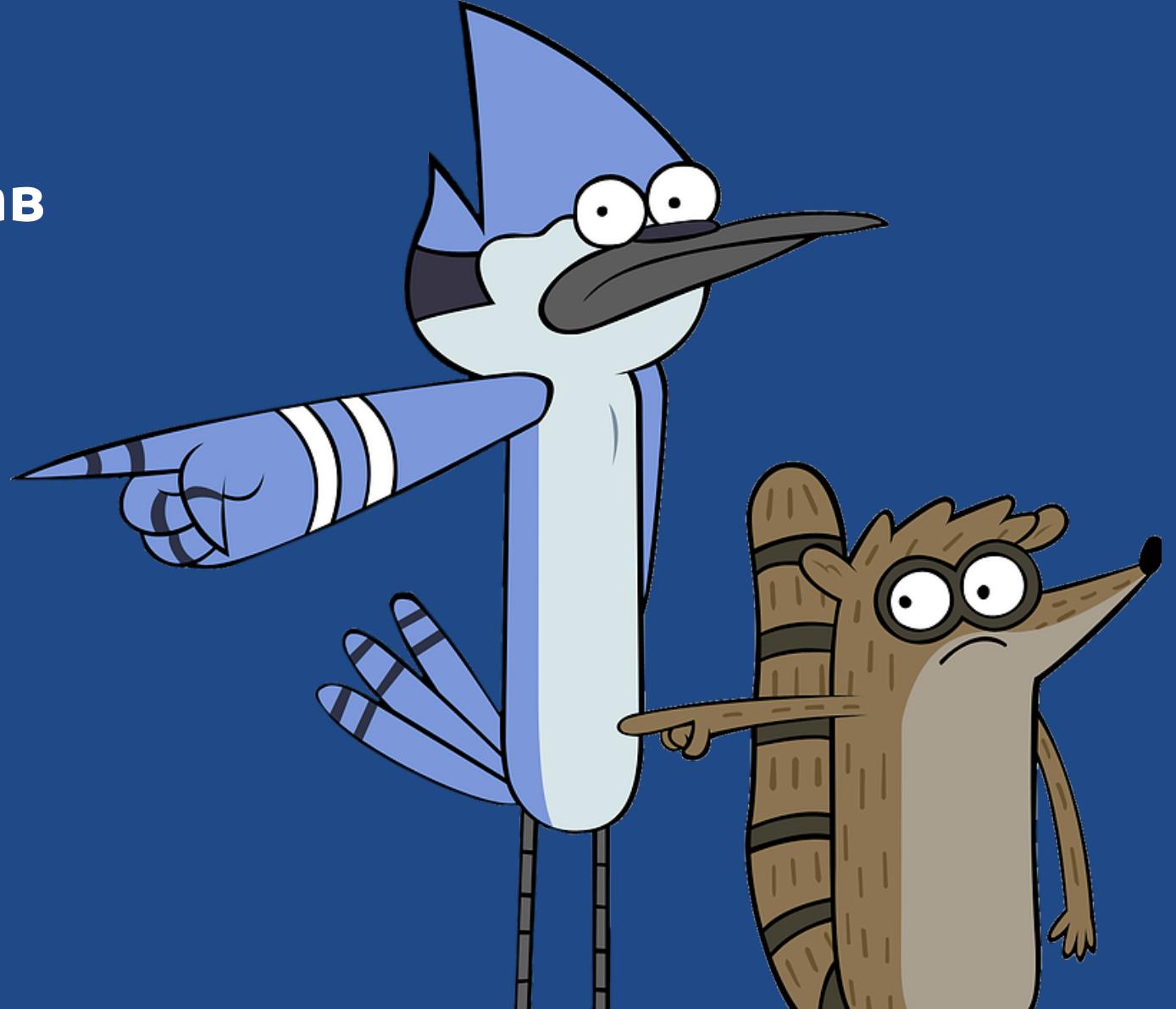




Ковалев Ярослав  
Инженер Nokia



# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Защита цифровых устройств
- Социальные сети
- Социальная инженерия
- Публичные Wi-Fi сети

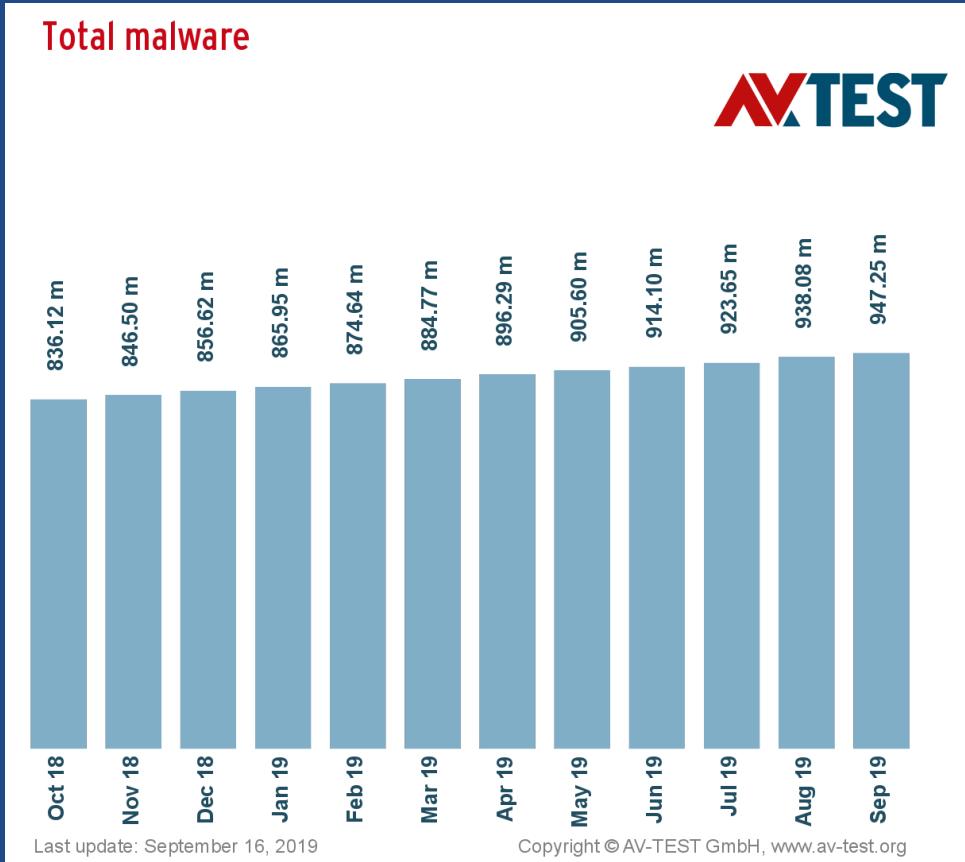
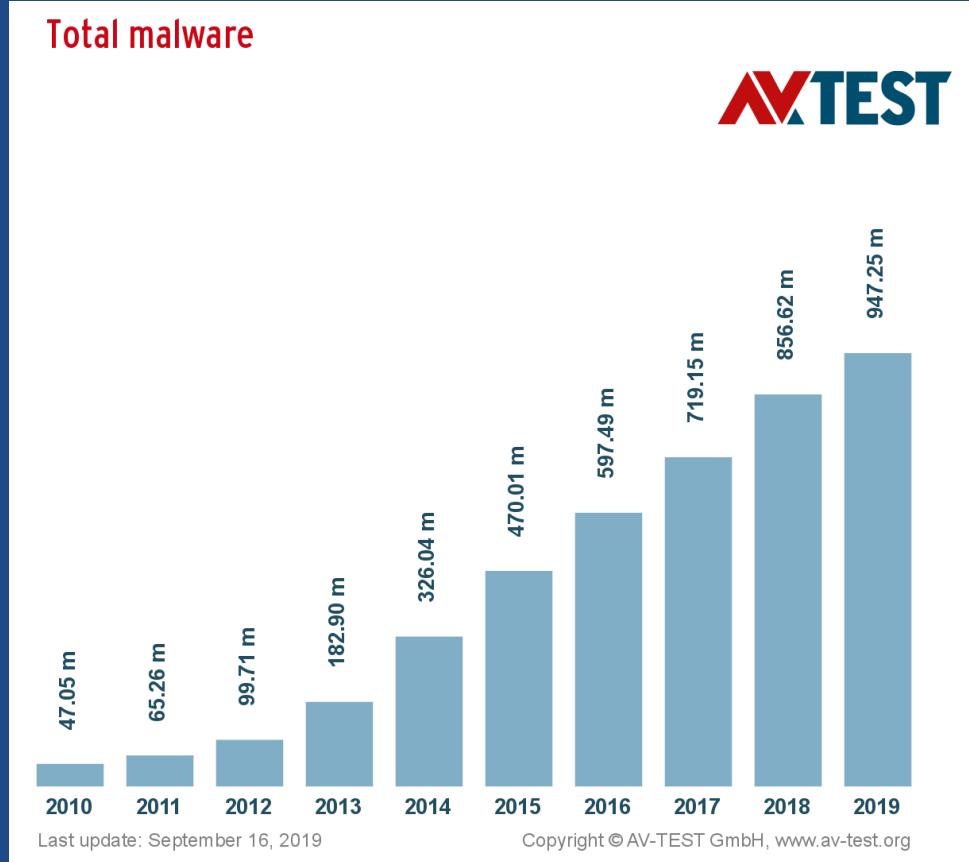


