



Информзашита
Системный интегратор

Киберразведка своими руками*

* без регистрации, без СМС


WWW.INFOSEC.RU


Определение Киберразведки

- Threat intelligence is actionable knowledge and insight on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision-making.
- Киберразведка - это знание и понимание злоумышленников и их вредоносных активностей, позволяющее защищающимся и их организациям минимизировать ущерб за счет принятия более эффективных решений в области безопасности.

Текущее состояние



- Фиды индикаторов компрометации 

- Коммерческая платформа для киберразведки 

- Закрытые отчеты вендоров 

- Аналитики 

- OSINT*-фиды

- Открытые платформы

- Открытые источники данных (OSINT)

- TI-комьюнити

- Понимание релевантных угроз



* *Open source intelligence*



Информзащита
Системный интегратор

Примеры применения бесплатных инструментов и OSINT в реальной жизни

WWW.INFOSEC.RU

Блиц опрос:

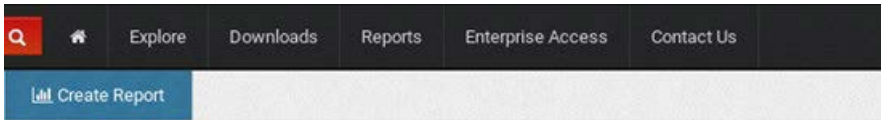
- `inurl:'MY-domain.com' filetype:doc`
- `inurl:'MY-domain.com' filetype:docx`
- `inurl:'MY-domain.com' filetype:xls`
- `inurl:'MY-domain.com' filetype:xlsx`
- `inurl:'MY-domain.com' filetype:pdf`

Google Dorks

- `intext:'OAO Domain' filetype:doc`
- `intext:'Domain' filetype:docx`
- `intitle:'Domain' filetype:pdf`

- `allintext`
- `fillinurl`
- `intitle:`
- `inurl:`
- `intext:`
- `define:`
- `site:`
- `phonebook:`
- `maps:`
- `info:`
- `link:`

Простой поиск через SHODAN



Domain names registrar REG.RU, Ltd
Added on 2017-08-01 GMT
Russian Federation
Details

```
HTTP/1.1 200 OK
Date: Fri, 02 Sep 2017 13:42:43 GMT
Server: Apache/2.2.22 (Debian)
Vary: Accept-Encoding
Content-Length: 1525
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" >
<html>
<head>
<title>Index of /</title>
</head>
<body>
<h1>Index...
```



Index of /

Name	Last modified	Size	Description
/ru/	21-Sep-2015 13:42	-	
/upgrade/	11-Feb-2013 17:34	-	
/2/	21-Mar-2016 16:37	-	
/tmp/	17-Dec-2015 22:22	-	
/tmp/	19-Dec-2017 17:01	-	

Apache/2.2.22 (Debian) Server at [redacted] Port 443



Index of [redacted]

[Name](#) [Last modified](#) [Size](#) [Description](#)

Parent Directory			
[redacted]upgrade.sql.gz	26-Feb-2016 17:16	694M	
analytics.txt	10-Feb-2016 14:11	147	

Table	Action	Rows	Type	Collation	Size	Overhead
adminnotification_inbox	Search Insert Empty Drop	68	InnoDB	utf8_general_ci	128 K	-
admin_assert	Search Insert Empty Drop	8	InnoDB	utf8_general_ci	16 K	-
admin_role	Search Insert Empty Drop	74	InnoDB	utf8_general_ci	48 K	-
admin_rule	Search Insert Empty Drop	4,424	InnoDB	utf8_general_ci	960 K	-
admin_user	Search Insert Empty Drop	57	InnoDB	utf8_general_ci	32 K	-
api2_acl_attribute	Search Insert Empty Drop	18	MyISAM	utf8_general_ci	9.6 K	-
api2_acl_role	Search Insert Empty Drop	2	InnoDB	utf8_general_ci	48 K	-
api2_acl_rule	Search Insert Empty Drop	8	InnoDB	utf8_general_ci	32 K	-
api2_acl_user	Search Insert Empty Drop	8	InnoDB	utf8_general_ci	32 K	-
api_assert	Search Insert Empty Drop	8	InnoDB	utf8_general_ci	16 K	-
api_role	Search Insert Empty Drop	5	InnoDB	utf8_general_ci	48 K	-
api_session	Search Insert Empty Drop	332	InnoDB	utf8_general_ci	80 K	-
api_session	Search Insert Empty Drop	3	InnoDB	utf8_general_ci	48 K	-
api_user	Search Insert Empty Drop	3	InnoDB	utf8_general_ci	16 K	-
[redacted]_city	Search Insert Empty Drop	4,683	InnoDB	utf8_general_ci	464 K	-
[redacted]_innerrayon	Search Insert Empty Drop	125	InnoDB	utf8_general_ci	32 K	-
[redacted]_rayon	Search Insert Empty Drop	422	InnoDB	utf8_general_ci	80 K	-
[redacted]_region	Search Insert Empty Drop	351	InnoDB	utf8_general_ci	112 K	-
color	Search Insert Empty Drop	719	InnoDB	utf8_unicode_ci	112 K	-
color_indexer	Search Insert Empty Drop	589	InnoDB	latin1_swedish_ci	96 K	-
rootcolor	Search Insert Empty Drop	8	InnoDB	latin1_swedish_ci	16 K	-

