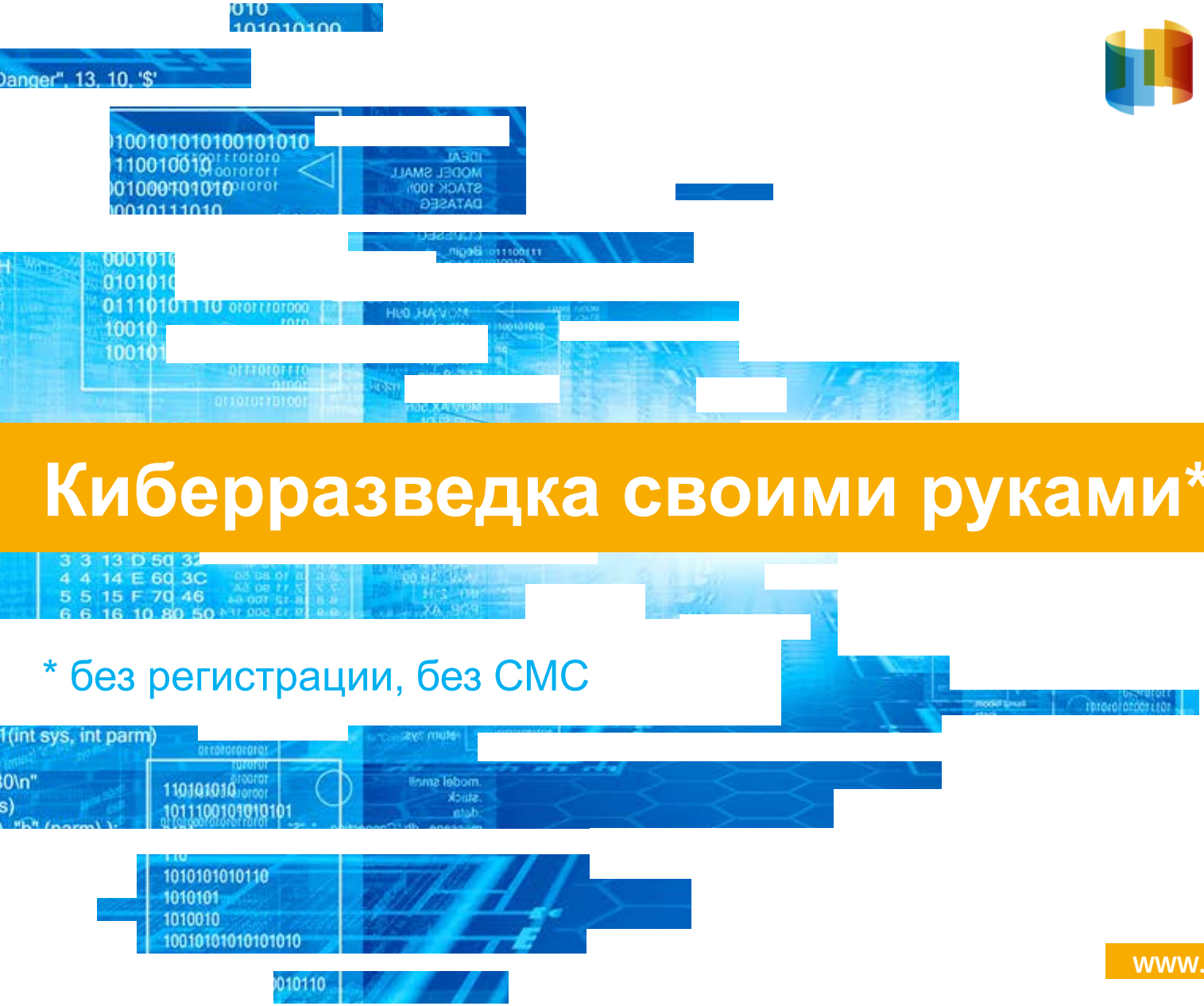


Информзащита
Системный интегратор

Кибербразведка своими руками*

* без регистрации, без СМС

WWW.INFOSEC.RU

Определение Кибербразведки

- 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.

