

Анастасия Гришина

Аналитик информационной безопасности

agrishina@ptsecurity.com

Веб-приложение — цель или средство?

Как и для чего на самом деле хакеры атакуют приложения

POSITIVE TECHNOLOGIES

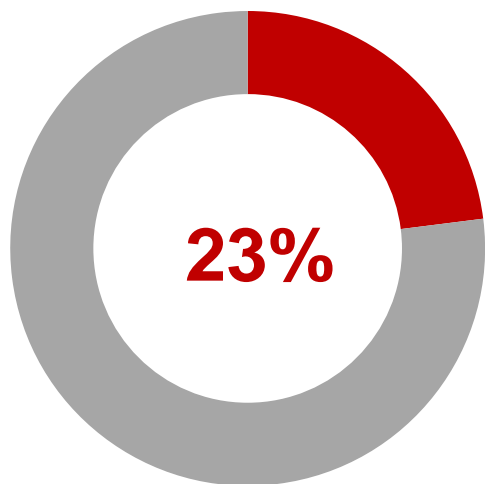
ptsecurity.com

- **Безопасность веб-приложений сегодня:** статистика атак, их последствия и мотивы злоумышленников
- Примеры (блок 1): когда веб-приложение является **целью** атаки
- Примеры (блок 2): когда веб-приложение является **средством** атаки
- Рекомендации: **как защититься** от атак на веб-приложения

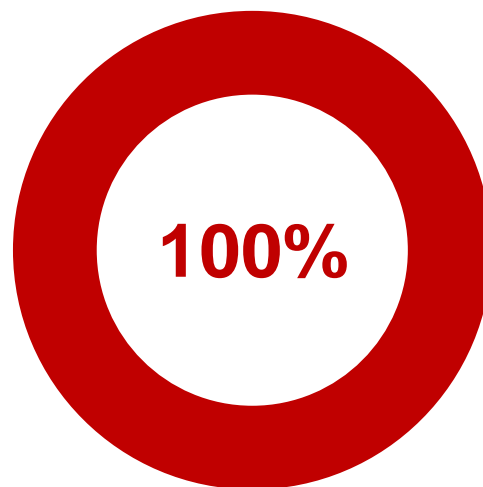


Безопасность веб-приложений сегодня

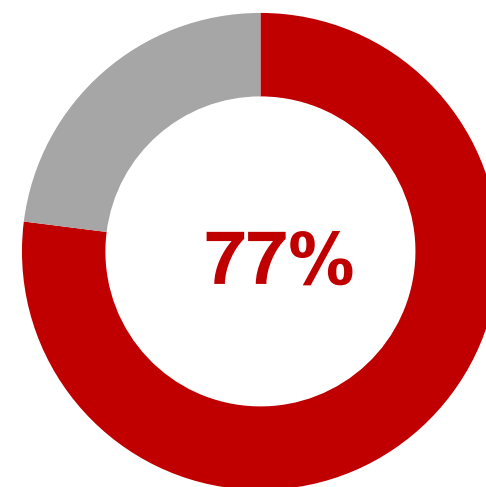
Доля кибератак на веб-ресурсы во II квартале 2017 года



Доля веб-приложений, в которых выявлены уязвимости

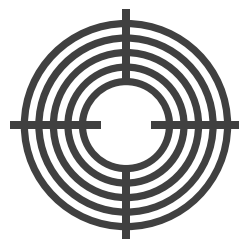
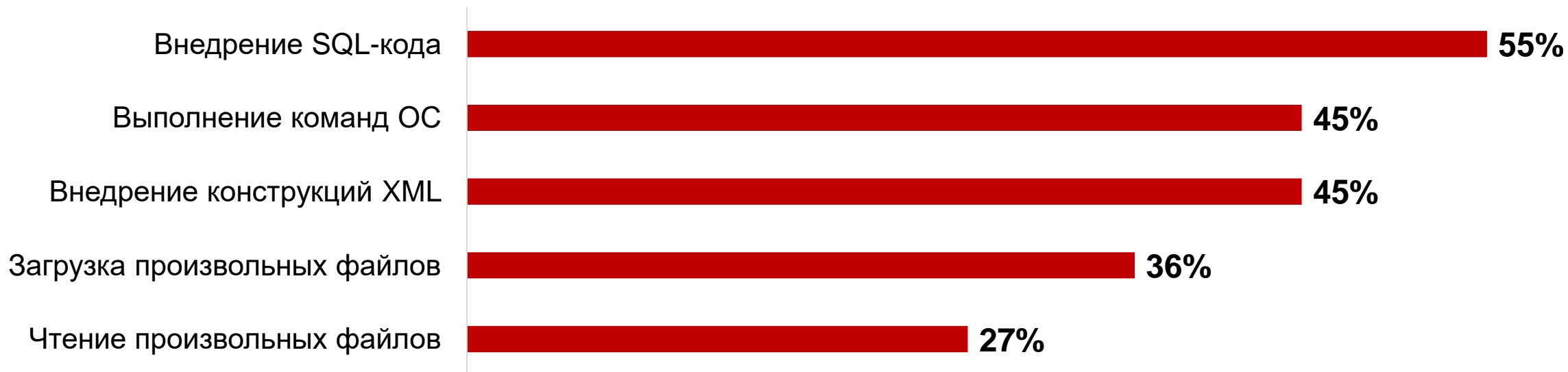


Доля векторов проникновения в локальную сеть, основанная на эксплуатации уязвимостей веб-приложений



Атаки на веб-приложения открывают перед злоумышленниками множество возможностей — от получения чувствительной информации до проникновения во внутреннюю сеть компании.

