UNIVERSITÀ DEGLI STUDI
DI TRENTO

Network Security

AA 2015/2016

Cybercrime economy

Dr. Luca Allodi

What is a market

- A market is a *system* by which services or goods are traded in exchange of a compensation

- There can be many types of markets
  - Financial markets
  - Work / Job position markets
  - ..

- A marketplace is a venue where the market is held
  - Physical (a town's square)
  - Virtual (a website, a chat, other or mixed means)
  - The terms "market" and "marketplace" will be used interchangeably in this lecture

What are the (cybercrime) black markets

- *.. a "black market" economy, built around for profit cybercrime, in which a large number of geographically distributed actors trade in data, knowledge and services [Kurt et al. 2015]*

→ Held in virtual marketplaces

  - Originally IRC
  - Now mostly web-forums

- Trading of
  - Attacking tools
  - Highly efficient exploits; Vulnerabilities
  - Accounts, money laundry, CCNs..

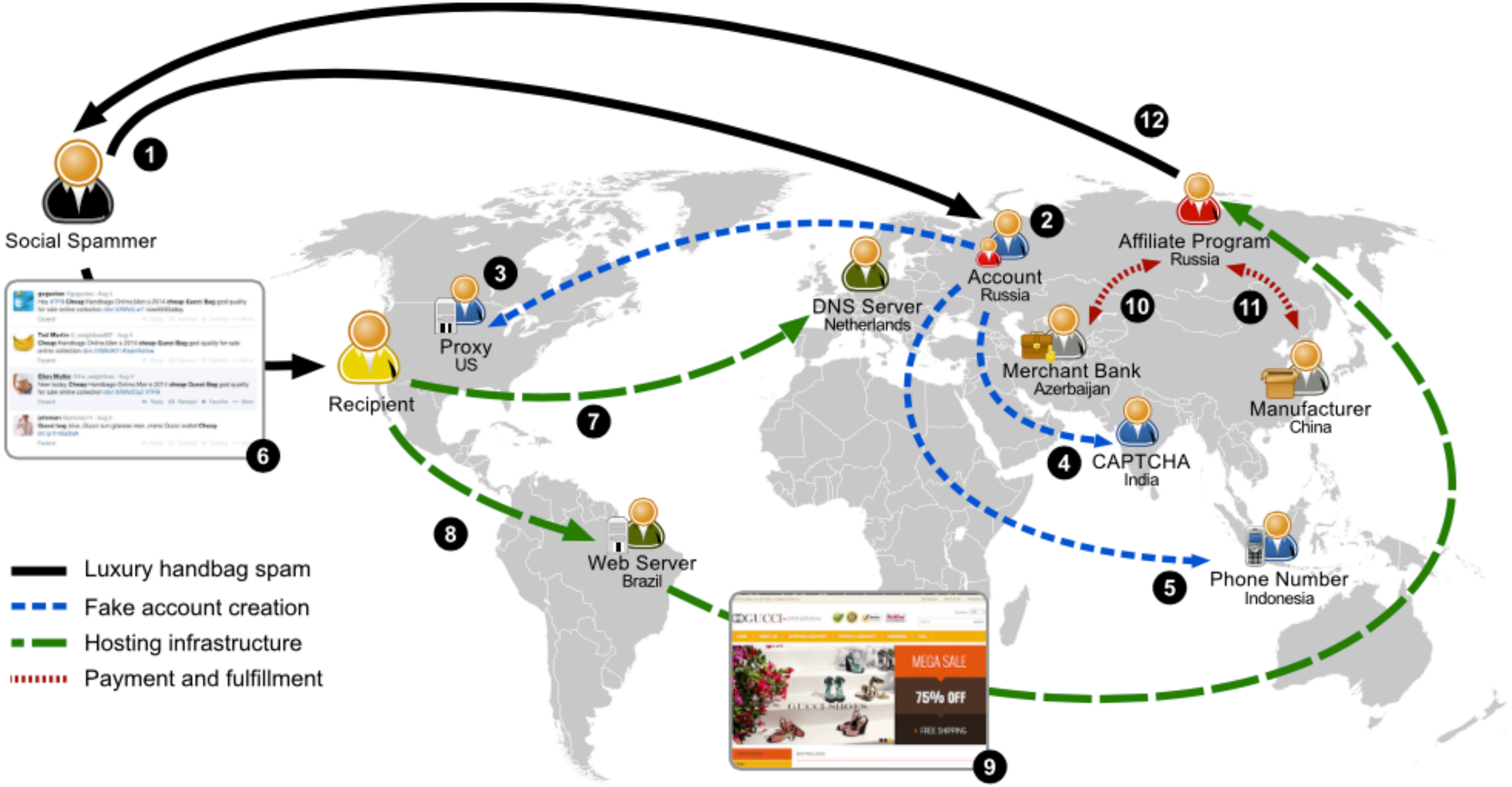
Underground-based market

- “TOR-based markets” →Can’t be reached from “standard” internet
  - → “a network inside the Network”
  - Typically drugs and other illegal good markets
- “Closed markets” → can be reached on the Internet
  - Most tech markets are of this type
  - Markets are closed, entry by selection
  - Organised in different markets
    - Typically “national” → Russian, chinese, brazilian
  - Among most influent there are Russian markets

Types of markets

- Low-tech markets
  - “Spamadvertised” or fake goods
  - Hosting, stolen credentials, ..
- High-tech markets
  - **Cybercrime markets**
    - **Attack delivery technologies**
    - **Malware/specialized payloads (Zeus, Clickbots, ..)**
  - “Private” markets
    - A few players selling high-tech malware to selected customers

Low-tech market –example [Kurt et al. 2015]



High-tech markets: cybercrime as market service

- **Technological vs human vectors for attacks**
  - We are interested in the former
- **Technical competences are concentrated in an underground market for attacks**
  - Trade of advanced exploitation vectors
    - Vulnerabilities, exploits and malware
    - Delivery mechanisms
- Exploit and tool developers sell the technology to multiple clients
  - Can combine several different technologies to personalise the attack

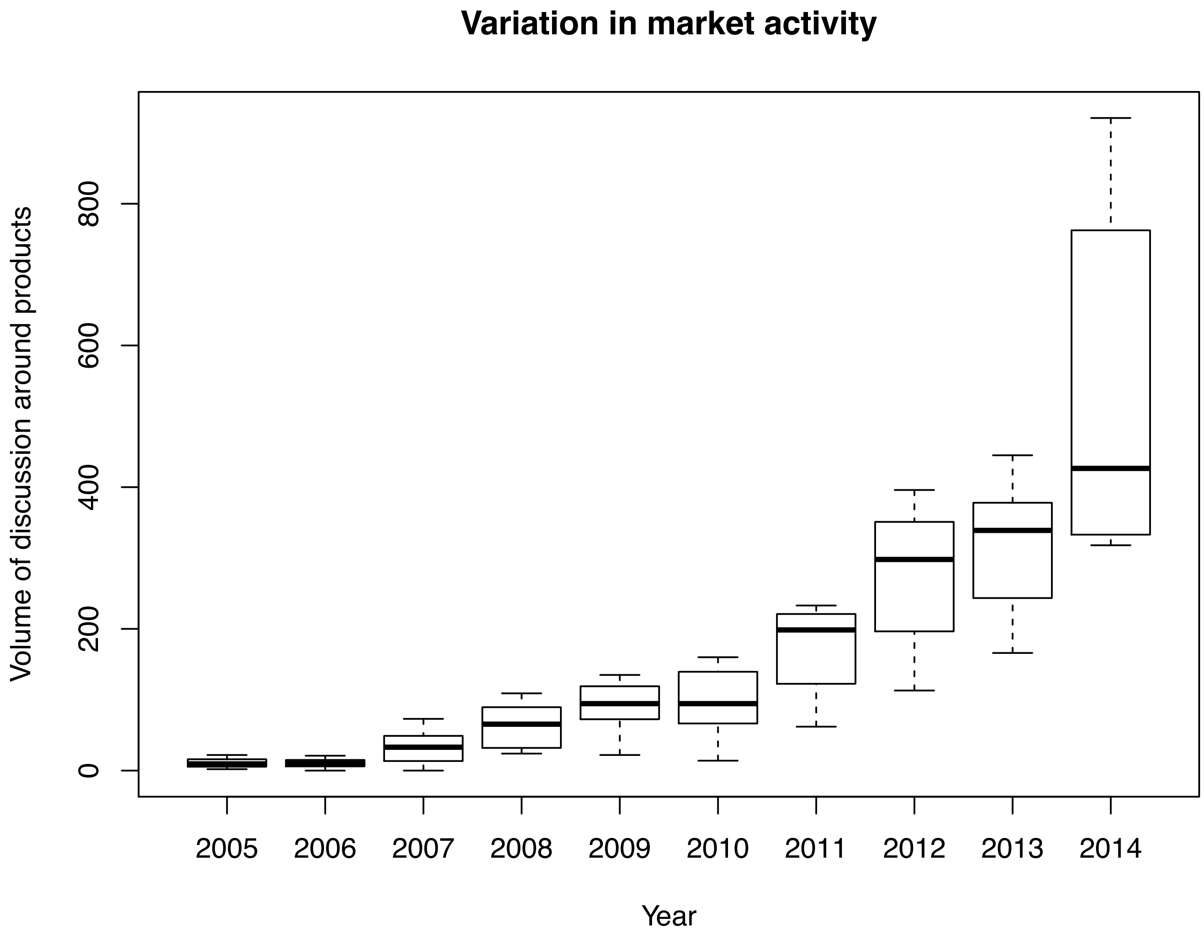
High-tech Cybercrime Markets

- This technology is traded in underground, closed markets
- **We have infiltrated several**
- Today we explore the most prominent one
  - Russian Market
  - On open Internet but closed access
    - Entry-barrier requires credible background, russian language, and passing an entry test
- Infiltrated for 4+ years
  - 1.5 years “break” as we’ve been kicked out of market
    - Much work to get back in
  - TOR access (to avoid firing too many alarms)