- Кибербразведка - 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

Информзащита
Системный интегратор

- 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

Блиц опрос:

Информзащита
Системный интегратор

- 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

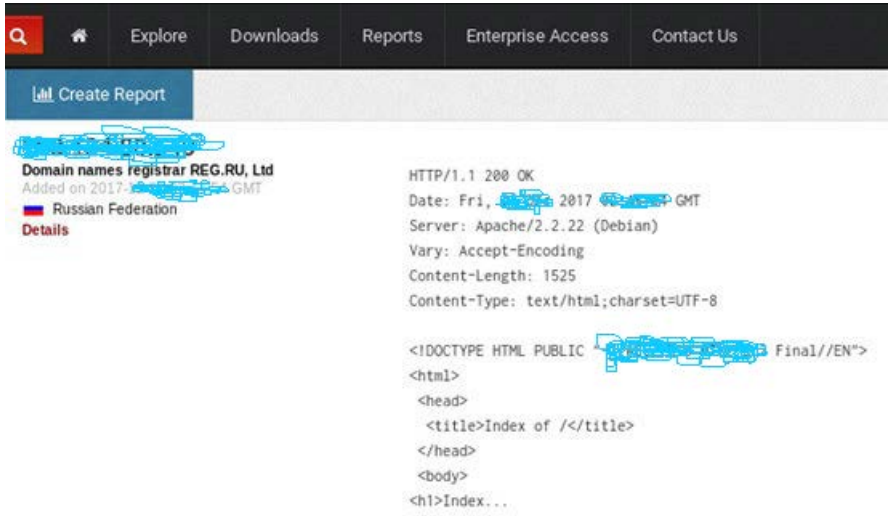
Информзащита
Системный интегратор

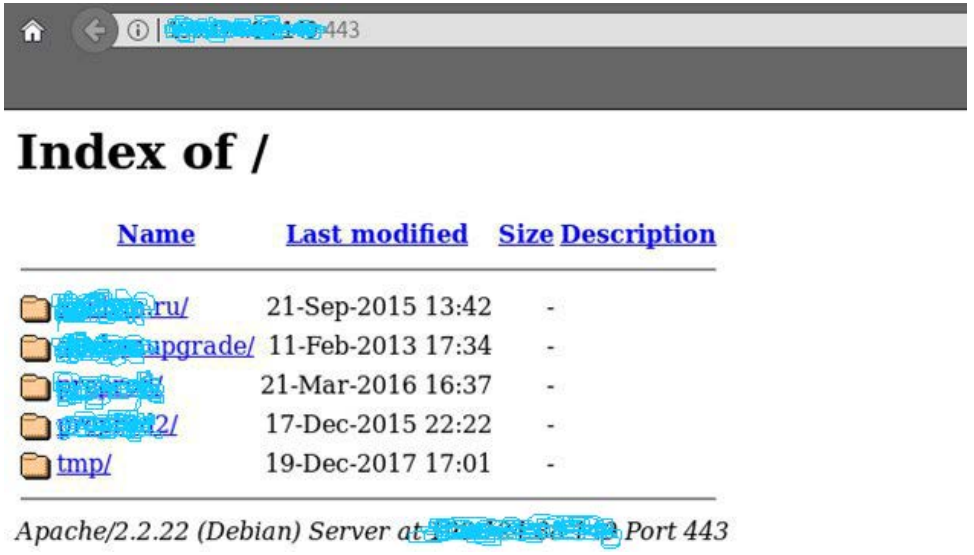
- intext:'OAO Domain' filetype:doc
- intext:'Domain' filetype:docx
- intitle:'Domain' filetype:pdf

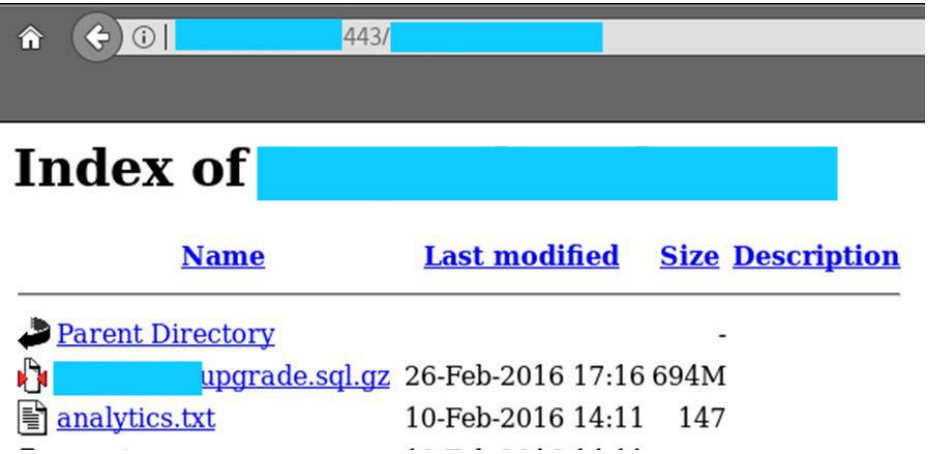
- allintext
- fllinurl
- intitle:
- inurl:
- intext:
- define:
- site:
- phonebook:
- maps:
- info:
- link:

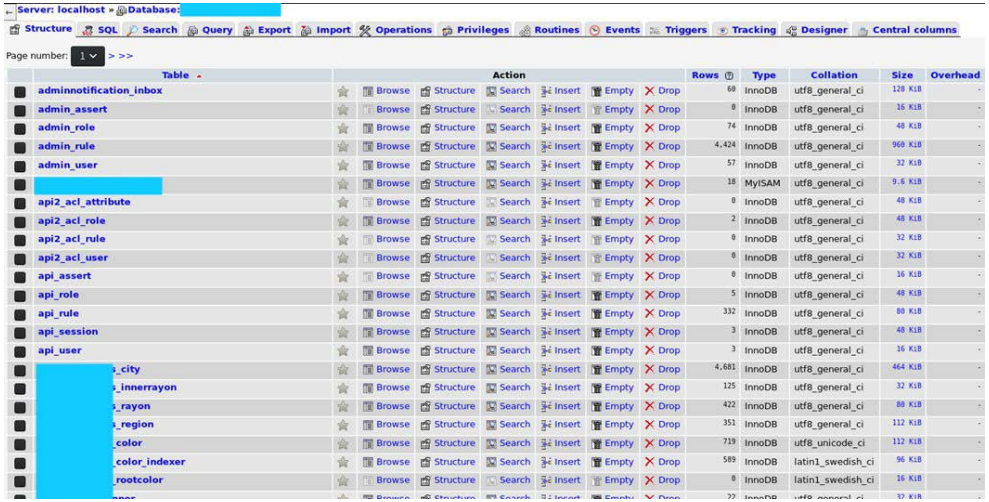
Простой поиск через SHODAN

Информзащита
Системный интегратор









Мониторинг репозиториев кода и иных публичных ресурсов

Информзащита
Системный интегратор

GitHub

PASTEBIN

Atlassian

Bitbucket

Мониторинг репозиториев кода и иных публичных ресурсов

Информзащита
Системный интегратор

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]

//mrazak
10.26.216.61
USDEVmorazak
Password : [redacted]

//vpn credentails for deloitte

https://aexternal.deloittenet.deloitte.com/my.policy#
sipatra
[redacted]

//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
[redacted]

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

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

Scumblr

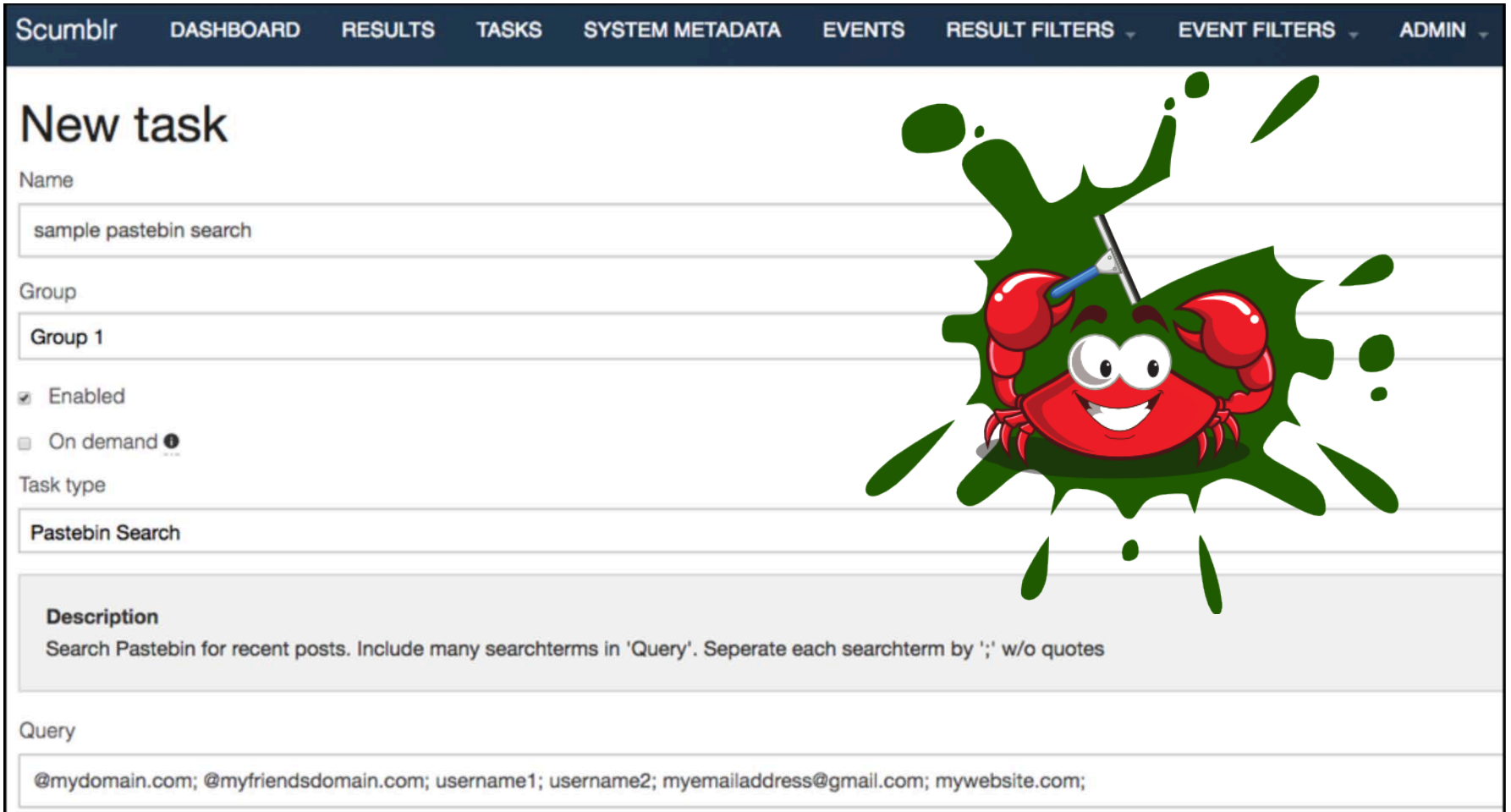
Информзащита
Системный интегратор

Netflix / Scumblr

Watch 392 | Unstar 2,289 | Fork 274

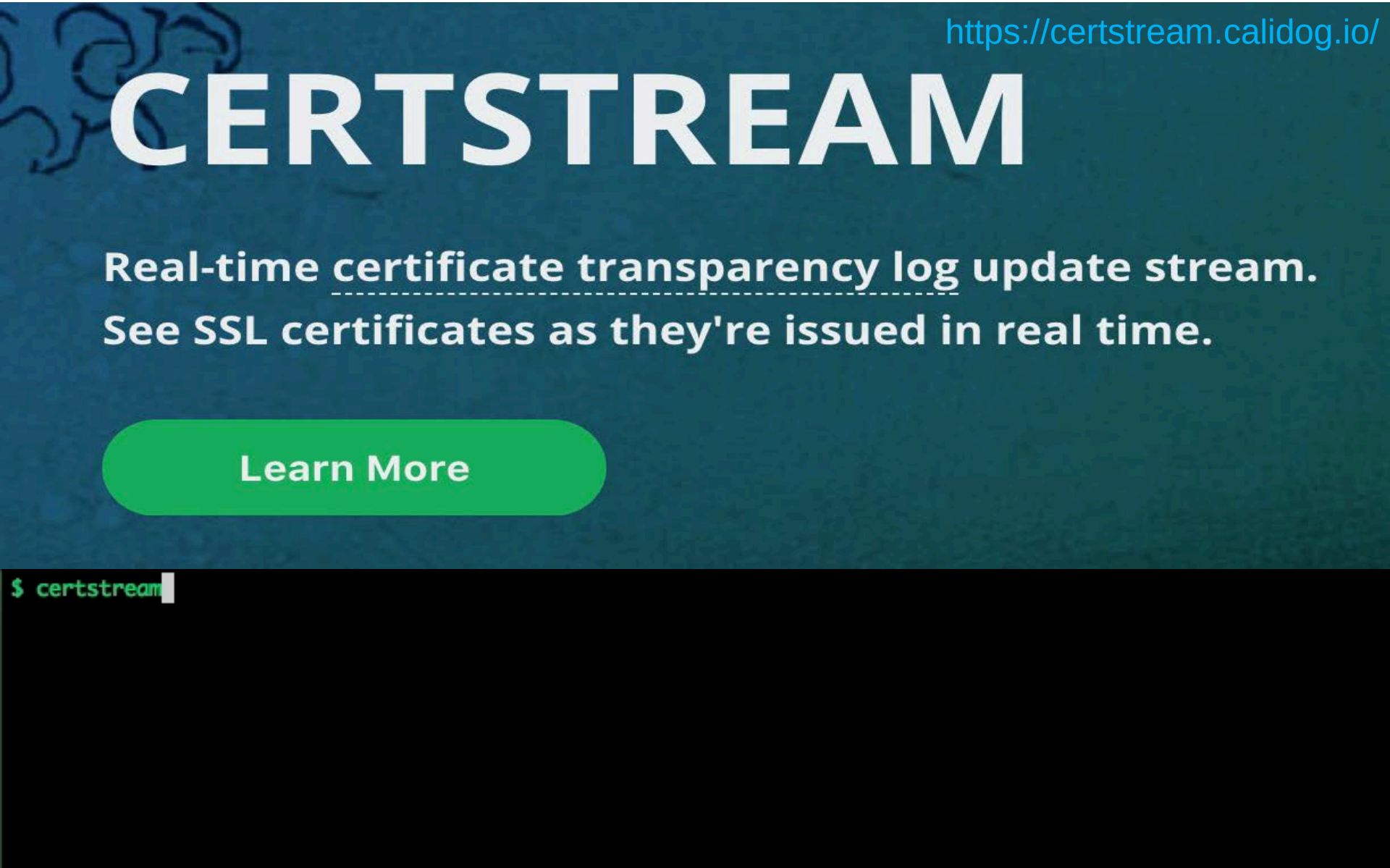
Code | Issues 20 | Pull requests 7 | Projects 0 | Wiki | Insights

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



Мониторинг SSL-сертификатов на предмет фишинга

Информзащита
Системный интегратор



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

Информзащита
Системный интегратор

Введите один домен

infosec.ru

☑ Отметить все

☑ Похожие по написанию **7**
☑ Замена на созвучные **16**
☑ Удвоение символа **7**
☑ Пропажа символа **11**
☑ Перестановка символов **6**
☑ 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

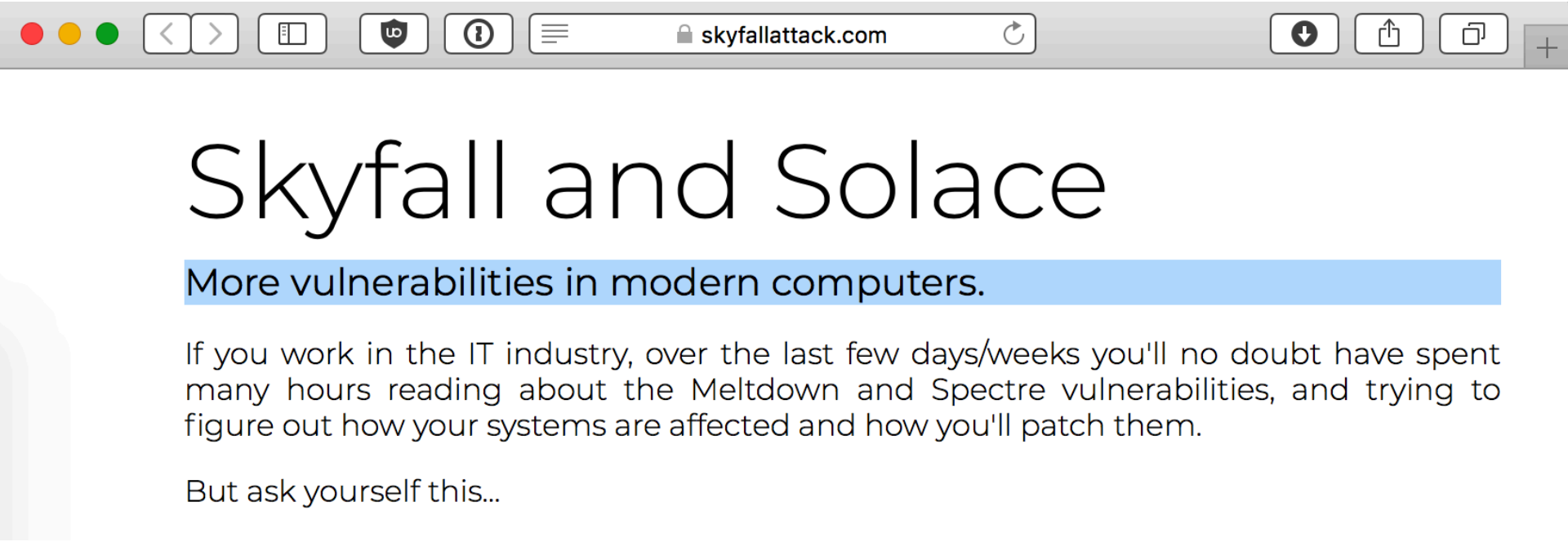
Recently DNS registered domains based on ‘\w+attack\.\w+”, more attacks to come? :-)

```
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

Информзащита
Системный интегратор

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



Другой юзкейс: мониторинг потенциальных атак

Информзащита
Системный интегратор

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 ...

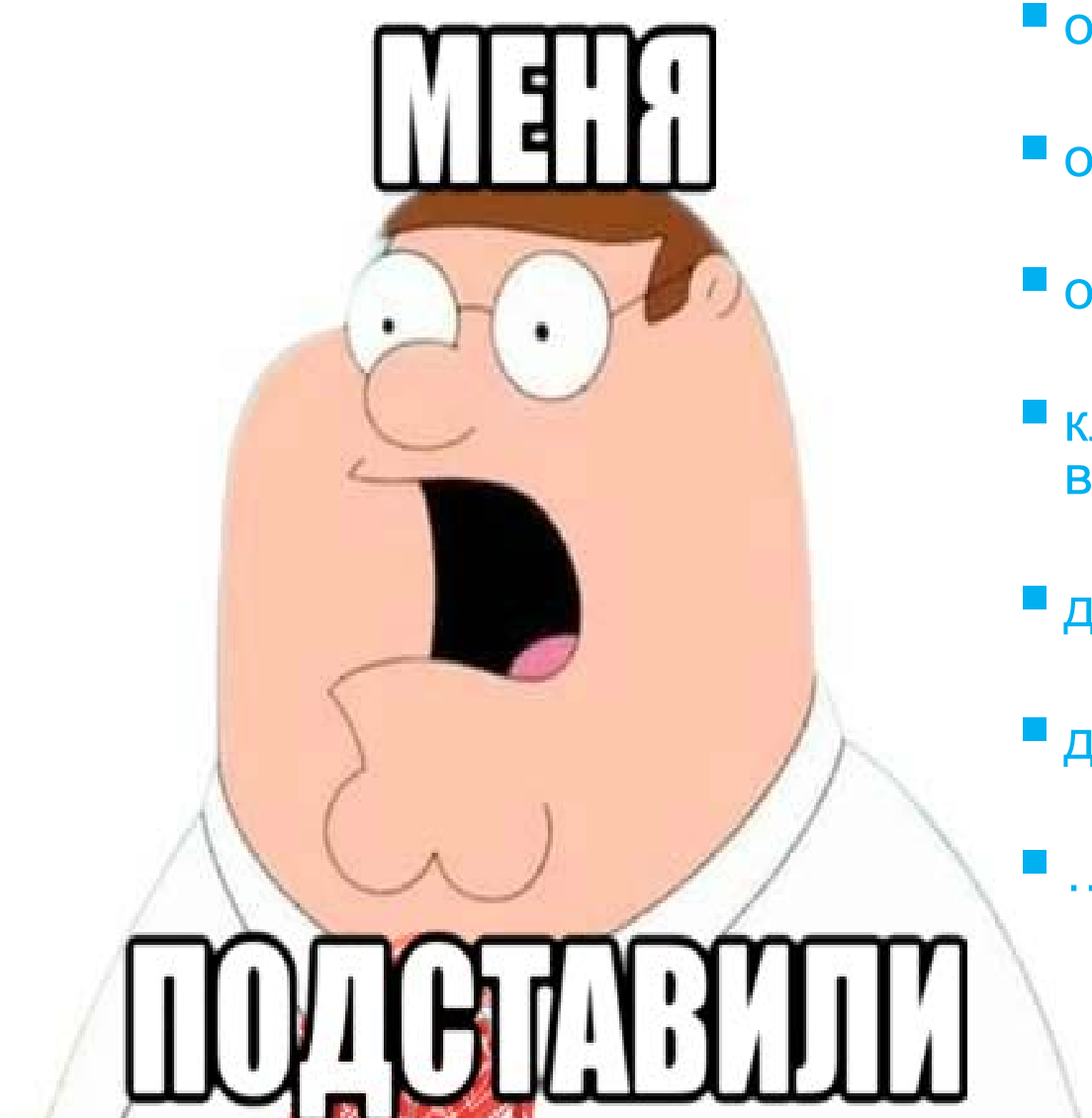
Honey-docs

Информзащита
Системный интегратор

- 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

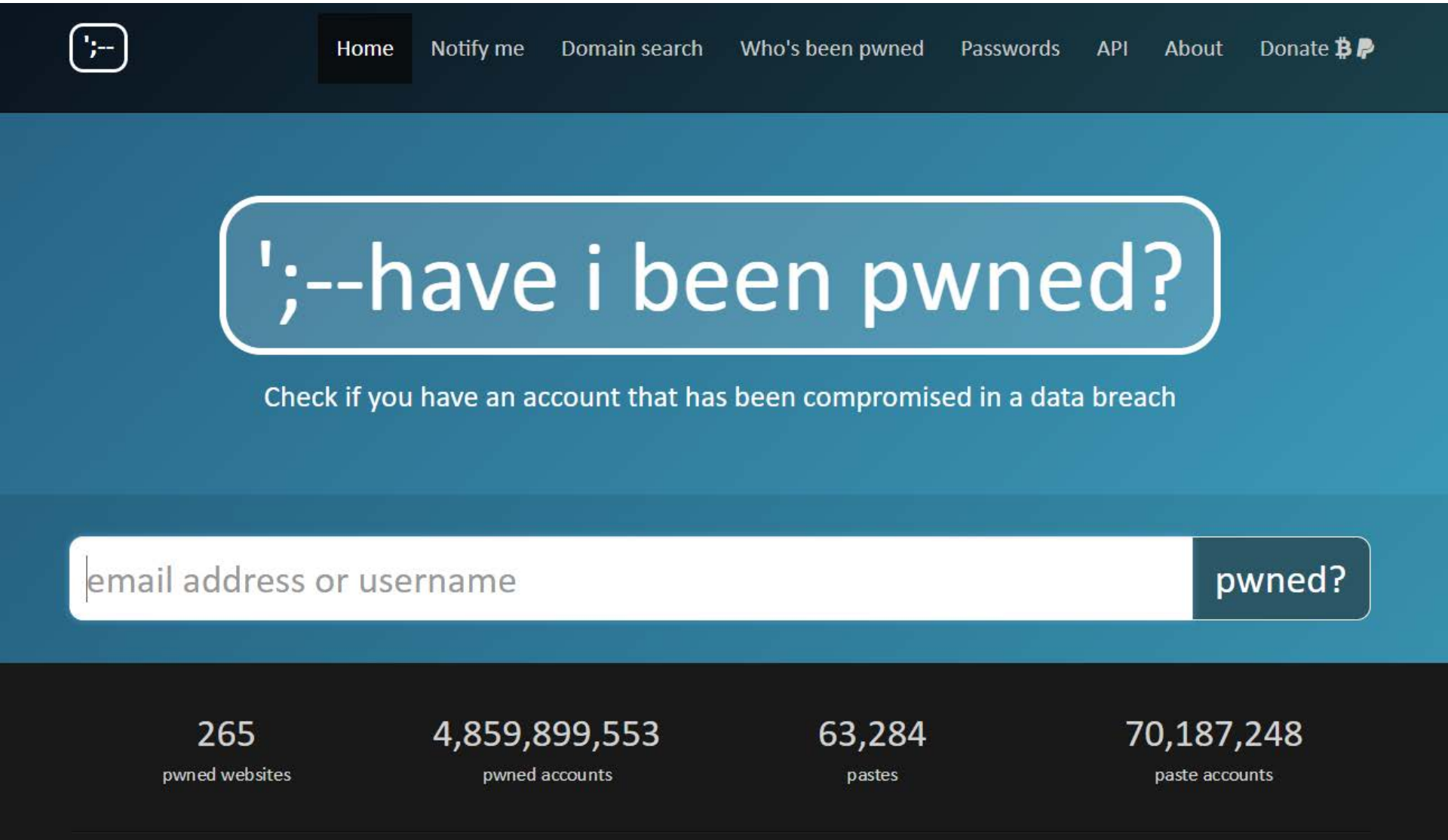
Информзащита
Системный интегратор



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

Слежка за взломами аккаунтов

Информзащита
Системный интегратор



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.

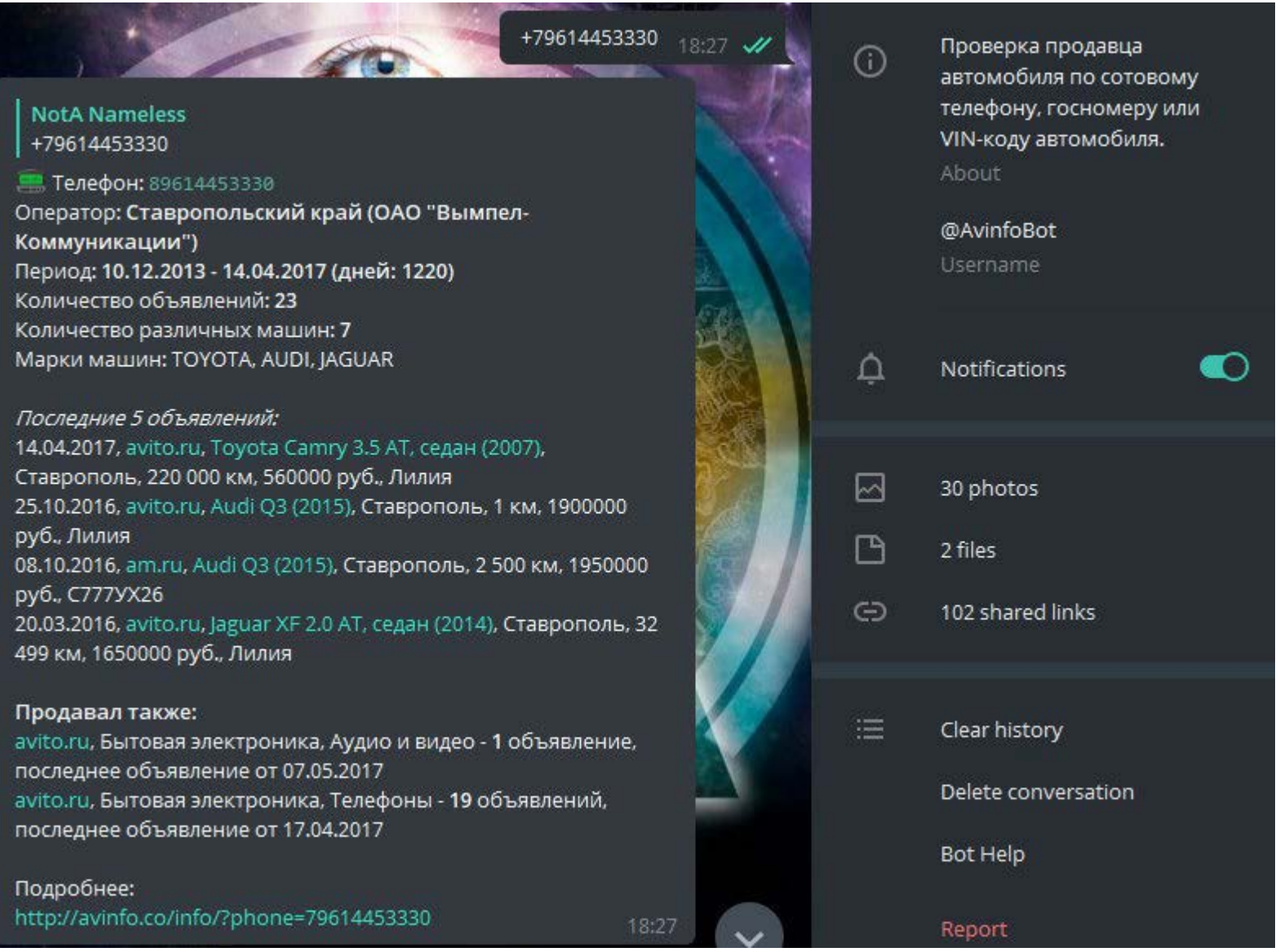
Compromised data: Email addresses, Passwords

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…

Информзащита
Системный интегратор



@AvInfoBot

Автоматизированная обработка индикаторов компрометации из отчетов

Информзащита
Системный интегратор

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**

Автоматизация

Информзащита
Системный интегратор

armbues / ioc_parser

<> Code | Issues 8 | Pull requests 9 | Projects 0 | Wiki | Insig

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,globalnetworkanalys.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
```

- 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**