Dmitry Slinkov, CISM
SWISS CYBER STORM 2015

Black market of cybercrime in Russia

WHOAMI

- Information Security Manager (Russia and CIS)

- Information Security Officer

- Information Security Consultant and Researcher

DISCLAIMER

- This was done in **research purposes only**
- All **LIVE** data is from **07.2015 – 10.2015**
- The story is not related with my **EMPLOYER**
- This data was shared with **NOBODY** before
- Thx to **graphite @ DCUA CTF team**

INTRODUCTION

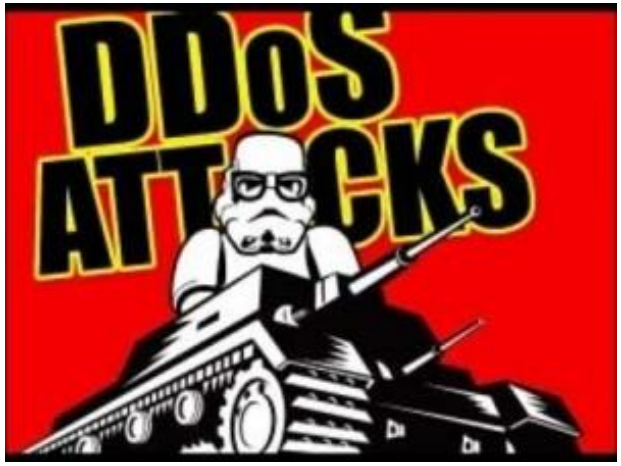
- What do I want?
  - Get understanding of the market
  - Test hackers services and their skills
  - Understand the balance between attack and defense costs
  - Do not finance cybercrime = only post payments ☺
  - Do not violate the law

CYBERCRIME MARKET OVERVIEW

- Services
  - Malware: Trojans, Cryptors, Botnets
  - **DDoS services**
  - **Hacking services: emails, web-sites**
  - Code sign certificates
  - Carding: Money laundering, CC requisites
  - Document scans
  - Anonymous proxies, servers, VPN, etc.
- Hackers boards: exploit.in, darkmoney.cc, antichat.ru, hpc.name, crimelow.com, migalki.net, etc.

DDoS services

- Lots of ads. about DDoS found



- Prices
  - From 50$ to 400$ per day
  - Depends on hosting type:
    Shared<VPS<VDS<AntiDDoS protected

- Some services offer DDoS attacks and protection in the same time! ☺

HONEYPOT INFO

Cheapest instance from big Cloud Hosting:

- 512MB
- 20 GB SSD
- 1 CPU Core
- Amsterdam data center
- No DDoS protection!

Web server:

- Ubuntu 14.04
- Apache/2.4.7
- Static HTML web-site

DDoS Experiment

- ddos-stress.cc:
  - 80$ per day or more
  - **Free test for 5-10 mins**
- DDoS services on crimelow.com board
  - **150$ per day or more**
  - **Free test for 2 mins**
- Promised attack profile:
  - GET requests
  - TCP flood
  - UDP flood

#NEGOTIATIONS

Me: I want to order DDoS on http://….e.su

Hacker: let me check

Hacker: It is protected by DDoS service, the cost is 100$ per day. Agree? Others will offer 150 and more…

Me: OK. Lets make a test.

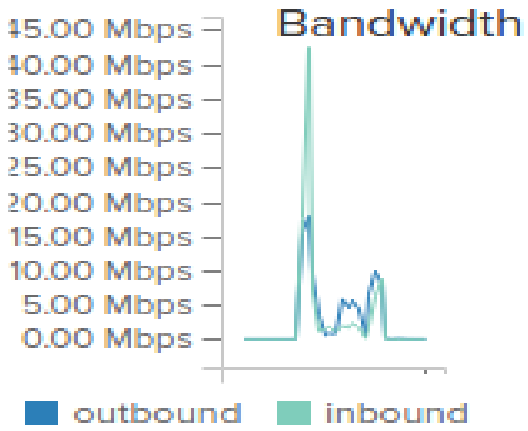
Hacker: I already did it.