Мониторинг репозиториев кода и иных публичных ресурсов

GitHub



PASTEBIN

Atlassian



Bitbucket

Мониторинг репозиториев кода и иных публичных ресурсов

https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/

Security

Deloitte is a sitting duck: Key systems with RDP open, VPN and proxy 'login details leaked'

Yes, that's Gartner's security consultancy of the year

By Iain Thomson in San Francisco 26 Sep 2017 at 20:33

78

On Tuesday, what seemed to be a collection of Deloitte's corporate VPN passwords, user names, and operational details were found lurking within a public-facing GitHub-hosted repository. These have since been

```
#rdps for flux
```

```
//asundhar  
10.26.131.101  
User Name : USDEVasundhar  
Password : [REDACTED]
```

```
//mrzak  
10.26.216.61  
USDEVmorazak  
Password : [REDACTED]
```

```
//vpn credentails for deloitte
```

```
https://aexternal.deloittenet.deloitte.com/my.policy#  
sipatra
```

```
//flux database info  
10.25.112.22; Database=Flux; User Id=Flux_User; Password=[REDACTED]
```

```
#test server web site flux  
https://ddisclosureanalytics.deloitte.com/flux/uploadtb  
usdevleeldridge
```

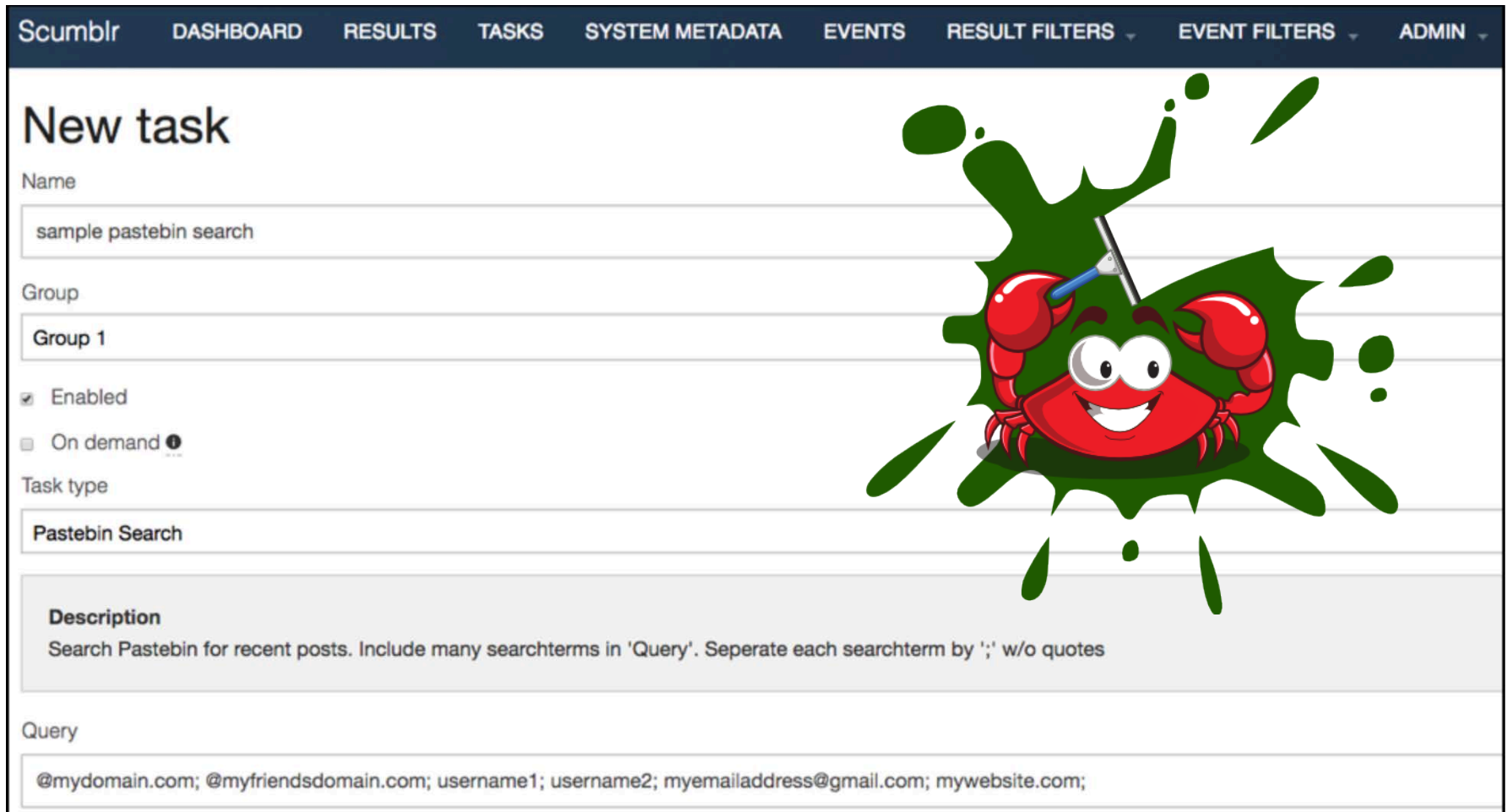
```
#other flux info  
//tfs  
http://tfs.deloitte.com:8080/tfs/its/FluxAnalysis/FluxAnalysis%20Te  
dhamb
```

```
//build forge  
http://buildforge.deloitte.com:8080/jas/LoginServlet;jsessionid=228  
UserName : asundhar  
Password: [REDACTED]
```

```
//project portfolio management
```



Web framework that allows performing periodic syncs of data sources and performing analysis on the identified results



The screenshot shows the Scumblr web interface. At the top is a navigation bar with links: Scumblr, DASHBOARD, RESULTS, TASKS, SYSTEM METADATA, EVENTS, RESULT FILTERS, EVENT FILTERS, and ADMIN. Below this is a 'New task' form with the following fields:

