Александр Голомоносов

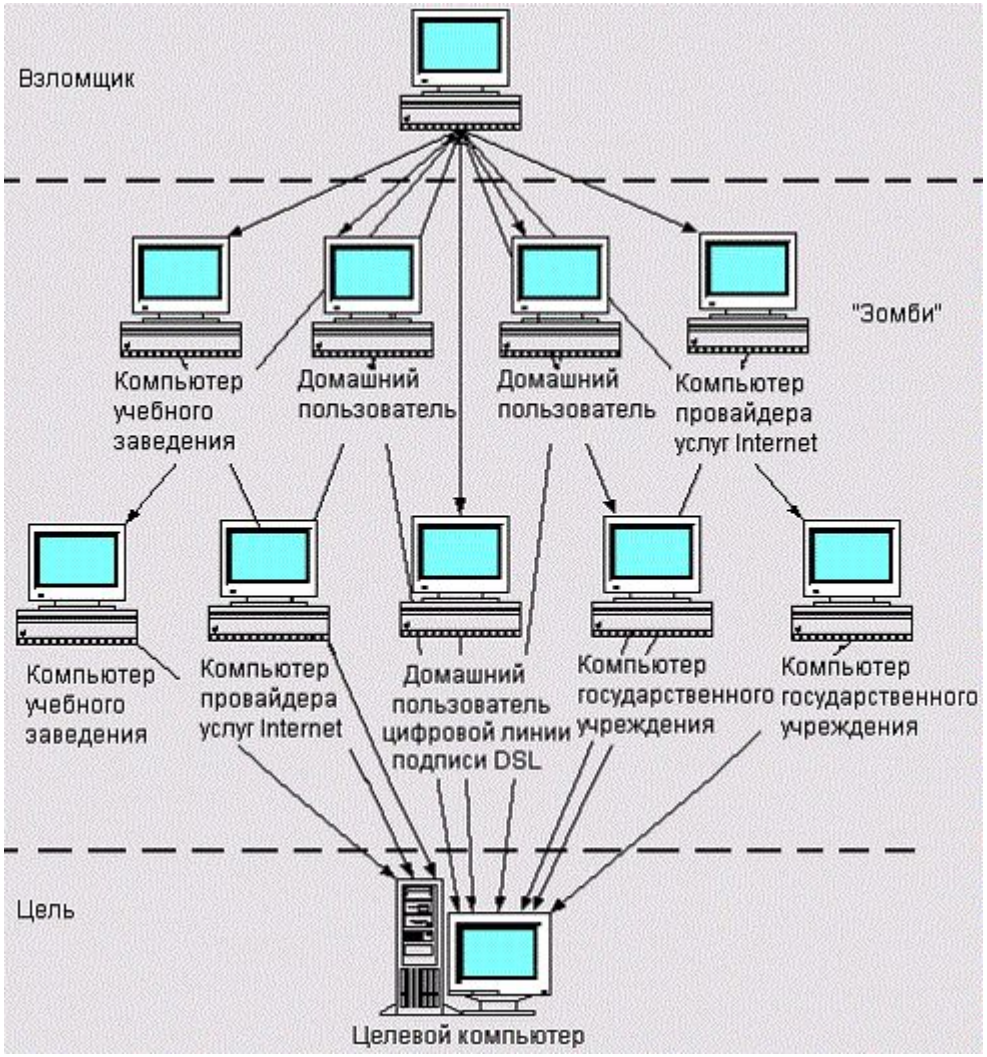
Кибербезопасность и хакинг

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 отрытом доступе в сети Интернет.**

DDos

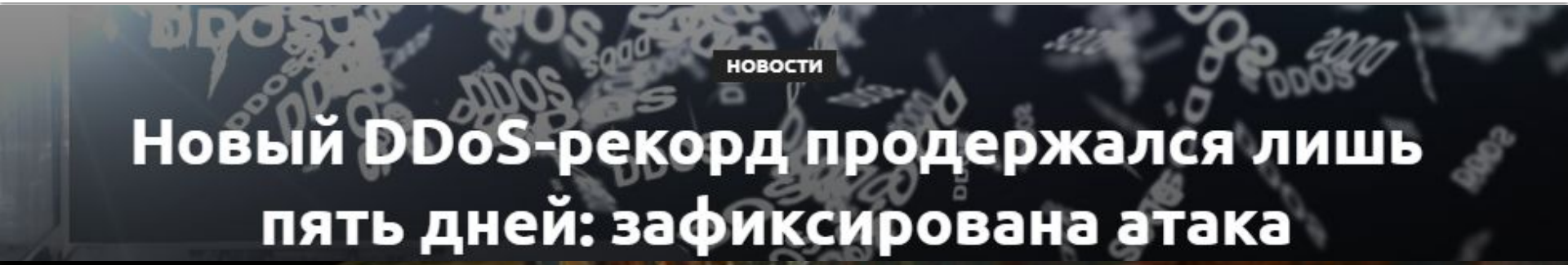
- *Distributed Denial of Service*

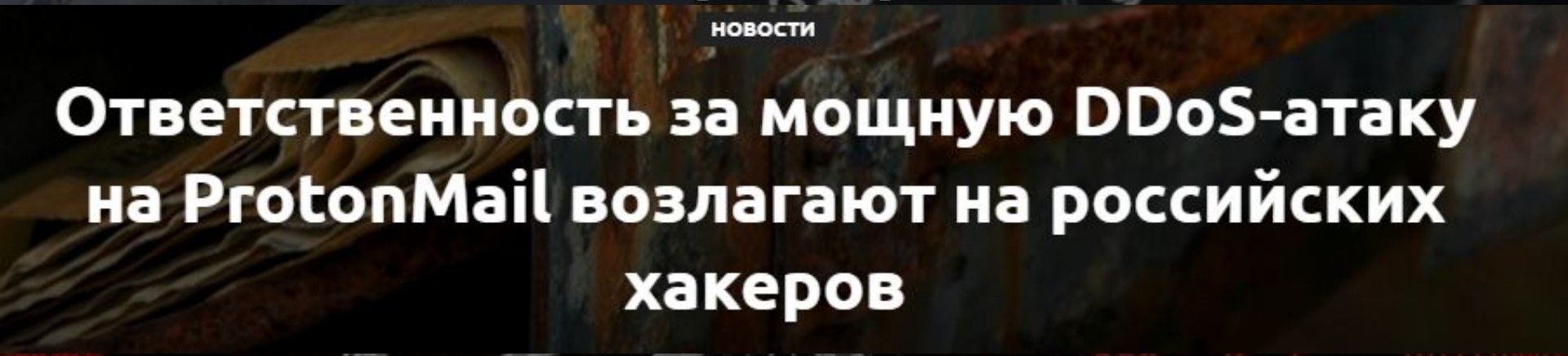


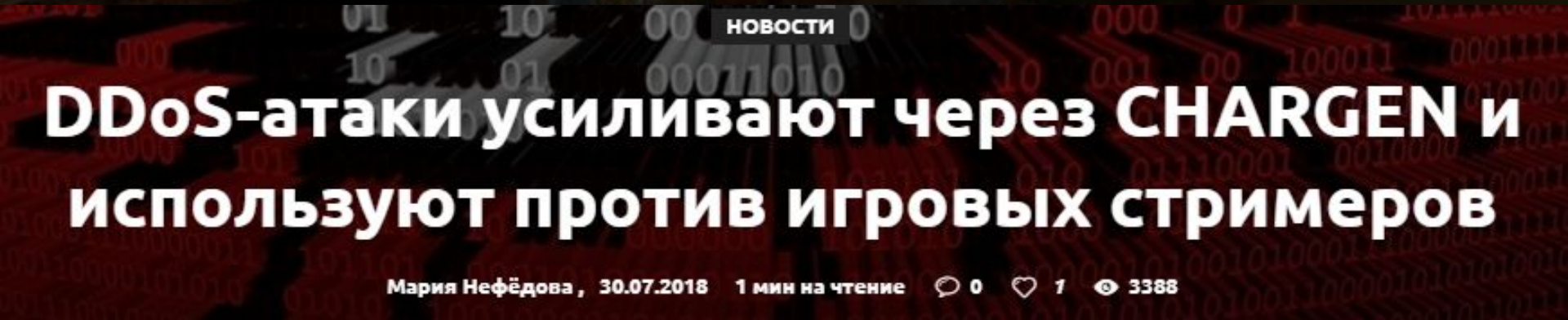

4:54:07
Script
Images
Misc
00000015


NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Saudi Arabia
Russia
Brazil
Netherlands
Iran
Moldova
South Korea
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Liechtenstein
Russia
Taiwan
Bulgaria
Spain
Mexico
ATTACK TYPES
SERVICE
PORT
pptp
microsoft-ds
unknown
telnet
unknown
unknown
netbios-dgm
LIVE ATTACKS
TIMESTAMP
ORGANIZATION
LOCATION
IP
LOCATION
TYPE
SERVICE
PORT
gifs.com