# Защита цифровых устройств

- Угрозы
- Антивирусная защита и обновление систем
- Проверка файлов
- Защита e-mail
- Пароли
- 2FA

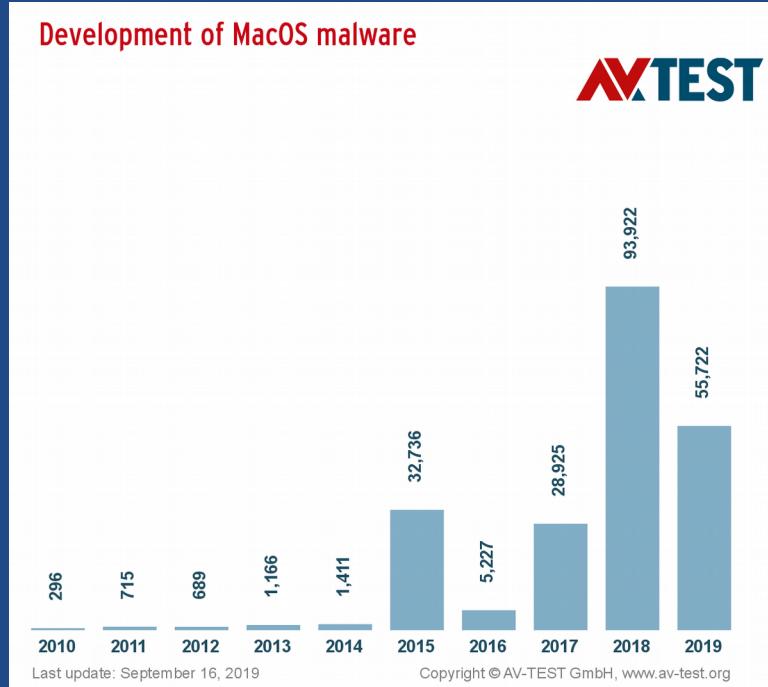
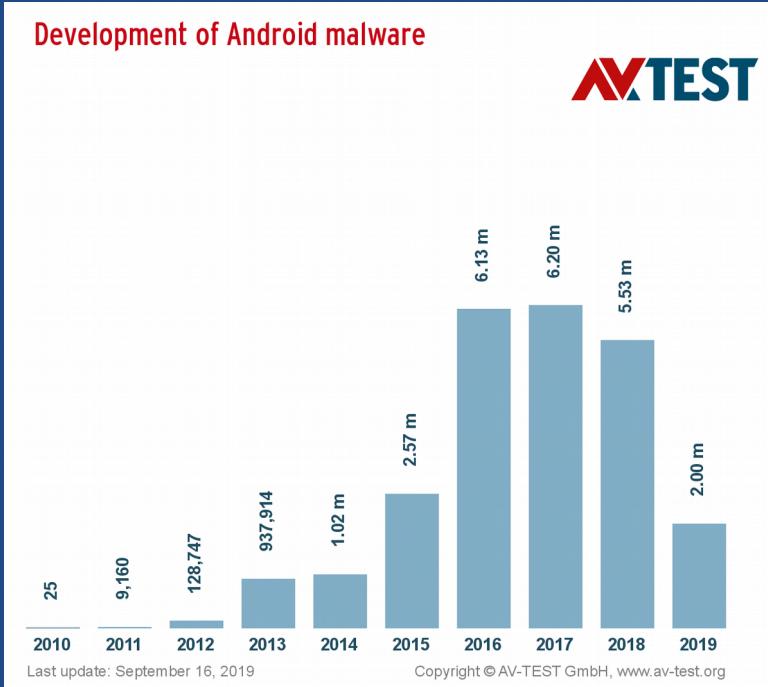


# Защита цифровых устройств



УГРОЗЫ

# Защита цифровых устройств



УГРОЗЫ

# Защита цифровых устройств

- Актуальность антивирусных баз
- Автоматическое обновление ОС
- Своевременное обновление драйверов и приложений



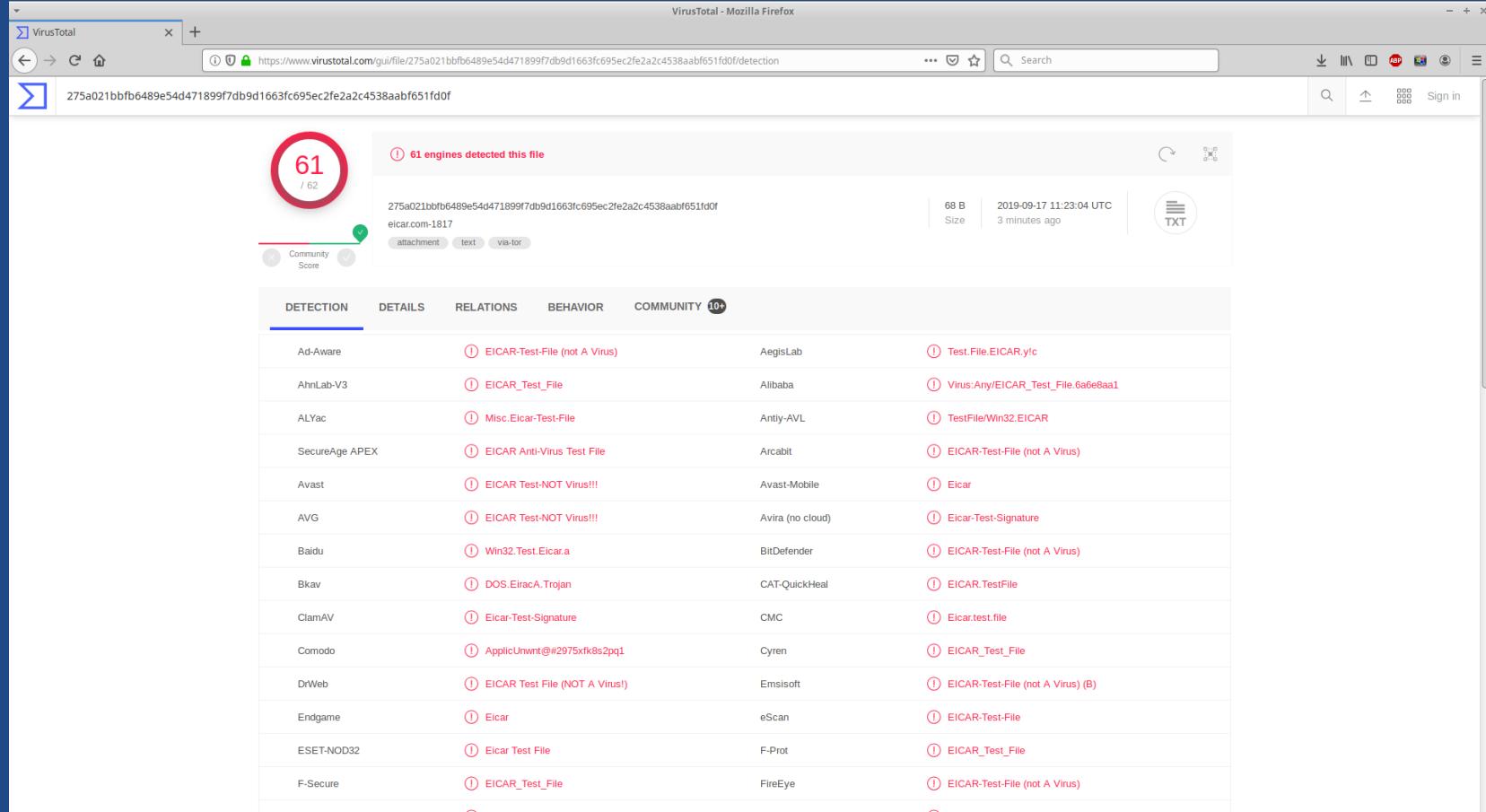
АНТИВИРУСНАЯ ЗАЩИТА И ОБНОВЛЕНИЯ СИСТЕМ

# Защита цифровых устройств

The screenshot shows a Mozilla Firefox browser window with the title bar "VirusTotal - Mozilla Firefox". The address bar displays the URL "https://www.virustotal.com/gui/home/upload". The main content area features the VirusTotal logo (a blue square with a white Greek sigma symbol) and the text "VIRUSTOTAL". Below the logo, a subtitle reads "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community". A central input field is divided into three tabs: "FILE" (underlined in blue), "URL", and "SEARCH". The "FILE" tab contains a file icon with a fingerprint and a "Choose file" button. At the bottom of the input field, a small note states: "By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#)." The footer of the page includes links for "VirusTotal", "Community", "Tools", "Premium Services", and "Documentation", along with their respective sub-links like "Contact Us", "Join Community", "API Scripts", and "Intelligence".