- Name: sample pastebin search
- Group: Group 1
- Enabled: Enabled, On demand
- Task type: Pastebin Search
- Description: Search Pastebin for recent posts. Include many searchterms in 'Query'. Separate each searchterm by ';' w/o quotes
- Query: @mydomain.com; @myfriendsdomain.com; username1; username2; myemailaddress@gmail.com; mywebsite.com;

On the right side of the form, there is a large illustration of a red cartoon crab with a blue and silver tool, surrounded by green splatters.

Мониторинг SSL-сертификатов на предмет фишинга



<https://certstream.calidog.io/>

CERTSTREAM

Real-time certificate transparency log update stream.
See SSL certificates as they're issued in real time.

Learn More

```
$ certstream
```

А что если мониторить партнеров, наиболее популярные сайты и т.п.

Введите один домен

Отметить все

Похожие по написанию **7**

Удвоение символа **7**

Перестановка символов **6**

Замена на созвучные **16**

Пропажа символа **11**

Соседний символ **38**

Соседний в строке **14**

Подобрать

Найдено: 99 (77 уникальных)

inosec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
infsec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
infoec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
infosc	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
infose	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
httpinfosec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
wwwinfosec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
wwinfosec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
infosecru	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel
nifosec	рф	ru	com.ru	net.ru	org.ru	spb.ru	msk.ru	su	com	net	org	info	biz	tel