-Новости


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

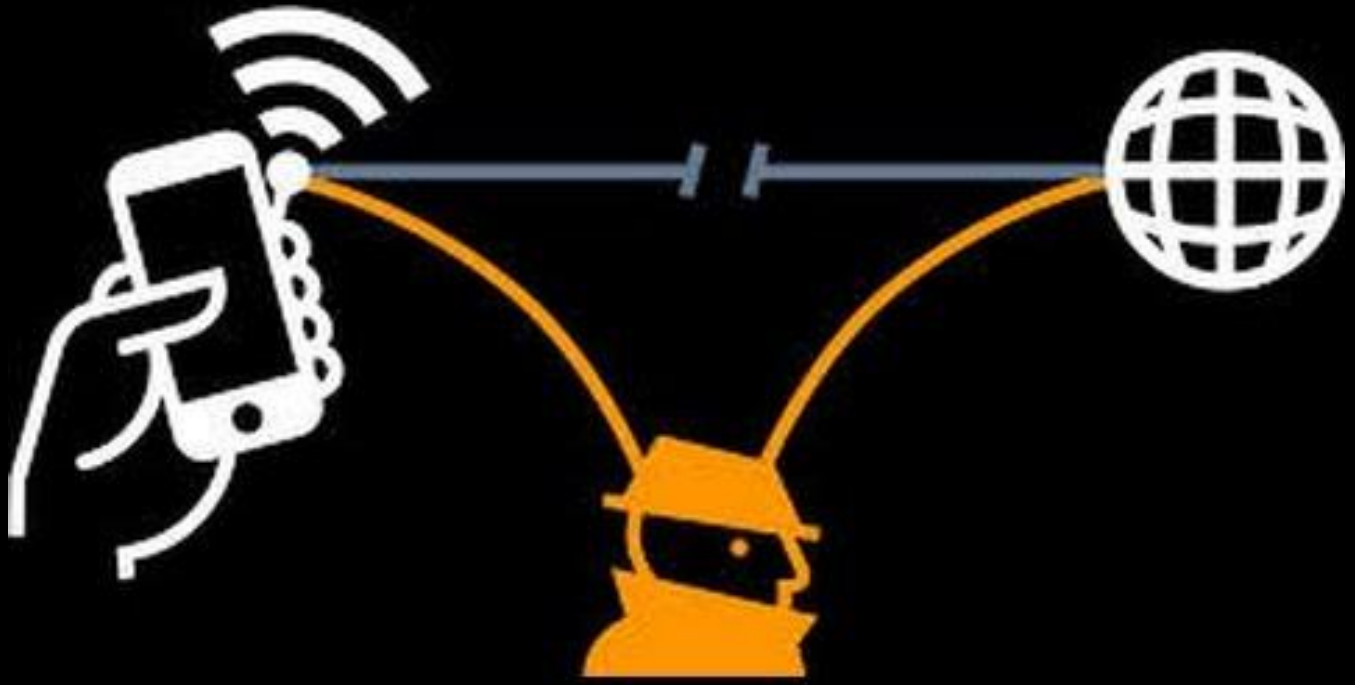

НОВОСТИ
Ответственность за мощную DDoS-атаку на ProtonMail возлагают на российских хакеров

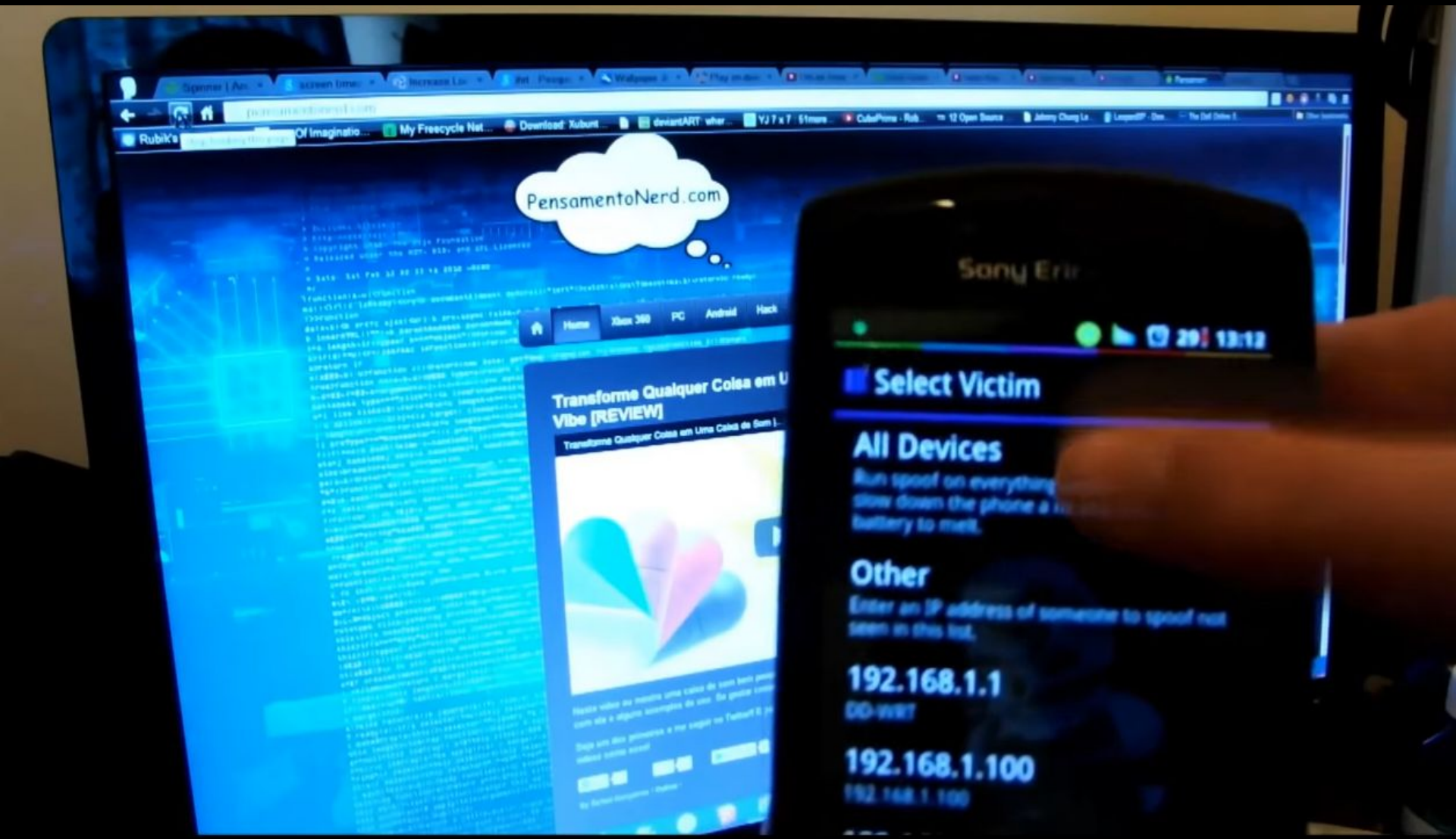

НОВОСТИ
DDoS-атаки усиливают через CHARGEN и используют против игровых стримеров
Мария Нефёдова , 30.07.2018 1 мин на чтение 0 1 3388

