

Александр Голомоносков

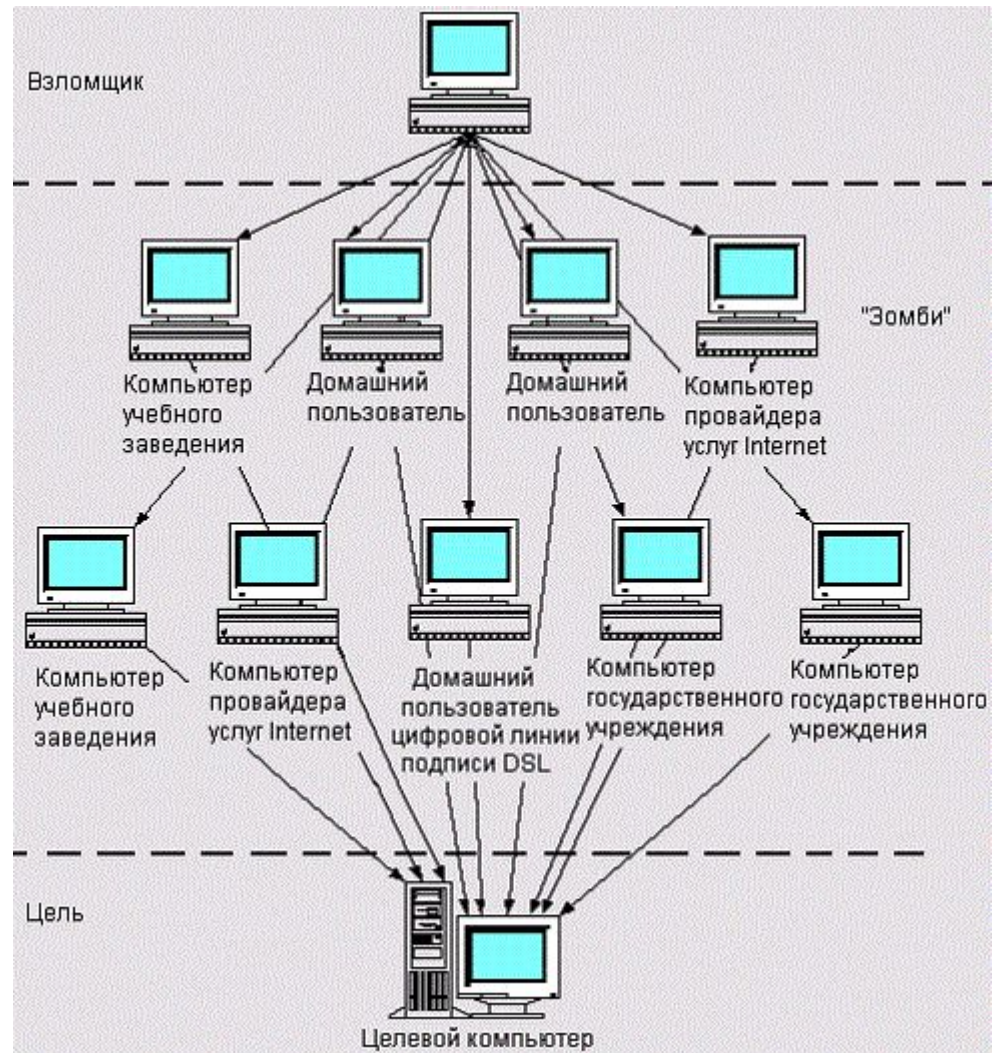
# Кибербезопасность и хакинг

# Disclaimer

- Доклад сделан исключительно с просветительскими и исследовательскими целями, для понимания механизмов защиты от взлома. Автор ни в коем случае не рекомендует использовать данную информацию для взлома, нанесения вреда или ущерба. Вся изложенная информация находится в открытом доступе в сети Интернет.

# DDoS

## ■ Distributed Denial of Service



4:54:07

Script

Images

Misc

00000015



# -Новости

НОВОСТИ

**Новый DDoS-рекорд продержался лишь пять дней: зафиксирована атака**

НОВОСТИ

**Ответственность за мощную DDoS-атаку на ProtonMail возлагают на российских хакеров**

НОВОСТИ

**DDoS-атаки усиливают через CHARGEN и используют против игровых стримеров**

Более 150 000 IoT-устройств были  
задействованы в ходе DDoS-атаки  
мощностью 1 Тб/с