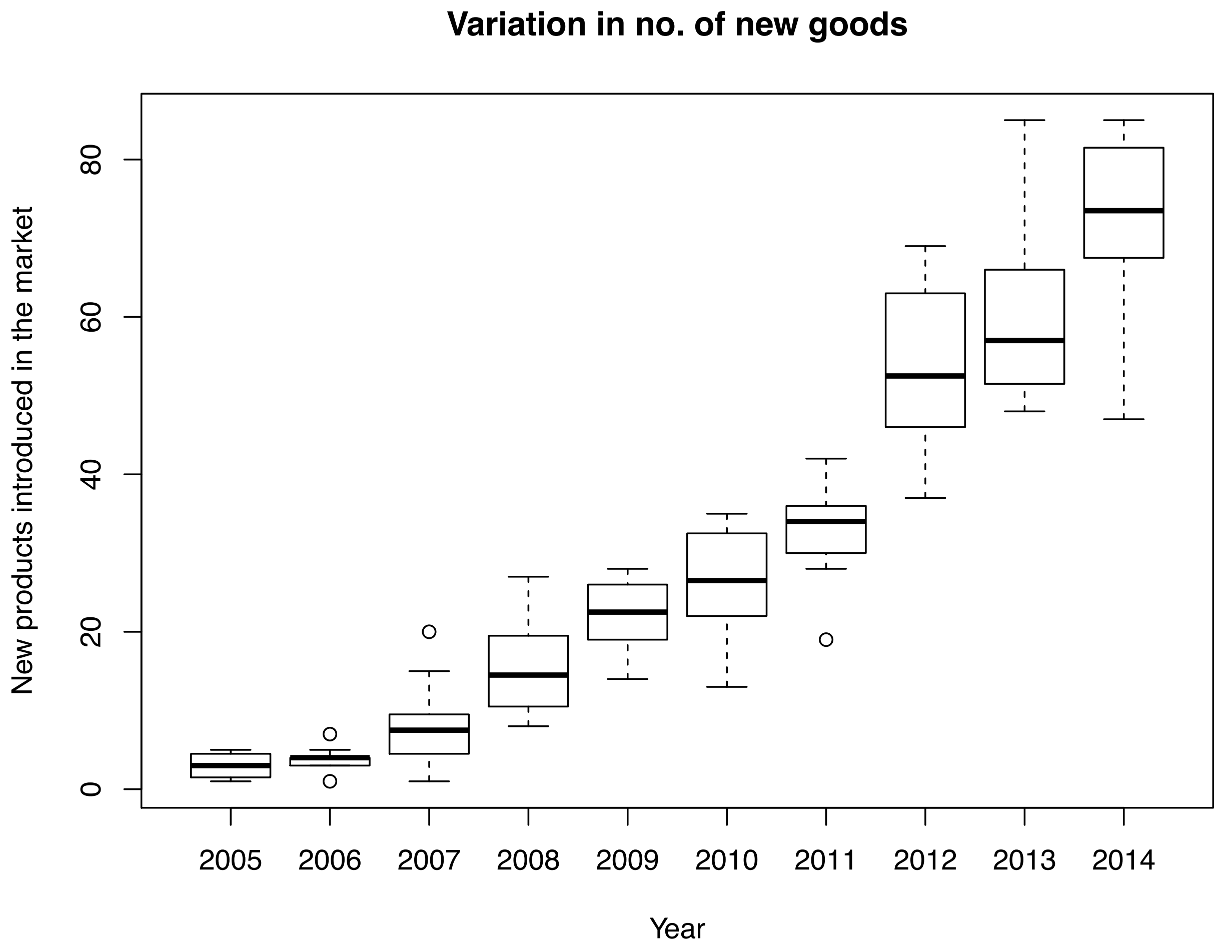
Market organisation

- Several “themes”
  - [Вирусология] → Virusologia → malware, exploits, packs, …
  - [Доступы] → Access → FTP Servers, shells, SQL-i, …
  - [Серверы] → Servers → VPN, proxies, VPS, hosting, …
  - [Социальные сети] → Social networks → accounts, groups, …
  - [Спам] → Spam → emailing, databases, mail dumps, …
  - [Траф] → Internet traffic→ connections, iframes, …
  - [Финансы] → finance → bank accounts, money exchange, …
  - [Работа] → Work → look up for and offer jobs
  - [Разное] → other

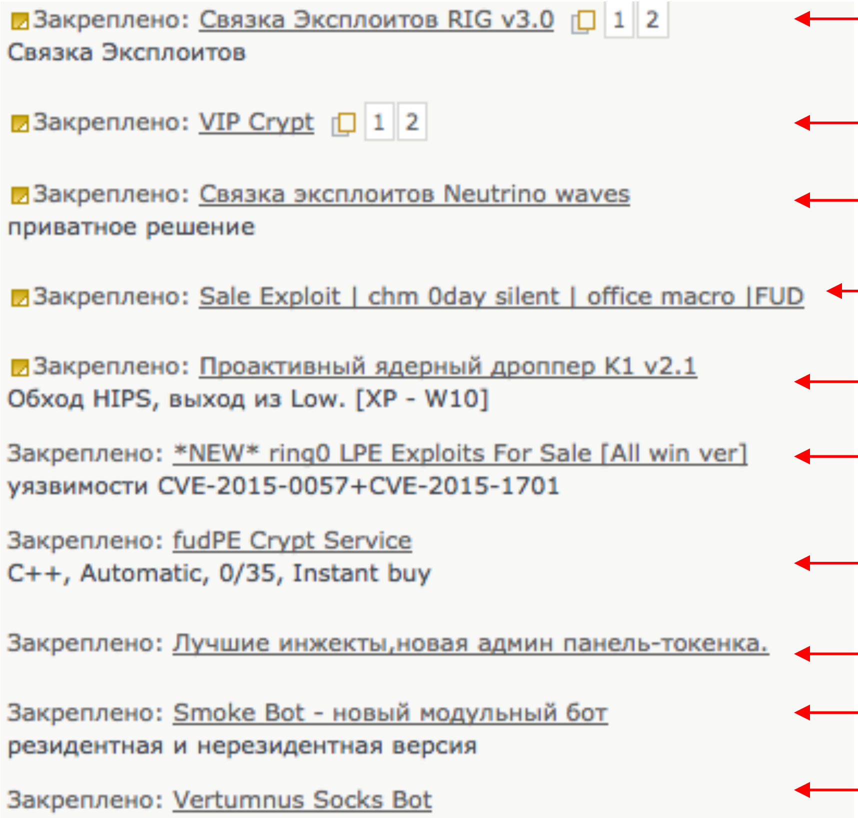
Market activity



Introduction of new goods in the market



Top 10 on “virusologia”



Закреплено: Связка Эксплоитов RIG v3.0 1 2
Связка Эксплоитов

Закреплено: VIP Crypt 1 2

Закреплено: Связка эксплоитов Neutrino waves
приватное решение

Закреплено: Sale Exploit | chm 0day silent | office macro |FUD

Закреплено: Проактивный ядерный дроппер K1 v2.1
Обход HIPS, выход из Low. [XP - W10]

Закреплено: *NEW* ring0 LPE Exploits For Sale [All win ver]
уязвимости CVE-2015-0057+CVE-2015-1701

Закреплено: fudPE Crypt Service
C++, Automatic, 0/35, Instant buy

Закреплено: Лучшие инжекты,новая админ панель-токенка.

Закреплено: Smoke Bot - новый модульный бот
резидентная и нерезидентная версия

Закреплено: Vertumnus Socks Bot

Exploit Kit “RIG v3”

Tool to encryptmalware

Exploit Kit “Neutrino”

Sale of Office exploits

Dropper “Nuclear” (EKit)