Наиболее распространенные уязвимости веб-приложений на сетевом периметре (доля систем)



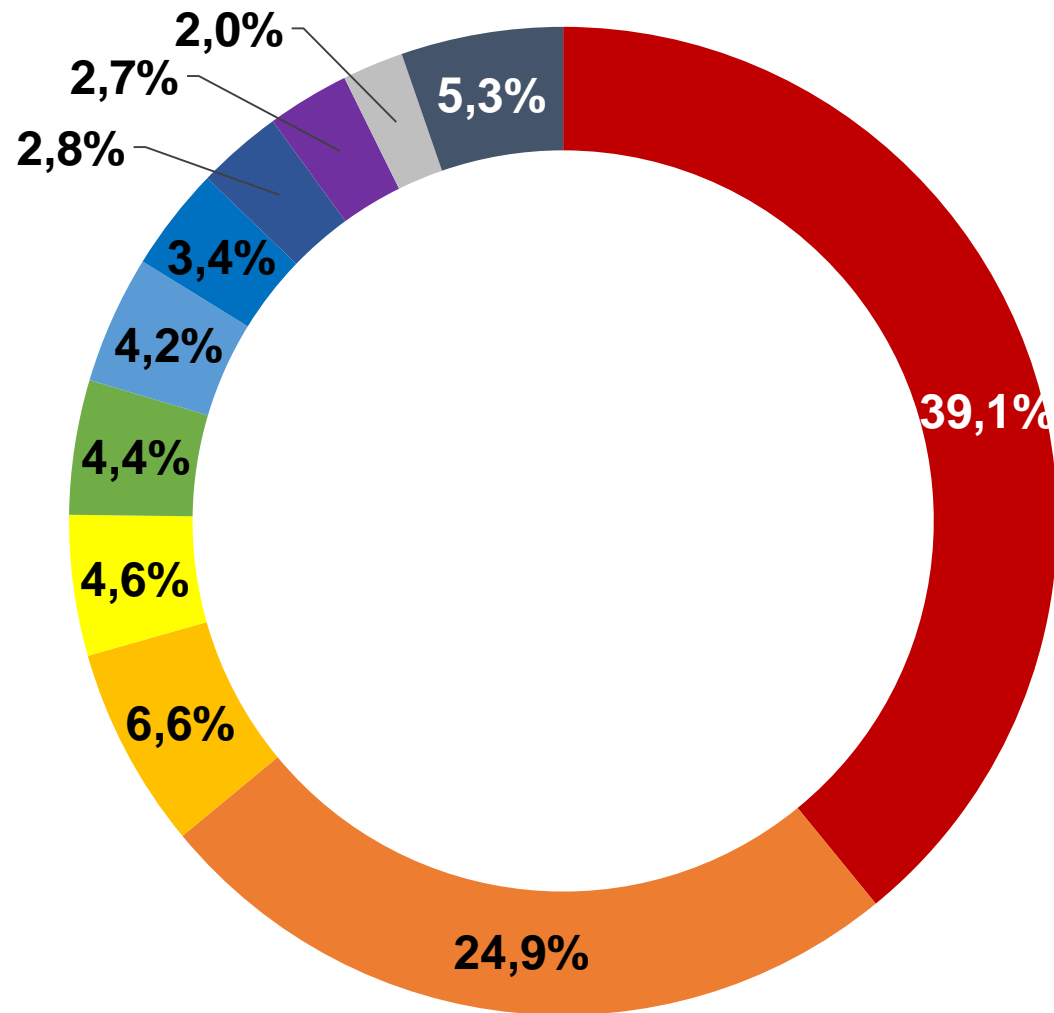
Поиск уязвимостей на общедоступных веб-ресурсах



Атака на веб-приложение



Возможность развития атаки на ресурсы внутренней сети



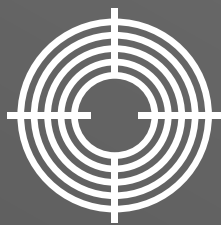
- Межсайтовое выполнение сценариев
- Внедрение SQL-кода
- Выход за пределы назначенного каталога
- Утечка информации
- Удаленное выполнение кода и команд ОС
- Внедрение конструкций XML
- Подделка запроса со стороны сервера
- Отказ в обслуживании
- Ошибка настройки контроля доступа для методов протокола HTTP
- Внедрение шаблона на стороне сервера
- Другие атаки

- Фишинг
- Распространение вредоносного ПО
- Кража информации из базы данных
- Дефейс и размещение компрометирующей информации
- Отказ в обслуживании
- Полный контроль над сервером
- Атаки на ресурсы внутренней сети компании

В итоге атаки на веб-приложения могут привести к существенным репутационным и финансовым потерям.

- Финансовая выгода
- Кибершпионаж
- Хактивизм
- Самоутверждение
- Любопытство





Когда приложение — цель атаки?

Веб-сайт сегодня для многих организаций является **ВИЗИТНОЙ карточкой**.



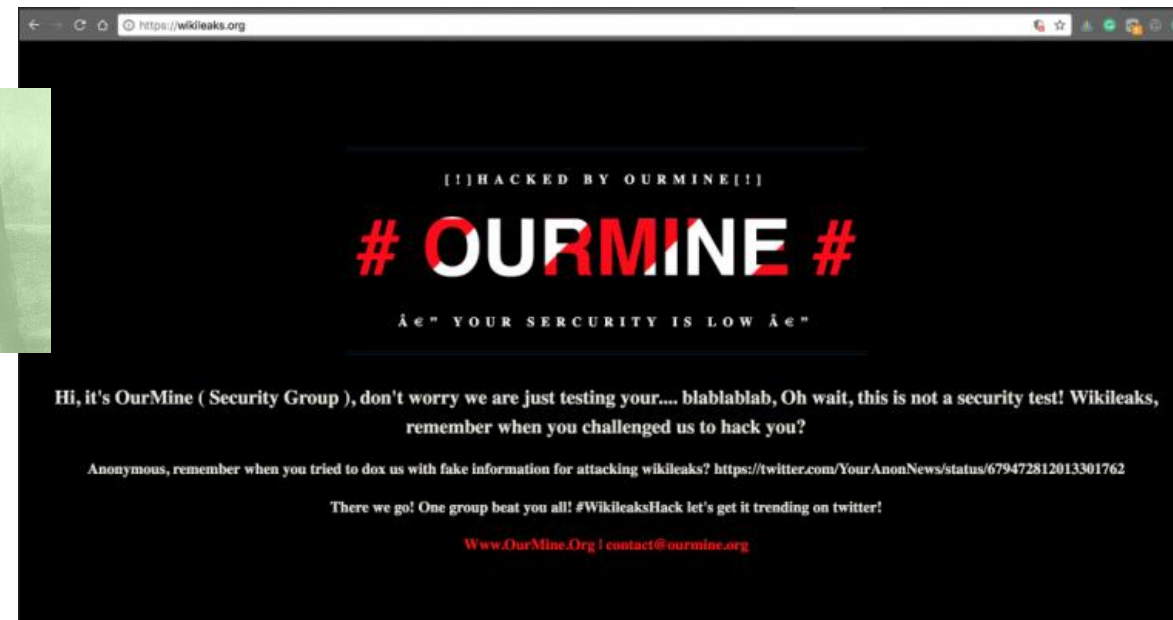
Цель: веб-сайты государственных структур Малайзии