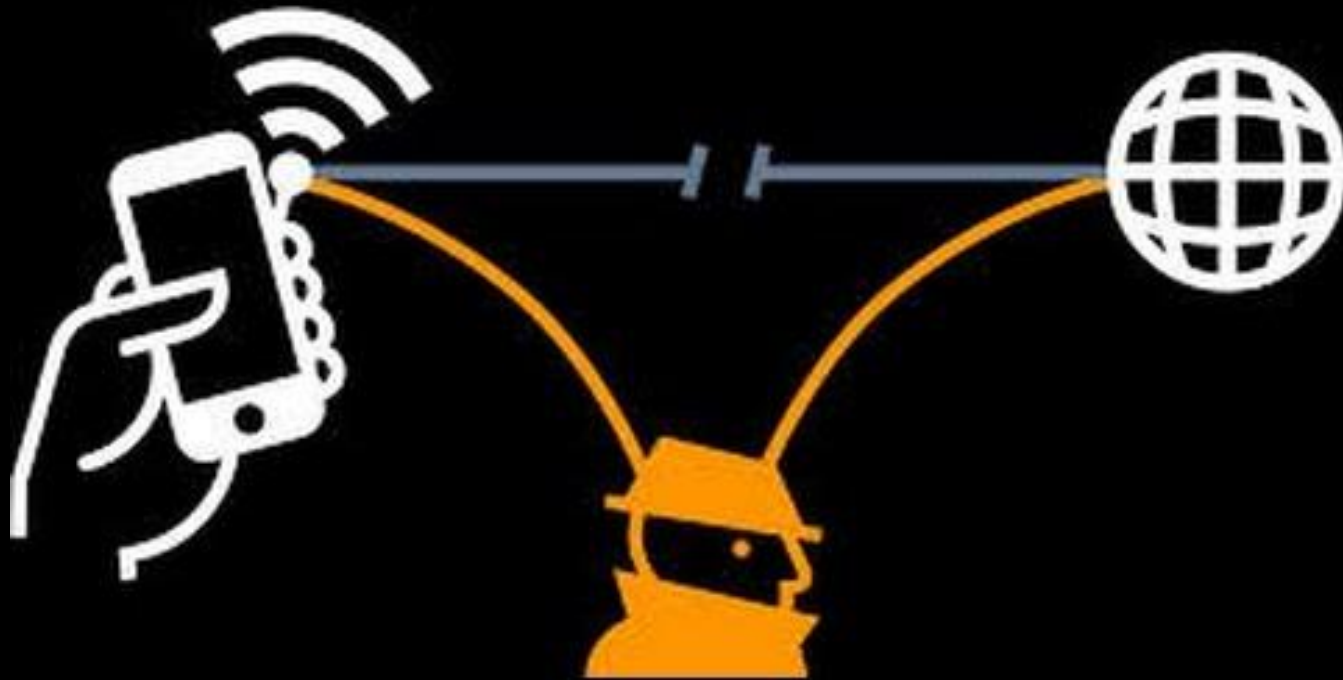


# WiFi

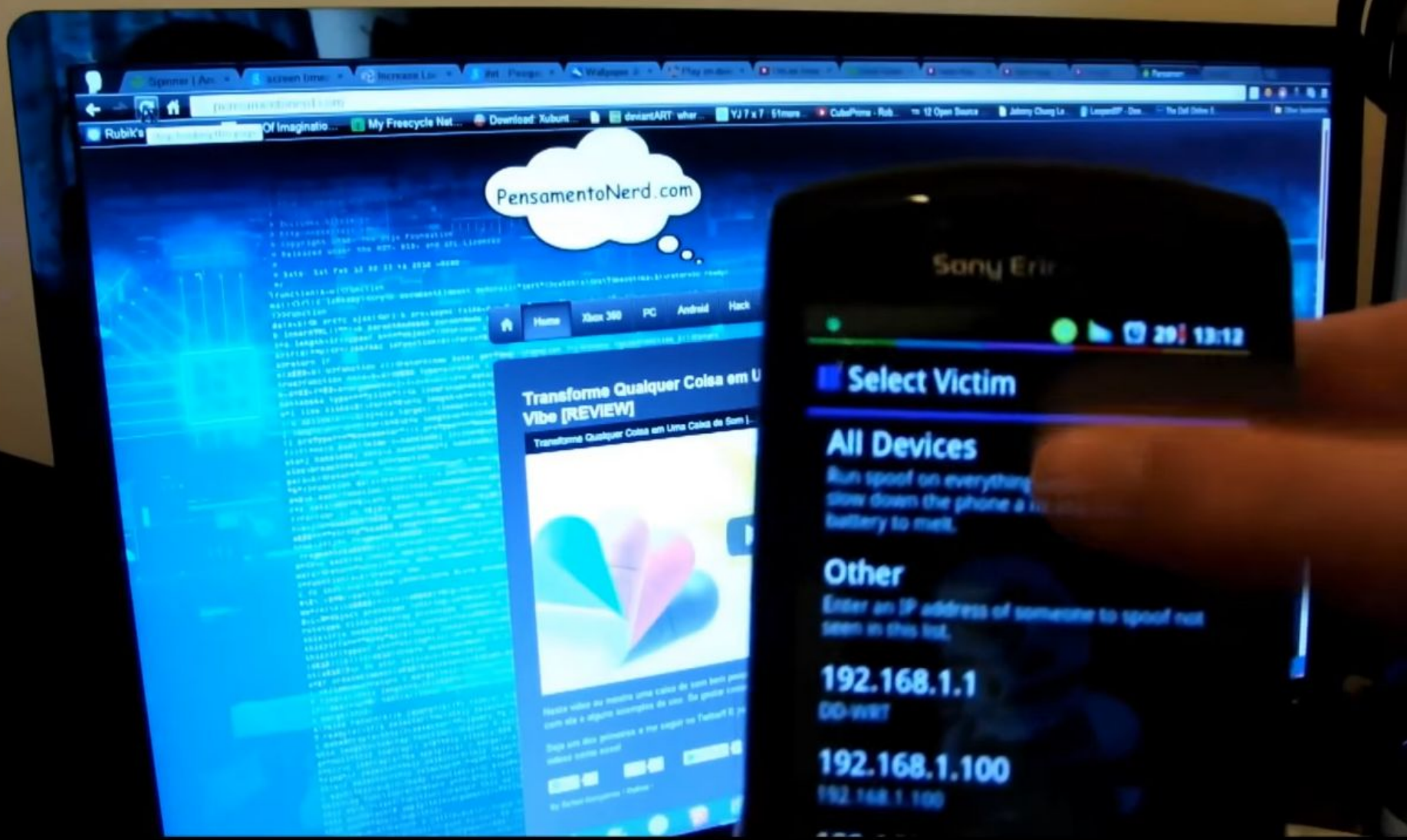




# -MITM (Man-In-The-Middle)







PensamentoNerd.com

Transforme Qualquer Coisa em Vibe [REVIEW]



### Select Victim

#### All Devices

Run spoof on everything to slow down the phone a little and battery to melt.