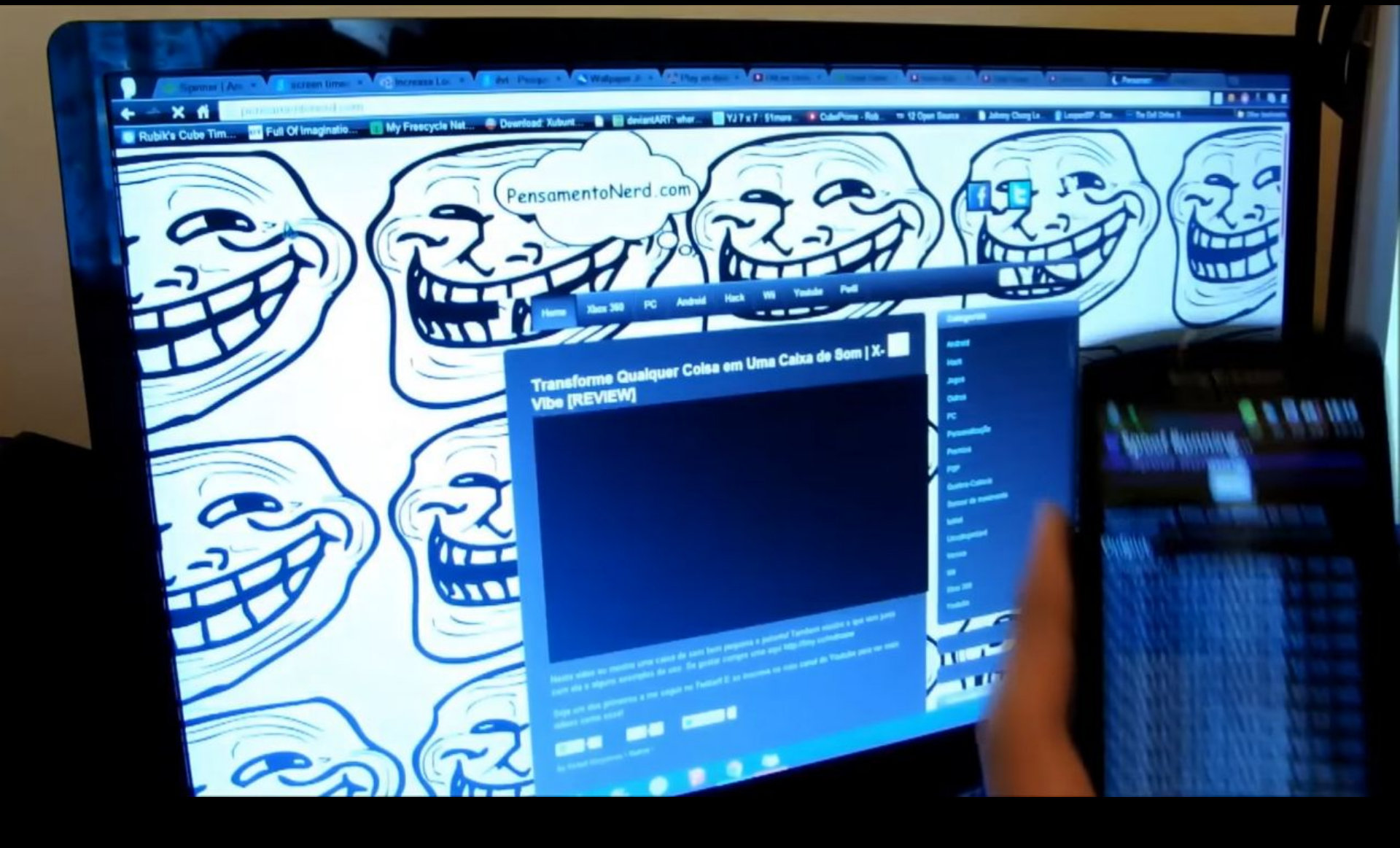
Более 150 000 IoT-устройств были задействованы в ходе DDoS-атаки мощностью 1 Тб/с

WiFi

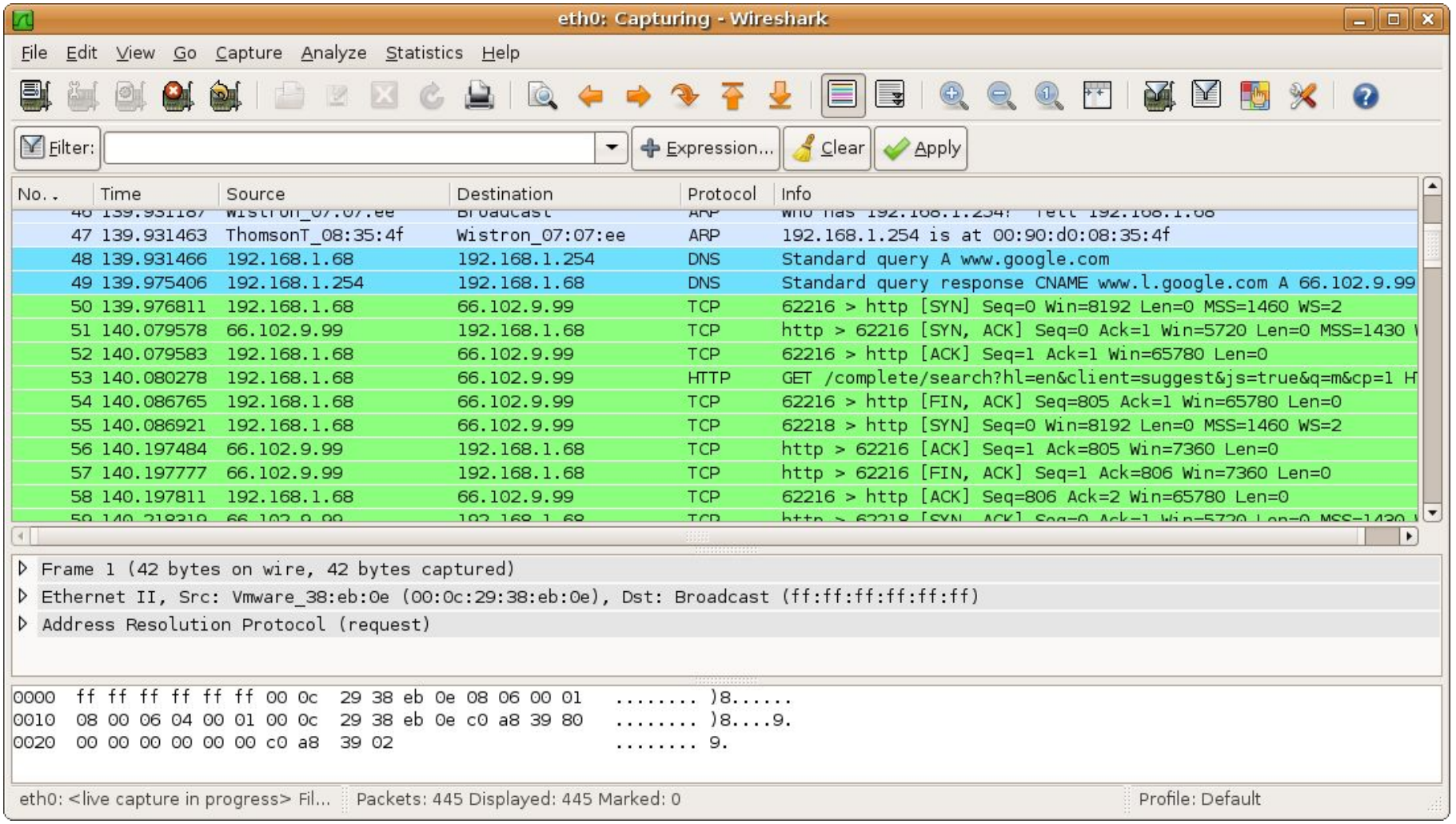
-MITM (Man-In-The-Middle)

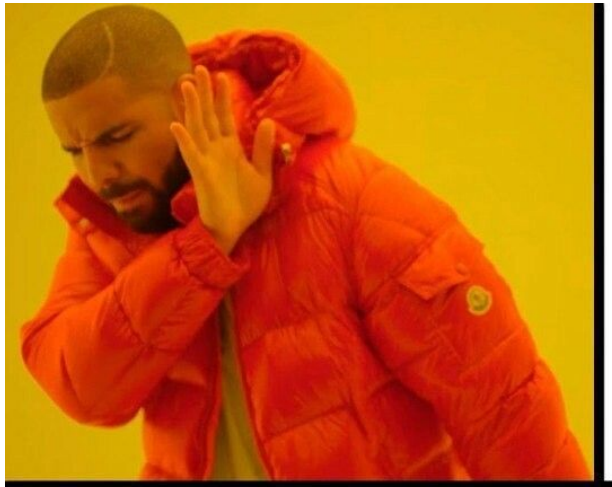



PensamentoNerd.com
Home
Xbox 360
PC
Android
Hack
Transforme Qualquer Coisa em U
Vibe [REVIEW]
Select Victim
All Devices
Other
192.168.1.1
192.168.1.100


PensamentoNerd.com
Home
Xbox 360
PC
Android
Hack
Wii
Youtube
Perfil
Transforme Qualquer Coisa em Uma Caixa de Som | X-Vibe [REVIEW]

-Wireshark


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
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
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
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