Когда: август 2017 г.

Последствия: дефейс 27 веб-сайтов¹

Кто: хакерская группировка из Индонезии

Что произошло: атака из-за ошибки в буклете 28-х Игр Юго-Восточной Азии



Цель: веб-сайт Wikileaks

Когда: 31 августа 2017 г.

Последствия: дефейс сайта в течение нескольких часов²

Кто: хакерская группировка OurMine

Что произошло: следов взлома в веб-сайте не обнаружено, предположительно проведена атака DNS Poisoning

1. <http://techwireasia.com/2017/08/indonesia-hackers-deface-malaysian-websites-sea-games-flag-blunder/#qD4222d8LF1HtZKw.97>

2. <https://www.theguardian.com/technology/2017/aug/31/wikileaks-hacked-ourmine-group-julian-assange-dns-attack>

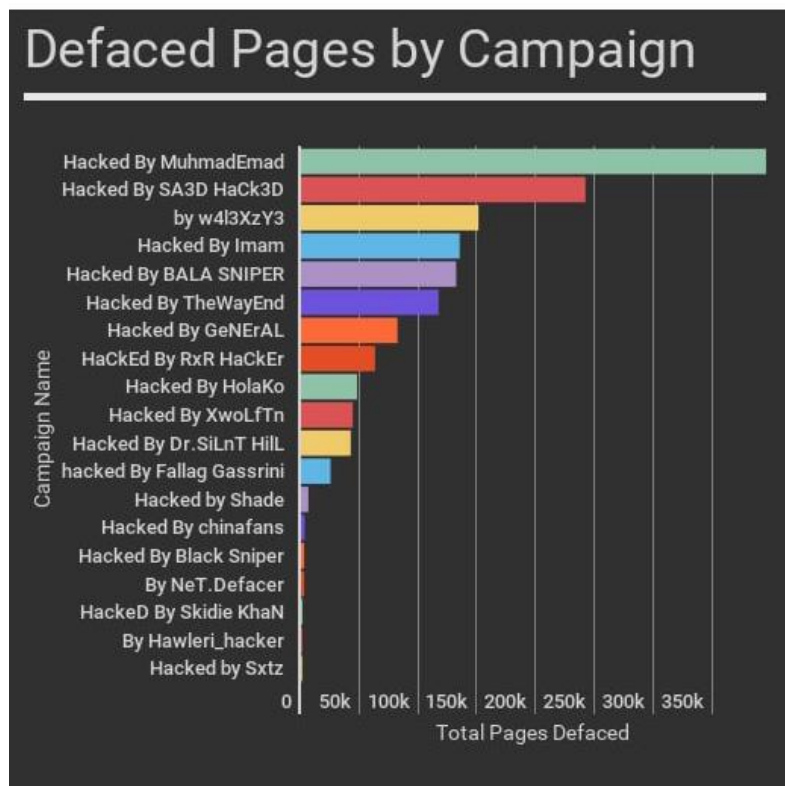
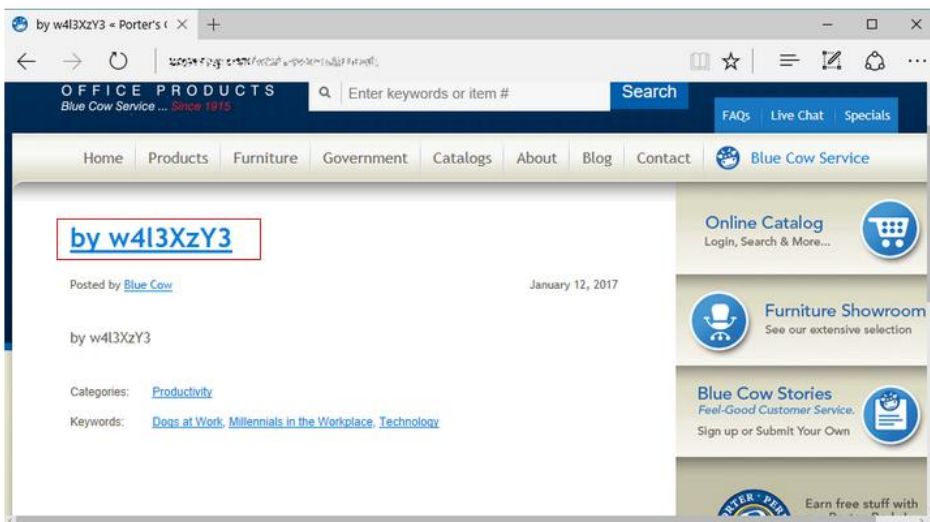
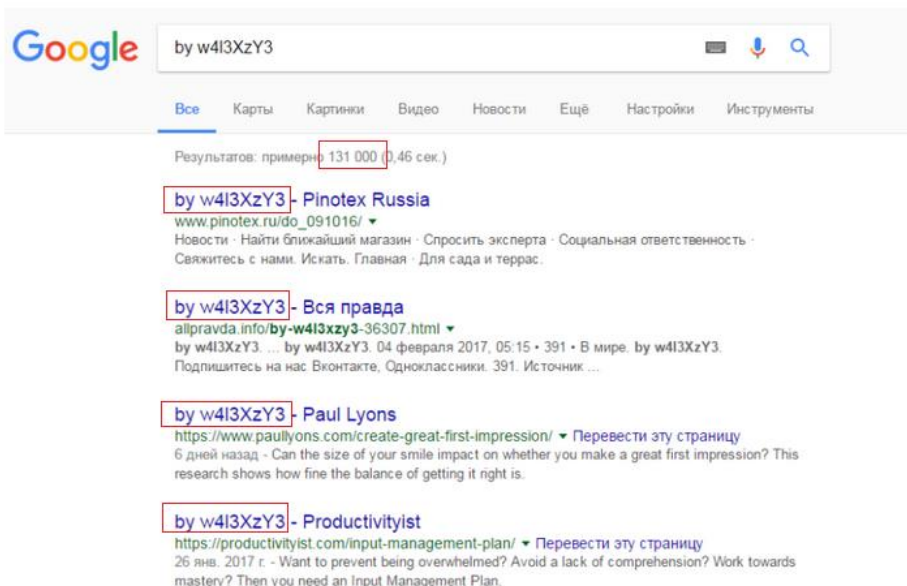
Цель: веб-сайты с CMS WordPress