#### Other

Enter an IP address of someone to spoof not seen in this list.

- 192.168.1.1
- DD-WRT
- 192.168.1.100
- 192.168.1.100



# -Wireshark

eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
46	139.931187	wistron_07:07:ee	Broadcast	ARP	who has 192.168.1.254? tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.219219	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

Frame 1 (42 bytes on wire, 42 bytes captured)

- Ethernet II, Src: Vmware\_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ..... )8.....
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ..... )8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 ..... 9.
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default



<http://>



<https://>

# -Etthepcap

Applications Places    Fri Sep 5, 15:05    root

ettercap 0.8.0

Start Targets Hosts View Mitm Filters Logging Plugins ?



# Ettercap

Privileges dropped to 0.0.0.0...

33 plugins  
42 protocol dissectors  
57 ports monitored  
16074 mac vendor fingerprint  
1766 tcp OS fingerprint  
2182 known services  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
6 hosts added to the hosts list...

root@kali: ~ ettercap 0.8.0

# -Перехват паролей

ettercap

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ▾ Connections ▾ Connection data ▾

192.168.1.33:53948

POST /?act=login HTTP/1.1.

Host: weblogin.vk.com.

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0.

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8.

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3.

Accept-Encoding: gzip, deflate.

Referer: http://vk.com/.

Cookie: remixlang=0; remixlhk=50419054637509b8aa; remixflash=0.0.0; remixscreen\_depth=24; remixdt=0; remixst=8b333fb9.

Connection: keep-alive.

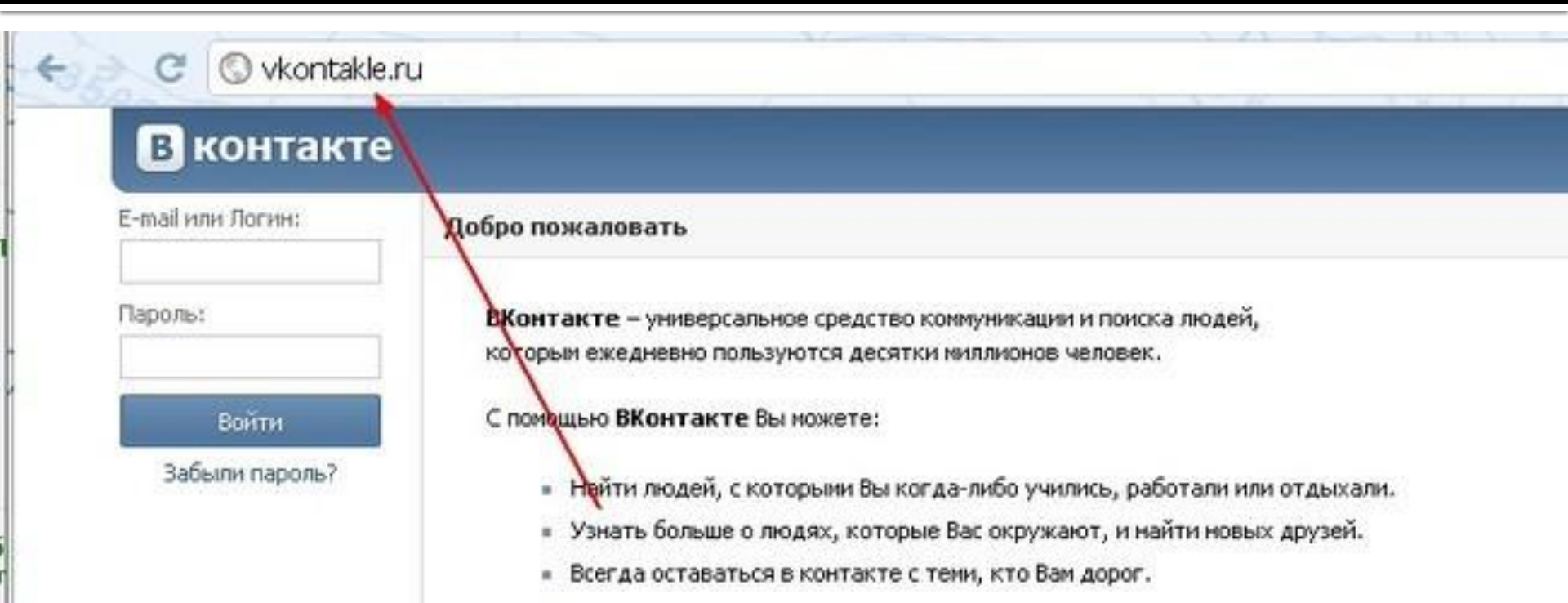
Content-Type: application/x-www-form-urlencoded.

Content-Length: 174.

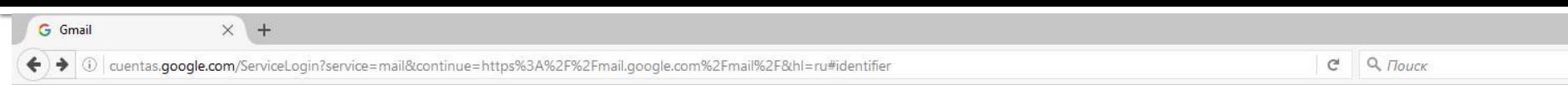
.  
act=login&role=al frame&expire=&captcha\_sid=&captcha\_key=&\_origin=http%3A%2F%2Fvk.com&ip\_h=5c16f336415e870c5f&lg\_h=0232aef7337a7782b7&email=emailforvk%40mail.ru&pass=ssfhy678



# Фишинг




# -Ettercap + SSLStrip+ + dns2проxy + Net-Creds = подмена https на http



Один аккаунт. Весь мир Google!