■ Свободен ■ Занят ■ Освобождается ■ На аукционе

1 2 3 4 5 6 7 8

Мониторинг информации о потенциальных атаках



Xavier Mertens

@xme

Follow



Recently DNS registered domains based on “\w+attack\.\w+”, more attacks to come? :-)

```
attack.domains
bigfootattack.com
negativeattack.com
stumpattack.com
controlattack.com
alkattack.tech
formattack.com
frapattack.com
polattack.com
salaryman-counterattack.com
stinkattack.com
verticalattack.com
buzzattack.net
dhaka-attack.com
otakuattack.com
meleeattack.com
melodyattack.com
shit-attack.com
tussyattack.com
ant-artattack.com
fattyattack.com
internetattack.win
surattack.com
doorattack.men
staticattack.com
daxattack.net
kaijackcardattack.com
maturesexattack.com
9deltaattack.com
dasattack.com
meltdownattack.com
pv-attack.com
spectreattack.com
tionattack.com
hashattack.chat
whenhornymonstersattack.com
xjattack.com
everythingisunderattack.com
```

Другой юзкейс: мониторинг потенциальных атак

- После Meltdown и Spectre: “новая” атака Skyfall.



Skyfall and Solace

More vulnerabilities in modern computers.

If you work in the IT industry, over the last few days/weeks you'll no doubt have spent many hours reading about the Meltdown and Spectre vulnerabilities, and trying to figure out how your systems are affected and how you'll patch them.

But ask yourself this...

Другой юзкейс: мониторинг потенциальных атак

Skyfall and Solace CPU vulnerabilities a hoax - Confirmed

<https://react-etc.net/entry/skyfall-and-solace-vulnerabilities> ▼

5 days ago - Details are still scarce, but both **Skyfall** and Solace vulnerabilities take use of the same **attack** vector as Meltdown and Spectre - speculative execution. According to the vulnerability information site, skyfallattack.com, it is another case where both Operating System creators like Microsoft, Apple and Google ...

Errata Security: "Skyfall attack" was attention seeking

<blog.erratasec.com/2018/01/skyfall-attack-was-attention-seeking.html> ▼

6 hours ago - "**Skyfall attack**" was attention seeking. After the Meltdown/Spectre attacks, somebody created a website promising related "Skyfall/Solace" attacks. They revealed today that it was a "hoax". It was a bad hoax. It wasn't a clever troll, parody, or commentary. It was childish behavior seeking attention. For all you ...

- Создаём файл типа “пароли.txt”, “bank-client-info.docx” и помещаем в папку с ограниченным доступом
- использование web beacon (canarytokens.org), при открытии документа злоумышленником получаем алерт
- Использование встроенного в Windows расширенного аудита и SACL, коррелируем события в SIEM




Другие юзкейсы использования honeytokens

МЕНЯ

ПОДСТАВИЛИ

- открытие word, pdf документов
- открытие папок в windows
- открытие приложения
- клонирование корпоративного вебсайта
- доступ к SQL базам данных
- доступ к SVN-репозиториям
- ...

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#) 

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

265

pwned websites

4,859,899,553

pwned accounts

63,284


pastes


70,187,248

paste accounts

Oh no — pwned!

Pwned on [2 breached sites](#) and found [no pastes](#) ([subscribe](#) to search sensitive breaches)

 [Notify me when I get pwned](#)

 [Donate](#)



Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



Exploit.In ([unverified](#)): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I been pwned](#).