Когда: начало 2017 г.

Последствия: дефейс более 1,5 млн веб-сайтов³

Кто: несколько десятков хакерских группировок

Что произошло: эксплуатация уязвимости в CMS WordPress



Google Search Console

Recommended Wordpress update available for

To: Webmaster of

Google has detected that your site is currently running Wordpress 4.7.0 or 4.7.1, an older version of Wordpress. Outdated or unpatched software can be vulnerable to hacking and malware exploits that harm potential visitors to your site. Therefore, we suggest you update the software on your site as soon as possible.

Following are one or more example URLs where we found pages that have outdated software. The list is not exhaustive.

Цель: веб-сайты госструктур Чехии

Когда: май 2016 г.

Последствия: отказ в обслуживании

Кто: хакерская группировка Anonymous

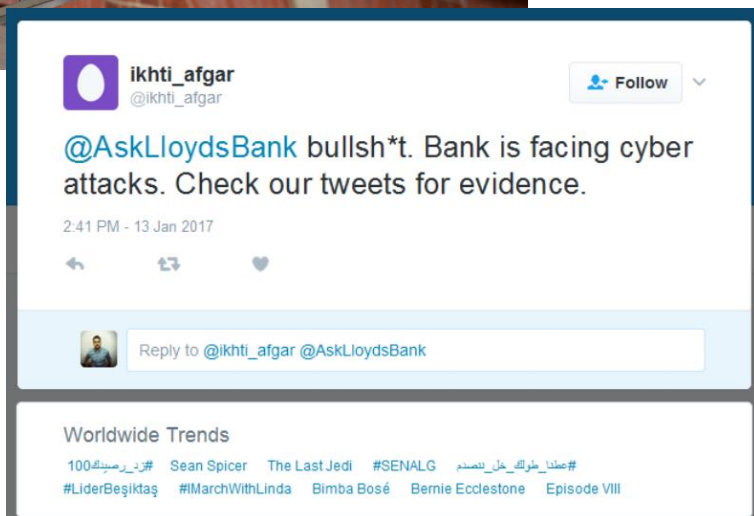
Что произошло: акция протеста против утверждения Сенатом Чехии закона о блокировке интернет-страниц с азартными играми



VS.



11 января 2017 г. британский банк Lloyds подвергся DDoS-атаке. В течение 2 дней клиенты банка наблюдали перебои в работе системы ДБО. Для прекращения атаки хакеры требовали выкуп в размере 100 BTC⁴.



Mine

Font: Small - Normal - Large

```
01. ----- Forwarded message -----
02. From: (hacked email account)
03. Date: Wed, 11 Jan 2017 09:42:51 +0000
04. Subject: The lloyds group online services and customers are in danger
05. To: [REDACTED]
06.
07. To whom it may concern,
08.
09. We have identified sever security issues related to
10. onlinebusiness.lloydsbank.co.uk and online.lloydsbank.co.uk.
11.
12. As an effect, both these services will be put offline starting from
13. the 11th of Jan 2017 @ 00:01 GMT until the are fixed.
14.
15. - The consultancy fee of 75,000 GBP must be paid via Bitcoin to the
16. following address:
17.
18. 1bnkwzj [REDACTED]
19.
20. That is Approx 100 BTC.
21.
22. Once paid, the services will be back online, you will get a list of
23. flaws related to both services, along with our disappearance.
24.
25. Feel free to test our capabilities and patience,
26. Good luck.
```