Войдите, чтобы перейти к Gmail

  
  
[Далее](#)  
[Нужна помощь?](#)

[Создать аккаунт](#)

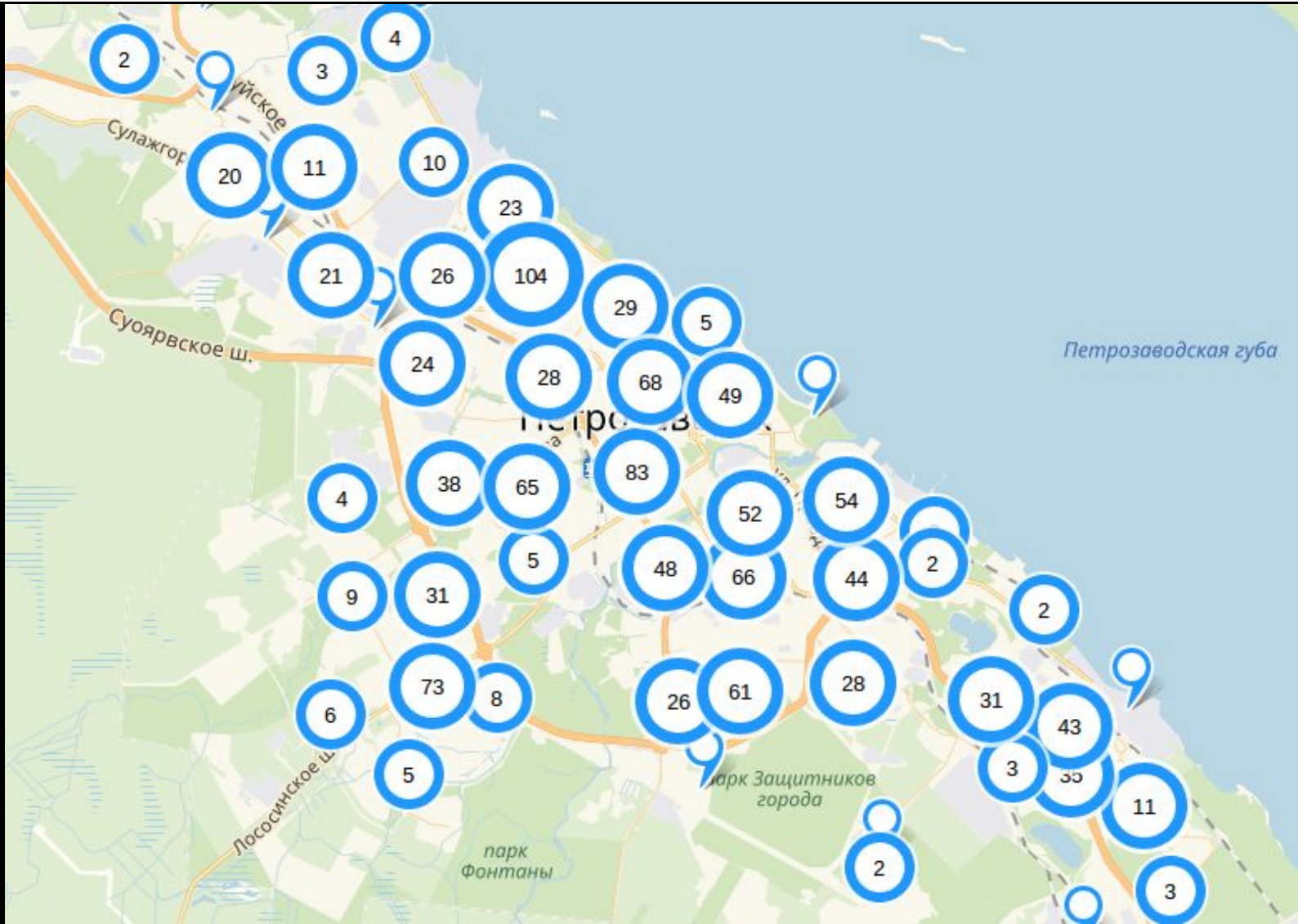
Один аккаунт для всех сервисов Google



# Атака на роутер



# -3wifi.stascorp.com

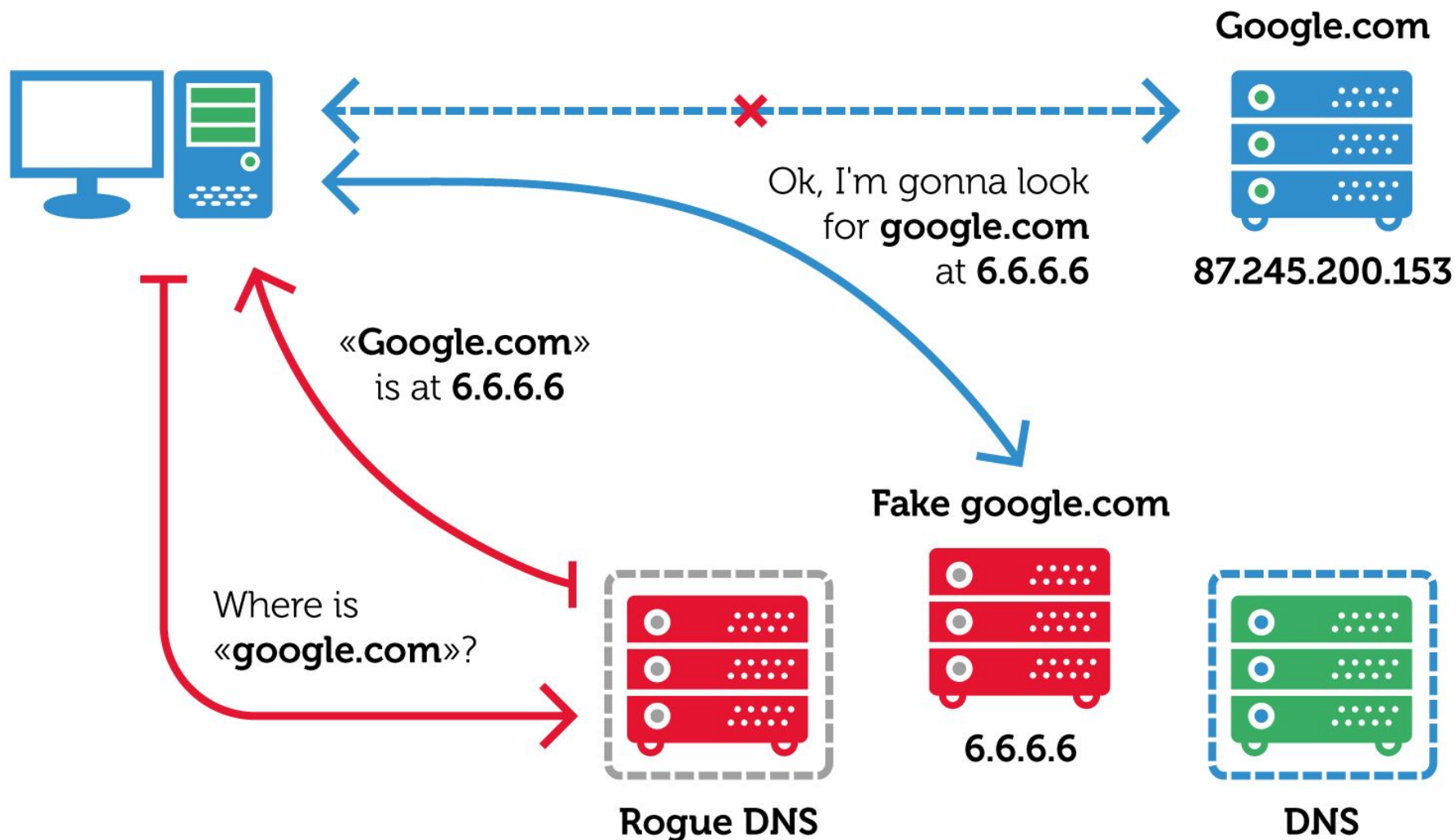


# -Bruteforce

```
root@bc - x root@bc -  
Aircrack-ng 1.1 r2178  
[00:01:26] 96980 keys tested (1133.04 k/s)  
Current passphrase: 6 WALTHER  
Master Key : 32 73 CF 2E 45 D2 7D D8 03 BF 12 80 8B F3 B7 18  
            88 13 C6 7F 09 44 C6 8D 16 EA 2A 38 AE AD FF 11  
Transient Key : 2F 54 4F 8E C8 26 B7 2E 72 6C 33 D2 8B E4 BD 29  