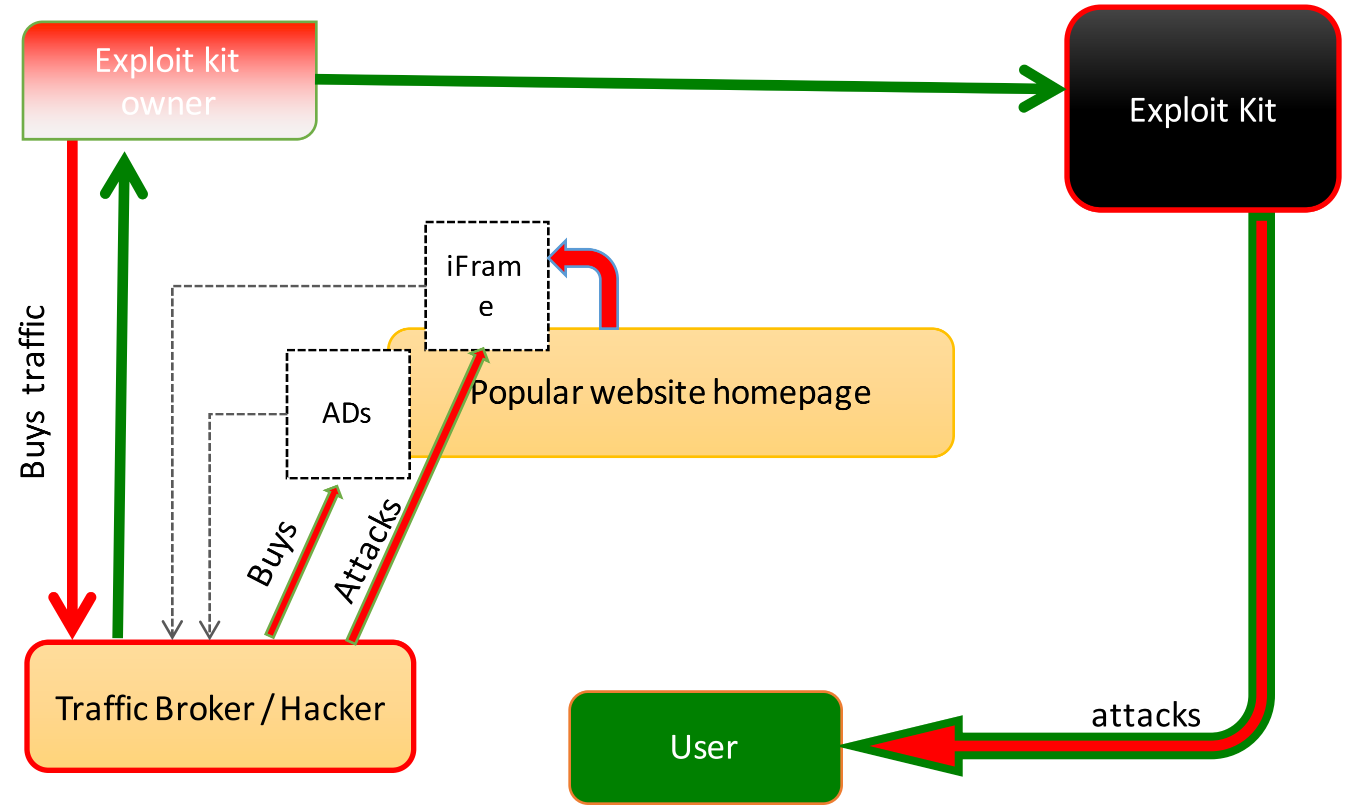
Kernel exploits for Windows

Crypt online service

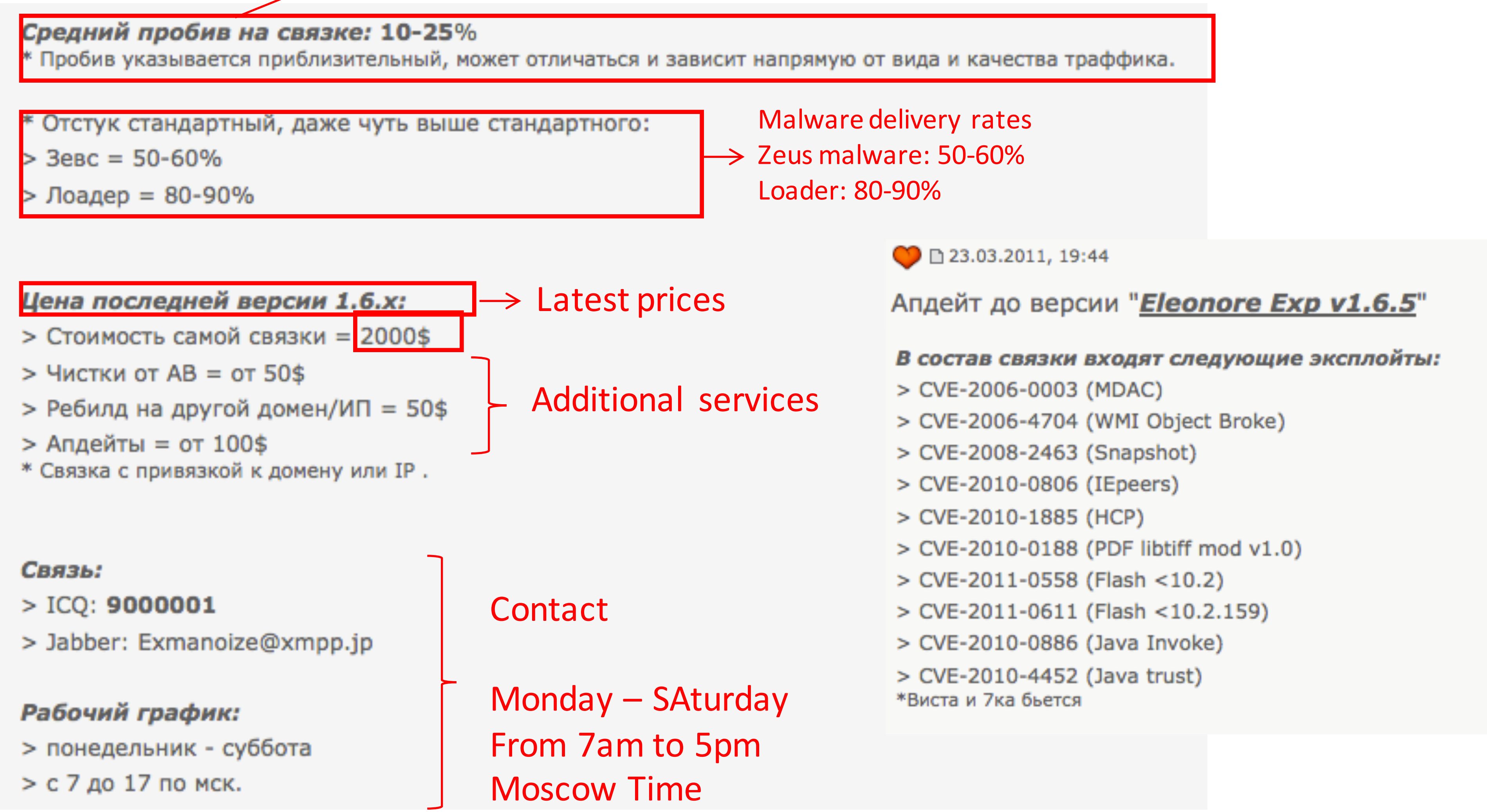
Web attacks injector

Malware bots

A reminder: exploit kits operation



Details of a kit in the market



Kit success rate → *success rates depend on quality of traffic

Средний пробив на связке: 10-25%
* Пробив указывается приблизительный, может отличаться и зависит напрямую от вида и качества траффика.

* Отстук стандартный, даже чуть выше стандартного:
> Зевс = 50-60%
> Лоадер = 80-90%

Malware delivery rates
Zeus malware: 50-60%
Loader: 80-90%

Цена последней версии 1.6.x:
> Стоимость самой связки = 2000$
> Чистки от АВ = от 50$
> Ребилд на другой домен/ИП = 50$
> Апдейты = от 100$
* Связка с привязкой к домену или IP .

Latest prices

Additional services

Связь:
> ICQ: **9000001**
> Jabber: Exmanoize@xmpp.jp

Рабочий график:
> понедельник - суббота
> с 7 до 17 по мск.

Contact

Monday – SAturday
From 7am to 5pm
Moscow Time

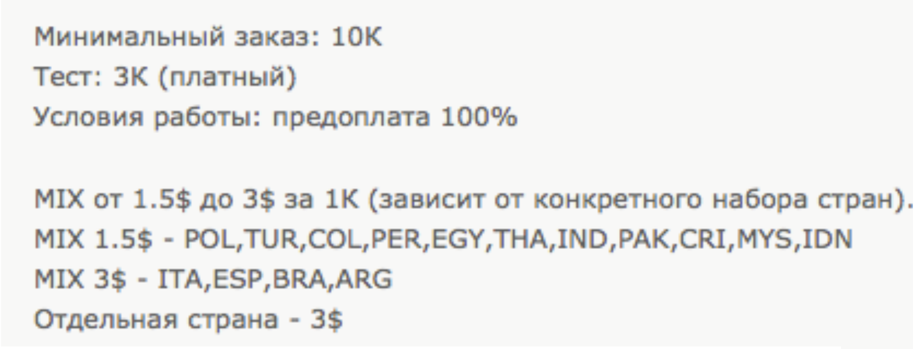
23.03.2011, 19:44

Апдейт до версии "**_Eleonore Exp v1.6.5_**"

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

Selling traffic

- Can buy traffic from “traffic brokers”
  - User does not have to click on anything
  - Automatic redirect
- High-quality traffic derives from selection of connection based on requested criteria
  - Geographic source
  - Installed software



Минимальный заказ: 10K

Тест: 3K (платный)

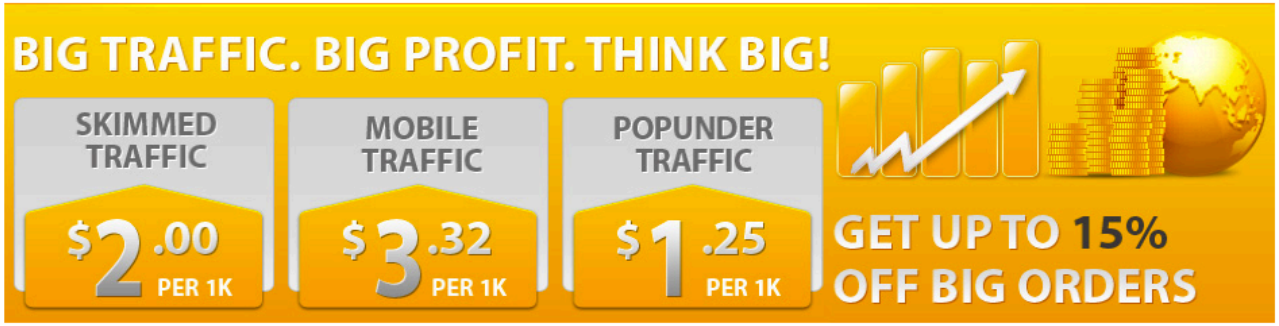
Условия работы: предоплата 100%

MIX от 1.5$ до 3$ за 1K (зависит от конкретного набора стран).

MIX 1.5$ - POL,TUR,COL,PER,EGY,THA,IND,PAK,CRI,MYS,IDN

MIX 3$ - ITA,ESP,BRA,ARG

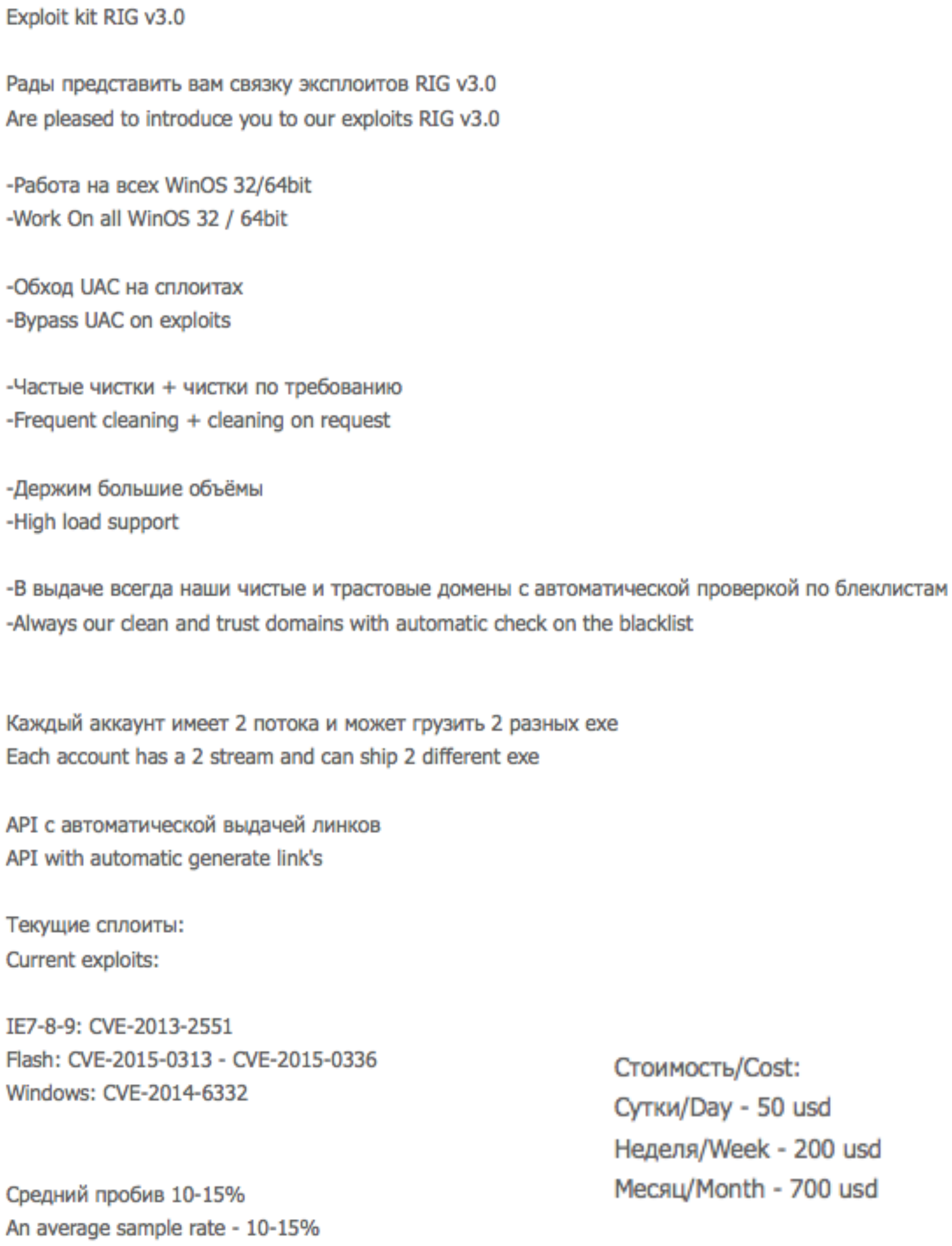
Отдельная страна - 3$



Infect 1 M machines: is it worth it?