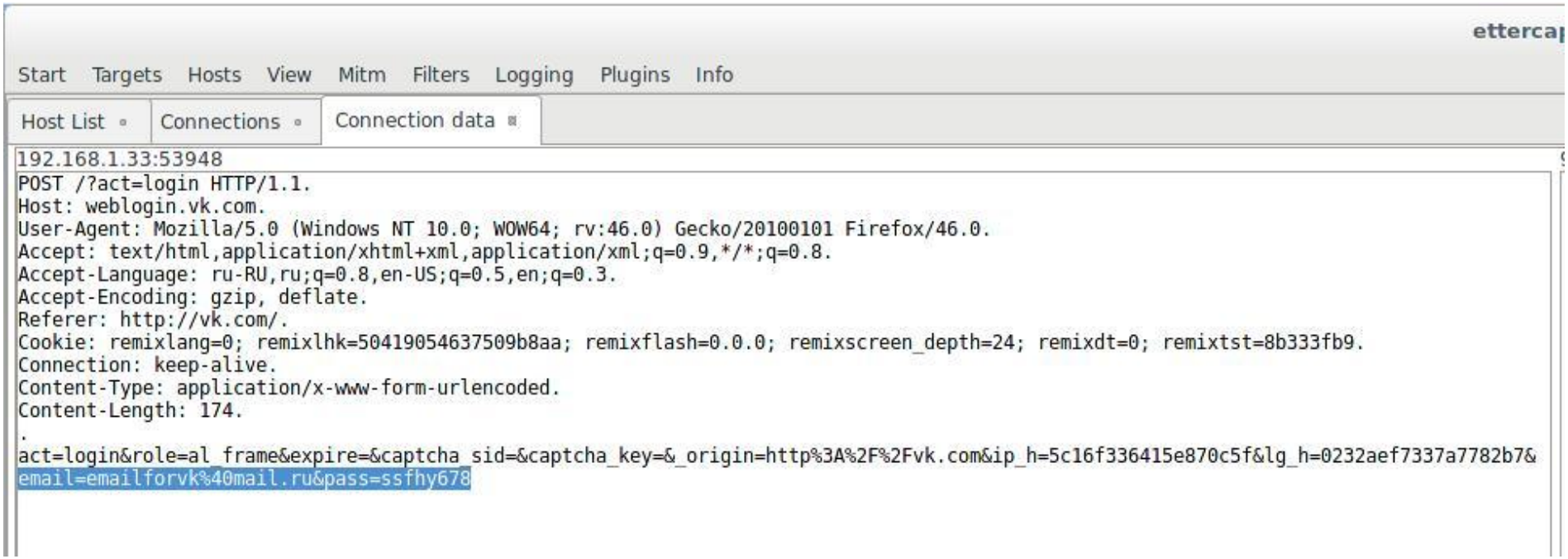
http://

https://

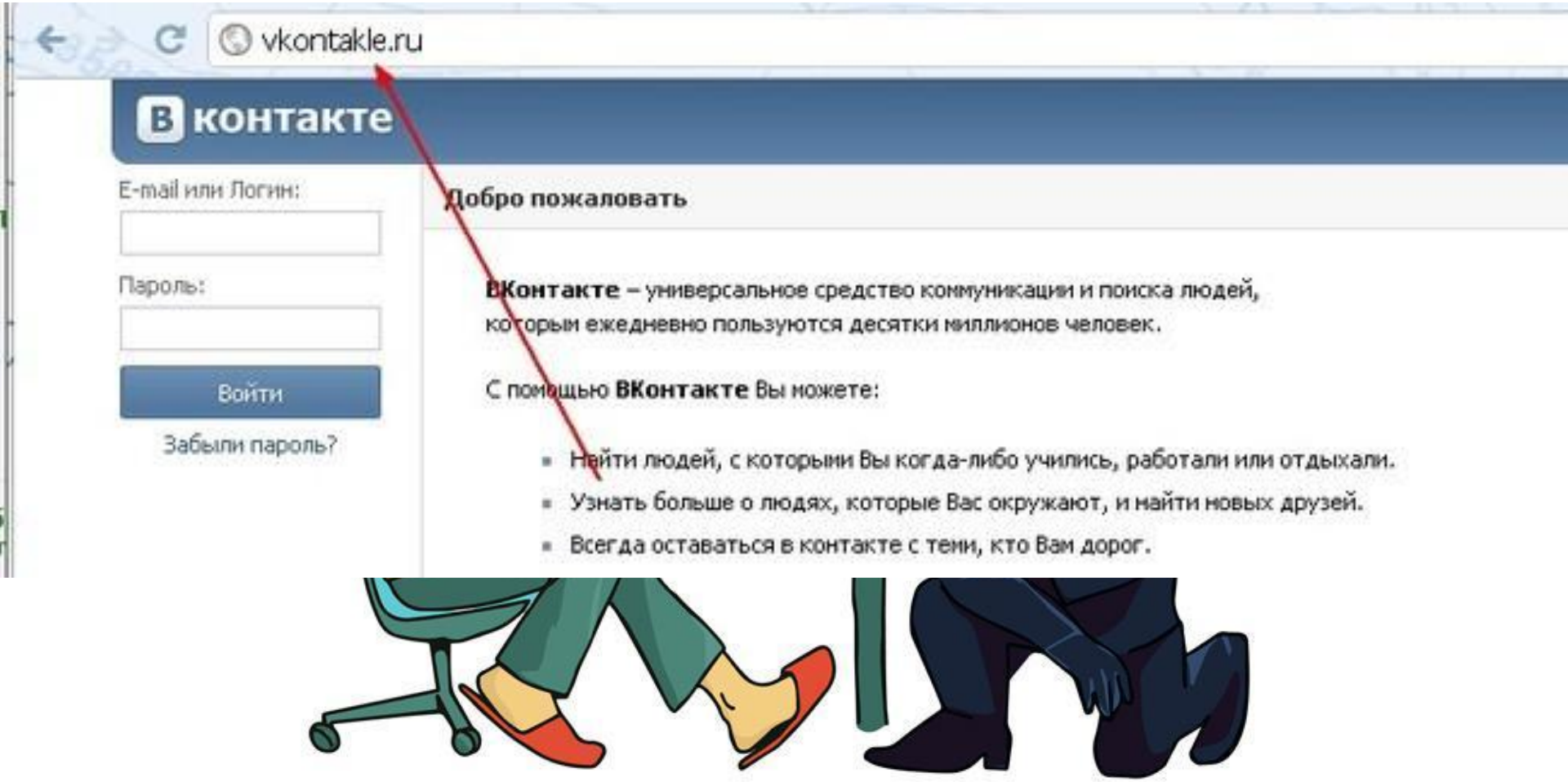
-Etthepcap


Applications Places
Fri Sep 5, 15:05
root
ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Ettercap
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