              FA 59 85 0E 23 D8 B1 2E 49 FC 3F 36 83 13 4D 27  
              9F DD 29 A7 3E 11 03 04 31 EF E6 F7 CA CD E6 37  
              64 69 0E B4 98 86 2D D9 1C 0F 90 45 FA 4B 6A 94  
EAPOL HMAC : 0B 4A 64 74 0C 03 AA DA 73 64 65 04 71 FD 4C 2F
```

**aircrack-ng OURFILE-01.cap -w /pentest/passwords/wordlists/darkc0de.lst**

# -Подмена DNS



# Удаленный доступ



# -Мобильные устройства

Моё  
Asa

Олег Ив

В

91  
870  
46  
LWAR  
62  
CA  
827A  
8A  
03  
MAL  
6F97





# -Шифровальщики

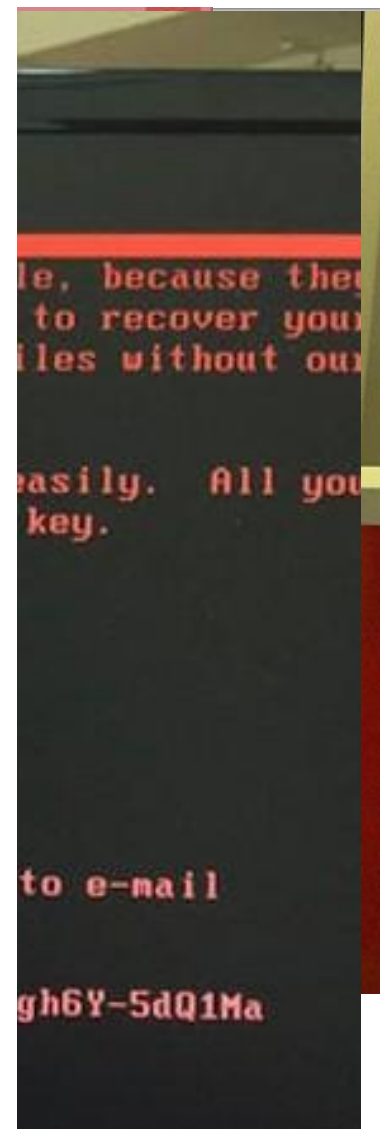
Город в Канаде был вынужден заплатить биткоины после атаки шифровальщика