Action	**Economic effort (1st year)**
Buy exploit kits (20% efficiency)	2000 USD
Required connections	5 x 10^6
Setup	50-150 USD
Traffic (assuming 2USD/1000 conn.)	10.000 USD
Maintenance (IP/domain flux, packing..)	150 USD
Updates (assuming 2/yr)	~ 200 USD
Total	**~ 12.400 USD – 12.500 USD**
Breakeven ROI/BOT	**~ 0.01 USD**

Another kit



Exploit kit RIG v3.0

Рады представить вам связку эксплоитов RIG v3.0
Are pleased to introduce you to our exploits RIG v3.0

-Работа на всех WinOS 32/64bit
-Work On all WinOS 32 / 64bit

-Обход UAC на сплоитах
-Bypass UAC on exploits

-Частые чистки + чистки по требованию
-Frequent cleaning + cleaning on request

-Держим большие объёмы
-High load support

-В выдаче всегда наши чистые и трастовые домены с автоматической проверкой по блеклистам
-Always our clean and trust domains with automatic check on the blacklist

Каждый аккаунт имеет 2 потока и может грузить 2 разных exe
Each account has a 2 stream and can ship 2 different exe

API с автоматической выдачей линков
API with automatic generate link's

Текущие сплоиты:
Current exploits:

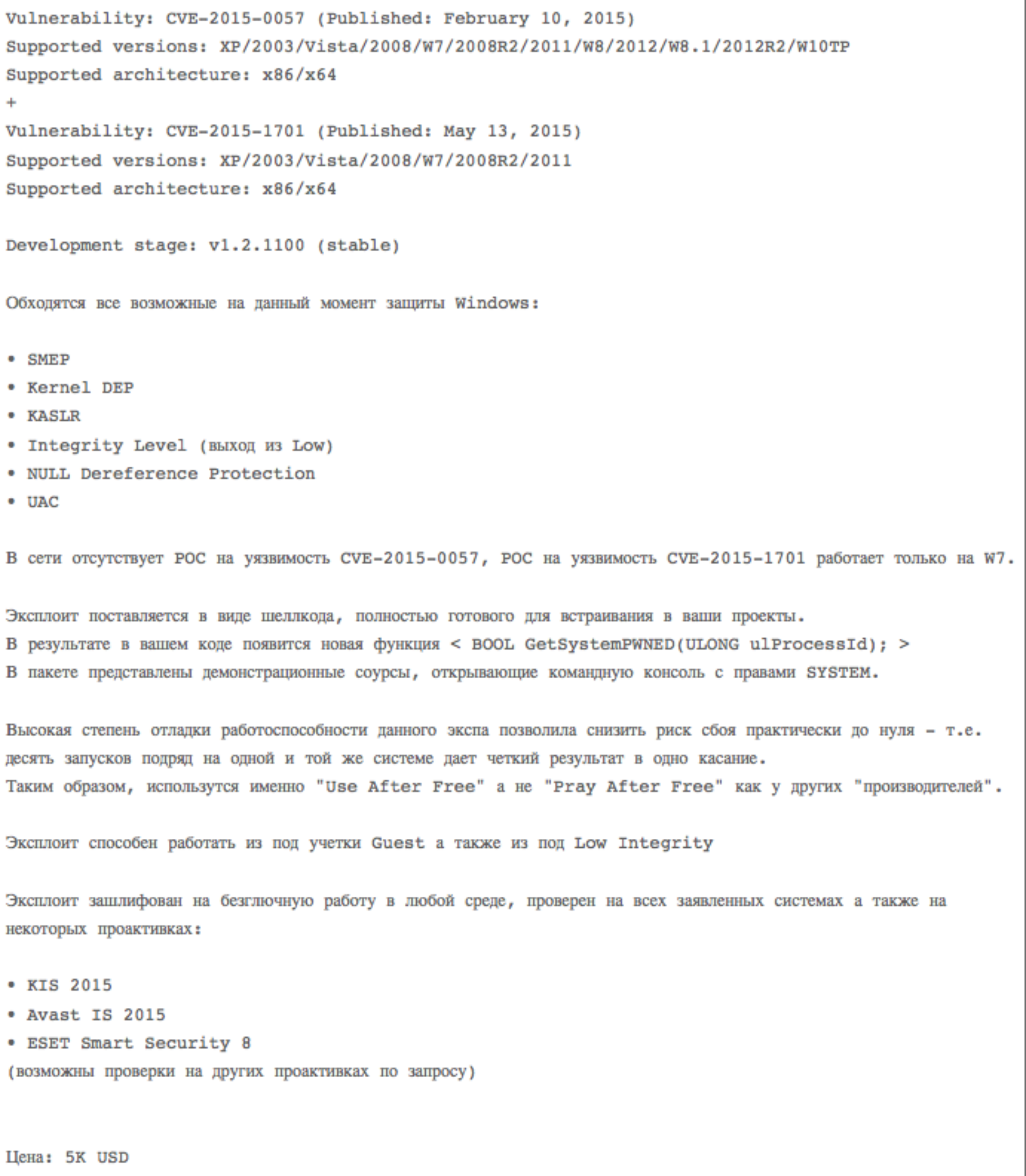
IE7-8-9: CVE-2013-2551
Flash: CVE-2015-0313 - CVE-2015-0336
Windows: CVE-2014-6332

Средний пробив 10-15%
An average sample rate - 10-15%

Стоимость/Cost:
Сутки/Day - 50 usd
Неделя/Week - 200 usd
Месяц/Month - 700 usd

Exploits

- The exploit has a fully customisable shellcode.
- The package includes a demo that opens a command console with SYSTEM privileges.
- The high degree of efficiency of the exploit reduces the risk of failure to virtually zero - that is, ten consecutive successful runs on the same system.
- Thus, it is best used "Use After Free" and not "Pray After Free" as it happens with other "manufacturers".
- Exploit tested for these Avs
- (can test against others upon request)
- Price: 5000 USD



Vulnerability: CVE-2015-0057 (Published: February 10, 2015)
Supported versions: XP/2003/Vista/2008/W7/2008R2/2011/W8/2012/W8.1/2012R2/W10TP
Supported architecture: x86/x64
+
Vulnerability: CVE-2015-1701 (Published: May 13, 2015)
Supported versions: XP/2003/Vista/2008/W7/2008R2/2011
Supported architecture: x86/x64

Development stage: v1.2.1100 (stable)

Обходятся все возможные на данный момент защиты Windows:

- SMEP
- Kernel DEP
- KASLR
- Integrity Level (выход из Low)
- NULL Dereference Protection
- UAC

В сети отсутствует POC на уязвимость CVE-2015-0057, POC на уязвимость CVE-2015-1701 работает только на W7.

Эксплоит поставляется в виде шеллкода, полностью готового для встраивания в ваши проекты.
В результате в вашем коде появится новая функция < BOOL GetSystemPWNED(ULONG ulProcessId); >
В пакете представлены демонстрационные соурсы, открывающие командную консоль с правами SYSTEM.

Высокая степень отладки работоспособности данного экспа позволила снизить риск сбоя практически до нуля - т.е. десять запусков подряд на одной и той же системе дает четкий результат в одно касание.
Таким образом, использутся именно "Use After Free" а не "Pray After Free" как у других "производителей".

Эксплоит способен работать из под учетки Guest а также из под Low Integrity

Эксплоит зашлифован на безглючную работу в любой среде, проверен на всех заявленных системах а также на некоторых проактивках:

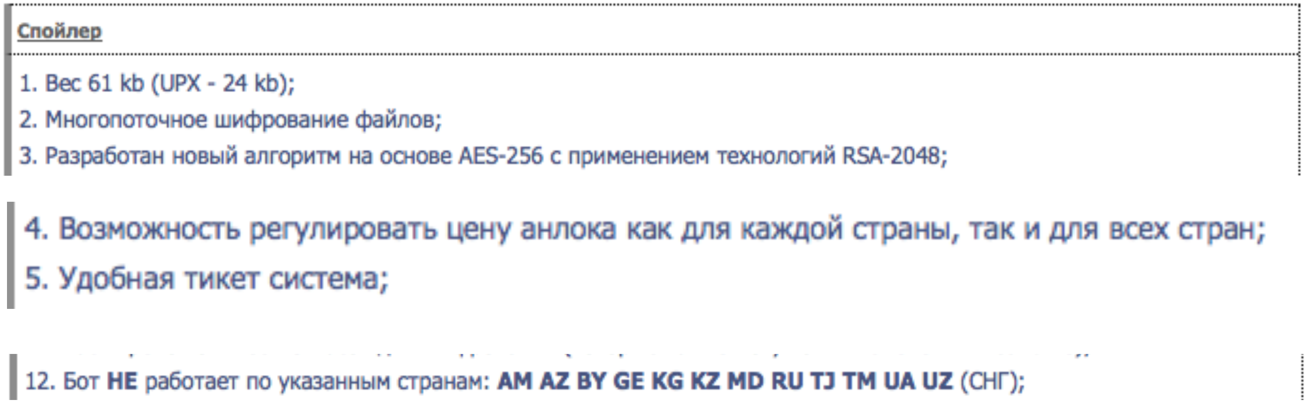
- KIS 2015
- Avast IS 2015
- ESET Smart Security 8

(возможны проверки на других проактивках по запросу)

Цена: 5K USD

Malware

- 1. 61 kb (UPX - 24 kb);
- 2. Multi-threaded file encryption;
- 3.New algorithm based on AES-256 using RSA-2048
- 4. You can set prices based on country
- 5. Handy ticket system
- ...
- 12. Infection disabled for these countries: AM AZ BY GE KG KZ MD RU TJ TM UA UZ (CSI);
- …
- 1. No price, get 50% of revenue.
- 2. Absolutely do not touch CSI countries.
- 3. Instant payments
- ....

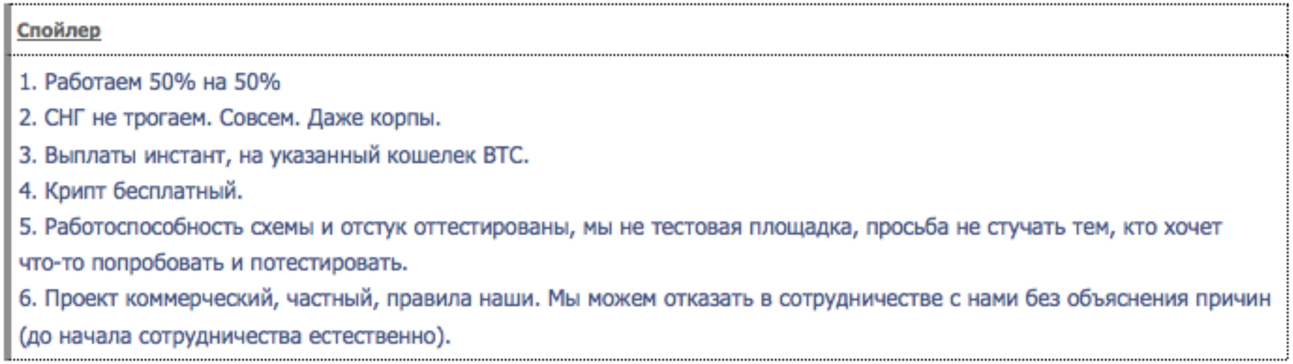


Спойлер

1. Вес 61 kb (UPX - 24 kb);
2. Многопоточное шифрование файлов;
3. Разработан новый алгоритм на основе AES-256 с применением технологий RSA-2048;

4. Возможность регулировать цену анлока как для каждой страны, так и для всех стран;
5. Удобная тикет система;

12. Бот **НЕ** работает по указанным странам: **AM AZ BY GE KG KZ MD RU TJ TM UA UZ** (СНГ);