ПРОВЕРКА ФАЙЛОВ

# Защита цифровых устройств



VirusTotal - Mozilla Firefox

Σ 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

61 / 62

61 engines detected this file

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f  
eicar.com-1817

attachment text via-tor

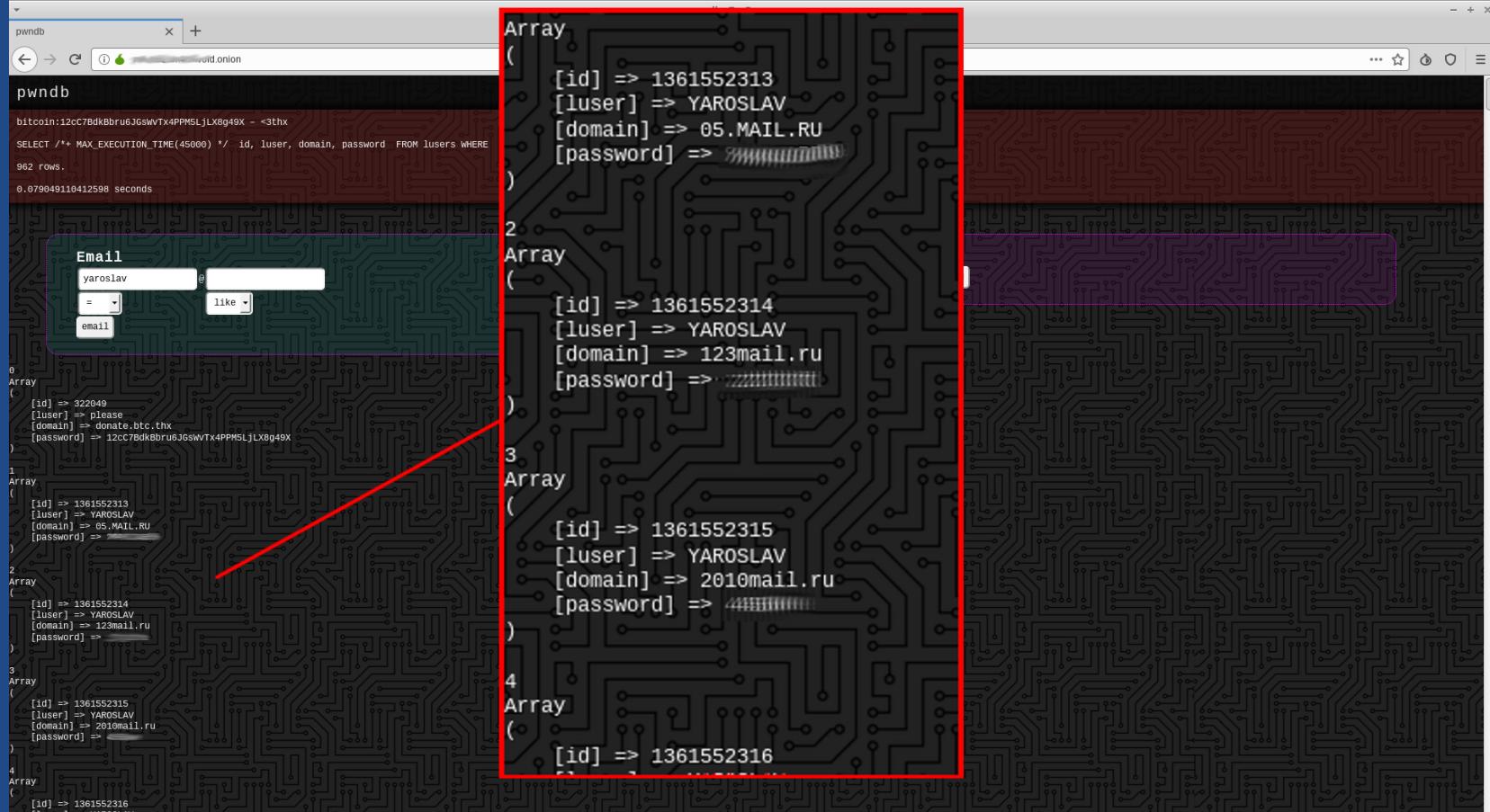
Community Score

Size: 68 B | Date: 2019-09-17 11:23:04 UTC | 3 minutes ago | TXT

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 10+
Ad-Aware	① EICAR-Test-File (not A Virus)	AegisLab	① Test.File.EICAR.ylc	
AhnLab-V3	① EICAR_Test_File	Alibaba	① Virus:Any/EICAR_Test_File.6a6e8aa1	
ALYac	① Misc.Eicar-Test-File	Antiy-AVL-	① TestFile/Win32.EICAR	
SecureAge APEX	① EICAR Anti-Virus Test File	Arcabit	① EICAR-Test-File (not A Virus)	
Avast	① EICAR Test-NOT Virus!!!	Avast-Mobile	① Eicar	
AVG	① EICAR Test-NOT Virus!!!	Avira (no cloud)	① Eicar-Test-Signature	
Baidu	① Win32.Test.Eicar.a	BitDefender	① EICAR-Test-File (not A Virus)	
Bkav	① DOS.EiracA.Trojan	CAT-QuickHeal	① EICAR.TestFile	
ClamAV	① Eicar-Test-Signature	CMC	① Eicar.test.file	
Comodo	① ApplicUrwnt@#2975fk8s2pq1	Cyren	① EICAR_Test_File	
DrWeb	① EICAR Test File (NOT A Virus!)	Emsisoft	① EICAR-Test-File (not A Virus) (B)	
Endgame	① Eicar	eScan	① EICAR-Test-File	
ESET-NOD32	① Eicar Test File	F-Prot	① EICAR_Test_File	
F-Secure	① EICAR_Test_File	FireEye	① EICAR-Test-File (not A Virus)	
Fortinet	① EICAR_TEST_FILE	GDStar	① EICAR_TEST_FILE	

ПРОВЕРКА ФАЙЛОВ

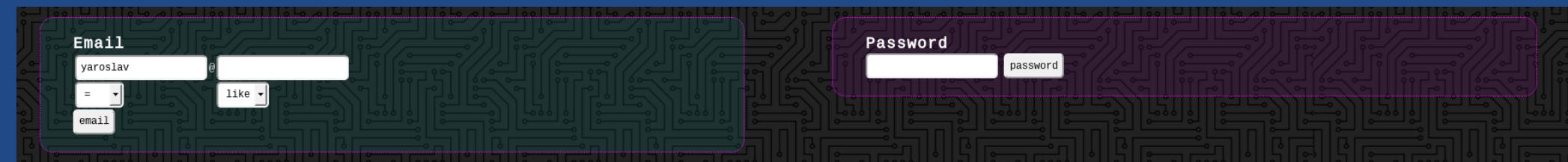
# Защита цифровых устройств



ЗАЩИТА Е-MAIL

# Защита цифровых устройств

Доступна проверка не только по адресу электронной почты, но и паролю:



ЗАЩИТА Е-MAIL

# Защита цифровых устройств

- Не использовать словарные фразы
- Не использовать личную информацию
- Не менее 10 символов
- Использовать спецсимволы и разный регистр букв

Пример хорошего пароля:

OktUjNast-UjRo6aOtE7

# Защита цифровых устройств

Мнемоническое запоминание сложного пароля:

*Октябрь уж наступил — уж роща отряхает*

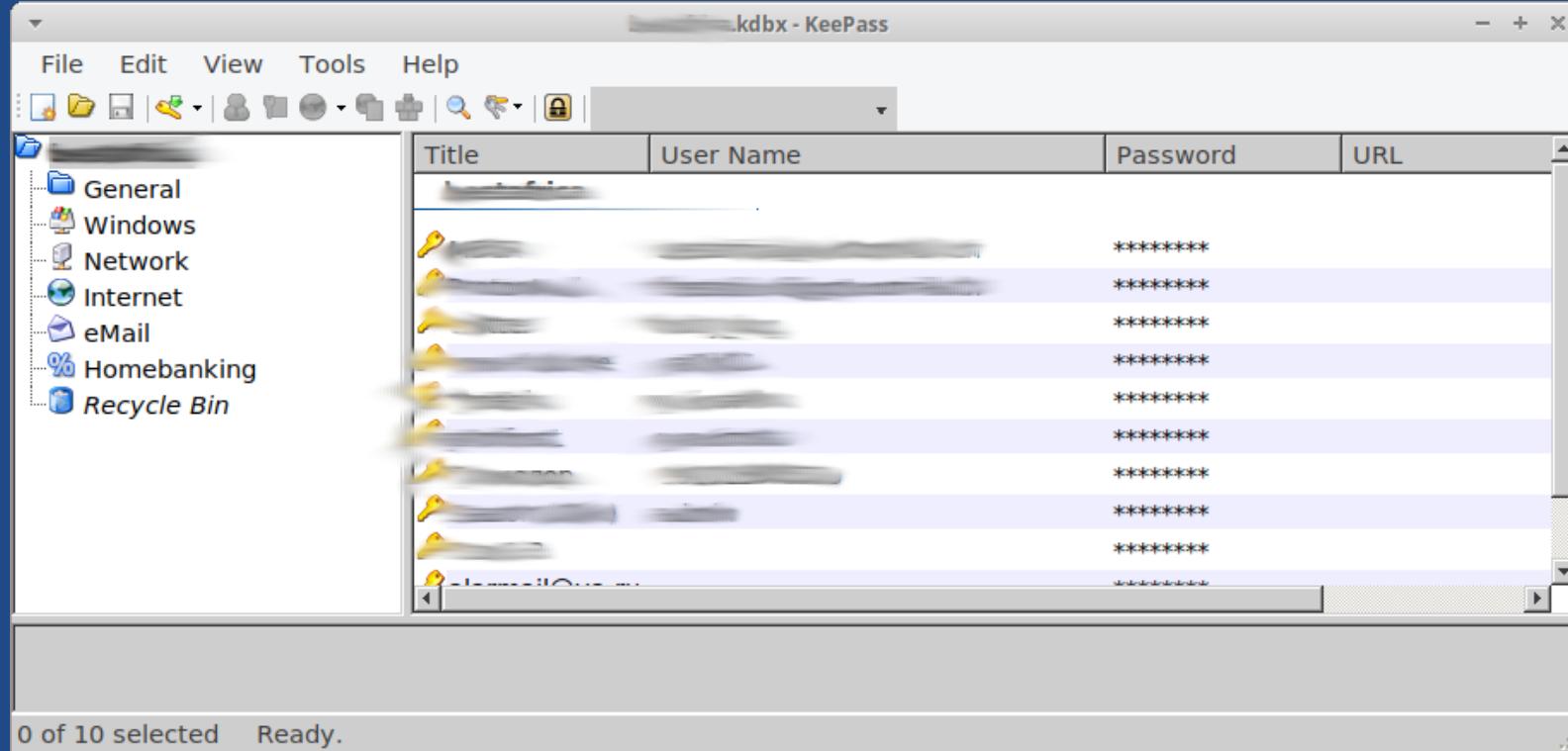
OktUjNast-UjRo6aOtE7



ПАРОЛИ

# Защита цифровых устройств

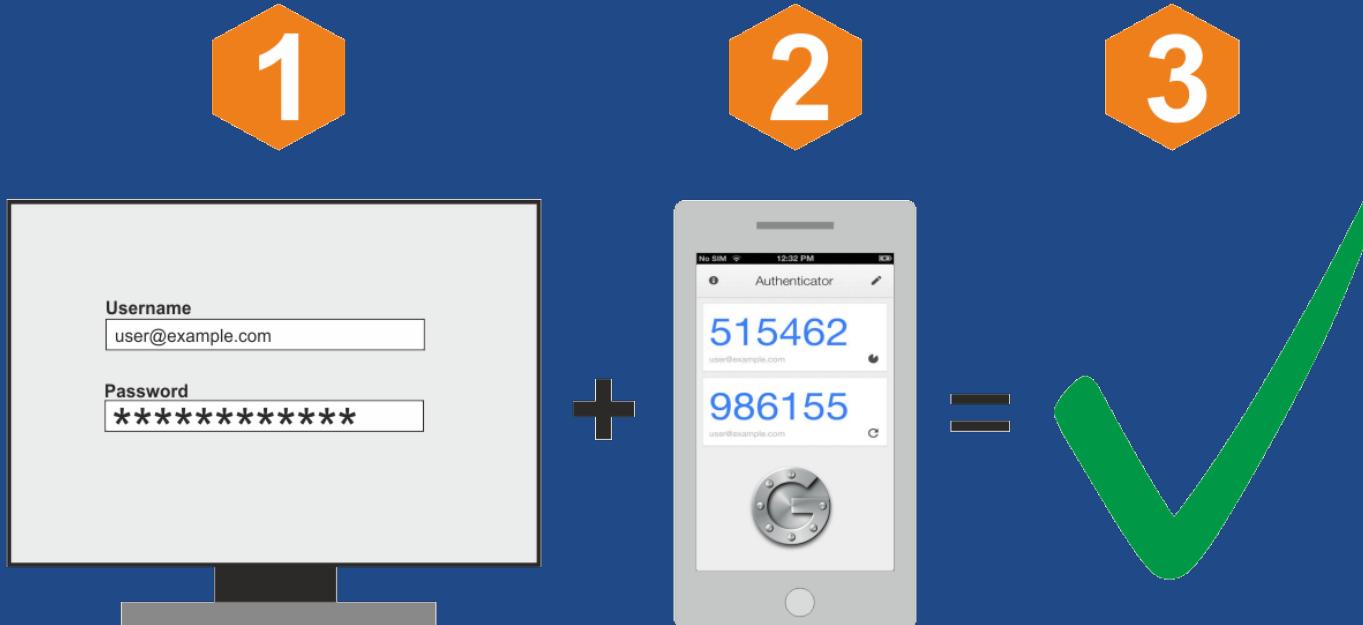
## KeePass:



ПАРОЛИ

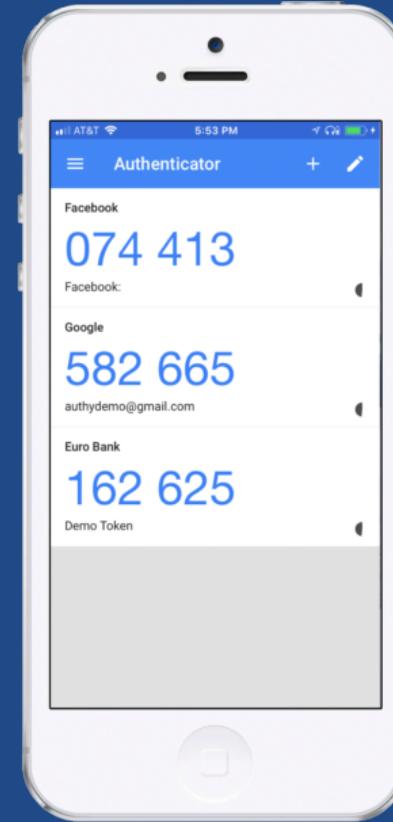
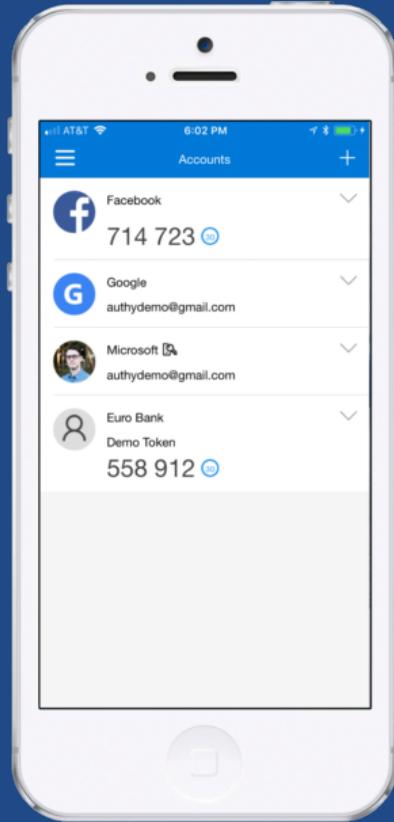
# Защита цифровых устройств