Me: I did not see. The web-site works.

Hacker: OK, for another 2 minutes.

1st DDoS Attack

- Packets per second: 80496
  - TCP: 78977
  - ICMP: 1519
- **Unique TCP source IPs: 2762344**
  - Port 80: 99.9%
  - Size: 40 bytes
  - **Type: ACK flood only**
- Unique ICMP source IPs: 33741



- Result: web-site was up during the attack

#DURING THE ATTACK

Me: web-site is still up

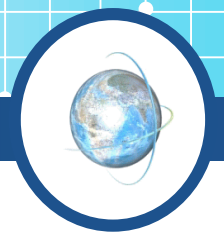
Hacker: there are 3 proxies, I want to find the real IP

Me: I thought it's just a VPS with a real IP…

Hacker: I will not take this web-site, seems that they were already attacked and there's a DDoS protection.

Me: Ok.

2nd DDoS Attack



- Packets per second: 39081 (about 1,1 Gb/s)
  - TCP: 710
  - UDP: 37720
  - ICMP: 651
- Unique TCP source IPs: 9316
  - Port 80: 99.95% of packets
  - **Type: HTTP session (ACK+SEQ) = Real PCs = Botnet**
  - Botnet location: **96% USA**, 4% other countries
- Unique UDP source IPs: 34300365
  - Port 27015: 99.99%
- Unique ICMP source IPs: 5549
- Result: web-site was down for 1 minute and … up again

DDoS Experiments Summary

- AV companies can detect botnets in this way
- Hackers purchase services of each other
  (2nd hacker wrote that he can purchase more bots for attack if I pay him)
- Attack profiles and professionalism of hackers vary a lot

- Seems that 5$ per months for Cloud Hosting can save your web-site from a mid-size DDoS ☺

Email hack services

- Hacking of corporate email
  - “Email for domain” services
  - Corporate email server
- Hacking of public services:
  - Russian: Mail.ru, Rambler.ru, Yandex.ru, etc.
  - International: Gmail.com, outlook.com, etc.
  - Popular in Europe: gmx.net(.de, .ch, etc.), bluewin.ch

#HONEYPOT INFO

Same hardware as before:

- 512MB
- 1 CPU Core
- 20 GB SSD
- Amsterdam

Email server:

- dovecot 2.2.9
- postfix 2.11.0

What was expected

To: Adrian [redacted]
Subject: (Important Document)

Good Morning all,

I just uploaded this docume http://tndthd.org/kuzey/images/gdocc/ **x .**
Для перехода щелкните ссылку

Vs 2.10.3 **View - Download**

Thank you,

--
D M W [redacted]
Director
T [redacted]
M [redacted]

Сообщение | invoice621785.pdf (466 Кбайт)

From: Sara [redacted] [mailto:sara [redacted]]
Subject: Unpaid invoic

To view your document, please open attachment.

Sara [redacted]
Accountant II

What was expected

DHL Logistik-Spezialist <schebitz@silberzahn-gmbh.de>

Ankц╪ndigung - Sendung 29165499211

DHL Transport-Team

DHL Sendungsverfolgung

Sendungsnummer	29165499211
Produkt / Service	DHL PAKET
Status vom Dienstag, 19.05.2015 01:47:36	Die Auftragsdaten zu dieser Sendung wurden vom Absender elektronisch an DHL übe
Zugestellt an	Bevollmächtigter

http://pawad.cddphayao.com/wnjzdfebkxj8rh
Для перехода щелкните ссылку

Detaillierte Empfängerinformationen anzeigen
(PDF-Dokument)