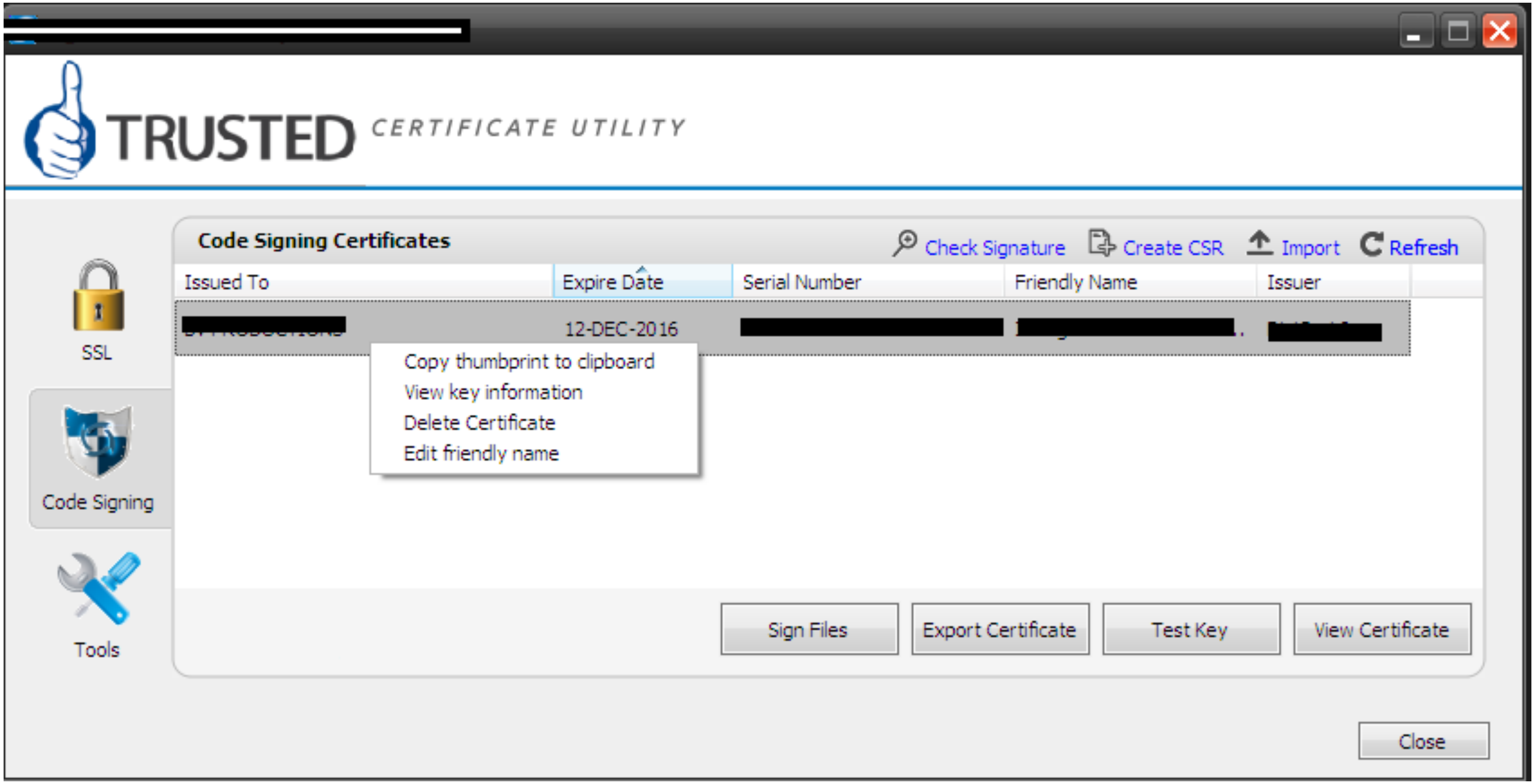


Спойлер

1. Работаем 50% на 50%
2. СНГ не трогаем. Совсем. Даже корпы.
3. Выплаты инстант, на указанный кошелек BTC.
4. Крипт бесплатный.
5. Работоспособность схемы и отстук оттестированы, мы не тестовая площадка, просьба не стучать тем, кто хочет что-то попробовать и потестировать.
6. Проект коммерческий, частный, правила наши. Мы можем отказать в сотрудничестве с нами без объяснения причин (до начала сотрудничества естественно).

Rogue Certificates

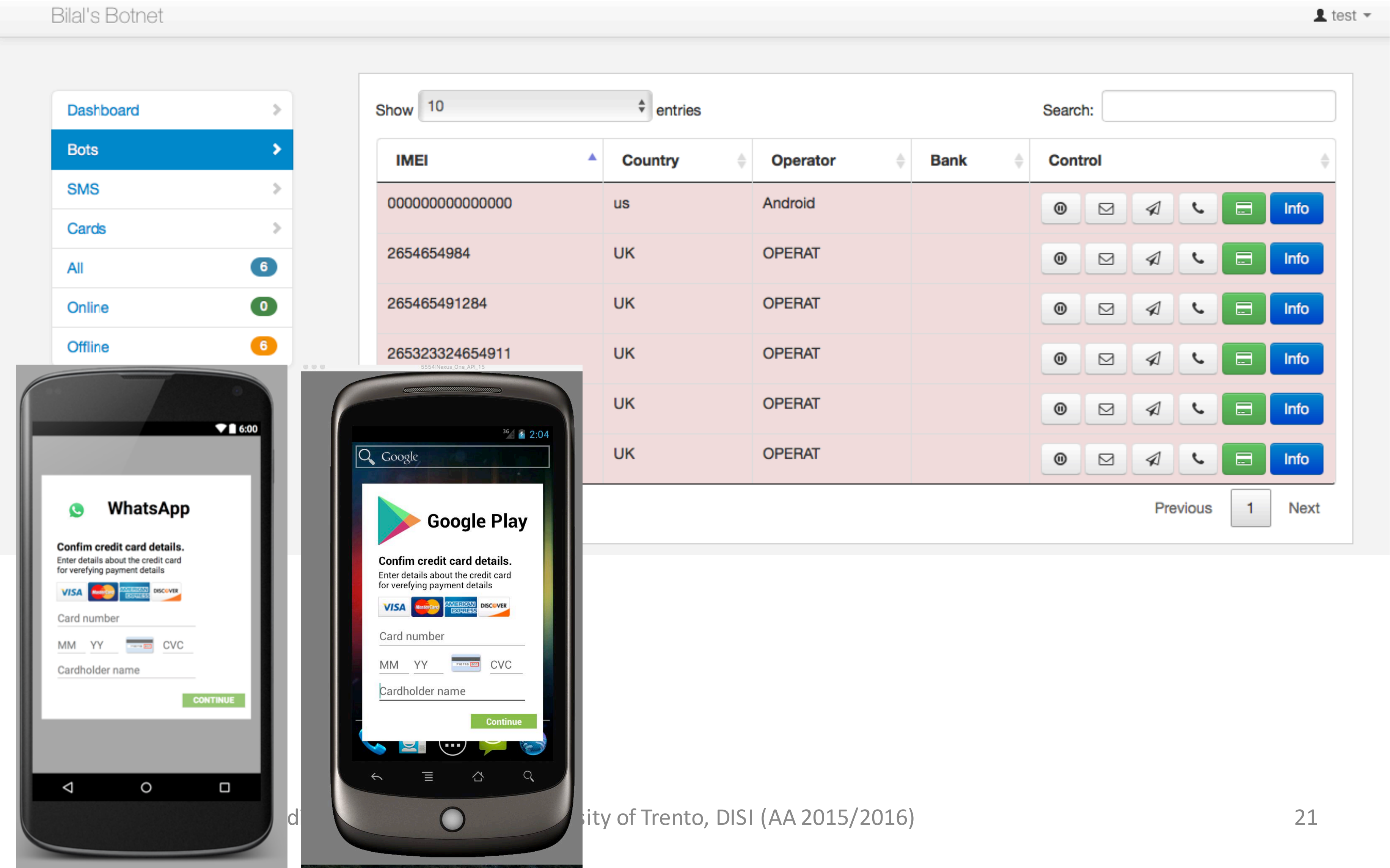
Price: 400 USD



[redacted]

Issued To	Expire Date	Serial Number	Friendly Name	Issuer
[redacted]	12-DEC-2016	[redacted]	[redacted]	[redacted]

Mobile bots



Bilal's Botnet

Show 10 entries Search:

IMEI	Country	Operator	Bank	Control
000000000000000	us	Android		Info
2654654984	UK	OPERAT		Info
265465491284	UK	OPERAT		Info
265323324654911	UK	OPERAT		Info
	UK	OPERAT		Info
	UK	OPERAT		Info

WhatsApp

Confim credit card details.
Enter details about the credit card for verefying payment details

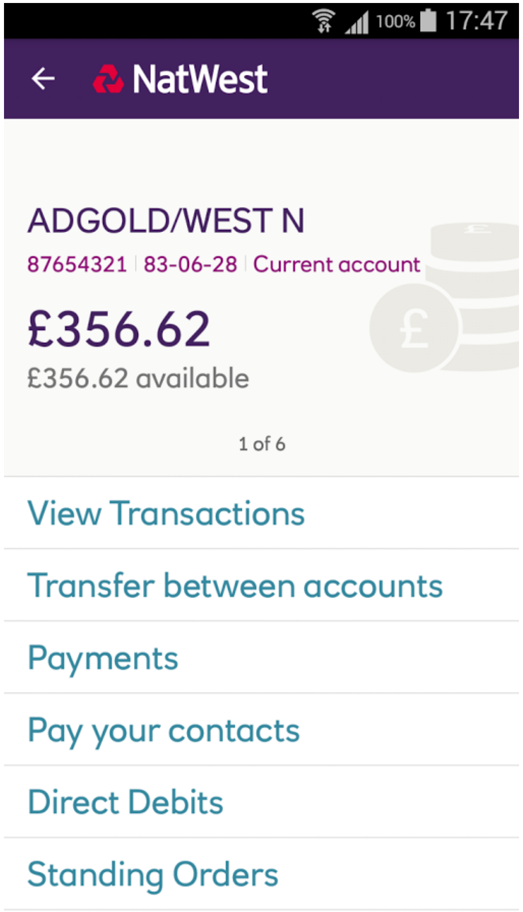
Google Play

Confim credit card details.
Enter details about the credit card for verefying payment details

Price: 4000$ lifetime updates

Mobile bots

Real App



100% 17:47

NatWest

ADGOLD/WEST N

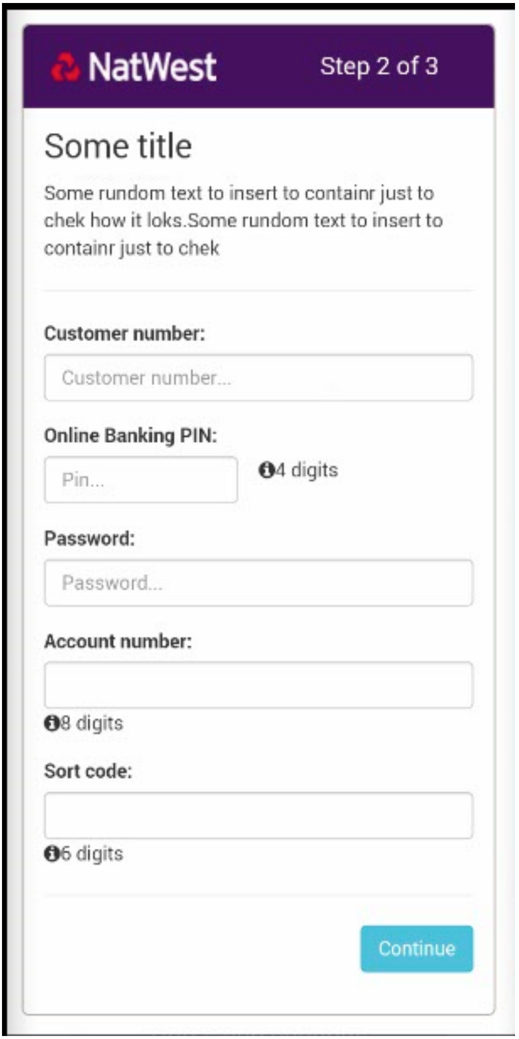
87654321 | 83-06-28 | Current account

£356.62

£356.62 available

1 of 6

Injected page



NatWest Step 2 of 3

Some title

Some rundom text to insert to containr just to chek how it loks.Some rundom text to insert to containr just to chek

Customer number: Customer number...

Online Banking PIN: Pin... 4 digits

Password: Password...

Account number:

8 digits

Sort code:

6 digits

Product demoing

Composition of an attack

- Elements of an attack
  - User connections
  - Attack delivery
  - Malware infection
  - Monetisation mechanism
- Notice that most products sold in the markets enable the attacker to only one of these steps
  - Traffic brokers, stolen accounts, .. → connections
  - Exploit kits, stand-alone exploits, .. → attack delivery
  - Ransomware, banking malware, .. → malware
  - CCNs, banking info, .. → monetisation
- Each of these steps can be combined by the attacker to obtain a set of characteristics that suits them
  - Traffic from northern Europe
  - Exploit kit for recent IE versions
  - Malware that does not infect CSI countries
  - Attack UK bank costumers

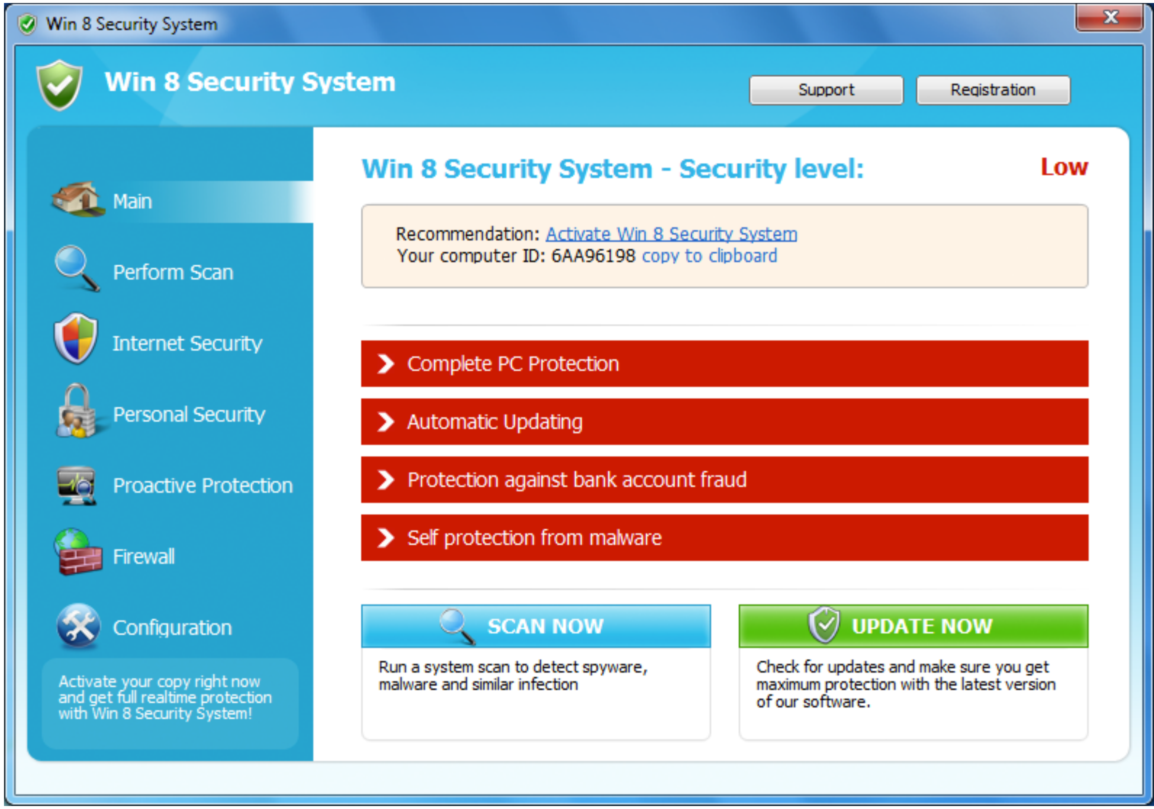
Monetisation

- Selling attacks for a price is not enough to justify the market
- It must be possible to "monetise" the traded technology
    - Several mechanisms to monetise infections are possible
- Very hard to estimate actual value (cost) of attacks for the attackers (victims)
    - Estimates vary greatly
    - Can be used to qualitatively frame the importance of these activities
- All the following is discussed in [Kurt et al. 2015]

“Spamvertised products”

- Spam techniques are used to advertise products
  - Stolen email accounts
  - Social networks
  - Mobile phones / calls..
- Victim is tricked into buying some counterfeit goods
  - Pharmaceutical / electronics / clothes..
  - Pirated software
  - Pornography, gambling, …
- Estimated value 12-90 million US dollars

Scareware



Activate your copy right now and get full realtime protection with Win 8 Security System!

Win 8 Security System - Security level: Low

Recommendation: Activate Win 8 Security System
Your computer ID: 6AA96198 copy to clipboard

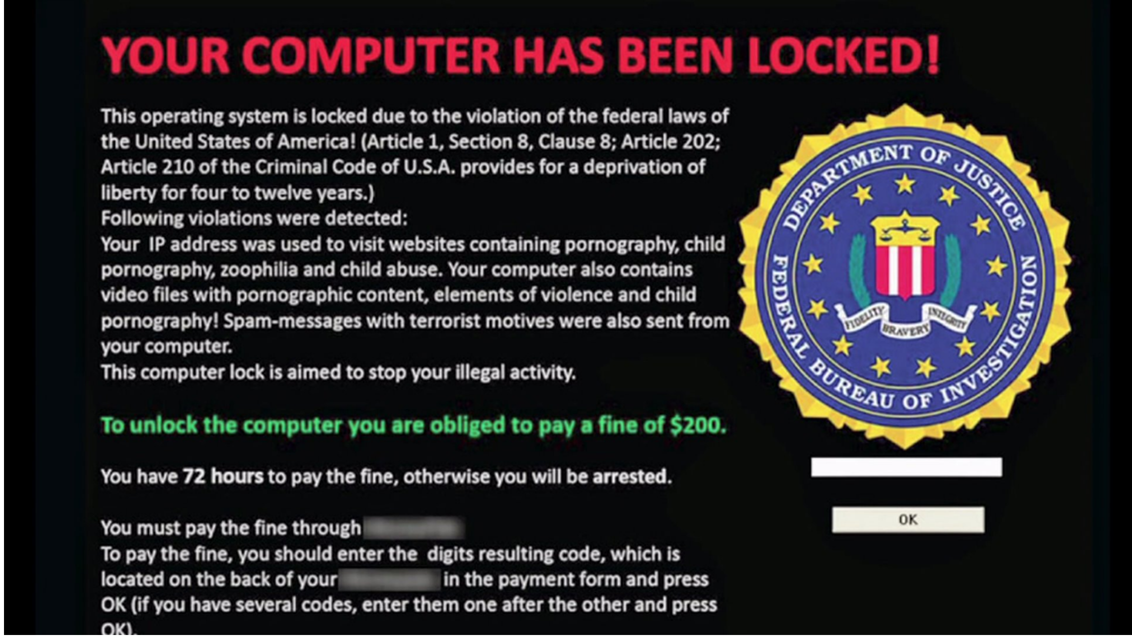
- Complete PC Protection
- Automatic Updating
- Protection against bank account fraud
- Self protection from malware

Run a system scan to detect spyware, malware and similar infection

Check for updates and make sure you get maximum protection with the latest version of our software.

- Uses a combination of social engineering and malware infection
- Convinces user they need to buy a product
  - FakeAV is typical example
- Message convinces user system is infected or at risk
  - Typically pay about 60$ to get the system “cleaned”
- Common threat before 2011
- Estimated value 130 million USD
  - Market dismantled by blocking transactions to FakeAV affiliate programs

Ransomware



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

- Again mixture Social engineering + technical attack
- Malware encrypts file on hard disk
  - Asks for money to give decryption key
  - Usually in the whereabouts of 100-200 $, up to 400 $.
- Can you identify social engineering techniques in the text above?
- Estimated value (Cryptolocker alone): ~ 3 Million USD

Click fraud

- Attacker registers with Ad Network
- Use infected systems to generate clicks on sourced advertisement
- Hard to distinguish between legitimate and fake click
  - Anomaly-based heuristics
- Estimated 20% of all clicks are generated by automatic bots
  - Detection rate up to 75%
- Estimated value ~ 20-30 million USD

Credit cards and banking

- Hard to cache-out credit cards
  - How to maintain anonimity?
- Typically use “money-mules”
  - Victims of social engineering attacks
  - Used by the victim as a proxy to cash CC value
    - Money mule send out of country expensive good to anonymous PO Box
    - Wire transfers to criminals
- Estimates are difficult to make

Market Fairness

- A market only exists when there are sellers that enter the markets and buyers that exchange money for products or services
- Imagine yourself (a criminal) trying to sell your product in a new market
  - Would you really mind scamming people if there is no "punishment" you fear?
  - Would you spend effort time and money in making a good product if you feel like anybody (e.g. the competition) can just ruin you by telling everybody you are a scammer?
- → Unfair market leads to low-quality tech
  - The system needs a mechanism to equilibrate incentives
  - One of the main results from [Akerloff 1970]
- Evidence that high-tech cybercrime markets address these problems with convincing instruments
  - We'll see three stories taken directly from the markets

Trials in cybercrime markets: The rules (in short)

- Anybody can report anybody else for trial
- Follow provided template for filing. Must include
  - Name and profile of the offender
  - Proof of the fact
- The reporter (accuser) and the reported (defender) enter the trial
- The defender has 24 hours to show up
  - In particularly complicated cases the defender can be given up to 7 days
    - → this decision is taken by the Judge (i.e. administrator)
- An investigation follows:
  - Witnesses are called
  - Evidence of either cases (accuser or defender) is provided
- Administrator takes a decision: Black List or Innocent

(1) The defender does not show up

- **October 2013**
- Accuser reports he has been scammed for 390 US $ by defender
- A moderator ("Arbiter") advices to

  "notify the defender with a personal message [about your report]"

- A third user shows up, reporting that

  "[Contacting the defender is] Useless, he has not been online for a long time"

- Administrator gives the defender 48 hours to show up
- Four days later (the 49th hour was Sunday) the administrator puts the defender in the black list

(2) The defender loses the trial

- **July 2012**
- Payment of 3000 WMZ not received;
  - defender is given 12 hours to show up
- Defender shows up after 4 hours
  - Brings evidence of payment (very long discussion)
    - Posts logs & screenshots of transaction
- Accuser answers that the payment has never been received
  - He/She accuses the defender to have “blocked” or “intercepted” the payment
  - Witnesses on his side show up to support his claims and trustworthiness
- Admin gives two options
  - 1) Defender must provide final proof of transaction commit
  - 2) Defender and Accuser resolve the case in private
- → after a month of discussion the defendant hasn’t provided conclusive evidence → he ends up “in the Black” (i.e. listed as an offender)

(3) The defender wins the trial

- **October 2012**
- Accuser reports a failure on the defender’s side to close a transaction
- Reports IRC log of their conversation
  - Accuser pays defender while the latter was offline
  - Defender does not acknowledge the payment and does not come back online in a comfortable “time lapse” for the defender
- Defender shows up shortly after, shows that he never cashed anything
- Admin intervenes and asks

  “[Accuser] please do moneyback. To be precise, [defender] do not touch the checks, and most importantly [accuser] get the money back in your wallet.”
- Accuser stops complaining
- Trial is closed and the defender is cleaned from any accusation

The MalwareLab

An application example

The MalwareLab

- Originally devised as a platform to test malware products as "software artifacts"
- Reproduce the malware in a controlled environment
  - Test, analyze and measure functionalities
  - Safe env to reproduce the Galileo RCS malware by HT
- Example of work: we tested 10 exploit kits to answer the following question:
  - *How resilient are Exploit Kits against software updates?*

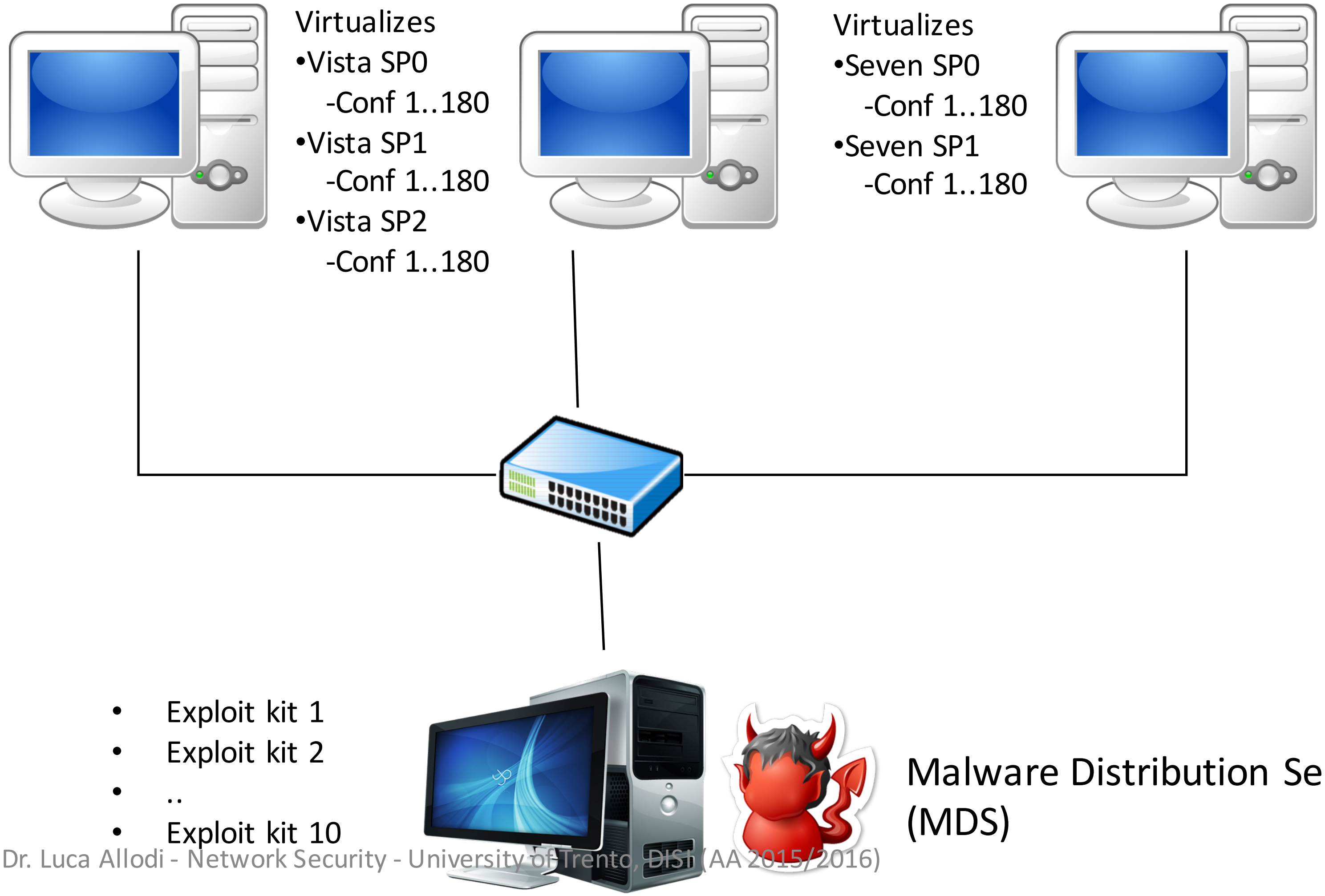
The Kits and The Victims

- Exploit kits span from (2007-2011)
  - How we chose the exploit kits
    - Release date
    - Popularity (as reported in industry reports)
    - CrimePack, Eleonore, Bleeding Life, Shaman, …
- Software: most popular one
  - Windows XP, Vista, Seven
      - All service packs are treated like independent operating systems
  - Browsers: Firefox, Internet explorer
  - Plugins: Flash, Acrobat Reader, Java
- 247 software versions
  - spanning from 2005 to 2013
- We randomly generate 180 sw combinations (x9 Operating Systems) to be the configurations we test
- Manual Test is Impossible → we need an automated platform

Configuration example

- One configuration for: Windows XP Service Pack 2
  - Firefox 1.5.0.5
  - Flash 9.0.28.0
  - Acrobat Reader 8.0.0.0
  - Quicktime 7.0.4.0
  - Java 1.5.0.7
- One configuration for: Windows Seven Service Pack 1
  - Firefox 8.0.1.0
  - Flash 10.3.183.10
  - Acrobat Reader 10.1.1.0
  - Quicktime: No version
  - Java 6.27

The experimental Infrastructure



VICTIM 1

Virtualizes:
- •XPSP0 -Conf 1..180
- •XP SP1 -Conf 1..180
- •XP SP2 -Conf 1..180
- •XPSP3 -Conf 1..180

VICTIM 2

Virtualizes
- •Vista SP0 -Conf 1..180
- •Vista SP1 -Conf 1..180
- •Vista SP2 -Conf 1..180

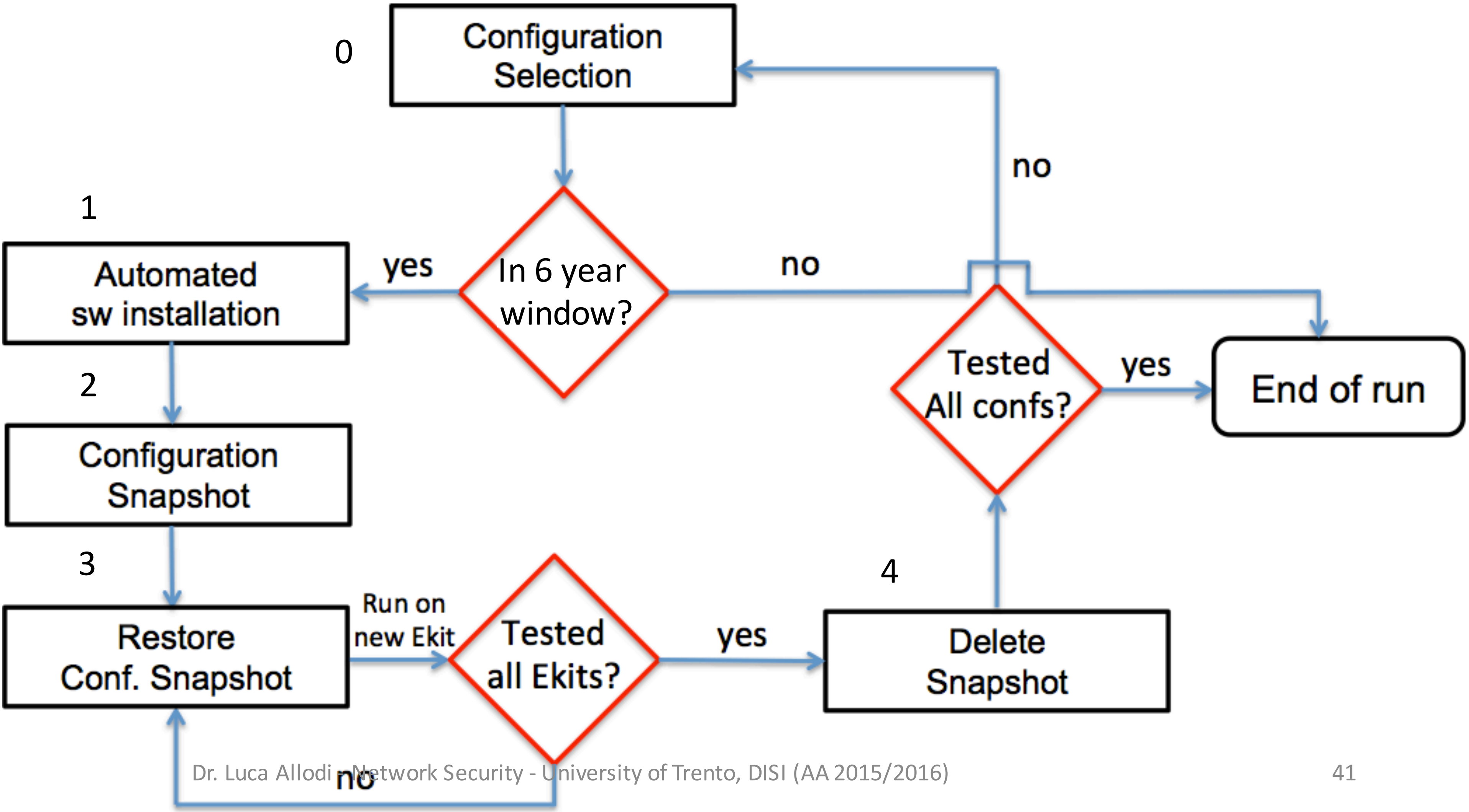
VICTIM 3

Virtualizes
- •Seven SP0 -Conf 1..180
- •Seven SP1 -Conf 1..180

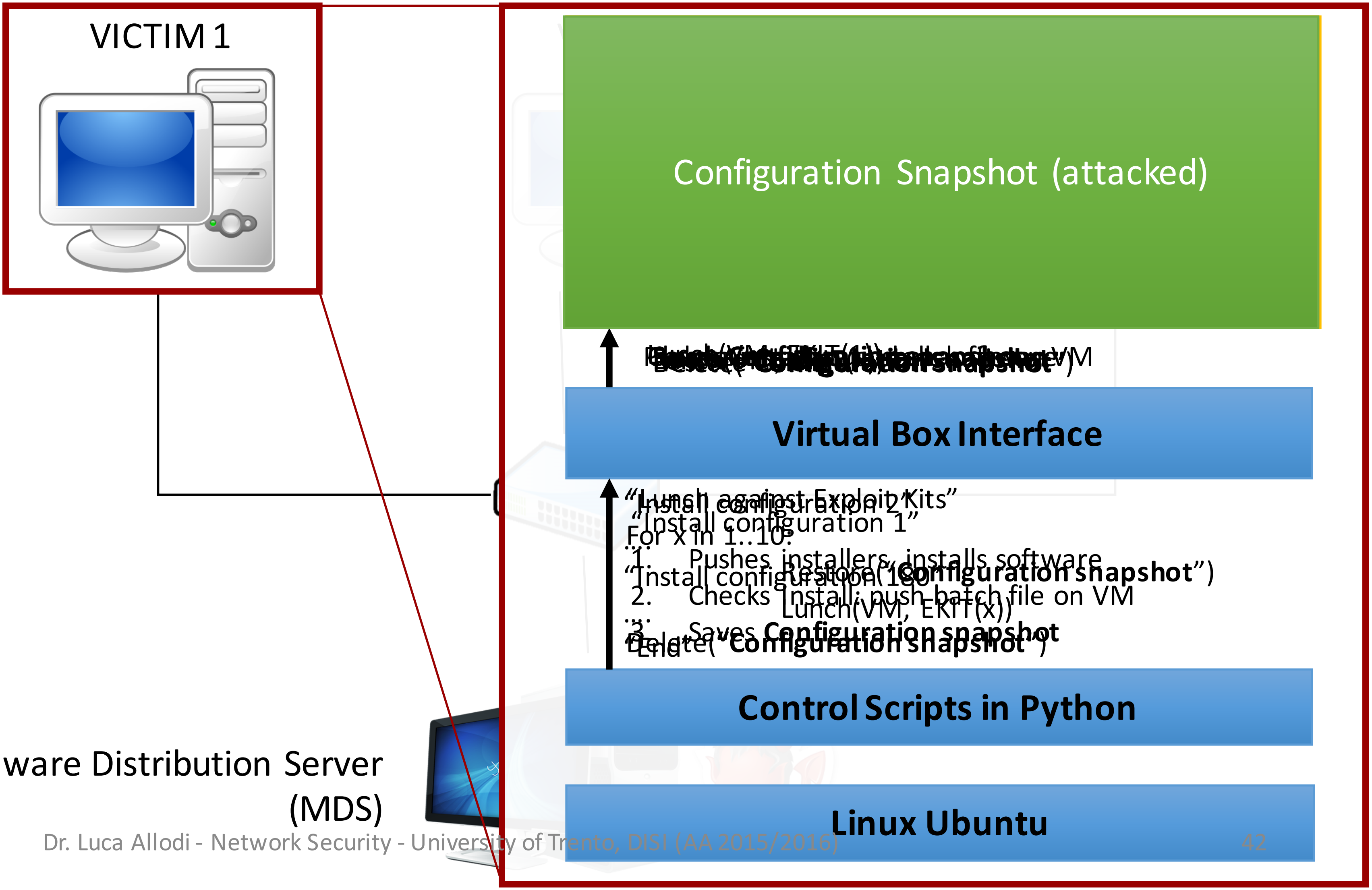
- Exploit kit 1
- Exploit kit 2
- ..
- Exploit kit 10

Malware Distribution Server (MDS)

Overview of the experiment



The experiment: VICTIM

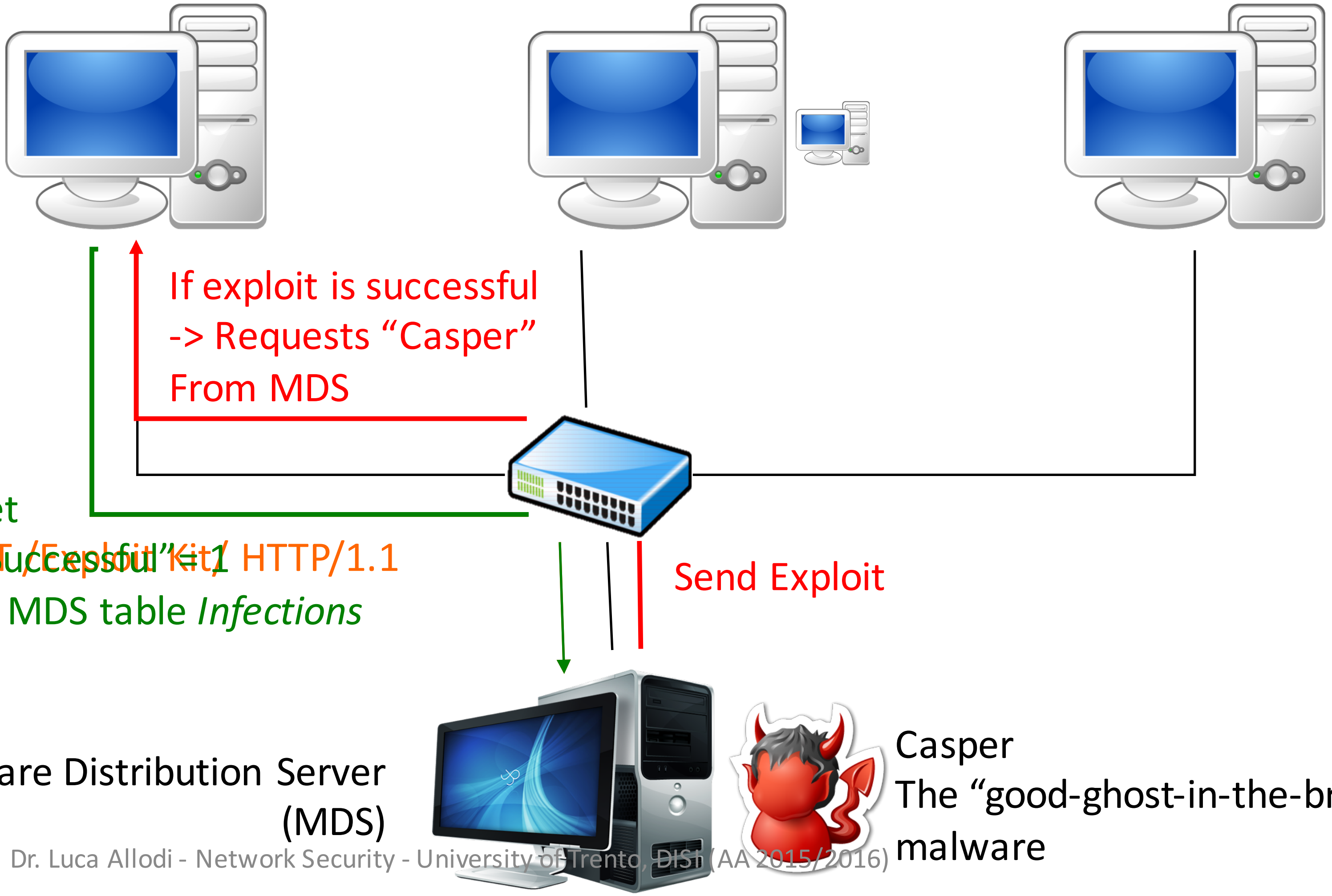


VICTIM 1
Configuration Snapshot (attacked)
Virtual Box Interface
Control Scripts in Python
Linux Ubuntu
Malware Distribution Server (MDS)

Lunch(VM, EKIT(i))
Delete(“Configuration snapshot”)
[illegible] VM

“Lunch against Exploit Kits”
“Install configuration 2”
“Install configuration 1”
For x in 1..10:
…
1. Pushes installers, installs software
“Install configuration 100”
Restore(“**Configuration snapshot**”)
2. Checks Install: push batch file on VM
Lunch(VM, EKIT(x))
…
3. Saves **Configuration snapshot**
Delete(“**Configuration snapshot**”)
End

Assessing exploit successes



VICTIM 1

VICTIM 2

VICTIM 3

If exploit is successful
-> Requests “Casper”
From MDS

Set
“Successful”=1
In MDS table *Infections*

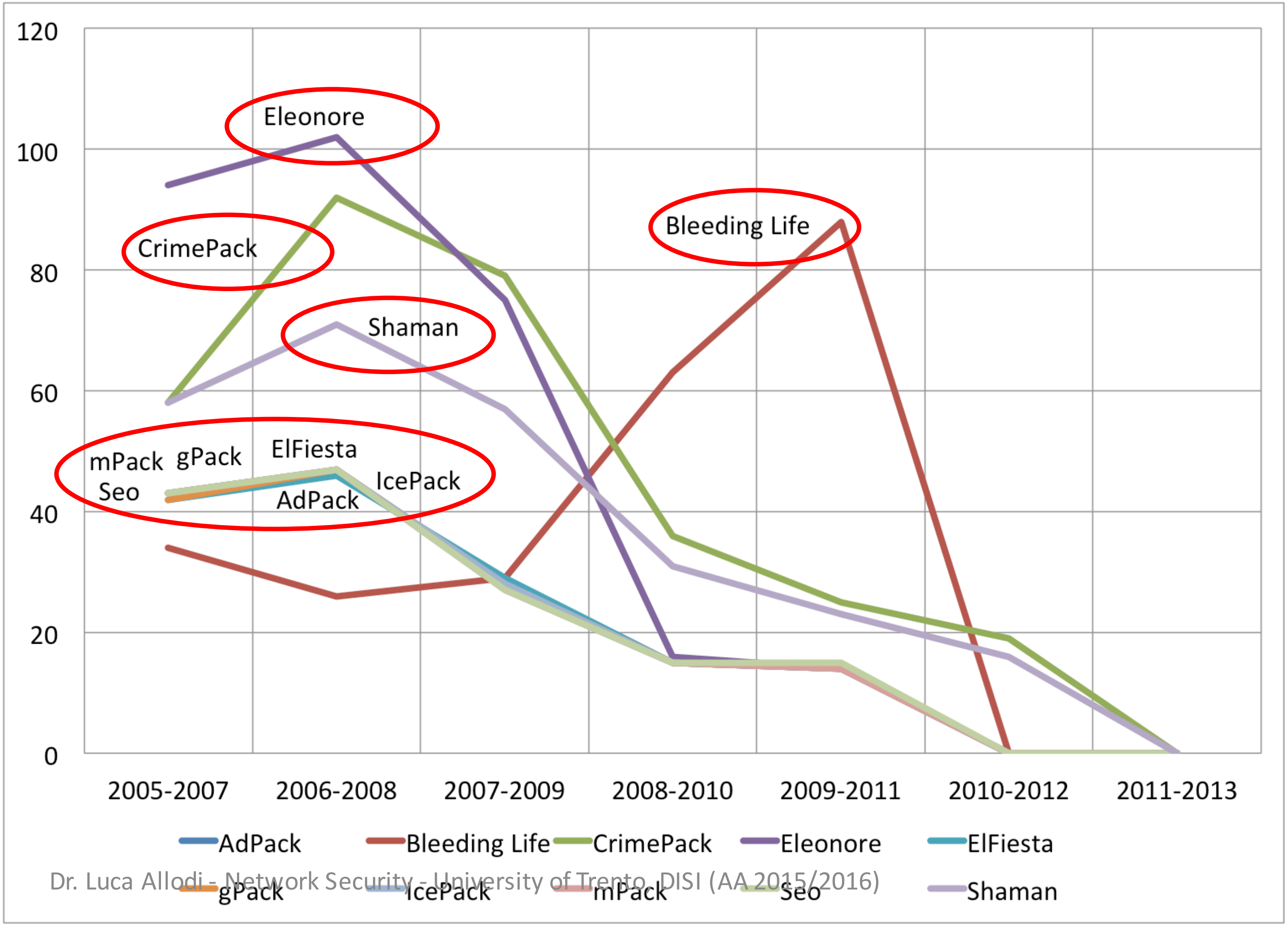
GET /Exploit Kit/ HTTP/1.1

Send Exploit

Malware Distribution Server
(MDS)

Casper
The “good-ghost-in-the-browser”
malware

Results: Infections



Interested in performing similar experiments?

- Could be subject for a research project or a thesis

Bibliography

- Grier, Chris, et al. "Manufacturing compromise: the emergence of exploit-as-a-service." *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012.
- L. Allodi, M. Corradin, and F. Massacci. Then and now: on the maturity of the cybercrime markets (the lesson that black-hat marketeers learned). *IEEE Trans. on Emerging Topics in Compu*ting, PP(99), 2015.
- Huang, Kurt Thomas Danny Yuxing, et al. "Framing Dependencies Introduced by Underground Commoditization." In Proceedings of WEIS 2015.