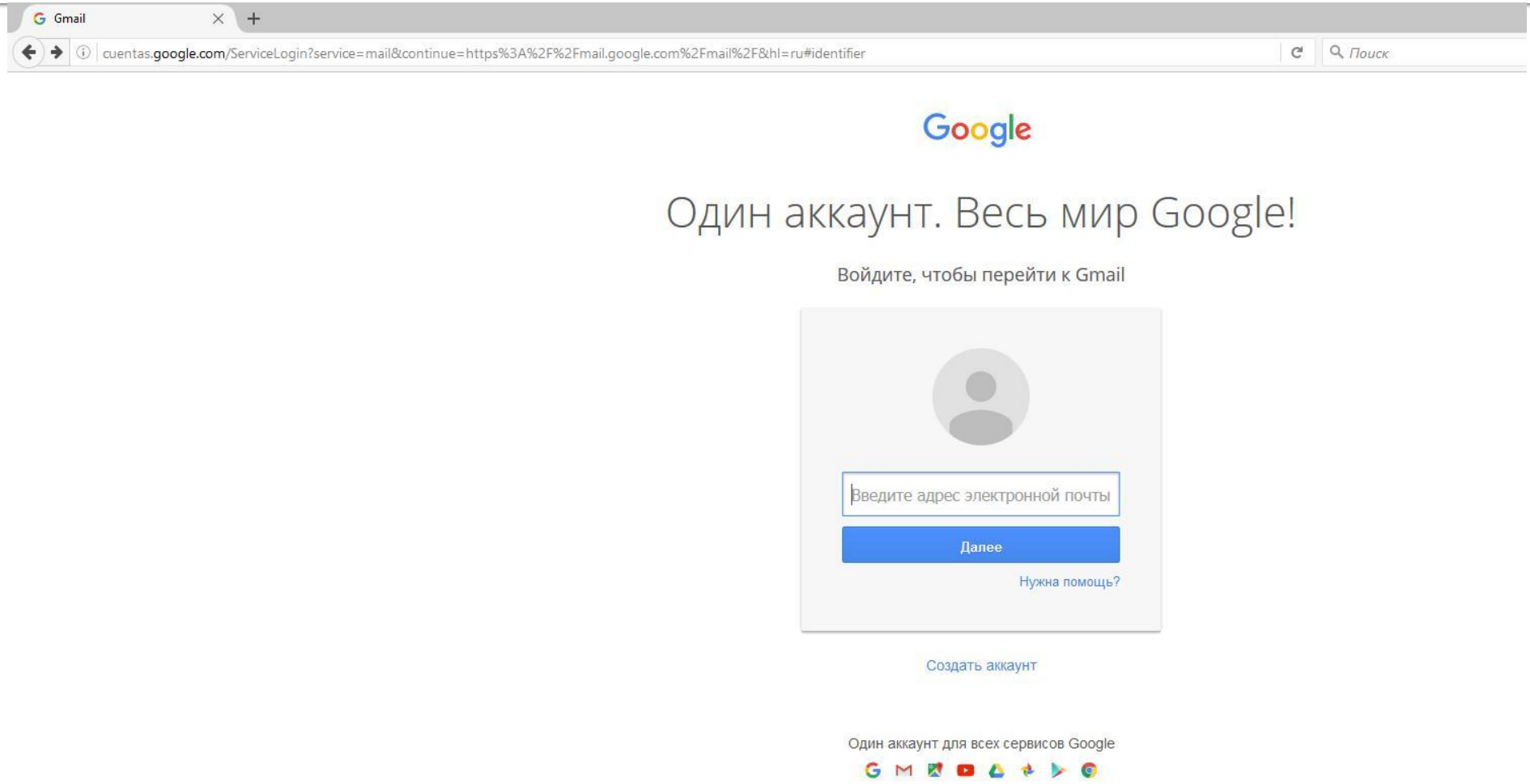
-Перехват паролей



Фишинг

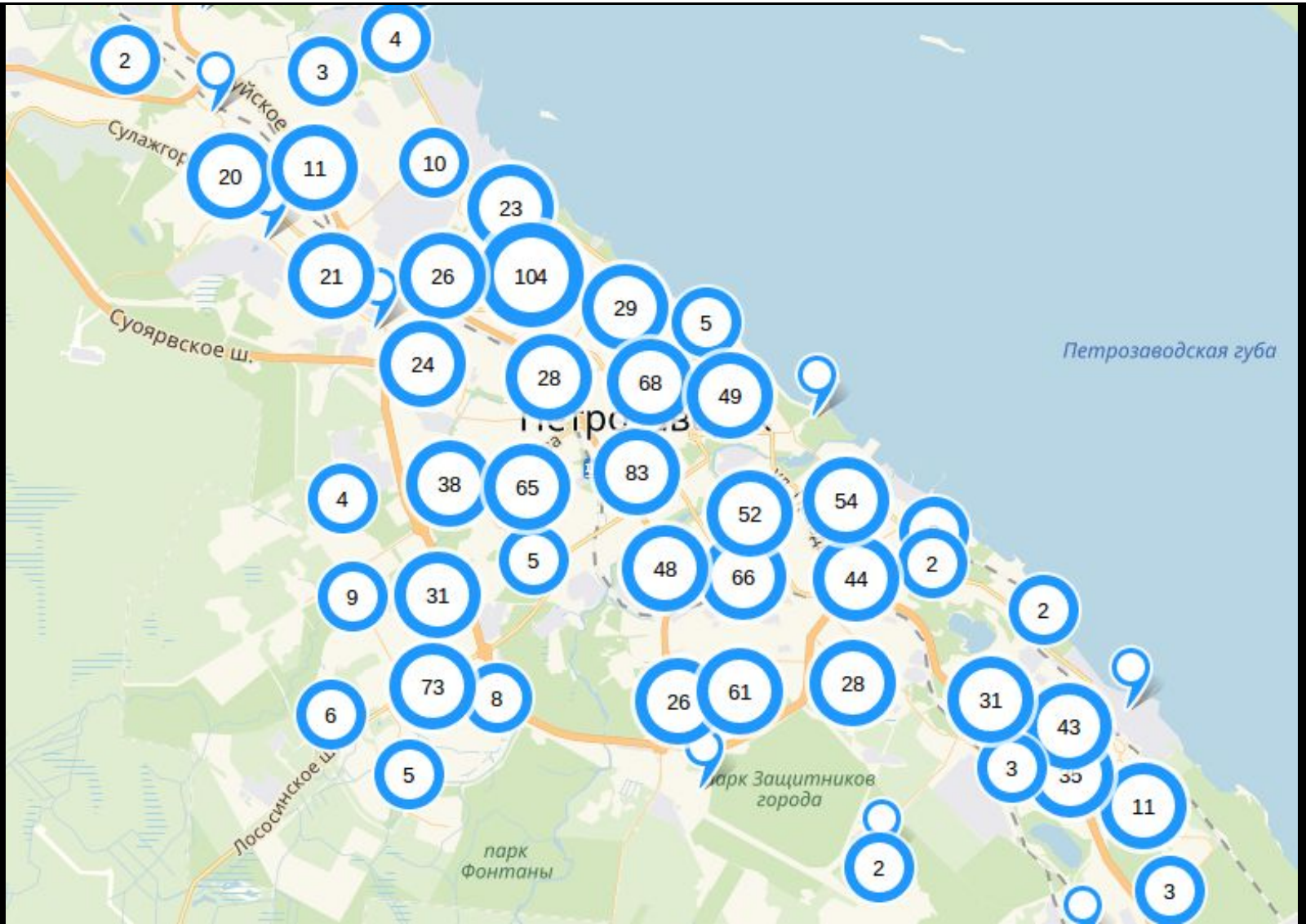

vkontakle.ru
ВКонтакте
E-mail или Логин:
Пароль:
Войти
Забыли пароль?
Добро пожаловать
ВКонтакте – универсальное средство коммуникации и поиска людей, которым ежедневно пользуются десятки миллионов человек.
С помощью ВКонтакте Вы можете:
Найти людей, с которыми Вы когда-либо учились, работали или отдыхали.
Узнать больше о людях, которые Вас окружают, и найти новых друзей.
Всегда оставаться в контакте с теми, кто Вам дорог.