Олег Иванов 12 сентября 2018 - 17:25

Общее

Вирусы-вымогатели

Вирусы-шифровальщики



# -Keylogger



# -Майнеры



# -Webcam



# -Поисковик Shodan

Shodan Search results for "default password":

- Total Results: 68,479
- Top Services:
  - Telnet: 19,737
  - HTTP (8080): 12,673
  - 8081: 8,322
  - Automated Tank Gauge: 7,161
  - HTTP: 2,601
- Top Countries:
  - TW: 10,079
  - US: 8,052
  - BR: 6,253
  - TH: 4,595
  - CN: 3,850
- Top Organizations:
  - TOT: 3,684
  - Digital United: 3,654
  - AboveNet Communicati...: 3,275
  - Chief Telecom: 1,157
  - Telecom Argentina S.A.: 695

Map showing search results distribution across the Americas, with the United States highlighted in red.

IP: 21.127.125.195  
125.125.127.82.in-addr.arpa

City: New York  
Country: United States  
Organization: Natural Wireless, LLC

Ports: 137, 8080

[View Details](#)

SHODAN IMAGES Search results for "web":

- Overview
- Contact Us

Grid of images including:

- A parking garage interior.
- A cluttered room with many items.
- A foggy outdoor scene with trees.
- A snowy outdoor scene with trees.
- A street scene with a white car and a building.

# Bluetooth-атака



**phd**  
Positive  
Hack  
Days

Взлом в прямом эфире: как хакеры проникают в ваши системы

1 257 просмотров

👍 23

💬 1

➦ ПОДЕЛИТЬСЯ

☰

⋮



**Positive Technologies**

Опубликовано: 6 июл. 2017 г.

**ПОДПИСАТЬСЯ 6,6 ТЫС.**

# USB

**USB killer v2.0** USB Device that Can Easily Burn Your PC



# USB



НОВОСТИ

## Вредоносный кабель USB нагроон компрометирует устройство за считанные секунды

Мария Нефёдова, 3 недели назад 3 мин на чтение 3 4 67791





# Кардинг

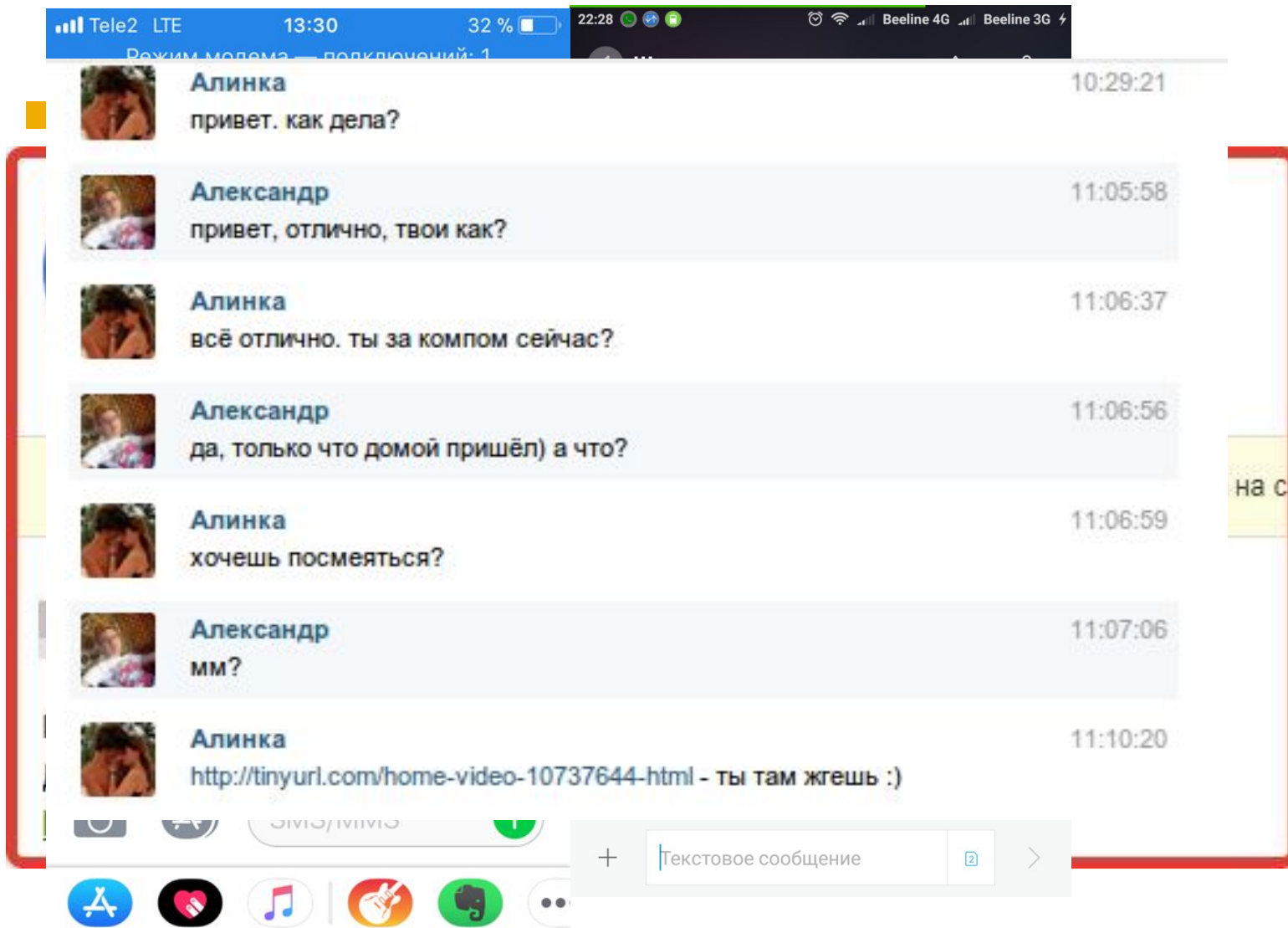
А ТЕПЕРЬ ФОКУСЫ  
С КАРТАМИ!



# ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ



# Не переходите по неизвестным ссылкам!



# Не скачивайте файлы!

The image shows a screenshot of a YouTube video player on an iPad. The video is titled "The Lumineers - Sleep On The Floor" by LumineersVEVO. A white dialog box is overlaid on the video, asking "Скачать файл?" (Download file?) with the text "The Lumineers - Sleep On The Floor - YouTube" and two buttons: "Заккрыть" (Close) and "Скачать" (Download). A red arrow points to the "Скачать" button. The video player interface includes a progress bar at 0:08 / 4:45, a title bar, and a list of recommended videos on the right. The iPad status bar at the top shows the time as 13:37 and 17% battery.

Скачать файл?  
The Lumineers - Sleep On The Floor - YouTube

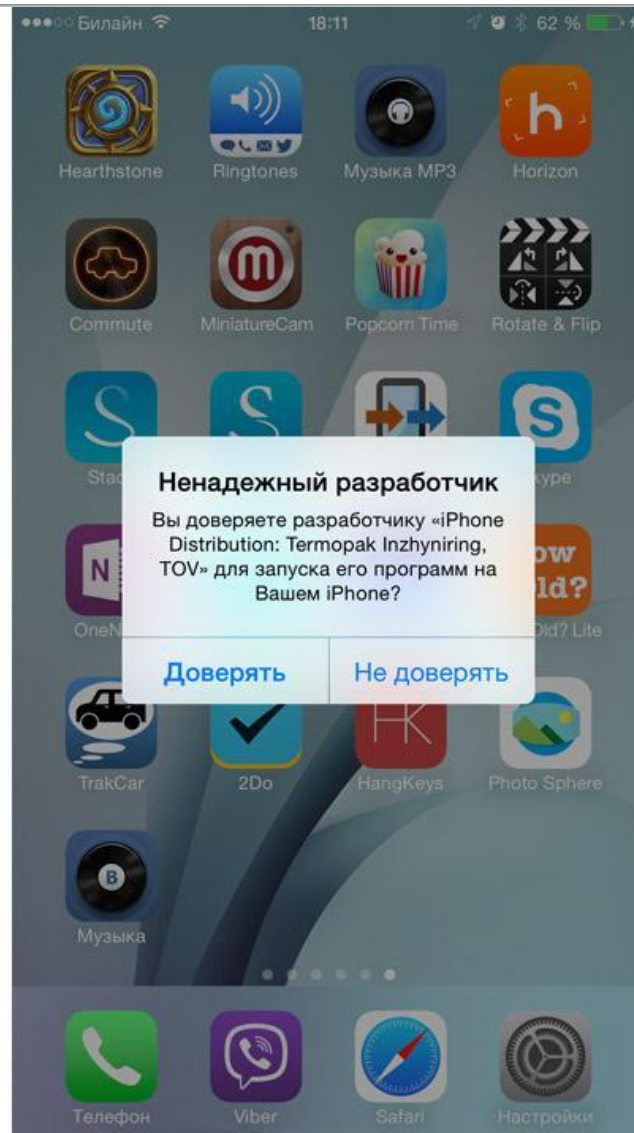
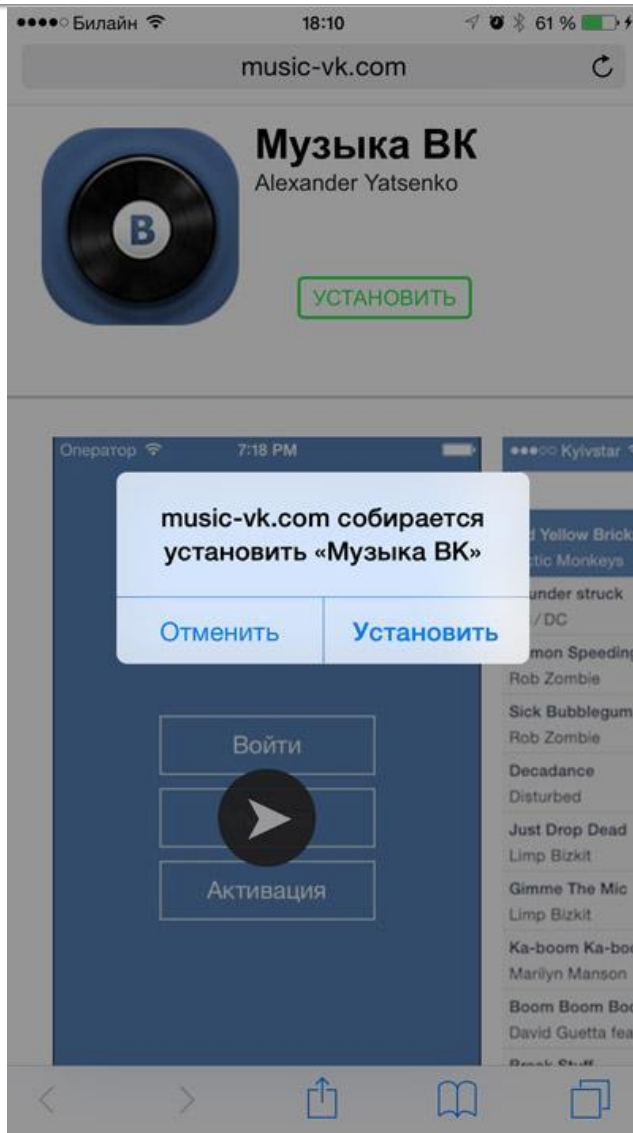
Заккрыть    Скачать

The Lumineers - Sleep On The Floor  
LumineersVEVO · 20 089 332 просмотра  
290 тыс. 4 тыс.