Deutsche Post DHL - The Mail & Logistics Group

What we got in fact

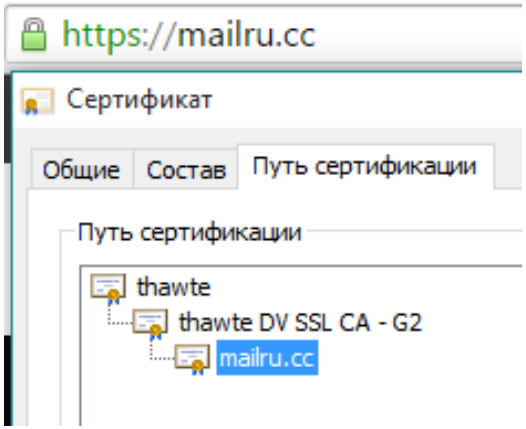
- Several spam emails to check server responses and target email
- Boring brute force attack:
  - 2-3 attempts per second
  - ~20 IPs
  - 9 attempts from 1 IP, then pause for this IP
  - Protocols:
    - IMAP
    - POP3
    - SSH
  - Users: admin, user, guest, support, test, root, ubnt, ubuntu, upload, vnc, webadmin, etc.
  - Still going…

Russian public services

- Just phishing ☺
  - Empty message with fake attachment (mini-image of invoice), leading to phishing web-page
  - Abuse from another user, follow the link and confirm that you are not a robot
  - Mailbox storage is running out, follow the link to increase
  - Message delivery failed, follow the link to retry

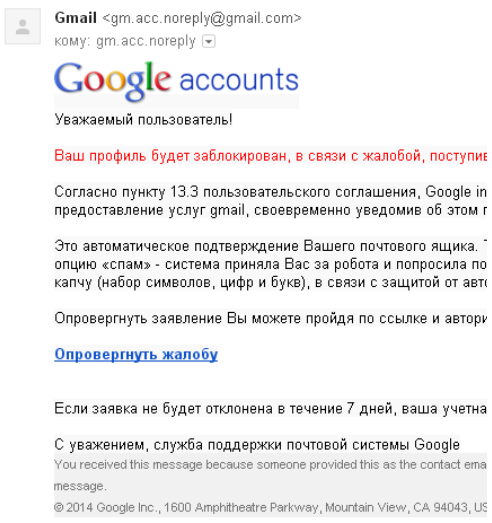
International public services

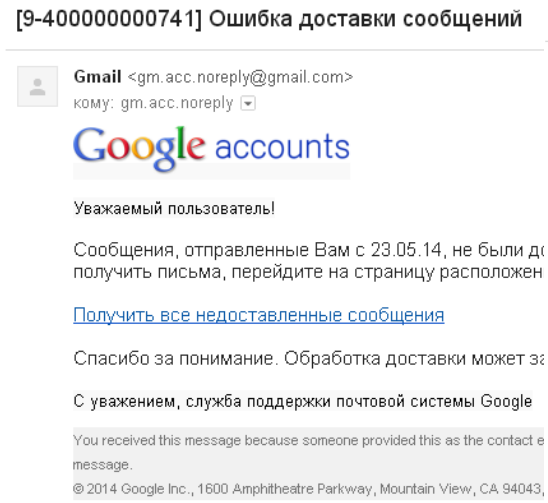
- gmx.ch and bluewin.ch
  - No reply from specialized hackers
    - algonco.com
    - pro-mail.net
    - gbimail.com
- Gmail
  - Lots of offers on different boards
    - mailru.cc (with SSL certificate!)
    - hpc.name
    - darkmoney.cc
    - etc.