-Ettercap + SSLStrip+ + dns2proxy + Net-Creds = подмена https на http

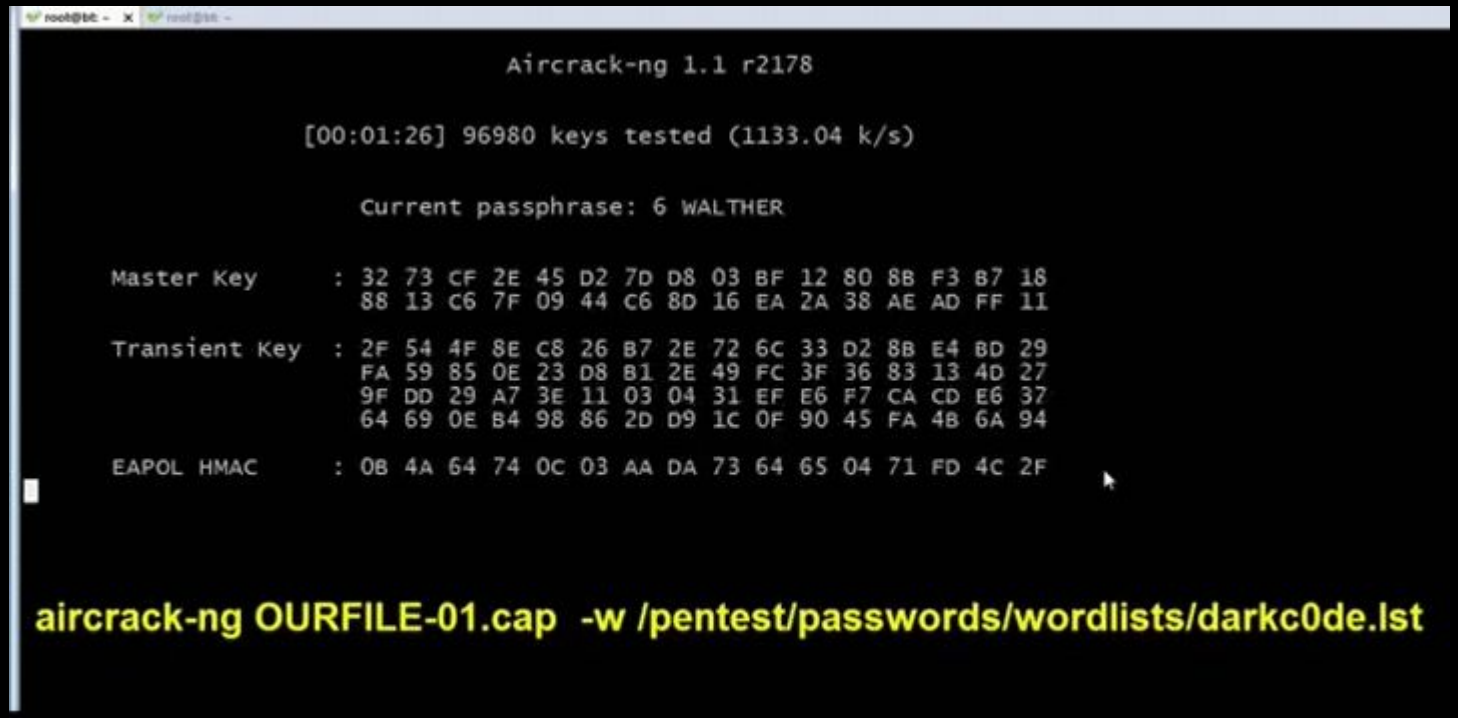


Атака на роутер

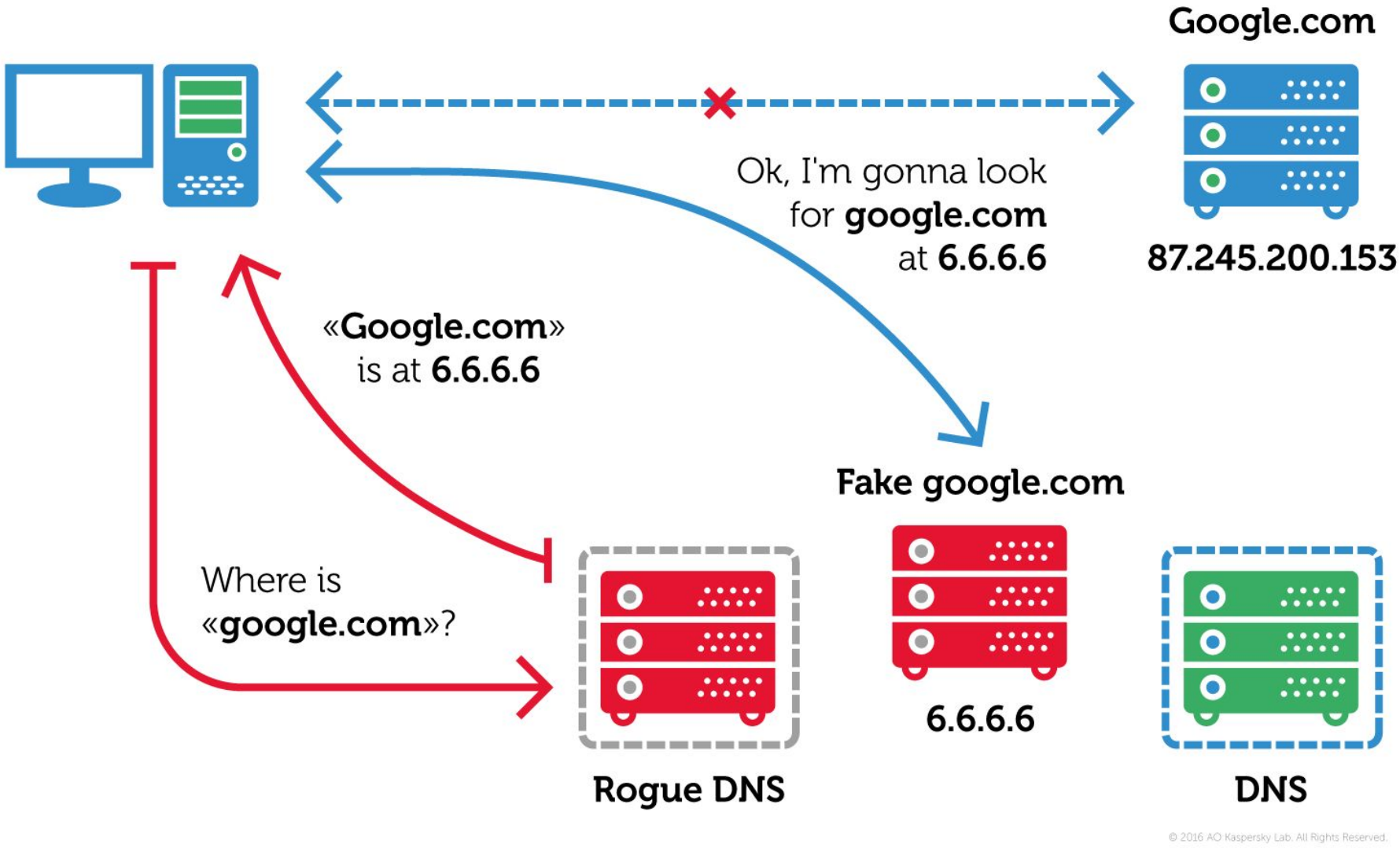
-3wifi.stascorp.com



-Bruteforce


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


Google.com
Ok, I'm gonna look for google.com at 6.6.6.6
87.245.200.153
«Google.com» is at 6.6.6.6
Fake google.com
Where is «google.com»?
6.6.6.6
Rogue DNS
DNS
© 2016 AO Kaspersky Lab. All Rights Reserved.