4. <https://xakep.ru/2017/01/24/lloyds-banking-group-ddos/>

Полный провал криптовалютного стартапа CoinDash

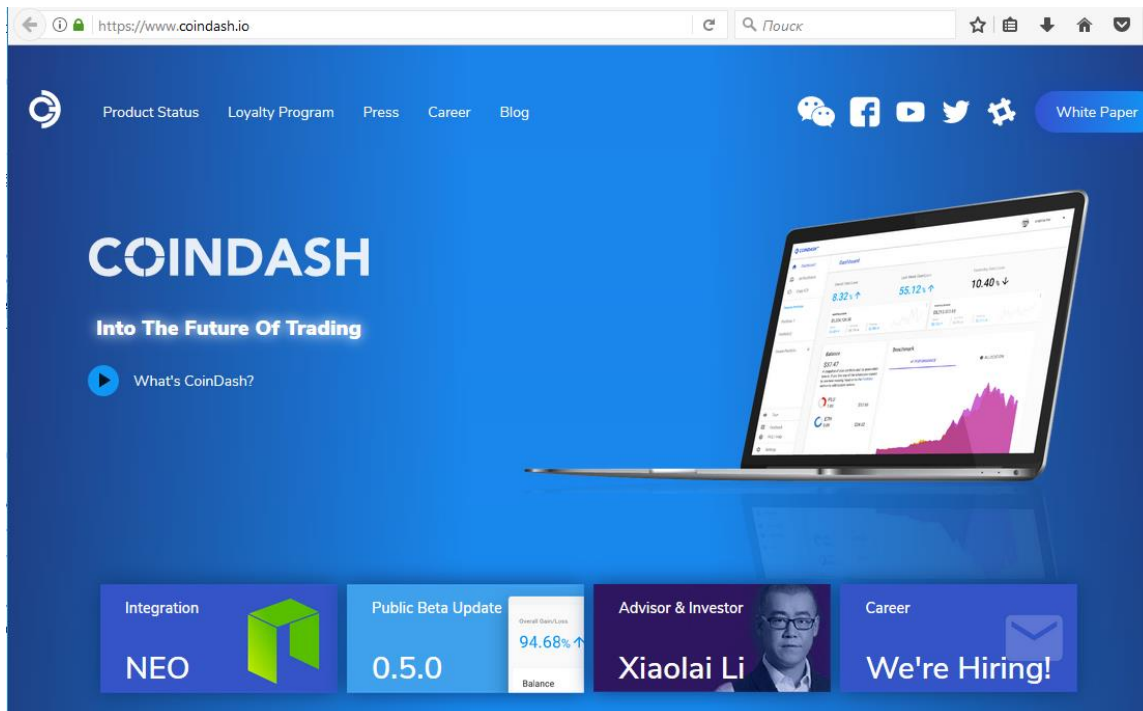
POSITIVE TECHNOLOGIES

Цель: веб-сайт криптовалютного стартапа CoinDash

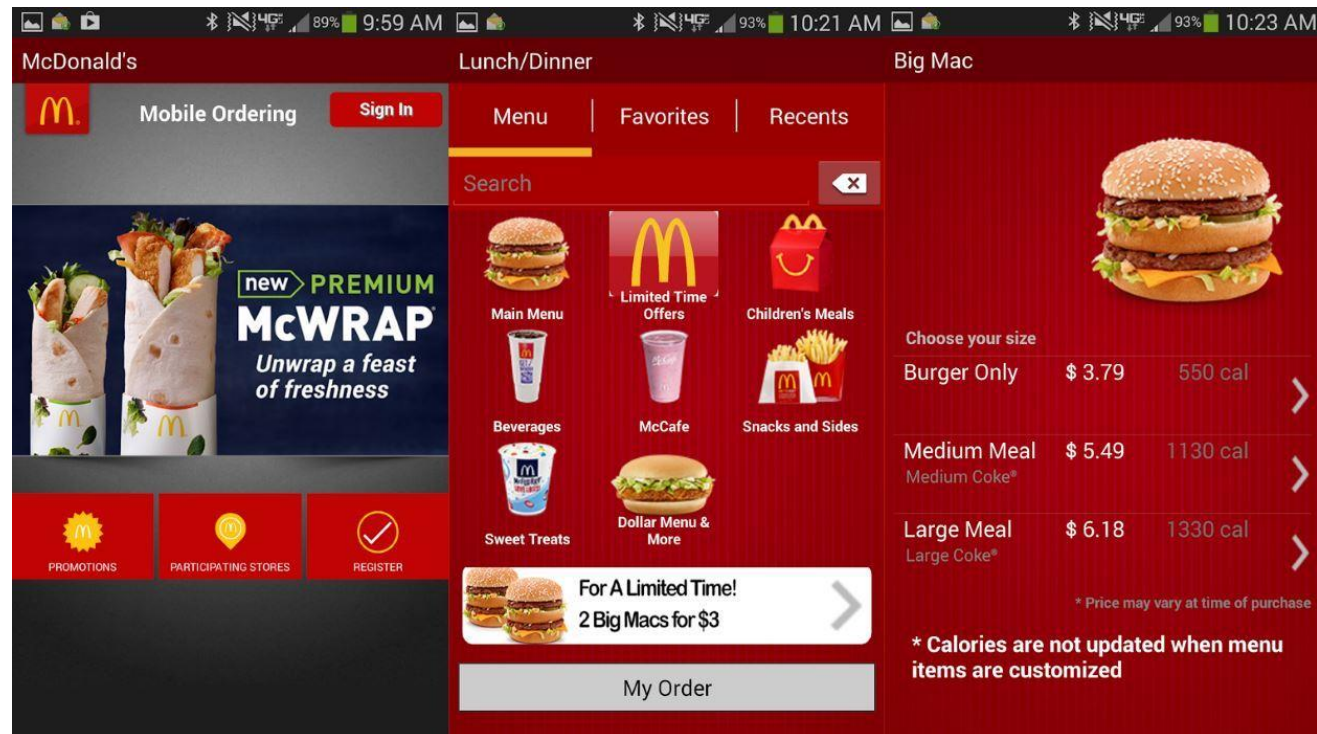
Когда: июль 2017 г.

Последствия: кража 43 488 ETH⁵

Что произошло: подмена адреса официального Ethereum-кошелька во время ICO



5. <https://xakep.ru/2017/07/18/coindash-hacked/>



Цель: веб-сайт доставки еды McDelivery в Индии

Когда: февраль-март 2017 г.