## 2FA - двухфакторная аутентификация



2FA

# Защита цифровых устройств



Google

Microsoft

2FA

# СОЦИАЛЬНЫЕ СЕТИ



# СОЦИАЛЬНЫЕ СЕТИ



ДАТА-ЦЕНТРЫ

# СОЦИАЛЬНЫЕ СЕТИ

Что скрыто от пользователя:

- Дата и время посещения профиля не в явном виде
- Привязка IP-адреса к записям, комментариям, статусам
- Метаданные документов
- История изменений профиля



# СОЦИАЛЬНЫЕ СЕТИ

16:07 | 0,1 КБ/с



## Настройки камеры

ОСНОВНЫЕ НАСТРОЙКИ

Сохранять место съемки



Звук затвора



Режим "В кармане"

Предотвращать случайные нажатия при помещении устройства в карман



Сохранять предыдущий режим

При запуске камеры переключаться в последний используемый режим



СЪЕМКА ФОТО

Дата и время на фото



Водяной знак устройства



Линии сетки



Фокус и снимок

Коснитесь экрана для фокусировки, затем еще раз, чтобы сделать снимок



Сканировать QR-коды

Сканировать QR-коды в режиме "Фото" может только основная камера



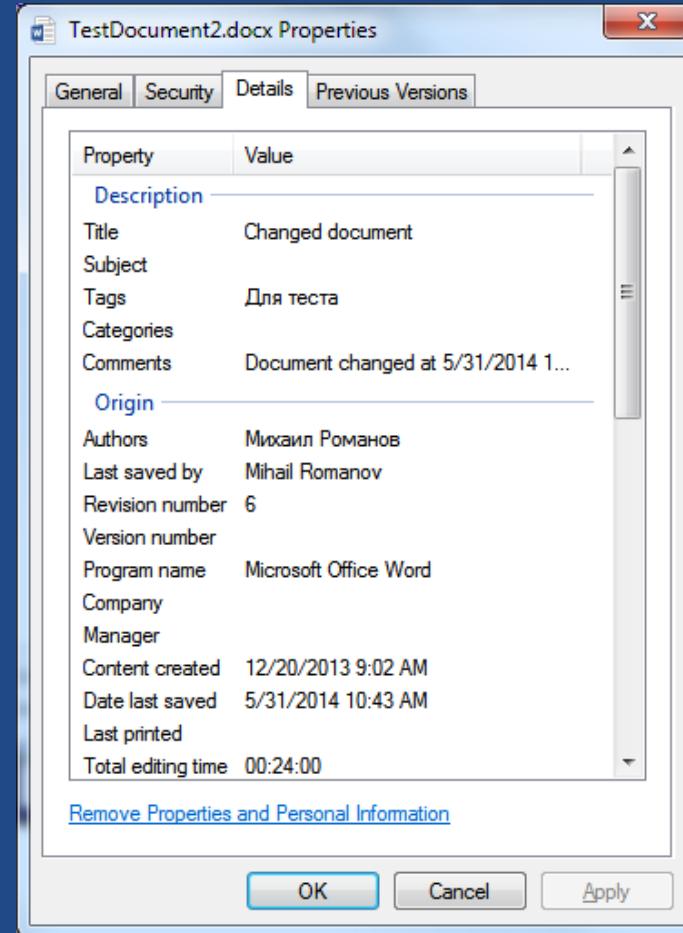
Долгое нажатие кнопки съемки

Серийная съемка >

<b>Model</b>	Redmi Note 7
<b>Software</b>	lavender-user 9 PKQ1.180904.001 V10.3.5.0.PFGRUXM release-keys
<b>Orientation</b>	Horizontal (normal)
<b>ModifyDate</b>	2019:09:17 16:09:26
<b>YCbCrPositioning</b>	Centered
<b>ISO</b>	500
<b>ExposureProgram</b>	Not Defined
<b>GPSLatitudeRef</b>	North
<b>GPSLatitude</b>	45.5777
<b>GPSLongitudeRef</b>	East
<b>GPSLongitude</b>	41.5335
<b>GPSAltitudeRef</b>	Above Sea Level
<b>GPSAltitude</b>	445.977 м
<b>GPSTimeStamp</b>	13:09:25
<b>GPSProcessingMethod</b>	GPS
<b>GPSDateStamp</b>	2019:09:17

Метаданные документов

# СОЦИАЛЬНЫЕ СЕТИ



Метаданные документов

# СОЦИАЛЬНЫЕ СЕТИ



damedvedev  [Подписаться](#)  ...

577 публикаций 2,7млн подписчиков Подписки: 1

**Дмитрий Медведев**  
Председатель Правительства России  
Prime Minister, Government of Russia  
[government.ru](#)

Подписаны stavart4200, ktsekhanova, stavbitaccelerator + еще 22

---

 [ПУБЛИКАЦИИ](#)  [ОТМЕТКИ](#)





ИИ

# СОЦИАЛЬНЫЕ СЕТИ

ПРОФИЛЯ  
medvedev

damedvedev

Подписаться

577 публикаций 2,7 млн подписчиков Подписки: 1

**Дмитрий Медведев**  
Председатель Правительства России  
Prime Minister, Government of Russia  
[government.ru](#)

Подписаны stavart4200, ktsekhanova, stavbitaccelerator + еще 22

---

ПУБЛИКАЦИИ      ОТМЕТКИ

На изображении может находиться: облако, небо и на улице

На изображении может находиться: небо, океан, лодка, на улице и вода

На изображении может находиться: цветок, небо, растение, облако, на улице и природа