Удаленный доступ

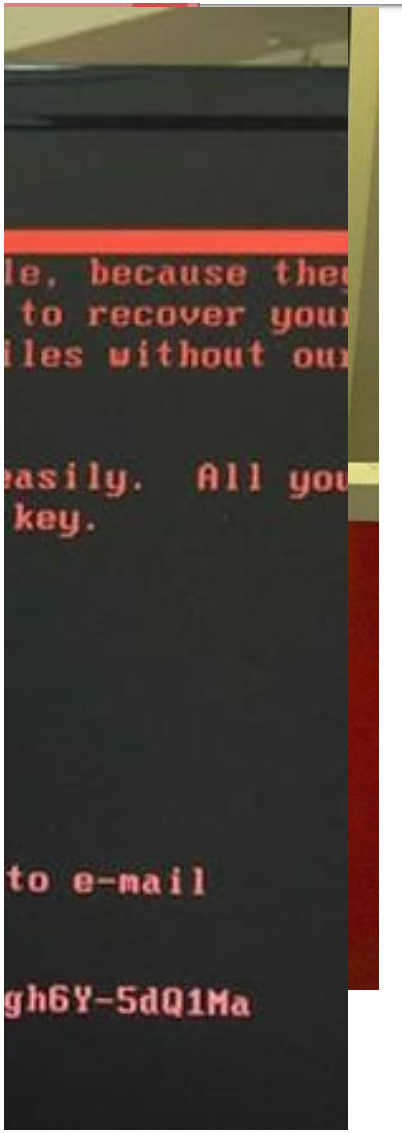
-Мобильные устройства

-Шифровальщики

Город в Канаде был вынужден заплатить биткоины после атаки шифровальщика

Олег Иванов 12 сентября 2018 - 17:25

Общее | Вирусы-вымогатели | Вирусы-шифровальщики

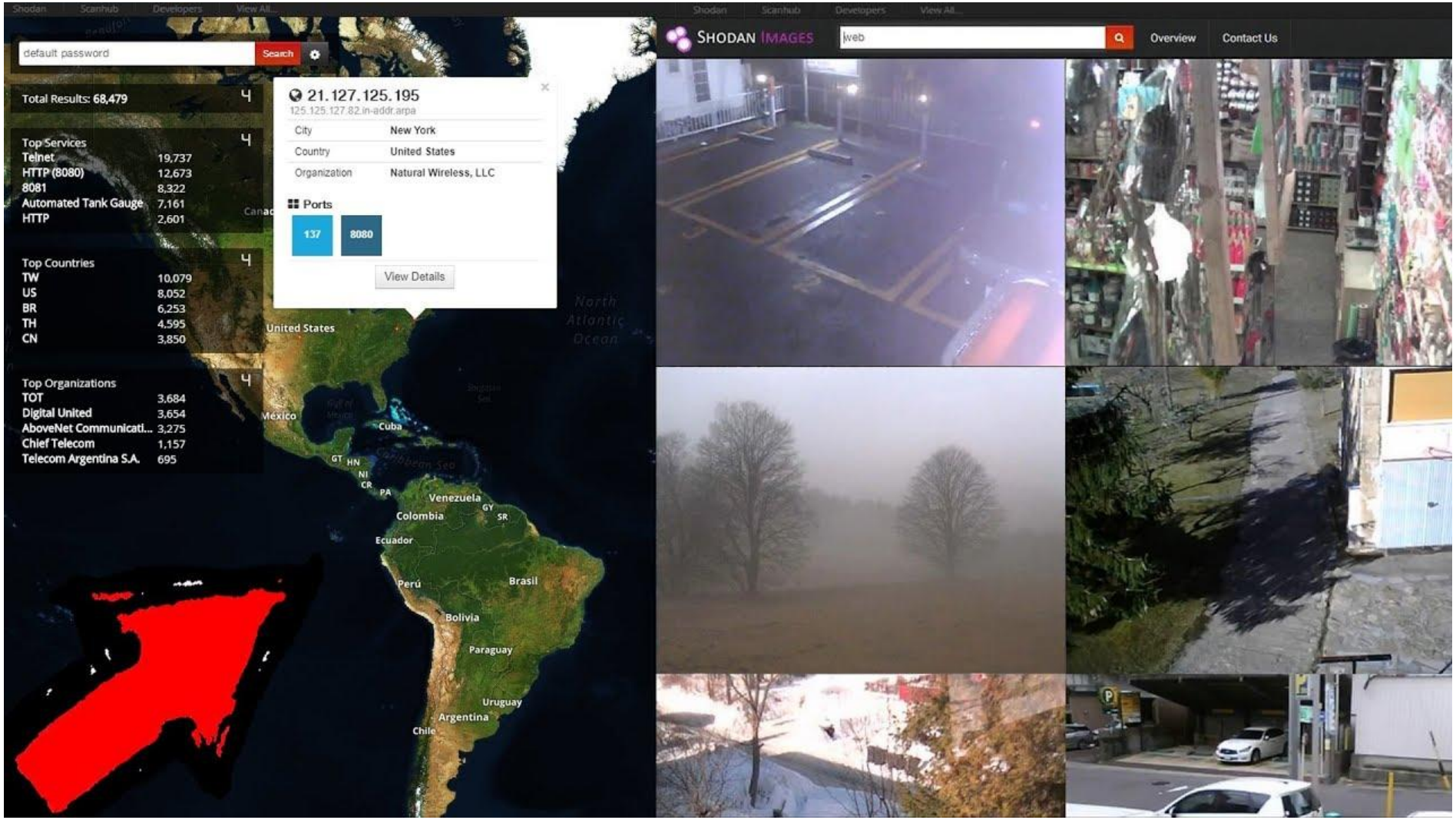


-Keylogger

-Майнеры

-Webcam

-Поисковик Shodan



Bluetooth-атака

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

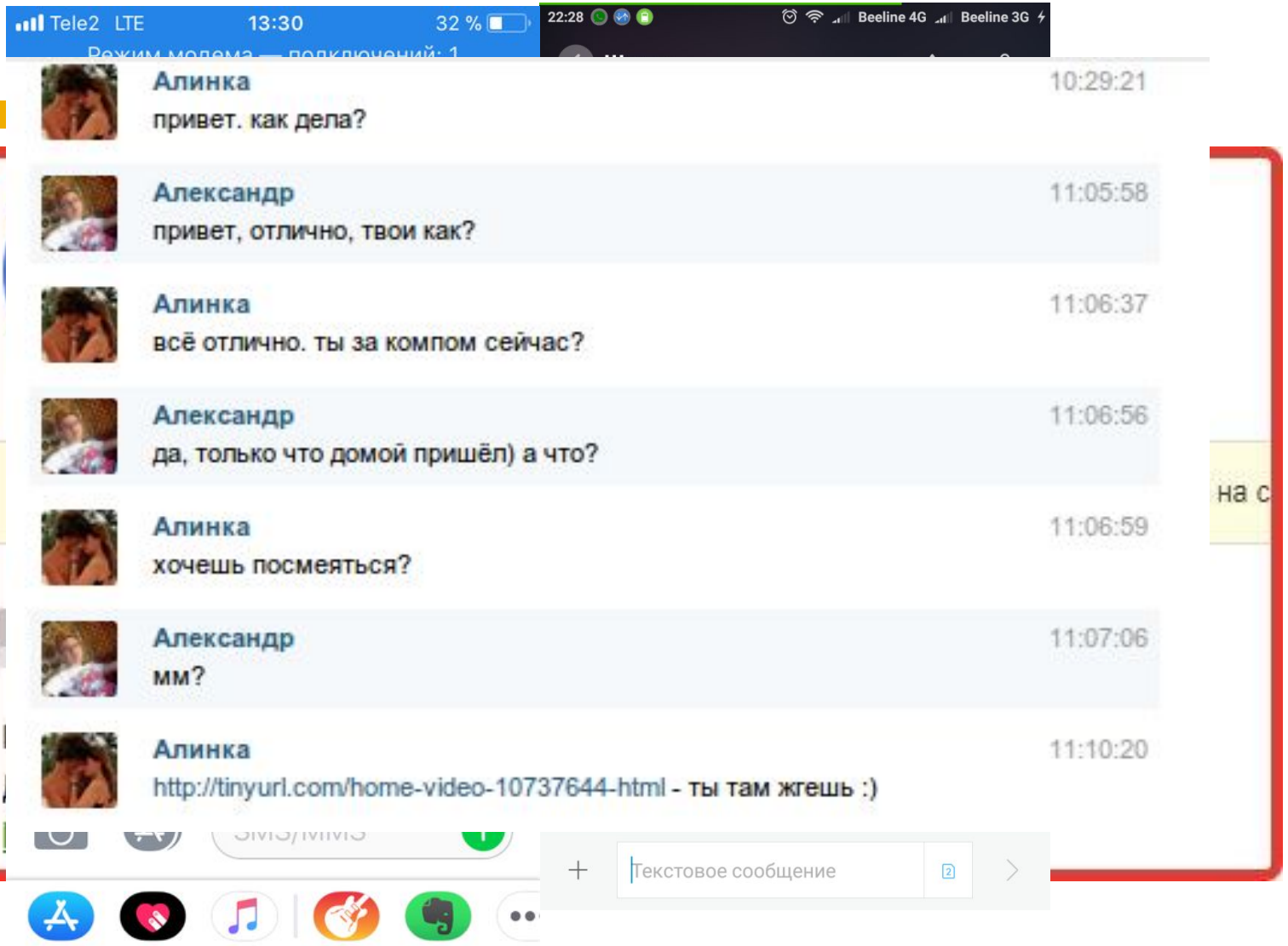
USB


НОВОСТИ
Вредоносный кабель USBHarpoon компрометирует устройство за считанные секунды
Мария Нефёдова , 3 недели назад 3 мин на чтение 3 4 67791