Последствия: утечка ПДн 2,2 млн клиентов⁶

Что произошло: эксплуатация ошибки в API

```
{"data":{"DOA":"","DOB":"","EmailID":"asf[REDACTED]@yahoo.com","FacebookID":"","GooglePlusID":"","ImageUrl":"","IsFBVerified":false,"LastAddressUsed":{"AddressTypeName":"","BuildingName":"","CityName":"","FlatNo":"10","ID":1777576,"Land5603167","Longitude":"","[REDACTED]","MapAddress":"","[REDACTED]partments,[REDACTED]411007,toreName":"","StreetName":""},"PhoneNo":"855[REDACTED]","ProfileID":179139,"ProfileName":"Asf[REDACTED]","Title":"Asf[REDACTED]","s":1}}{"data":{"DOA":"","DOB":"","EmailID":"kl[REDACTED]@gmail.com","FacebookID":"","GooglePlusID":"","ImageUrl":"","IsVerified":false,"PhoneNo":"98[REDACTED]","ProfileID":179140,"ProfileName":"R[REDACTED]","Title":"R[REDACTED]"},"m":"Record found","DOB":"","EmailID":"ml[REDACTED]@gmail.com","FacebookID":"","GooglePlusID":"","ImageUrl":"","IsFBVerified":false,"IsGPVerified":false,"ProfileID":179141,"ProfileName":"Ml[REDACTED]","Title":"Ml[REDACTED]"},"m":"Record found","s":1}^C
```

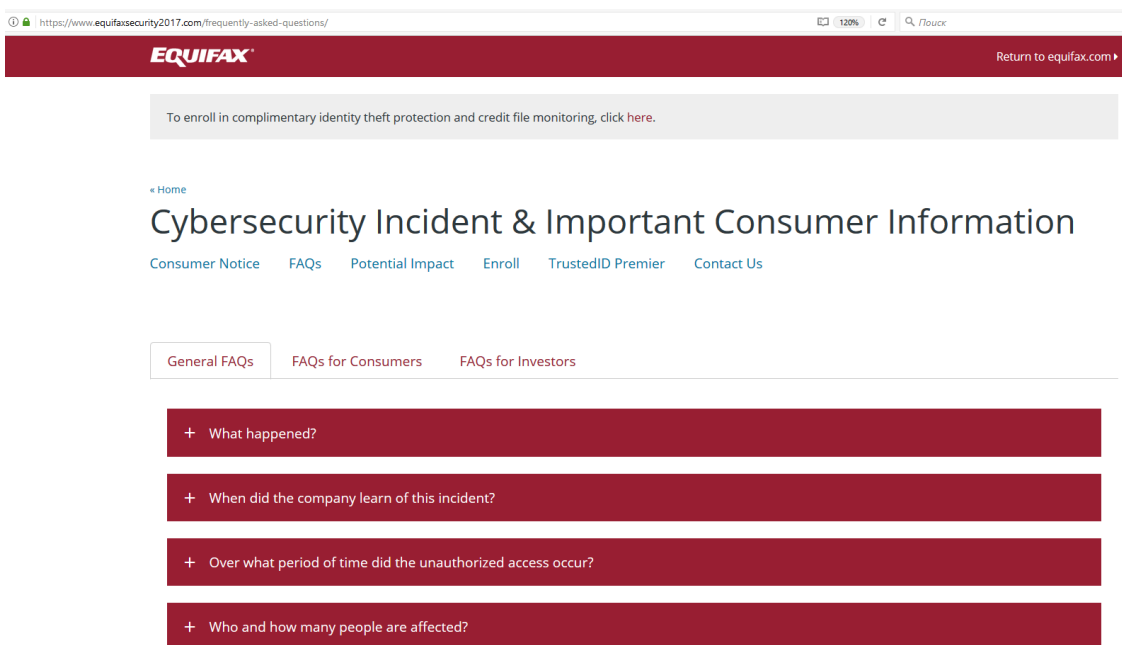
6. <http://securityaffairs.co/wordpress/57290/data-breach/mcdonalds-mcdelivery-flaw.html>

Цель: веб-сайт североамериканского подразделения компании Equifax

Когда: июль 2017 г., но может быть и раньше

Последствия: утечка ПДн **143 млн человек**

Что произошло: эксплуатация критической уязвимости (10 баллов по шкале CVSS v.3) [CVE-2017-5638](#) во фреймворке Apache Struts⁷;



- What happened?

We identified a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. We discovered the unauthorized access and acted immediately to stop the intrusion. We promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. We also reported the criminal access to law enforcement and continue to work with authorities.

- What was the vulnerability?

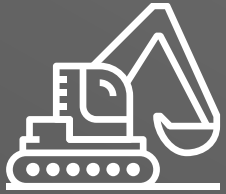
Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

Цель: веб-сайт информационно-аналитического центра обработки результатов государственных экзаменов (ЕГЭ и ГИА)

Когда: в начале лета 2016 г.