На изображении может находиться: облако, небо, океан, на улице, природа и вода

На изображении может находиться: небо, облако и на улице

На изображении может находиться: 2 человека, люди на сцене, толпа и на улице

ИИ

# СОЦИАЛЬНЫЕ СЕТИ

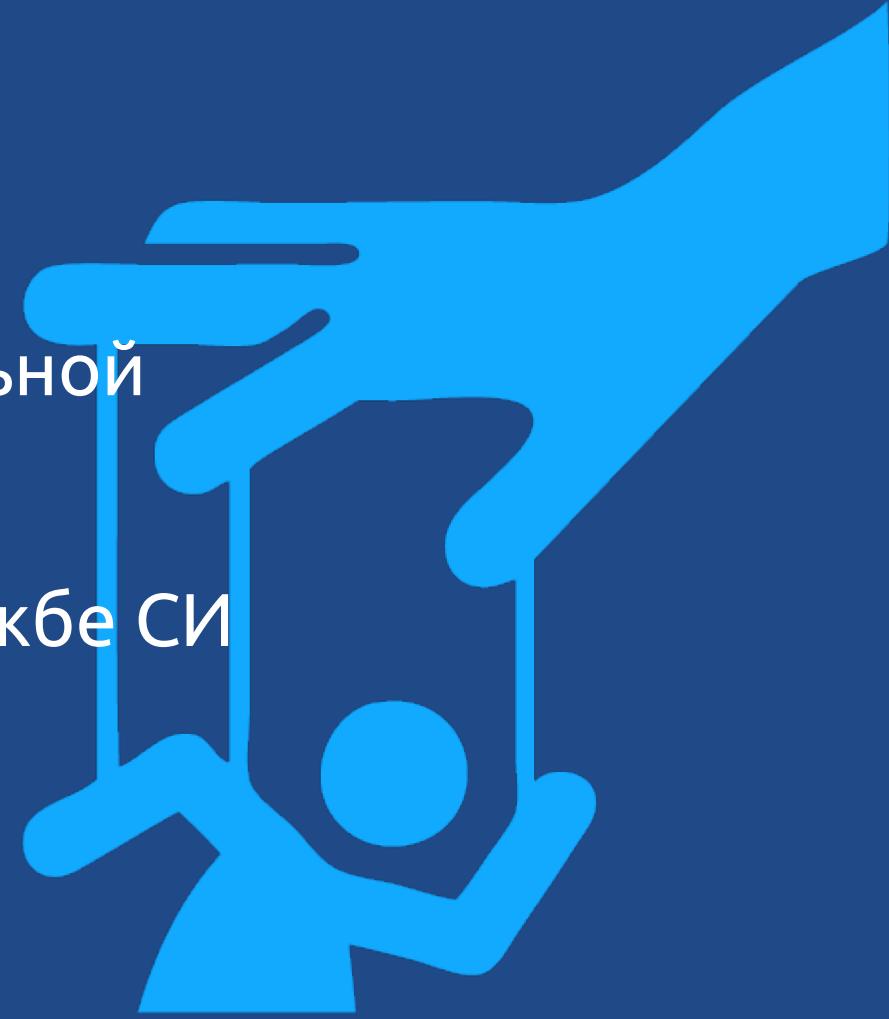


На изображении может находиться: 2 человека, люди на сцене, толпа и на улице

ИИ

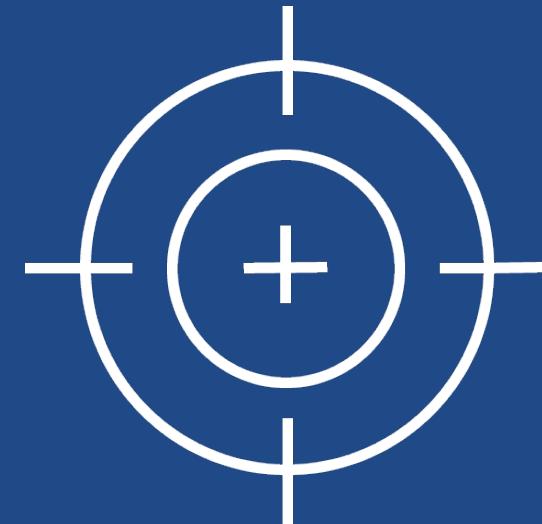
# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Атака на человека, а не на информационную систему
- Технические средства в социальной инженерии
- Open Source INTeelligence на службе СИ
- Последствия



# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Уверенность
- Знание контекста
- Обращение к авторитету
- Обращение к эмоциям
- Эксплуатация эмоций (страх, лень, жадность)
- Контроль внимания



Атака на человека, а не на информационную систему

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Фишинг
  - сбор аутентификационных данных
  - запуск вредоносных приложений
- Спирфишинг
- Кликджекинг
- “Road apple”



Технические средства в социальной инженерии

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

## OSINT (Open Source INTelligence)



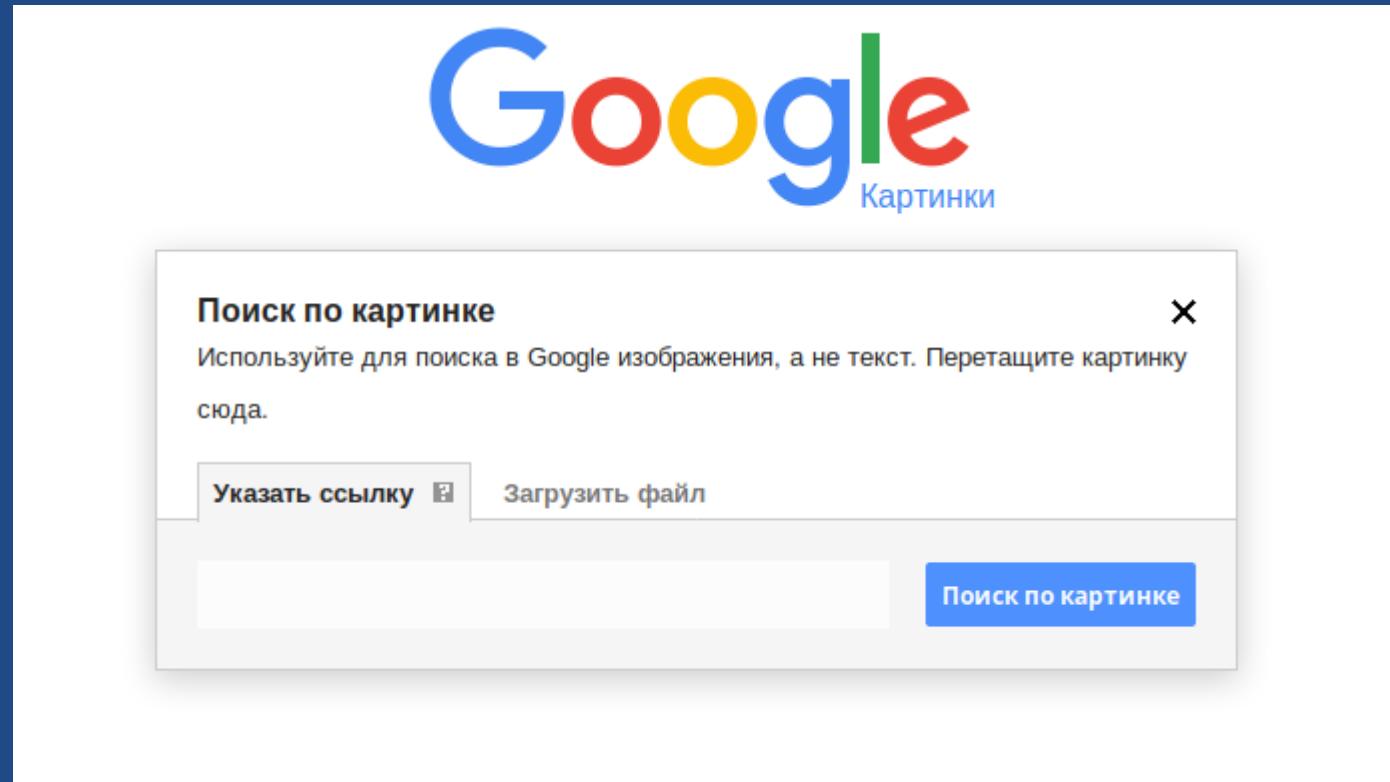
поиск, сбор и анализ информации, полученной из общедоступных источников

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Анализ социальных сетей
  - Анализ школьного сайта
  - Анализ блога
  - Поисковые системы
  - Радиомониторинг



# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

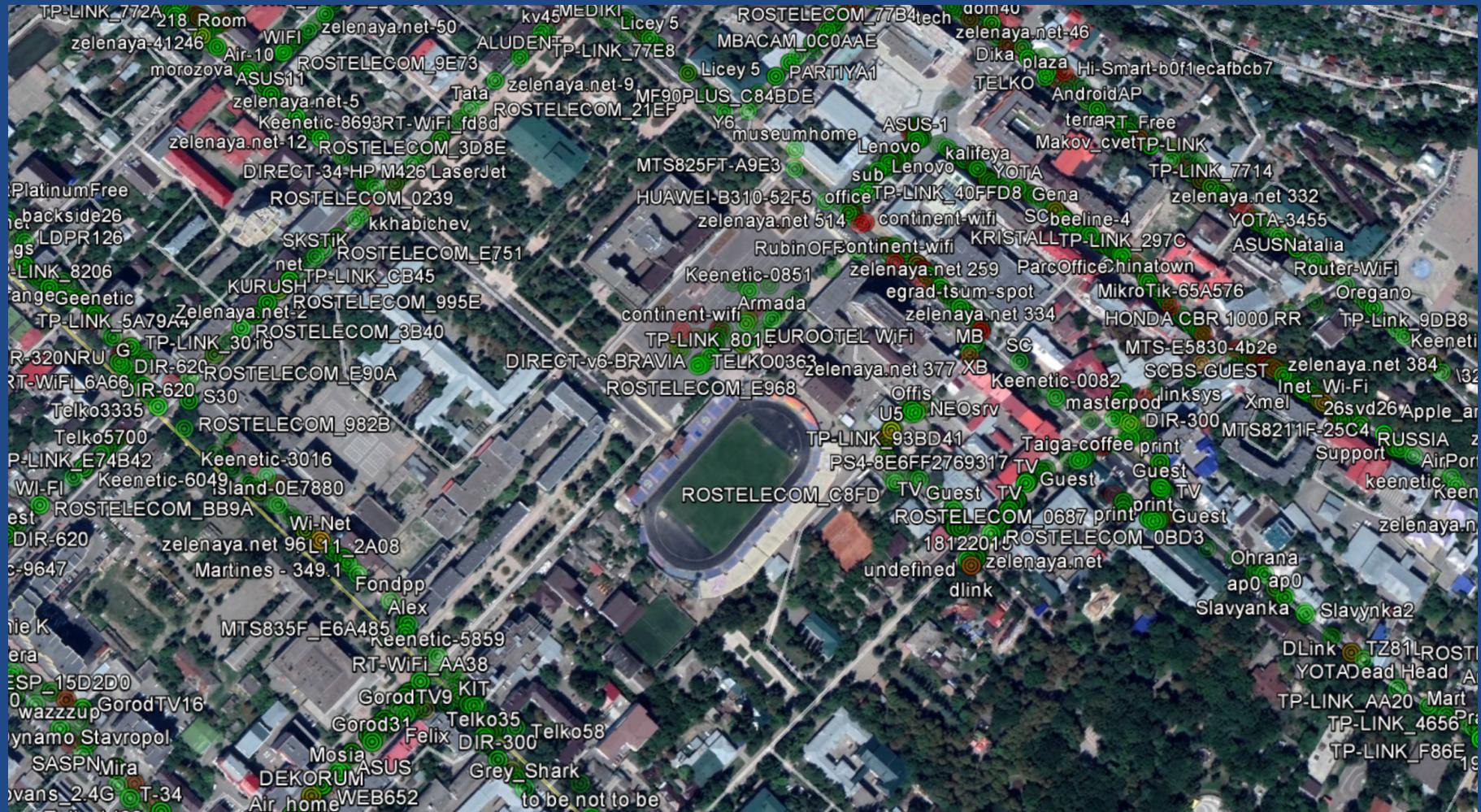


OSINT

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

0	0	11	54e	WPA2 CCMP	PSK	ROSTELECOM_E897
0	0	1	54e	WPA2 CCMP	PSK	lily
4	0	3	54e	WPA2 CCMP	PSK	diatecnew2
<hr/>						
PWR	Rate	Lost	Frames	Probe		
3:BF	-86	0 - 1	0		1	
F:29	-91	0 - 1	0		1	
4:DA	-61	0 - 1	0		1	
1:D8	-68	0 - 1	0		12	
7:64	-73	0 - 1	0		7	
7:22	-83	0 - 1	0		3	
3:3C	-84	0 - 1	0		4	
1:EE	-85	0 - 1	0		1	VALERA
2:E5	-88	0 - 1	0		3	Kodzoeva
F:32	-89	0 - 1	0		3	
E:32	-90	0 - 1	0		1	
					2	Ervin1988

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



OSINT

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

```
root@localhost: /home/TheHackToday/blueborne-scanner
File Edit View Search Terminal Help
root@localhost:/home/TheHackToday/blueborne-scanner# python2.7 bluebornescan.py

hook's Blueborne Android scanner v0.01

searching for devices
9C:A5:C0:05:C4:8B - Endasmu - !!! IS Vulnerable
```

Apple devices scanner						
Mac	State	Device	WI-FI	OS	Phone	Time
50:2D:AC:99:12:94	Off	iPhone	On	iOS12		1563353463
7E:B5:C1:97:E4:C9	Home screen	MacBook	On	Mac OS		1563353463
51:7B:B1:BB:E5:51	Lock screen	iPhone	On	iOS12		1563353463
56:E6:3F:CD:76:86	Off	Watch	On	WatchOS		1563353453
6B:54:70:E6:25:7D	Home screen	iPhone	On	iOS12		1563353463
49:5E:D2:98:47:47	Off	iPhone	On	iOS12		1563353463
41:CE:CF:85:21:B8	Off	Watch	On	WatchOS		1563353463

OSINT

# ПУБЛИЧНЫЕ Wi-Fi СЕТИ

- “Человек посередине”:
  - Перехват трафика
  - Вмешательство в трафик
- Прямые атаки на устройства



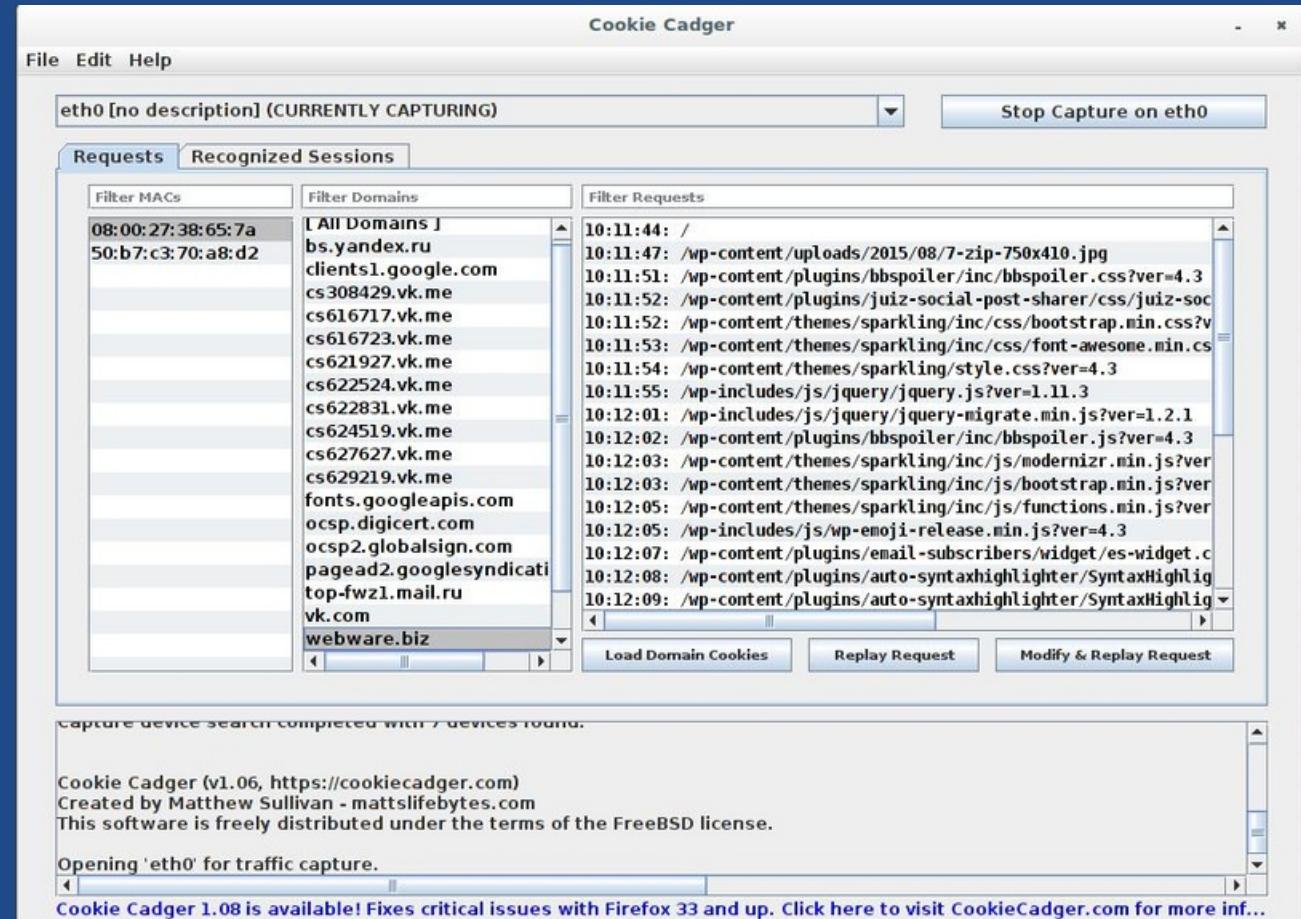
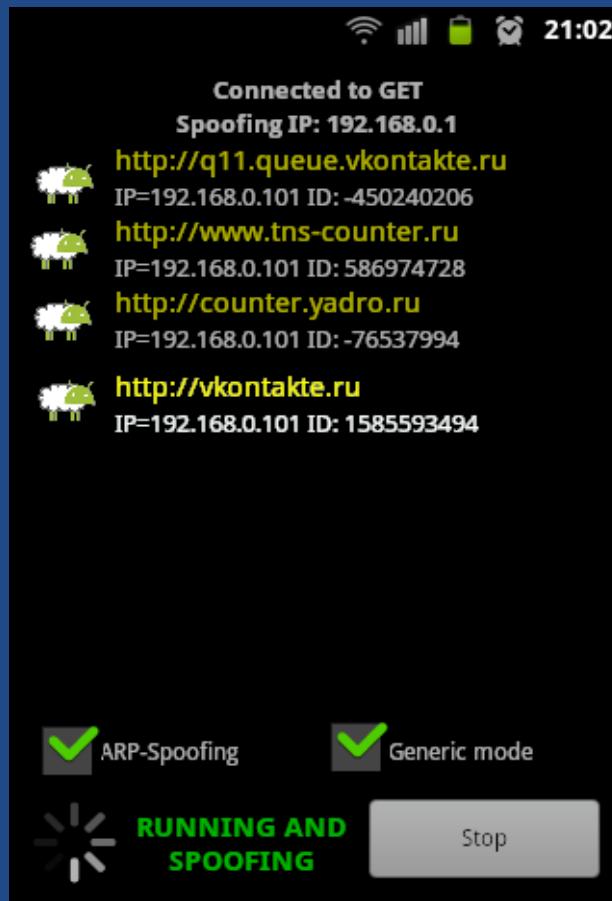
# ПУБЛИЧНЫЕ Wi-Fi СЕТИ



