applied Informatics in Economics major). Citizen-

Parameters estimation (L)

- L=time dedicated to legal activities
- Hackers are usually young and well educated
 - Meaning they spend time studying and working

novich, Sverdlovsk region, Russia. Education: Professional Pedagogical University of Russia (Applied Informatics in Economics major). Citizenship, Russia. Education: Graduated in 2003 from the School of Computer Systems and Programming of Saint Petersburg State University of Aerospace Instrumentation. Citizenship: Russian

Parameters estimation (L)

- L=time dedicated to legal activities
- Hackers are usually young and well educated
 - Meaning they spend time studying and working
- Does not take a lot of time to run a cyber-criminal activity

“Botnet operation is a mini job, once a day you check for 30minutes, pay once a month server bills, sell for about an hour information on the market and enhance your code if you feel like it. I was thinking about working for Kaspersky, but these guys want all kinds of phony diplomas and can't even recognize native code (see the duqu 'incident'). The profit? Depends, sometimes 400\$ a day, sometimes none, but a steady 40\$ a day with bitcoins alone.”

Parameters estimation ($L=0.9$)

- L =time dedicated to legal activities
- Hackers are usually young and well educated
 - Meaning they spend time studying and working
- Does not take a lot of time to run a cyber-criminal activity

“Botnet operation is a mini job, once a day you check for 30minutes, pay once a month server bills, sell for about an hour information on the market and enhance your code if you feel like it. I was thinking about working for Kaspersky, but these guys want all kinds of phony diplomas and can't even recognize native code (see the duqu 'incident'). The profit? Depends, sometimes 400\$ a day, sometimes none, but a steady 40\$ a day with bitcoins alone.”

Simulations

- We run simulations changing one parameter at a time,
 - From 0.05
 - To 1
 - With 0.05 steps

Simulations

- We run simulations changing one parameter at a time,
 - From 0.05
 - To 1
 - With 0.05 steps
- Each run simulates the policy maker enforcing a policy addressing one particular aspect of the hacker decisional model

Simulation results

Changes in key variable	Model 1 <i>p</i> changes	Model 2 <i>q</i> changes	Model 3 <i>S</i> changes	Model 4 <i>C</i> changes	Model 5 <i>B</i> changes	Model 6 <i>Z</i> changes	Model 7 <i>t</i> changes
0.05						Succeed	
0.1						Succeed	
0.15						Succeed	
0.2						Succeed	
0.25						Succeed	
0.3						Succeed	
0.35						Succeed	
0.4						Succeed	
0.45						Succeed	
0.5						Succeed	
0.55		Succeed	Succeed			Succeed	
0.6		Succeed	Succeed			Succeed	
0.65		Succeed	Succeed			Succeed	
0.7	Succeed	Succeed	Succeed				
0.75	Succeed	Succeed	Succeed				
0.8	Succeed	Succeed	Succeed				
0.85	Succeed	Succeed	Succeed				
0.9	Succeed	Succeed	Succeed				
0.95	Succeed	Succeed	Succeed				
1	Succeed	Succeed	Succeed				



Thanks

Questions?

luca.allodi@unitn.it