6 300 КОММЕНТАРИЕВ

Браузер    Downloads    Файлы    More

# Не устанавливайте подозрительные приложения



# Никаких USB



# Только свой мобильный интернет (свой WiFi)

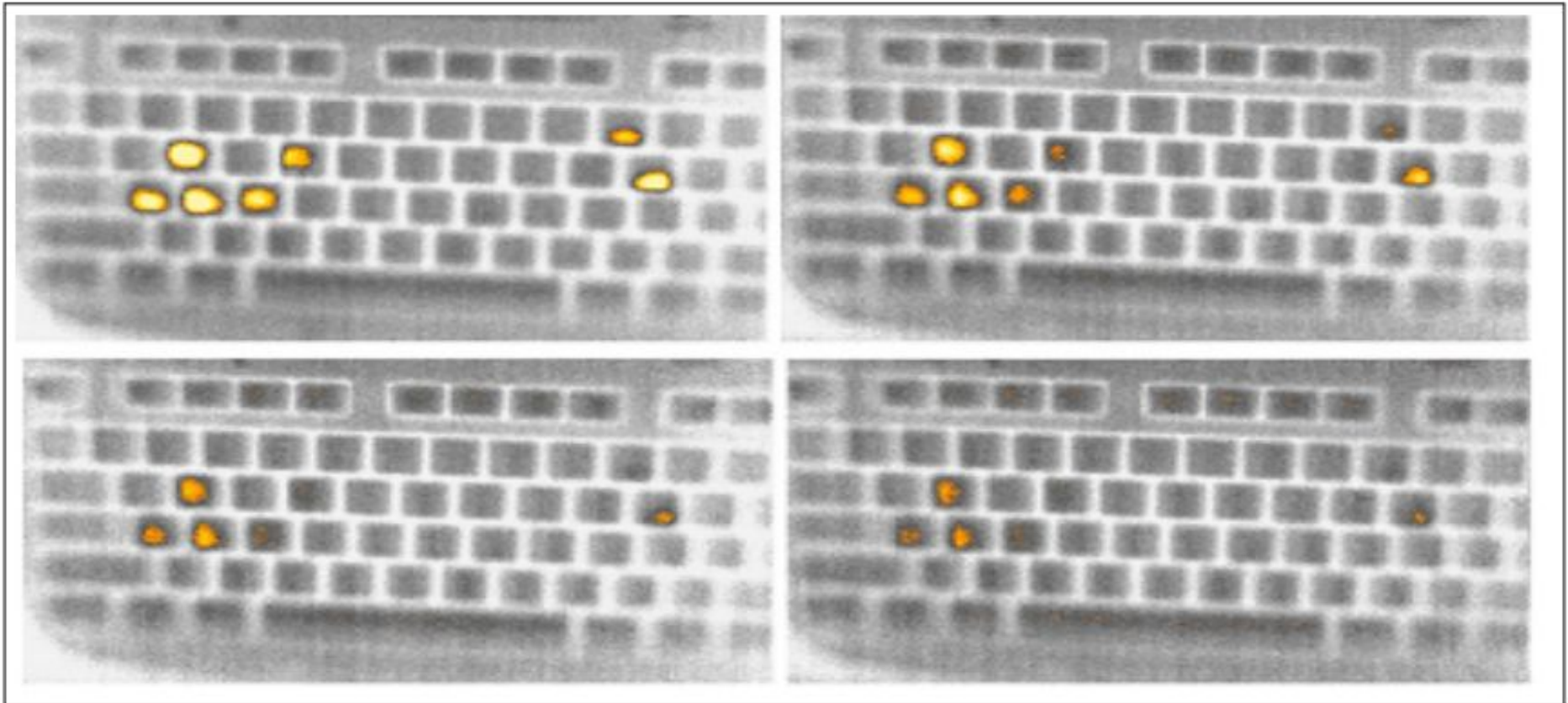


# Сложные пароли

Плохие пароли	Хорошие пароли
123456789 password qwerty master login1 1a2s3d4f5g	D)dzq4Smo@ 4j~8GvG{qB Re18ZEVH1# Hx4@5g8DoJ %FfZMv4vDu pWjtbQ\$g6B



P.S.





**Авиакомпания British Airways обнаружила еще 185 000 пользователей, пострадавших от утечки данных**

**Новый вредонос для Mac внедряет рекламу в зашифрованный трафик**

**В сети обнаружили данные 420 000 сотрудников Сбербанка**

**У авиакомпании Cathay Pacific похитили личные данные 9,4 млн пассажиров**

# Источники

- **hackware.ru** - этичный хакинг и тестирование на проникновение;
- **haker.ru** - ресурс, посвященный информационной безопасности;
- **youtube.com/overbafer1/** - канал о методах взлома и защиты, гаджетах и др.;
- **phdays.com** - международный форум по практической безопасности;
- **kali.org** - Penetration Testing and Ethical Hacking Linux Distribution;
- **kaspersky.ru** – Лаборатория Касперского;
- **vk.com/itcookies** – сообщество программистов;
- **anti-malware.ru** – информационно-аналитический центр по информационной безопасности.

Спасибо за внимание!