**HACKERMAN**

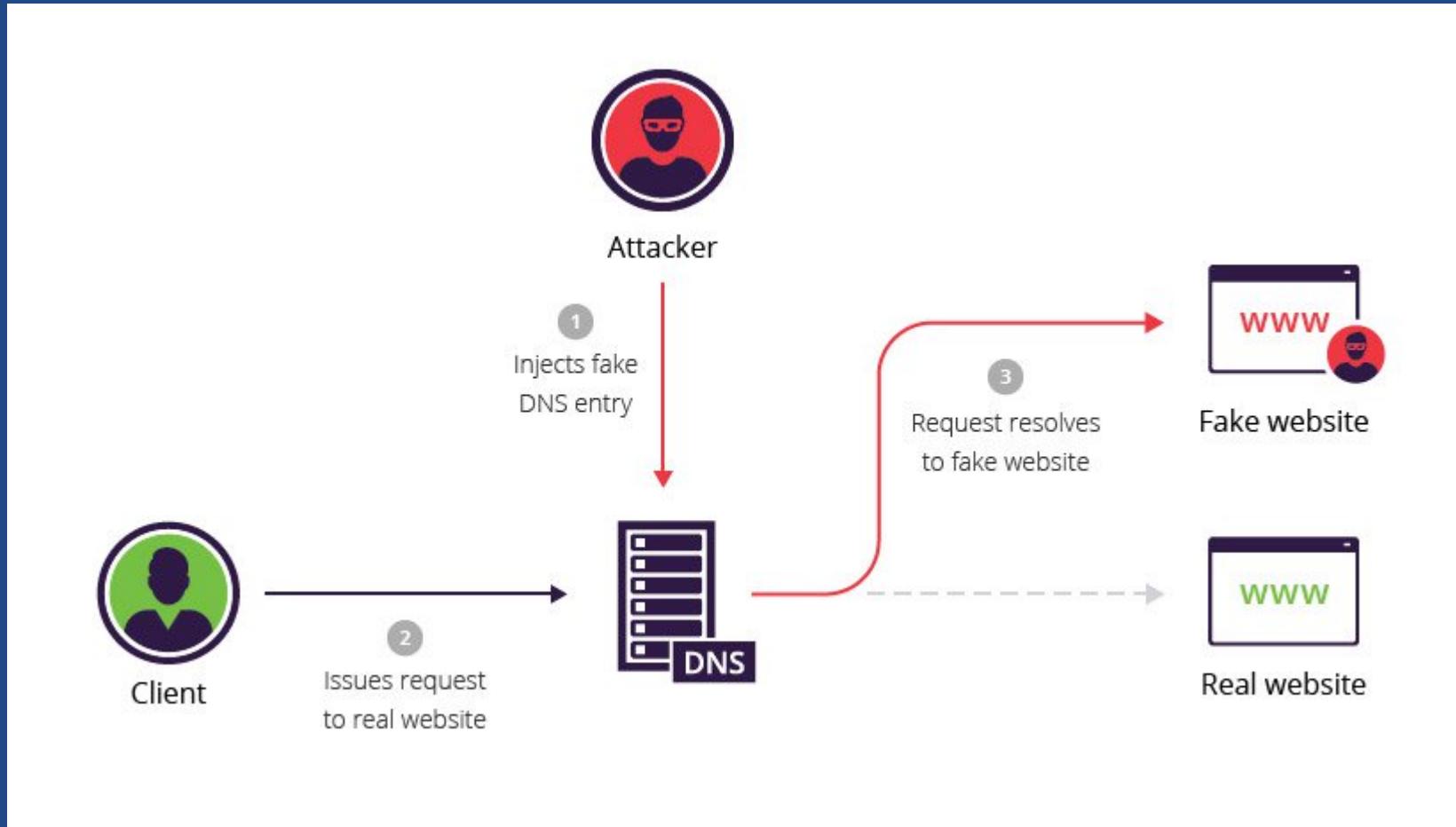
Человек посередине

# ПУБЛИЧНЫЕ Wi-Fi СЕТИ



Перехват трафика

# ПУБЛИЧНЫЕ Wi-Fi СЕТИ



Человек посередине

# ПУБЛИЧНЫЕ Wi-Fi СЕТИ

\*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
172	10.8306270	192.168.43.42	69.195.124.112	HTTP	433	GET / HTTP/1.1
188	11.6480510	69.195.124.112	192.168.43.42	HTTP	1188	HTTP/1.1 200 OK (text/html)
325	23.5363370	108.160.162.52	192.168.43.42	HTTP	233	HTTP/1.1 200 OK (text/plai
326	23.5481440	192.168.43.42	108.160.162.52	HTTP	362	GET /subscribe?host_int=740
384	26.8239240	192.168.43.42	69.195.124.112	HTTP	724	POST /index.php HTTP/1.1
400	27.7500490	69.195.124.112	192.168.43.42	HTTP	1254	HTTP/1.1 302 Moved Temporar
402	27.7534960	192.168.43.42	69.195.124.112	HTTP	567	GET /dashboard.php HTTP/1.1
424	28.5163760	192.168.43.42	108.160.162.52	HTTP	362	[TCP Retransmission] GET /s
425	28.7380900	69.195.124.112	192.168.43.42	HTTP	1322	HTTP/1.1 200 OK (text/html)

Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0

Ethernet II, Src: IntelCor\_a6:c5:43 (60:36:dd:a6:c5:43), Dst: SamsungE\_51:12:f3 (10:d5:42:51:1)

Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1)

Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, Len: 724

Hypertext Transfer Protocol

Line-based text data: application/x-www-form-urlencoded

email=admin%40google.com&password=Password2010&remember\_me=Remember+me

all POST variables have been captured in plaintext

Frame (frame), 724 bytes

Packets: 666 · Disp... · Profile: Default

Человек посередине

## ПУБЛИЧНЫЕ Wi-Fi СЕТИ

# ЭКСПЛОЙТЫ И УЯЗВИМОСТИ НУЛЕВОГО ДНЯ

root@kpl:~# msfpro  
[\*] Starting Metasploit Console...

3Kom SuperHack II Logon

User Name: [ security ]  
Password: [ ]  
[ OK ]

https://metasploit.com



```
[=] metaexploit v4.17.34-dev
+ --|= 1854 exploits - 1186 auxiliary - 334 post
+ --|= 541 payloads - 44 encoders - 10 nops
+ --|= Free Metasploit Pro trial: http://r-7.co/trymsp

[+]
[+] Metasploit Pro extensions have been activated
[+]
[*] Successfully loaded plugin: pro
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:3908:in `codepoints': invalid byte sequence in UTF-8 (ArgumentError)
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:3908:in `rl_col_width'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:1721:in `block in expand_prompt'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/active_support-4.2.11/lib/active_support/core_ext/range/each.rb:7:in `each'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/active_support-4.2.11/lib/active_support/core_ext/range/each.rb:7:in `each_with_time_zone'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:1696:in `expand_prompt'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:1784:in `rl_expand_prompt'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:1809:in `rl_set_prompt'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/rb-readline-0.5.5/lib/rb readline.rb:4866:in `readline'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/rex/ui/text/input/readline.rb:162:in `readline_with_output'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/rex/ui/text/input/readline.rb:100:in `pgets'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/rex/ui/text/shell.rb:399:in `get_input_line'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/rex/ui/text/shell.rb:34:in `run'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/metasploit/framework/command/console.rb:48:in `start'
  from /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.17.34/lib/metasploit/framework/command/base.rb:82:in `start'
  from /opt/metasploit/apps/pro/engine/lib/metasploit/pro/engine/command/console.rb:38:in `start_local'
  from /opt/metasploit/apps/pro/engine/lib/metasploit/pro/engine/command/console.rb:19:in `start'
  from /opt/metasploit/apps/pro/engine/lib/metasploit/pro/engine/command/base.rb:66:in `start'
  from /opt/metasploit/apps/pro/engine/msfpro:17:in <main>'
```

# Прямые атаки

# ВОПРОСЫ?