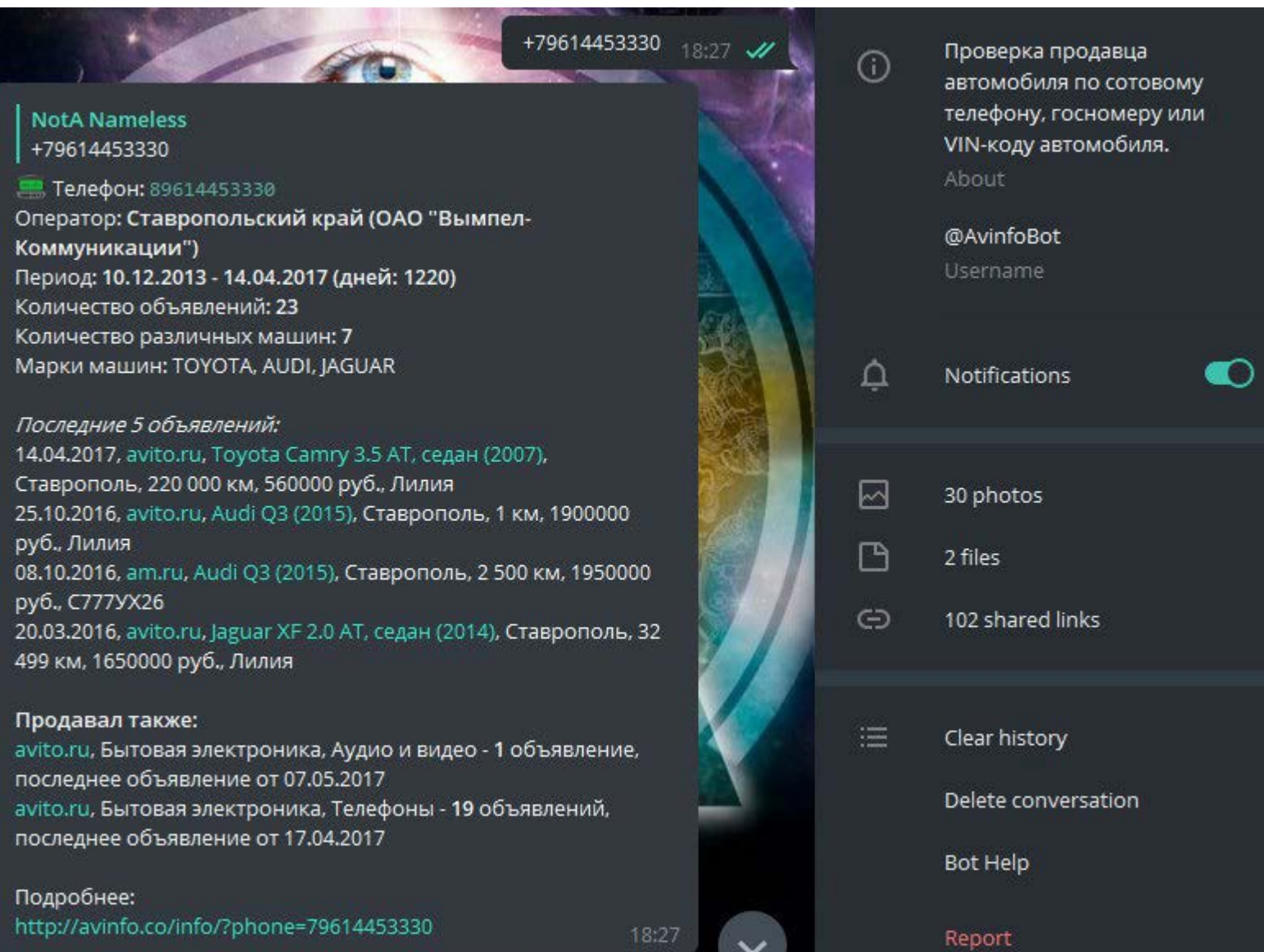
Compromised data: Email addresses, Passwords



LinkedIn: In May 2016, [LinkedIn had 164 million email addresses and passwords exposed](#). Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Казалось бы, какая связь...



The image shows a Telegram chat interface. On the left is a chat window with a bot named 'NotA Nameless'. The chat header shows the phone number +79614453330 and the time 18:27 with a double checkmark. The chat content includes the bot's name, phone number, and a detailed profile: 'Телефон: 89614453330', 'Оператор: Ставропольский край (ОАО "Вымпел-Коммуникации")', 'Период: 10.12.2013 - 14.04.2017 (дней: 1220)', 'Количество объявлений: 23', 'Количество различных машин: 7', and 'Марки машин: TOYOTA, AUDI, JAGUAR'. It also lists 'Последние 5 объявлений' with dates, platforms, car models, and prices. At the bottom, it says 'Продавал также:' followed by two entries for 'avito.ru' with dates. A link 'http://avinfo.co/info/?phone=79614453330' is provided. On the right is the bot's profile page, showing the name 'Проверка продавца автомобиля по сотовому телефону, госномеру или VIN-коду автомобиля.', the username '@AvinfoBot', and various settings like 'Notifications' (turned on), '30 photos', '2 files', '102 shared links', 'Clear history', 'Delete conversation', 'Bot Help', and 'Report'.

+79614453330 18:27 ✓✓

NotA Nameless
+79614453330

Телефон: 89614453330
Оператор: Ставропольский край (ОАО "Вымпел-Коммуникации")
Период: 10.12.2013 - 14.04.2017 (дней: 1220)
Количество объявлений: 23
Количество различных машин: 7
Марки машин: TOYOTA, AUDI, JAGUAR

Последние 5 объявлений:
14.04.2017, [avito.ru](#), Toyota Camry 3.5 AT, седан (2007), Ставрополь, 220 000 км, 560000 руб., Лилия
25.10.2016, [avito.ru](#), Audi Q3 (2015), Ставрополь, 1 км, 1900000 руб., Лилия
08.10.2016, [am.ru](#), Audi Q3 (2015), Ставрополь, 2 500 км, 1950000 руб., C777УХ26
20.03.2016, [avito.ru](#), Jaguar XF 2.0 AT, седан (2014), Ставрополь, 32 499 км, 1650000 руб., Лилия

Продавал также:
[avito.ru](#), Бытовая электроника, Аудио и видео - 1 объявление, последнее объявление от 07.05.2017
[avito.ru](#), Бытовая электроника, Телефоны - 19 объявлений, последнее объявление от 17.04.2017

Подробнее:
<http://avinfo.co/info/?phone=79614453330>

18:27

Проверка продавца автомобиля по сотовому телефону, госномеру или VIN-коду автомобиля.
About
@AvinfoBot
Username

Notifications

30 photos
2 files
102 shared links

Clear history
Delete conversation
Bot Help
Report

@AvInfoBot

Автоматизированная обработка индикаторов компрометации из отчетов



FinCERT Банка России

PC-V-EQUATION_GRP-20170602-01

Рассылка информации о сетевых индикаторах Equation Group

1. Краткое описание угрозы

В связи с высоким уровнем опасности внедрения вредоносного программного обеспечения Equation Group (США) и в преддверии проведения Кубка конфедераций, просим вас проверить Ваши информационные системы на наличие возможного заражения программным обеспечением Equation Group. Основным индикатором заражения являются частые запросы на адреса, указанные в разделе 2.

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	-
2	Блокировка запросов	waeservices.com www.waeservices.com quik-serv.com speedynewsclips.com thesuperdeliciousnews.com fnlpic.com gar-tech.com avidnewssource.com globalnetworkanalys.com zhalehziba.com technicserv.com rapidlyserv.com selective-business.com charging-technology.com crisptic01.net

 [armbues / ioc_parser](#)


 Code

 Issues **8**

 Pull requests **9**

 Projects **0**

 Wiki

 Insights

Tool to extract indicators of compromise from security reports in PDF format

```
/tmp >>> iocp -d FinCERT-20170602-01.pdf
FinCERT-20170602-01.pdf,1,Host,waeservices.com
FinCERT-20170602-01.pdf,1,Host,www.waeservices.com
FinCERT-20170602-01.pdf,1,Host,quik-serv.com
FinCERT-20170602-01.pdf,1,Host,speedynewsclips.com
FinCERT-20170602-01.pdf,1,Host,thesuperdeliciousnews.com
FinCERT-20170602-01.pdf,1,Host,fnlpic.com
FinCERT-20170602-01.pdf,1,Host,gar-tech.com
FinCERT-20170602-01.pdf,1,Host,avidnewssource.com
FinCERT-20170602-01.pdf,1,Host,globalnetworkkanalys.com
FinCERT-20170602-01.pdf,1,Host,zhalehziba.com
FinCERT-20170602-01.pdf,1,Host,technicserv.com
FinCERT-20170602-01.pdf,1,Host,rapidlyserv.com
FinCERT-20170602-01.pdf,1,Host,selective-business.com
```



БДИТЕЛЬНОСТЬ- НАШЕ ОРУЖИЕ

- Следите за ИБ-community и opensource
- Отслеживайте релевантные вам угрозы
- Экономьте время и ресурсы, автоматизируйте!!

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

24x7x365

«ИНФОРМЗАЩИТА»:

- СИСТЕМНЫЙ ИНТЕГРАТОР WWW.INFOSEC.RU
- СЕРВИСНЫЙ ЦЕНТР WWW.ITSOC.RU
- УЧЕБНЫЙ ЦЕНТР WWW.ITSECURITY.RU