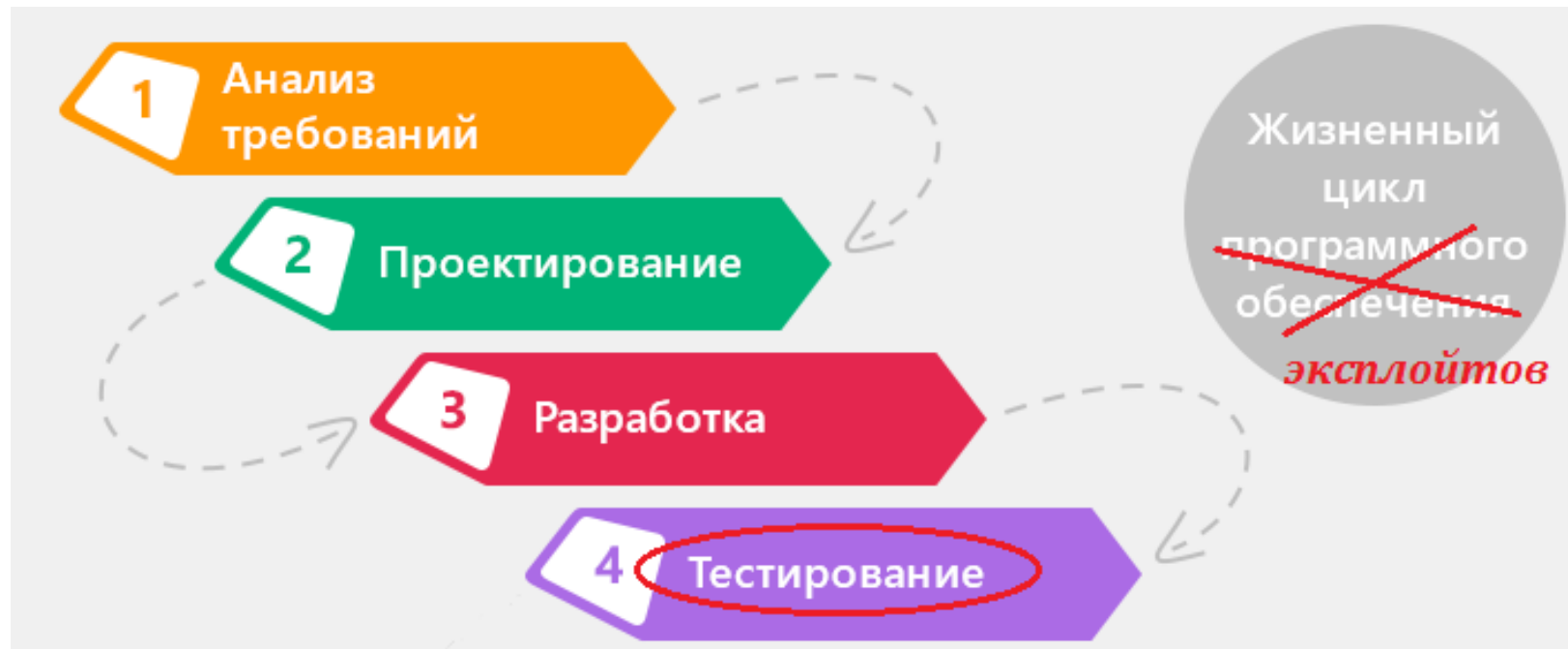
Что произошло: WAF фиксировал **более 20 тысяч атак в день** при среднем числе атак на веб-приложения других организации от 300 до 800 в день.





Когда приложение — средство атаки?

Для проверки работоспособности новых эксплойтов хакеры могут использовать произвольные веб-ресурсы.



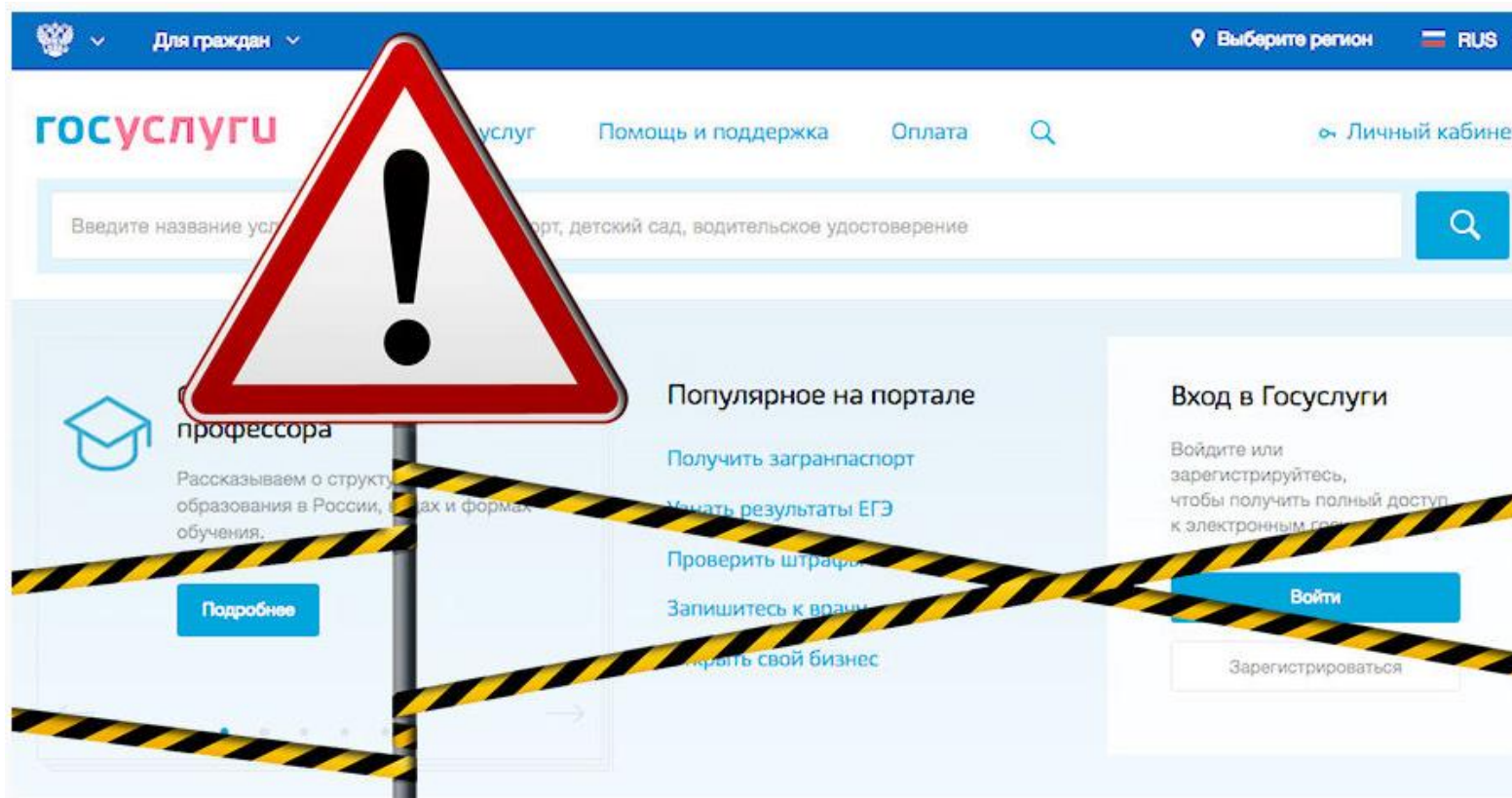
Любой веб-ресурс может стать **тестовой площадкой** для злоумышленников.