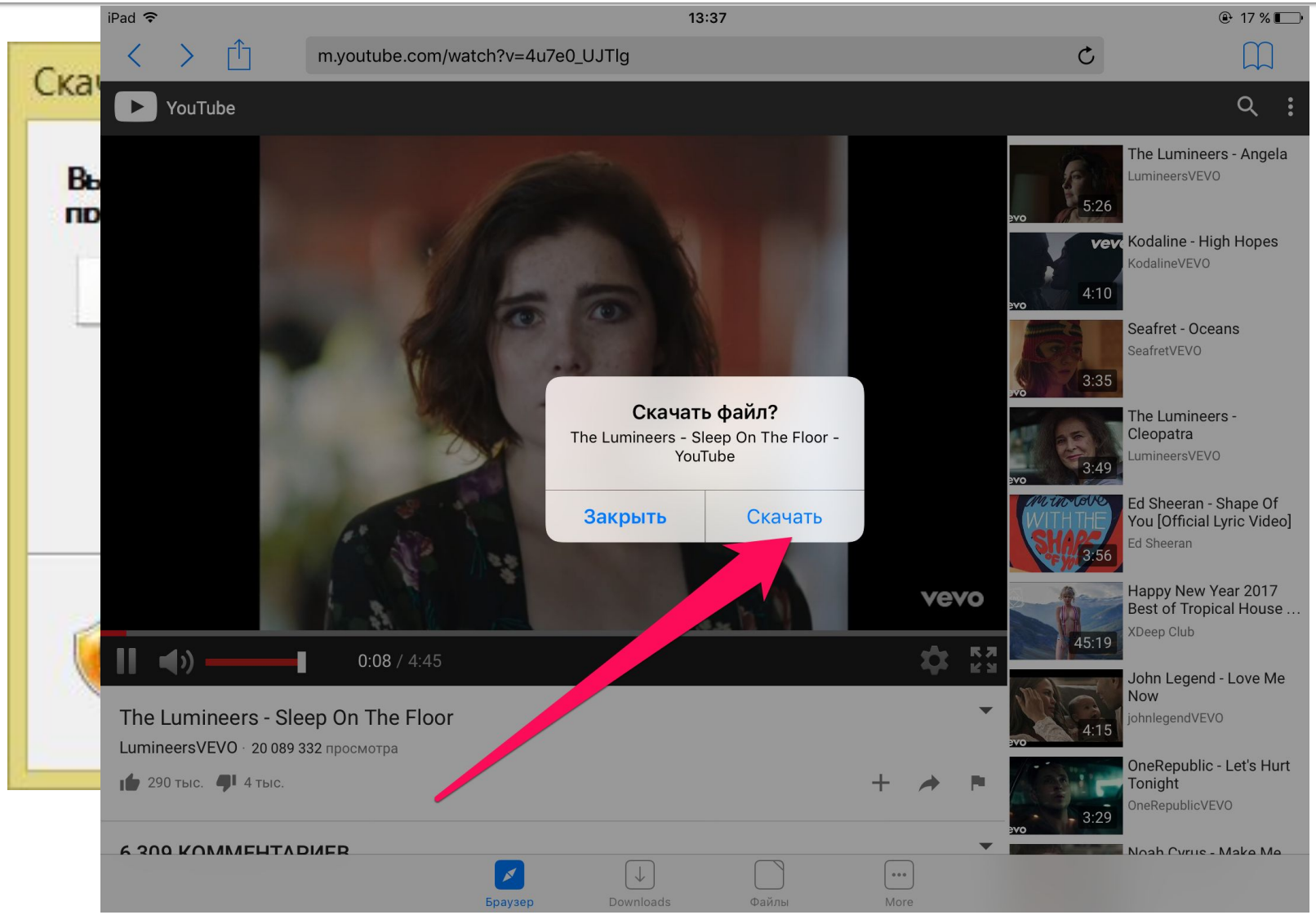
Кардинг

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

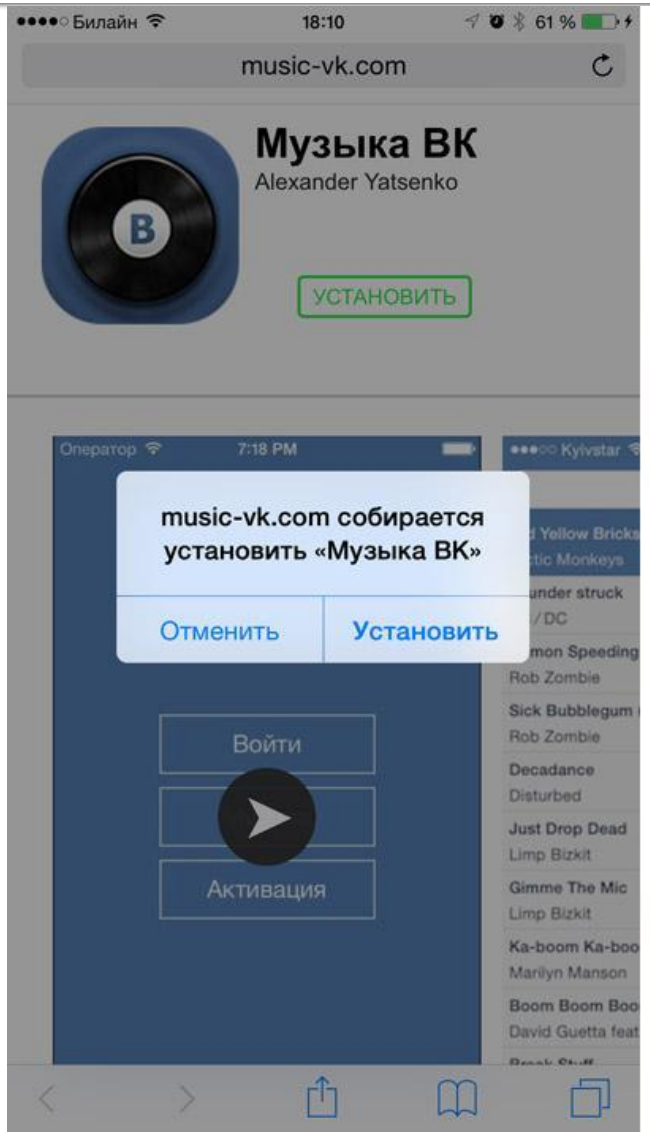
Не переходите по неизвестным ссылкам!

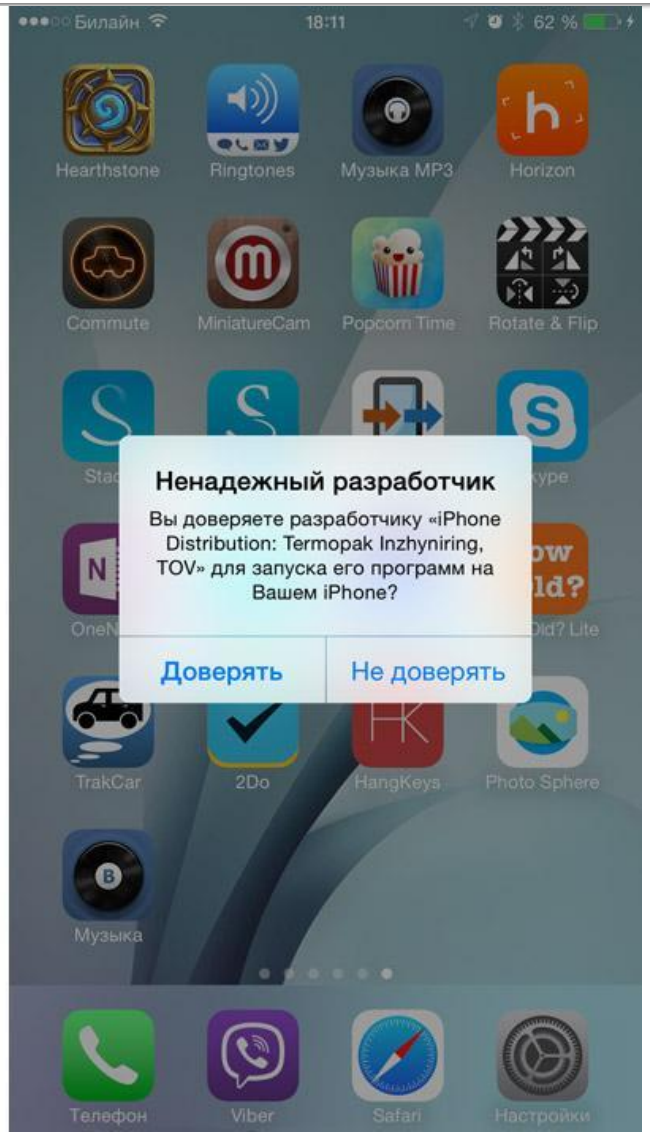


Не скачивайте файлы!



Не устанавливайте подозрительные приложения





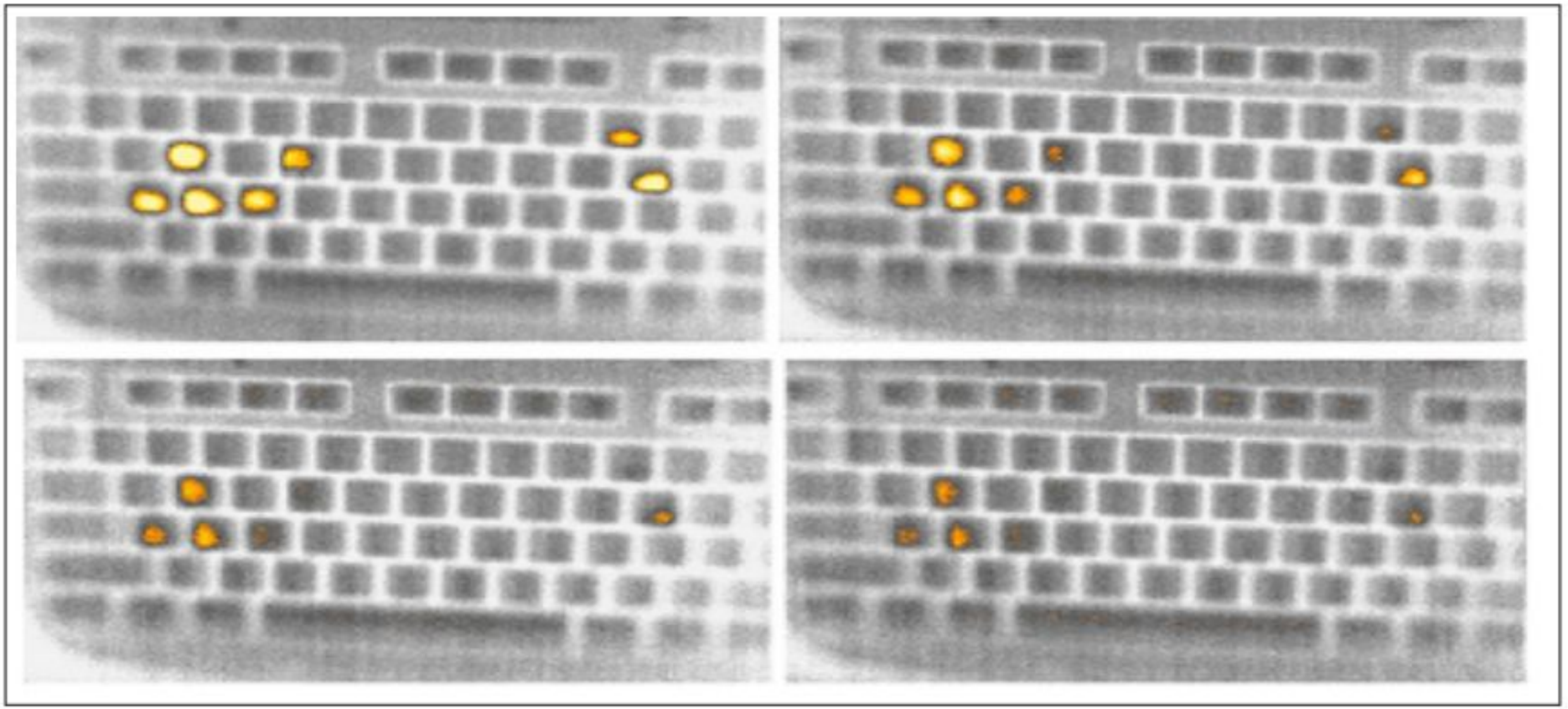
Никаких USB

Только свой мобильный интернет (свой WiFi)

Сложные пароли

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

P.S.



¯_(ツ)_/¯

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

Мария Нефёдова , 1 week назад 1 мин на чтение 0 0 2145

Источники

- **hackware.ru** - этичный хакинг и тестирование на проникновение;
- **xakep.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!