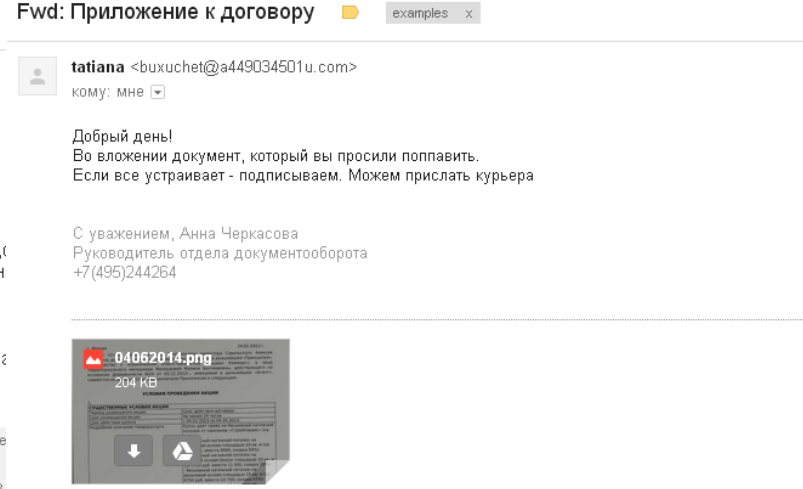


Gmail

- Blank email with attachments send from other Gmail mailbox
- Sent from special email servers
- “Technical” messages: Delivery fail, Abuse
- Message IDs: for tracking?







Gmail

Google accounts

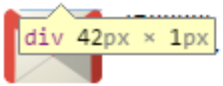
To continue to work with your mailbox (send, receive and store your messages and files) please increase your mailbox size in Preferences: Google Drive storage.
This action is required due to changes in email handling standards.

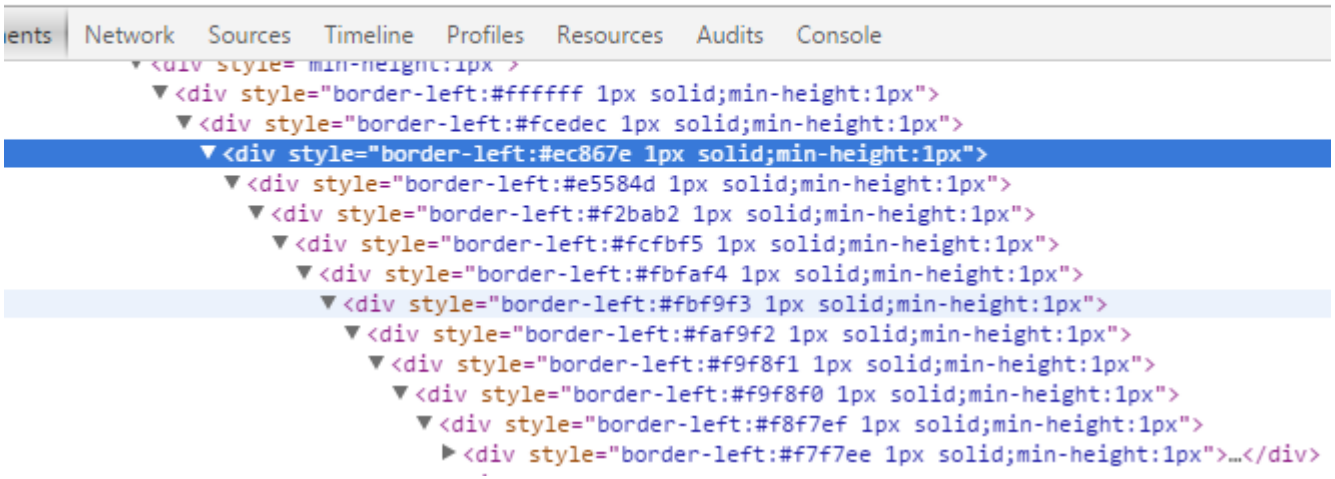
We wish you a pleasant experience!
Gmail Team

Layout Wonders

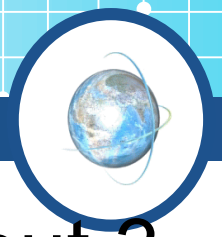
- Img files logo is filtered by Gmail

- Pixel painting via HTML – passed through!





Public Services Summary



- “Email for domain” service: same tools, but 3 times more expensive ☺
- Mass service: lots of offers, message IDs
- Good phishing messages
- Foreign Email services are not represented in mass-segment
- 2-factor authentication rules
- Big part of this market can be destroyed if Email companies will order such services and tune their filters examples

Overall

- Black market in Russia is available for everyone
- Language remains a barrier for hackers
- Authorities and AV companies are not effective
- Hackers are not afraid to accept offers from unknown person
- You can get some profit out of that ☺

- Only free services were tested, but there are 0-days on sale…

Thank you for attention!

- Questions?