Цель: пользователи веб-сайта gosuslugi.ru

Когда: июль 2017 г.

Последствия: проведение атак на пользователей веб-приложения⁸

Что произошло: предположительно из-за уязвимости XSS на сайте был внедрен вредоносный код, который оказался рекламным программным обеспечением (adware)



8. <https://news.drweb.ru/show/?i=11373&c=5&lng=ru&p=0>

Цель: пользователи веб-сайтов для бухгалтеров, HR-менеджеров и юристов

Когда: первый квартал 2017 г.

Последствия: хищение денежных средств со счетов различных компаний, точный размер ущерба не установлен⁹

Что произошло: заражение пользователей веб-сайтов трояном Buhtrap



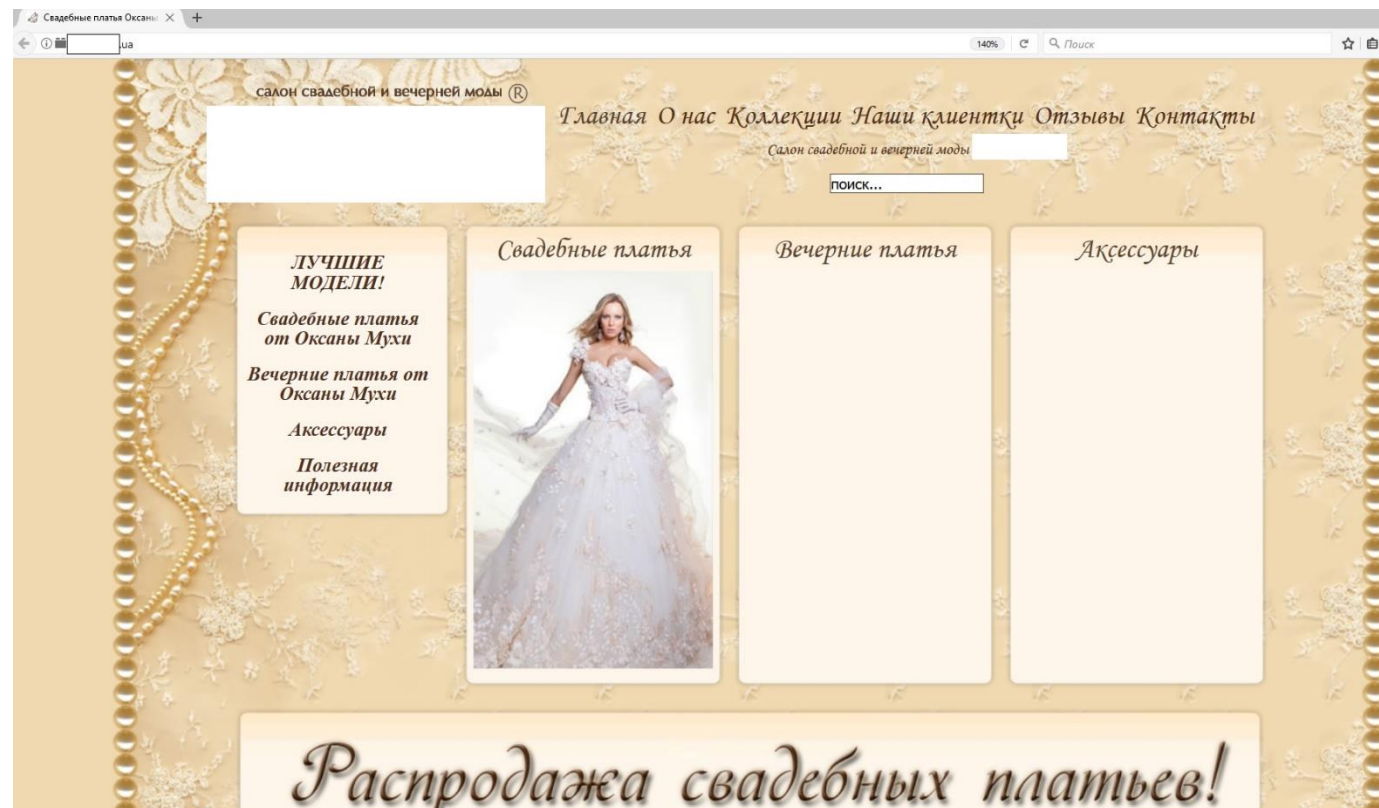
Легкомысленное отношение к безопасности веб-приложения способствует распространению вредоносного программного обеспечения и **может привести к хищению денежных средств у пользователей.**

9. <https://www.group-ib.ru/blog/buhtrap>

Что общего может быть между группировкой **Cobalt** и сайтом салона свадебной и вечерней моды?



?



Приложение может стать **промежуточным звеном** в целевой атаке.



Как защитить приложение от атак?



1. Использовать межсетевой экран уровня приложений (web application firewall).



2. Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.



3. Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.



4. Своевременно обновлять используемое ПО.



5. Использовать строгую парольную политику, особенно для привилегированных учетных записей.

В первой половине 2017 г. «Недостаточная защита от атак на веб-приложения» рассматривалась OWASP как одна из наиболее критически опасных уязвимостей и была включена в проект списка OWASP TOP-10 (2017).

Читайте наши исследования: ptsecurity.com/ru-ru/research/analytics/

1. Уязвимости веб-приложений (2017): ptsecurity.com/upload/corporate/ru-ru/analytics/Web-vulners-2017-rus.pdf
2. Статистика атак на веб-приложения: II квартал 2017: blog.ptsecurity.ru/2017/09/web-apps-attacks-2017.html#more
3. Уязвимости корпоративных информационных систем (2017):
ptsecurity.com/upload/corporate/ru-ru/analytics/Corp-Vulnerabilities-2017-rus.pdf
4. Актуальные киберугрозы: II квартал 2017: ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf
5. Cobalt strikes back: новые атаки на финансовые организации (2017):
ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-2017-rus.pdf



Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru