Дмитрий Сивоконь,

Директор региональных продаж
Positive Technologies

Актуальные киберугрозы.
По следам аналитики Positive Technologies

POSITIVE TECHNOLOGIES

ptsecurity.com

Positive Technologies в цифрах

POSITIVE TECHNOLOGIES

16 лет опыта

200+ Аудиты защищенности ежегодно

1000+ Крупных внедрений

sochi.ru 2014

UNIVERSIADE KAZAN 2013 RUSSIA

Экспертиза

150+ Обнаруженных уязвимостей нулевого дня в АСУ ТП

30+ Обнаруженных уязвимостей нулевого дня в телеком

400+ Исследований безопасности веб-приложений

Сообщество

phd Positive Hack Days

международный форум по практической информационной безопасности

SecurityLab.ru by Positive Technologies

Информационный портал о событиях в сфере защиты информации, Интернет-права и новых технологиях

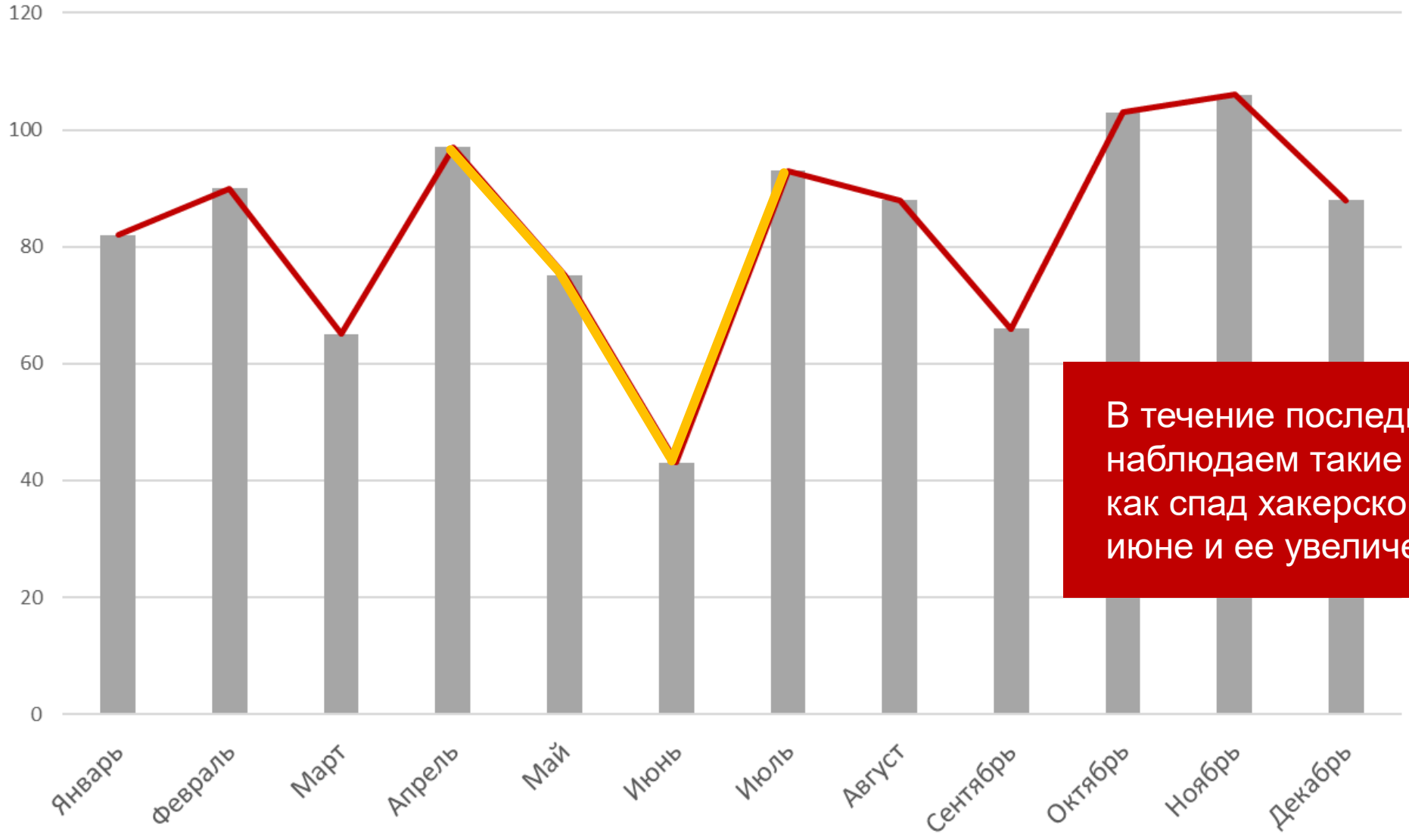
Positive Education

Образовательная программа

50+ ведущих ВУЗов

Динамика кибератак

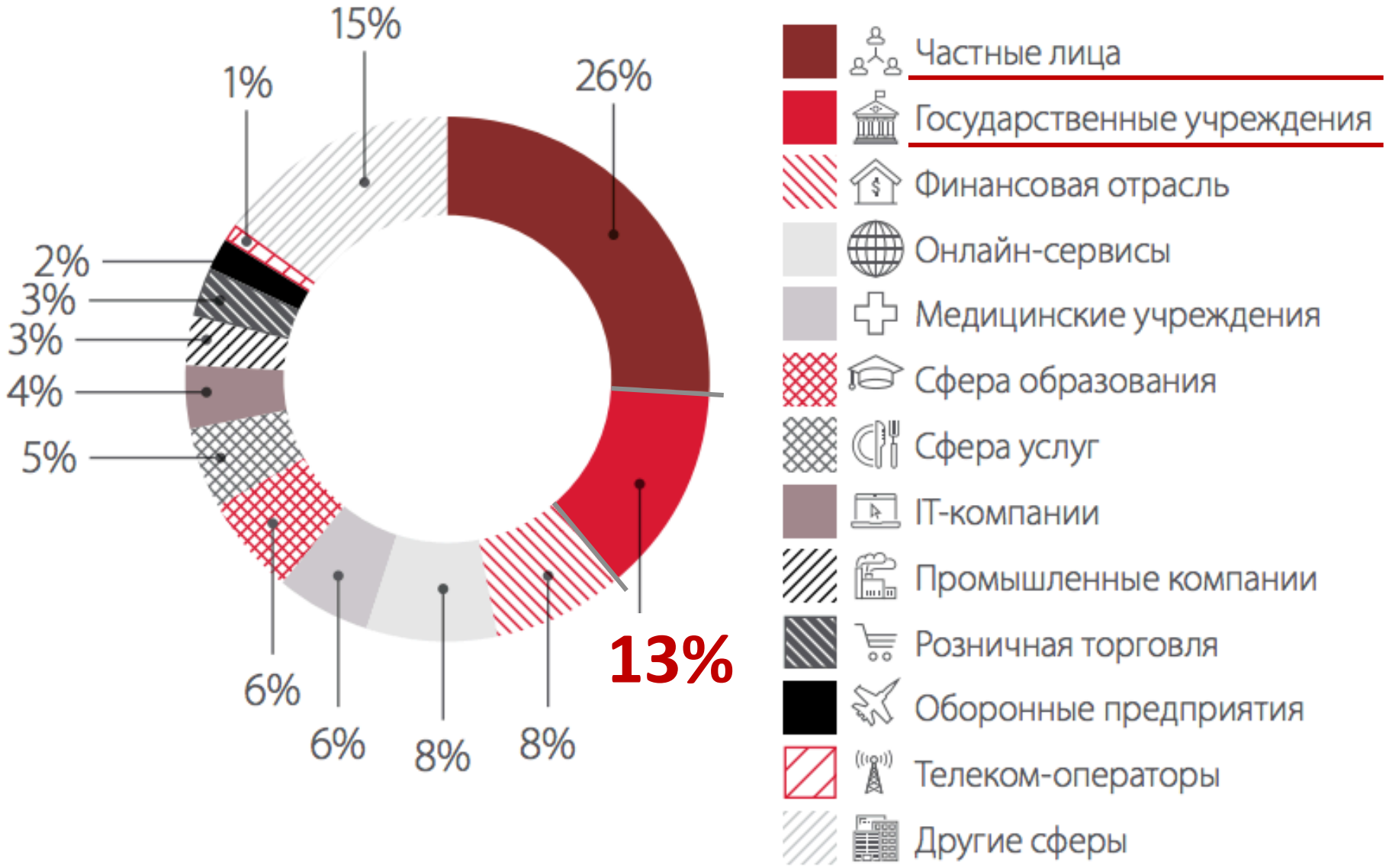
POSITIVE TECHNOLOGIES



В течение последних двух лет мы наблюдаем такие закономерности, как спад хакерской активности в мае-июне и ее увеличение под конец года

Классификация жертв по отраслям

POSITIVE TECHNOLOGIES



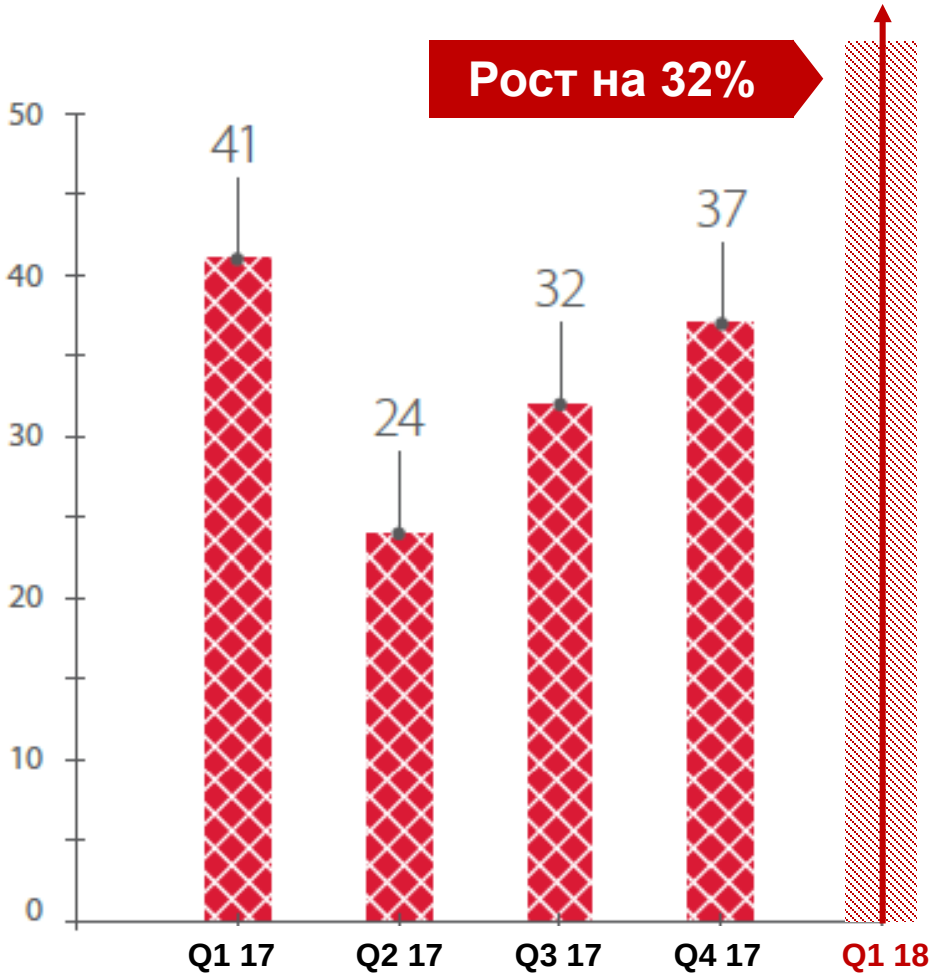
Мотивы киберпреступников

POSITIVE TECHNOLOGIES

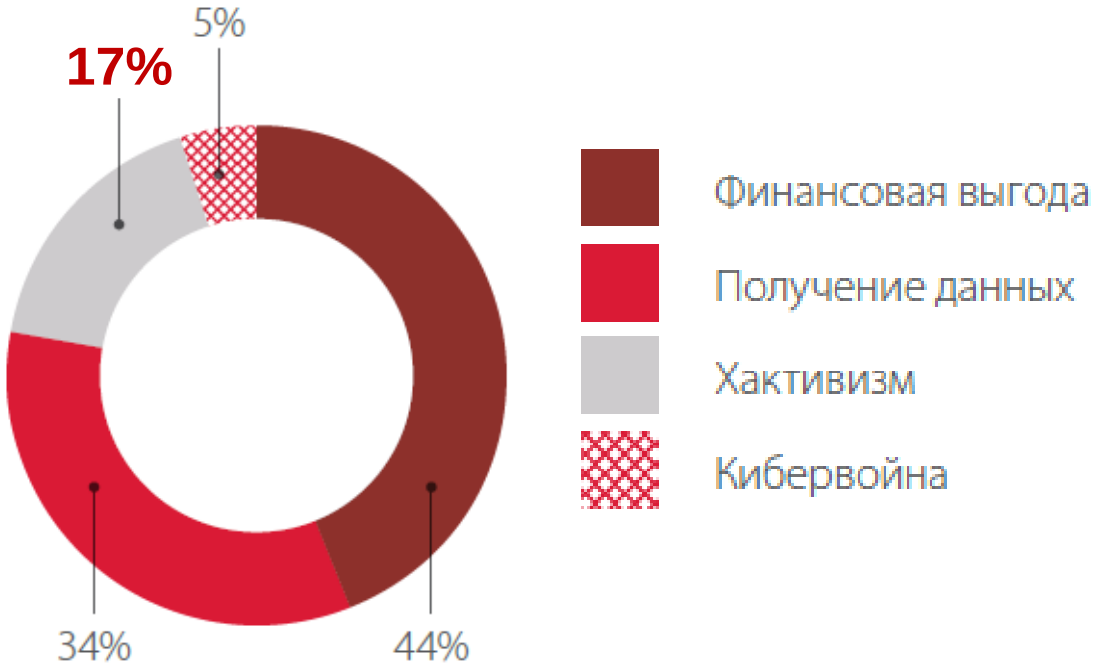
Основными мотивами хакеров в государственном секторе остаются: хактивизм и хищение данных

Атаки на государственные организации

POSITIVE TECHNOLOGIES



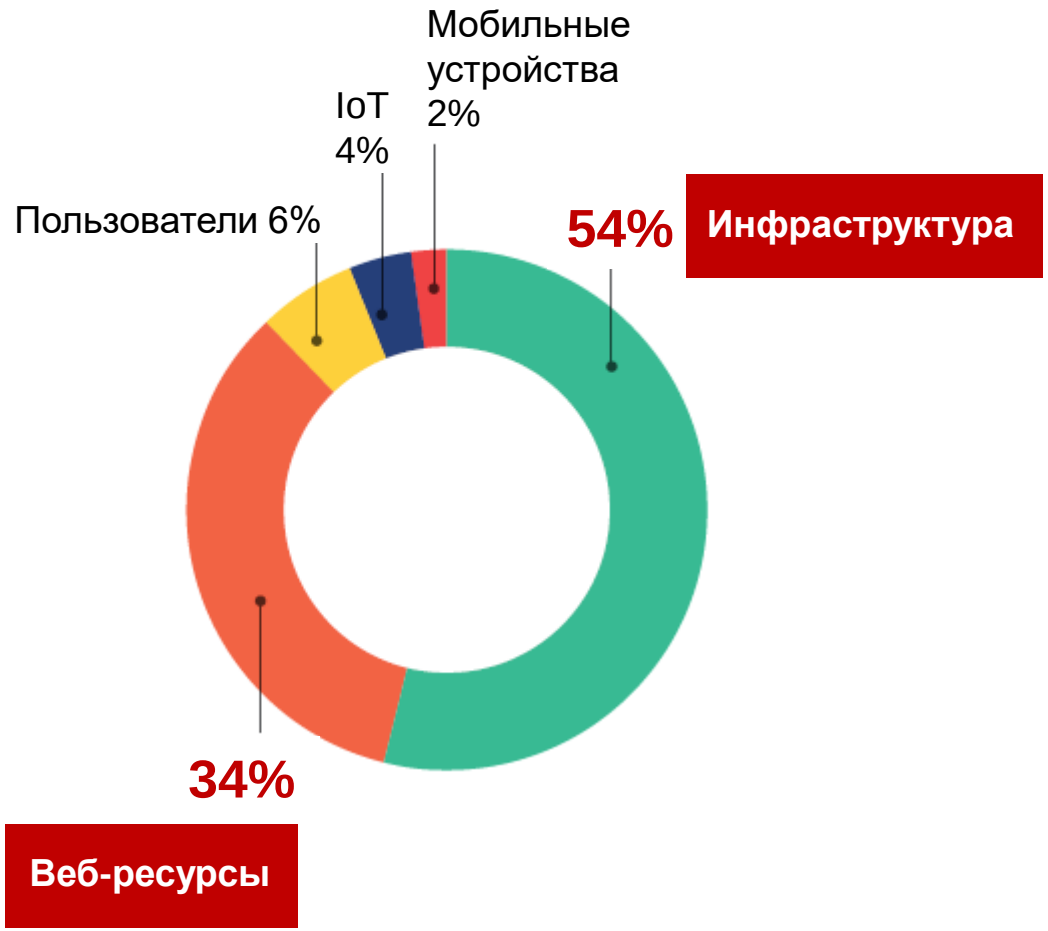
Количество атак на государственные организации в 2017 году



Мотивы атак

Типовые объекты атак на государственные организации

POSITIVE TECHNOLOGIES

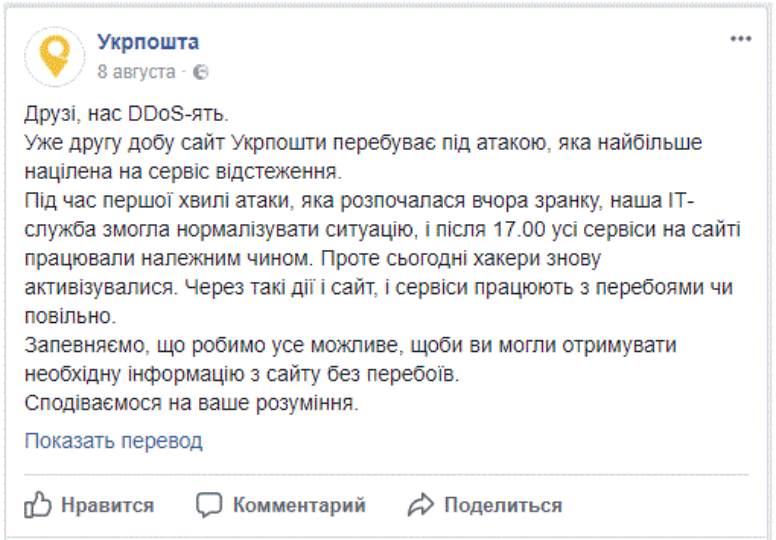


Объекты атак

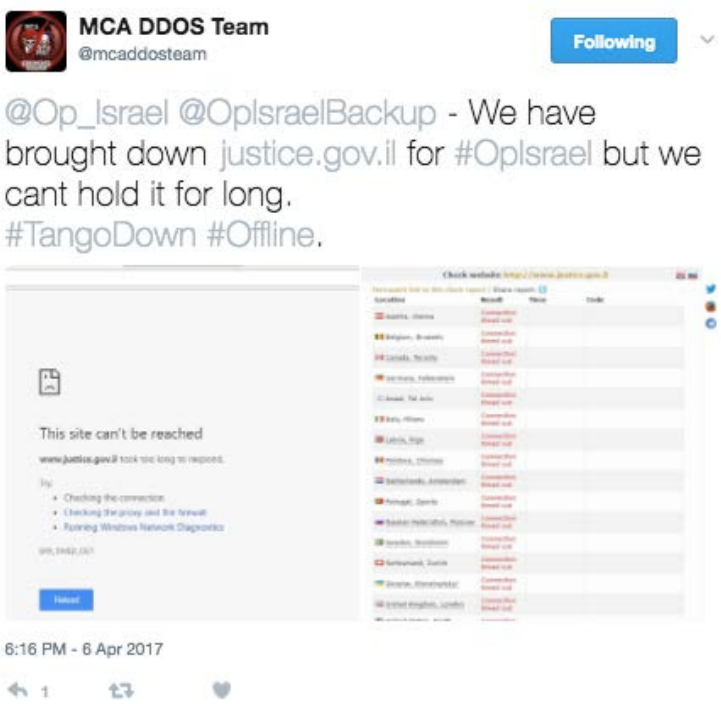
Методы атак

DDoS Атаки

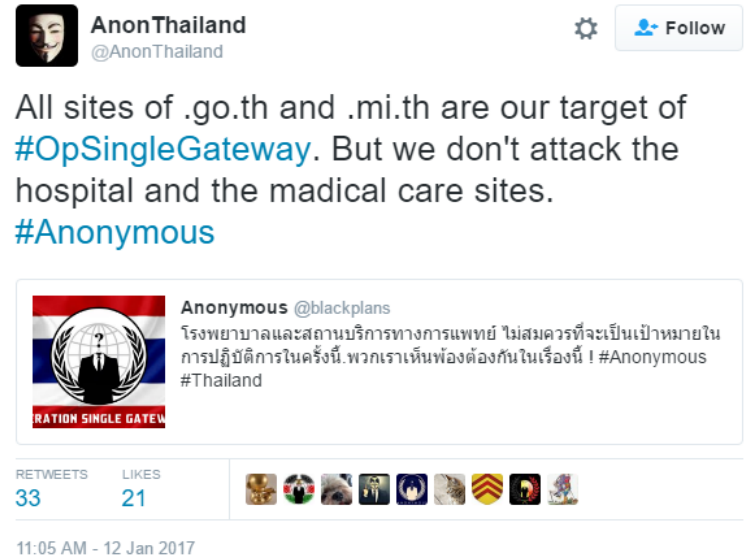
POSITIVE TECHNOLOGIES



DDoS-атака на онлайн-сервисы украинской почты



DDoS-атака на правительство Израиля



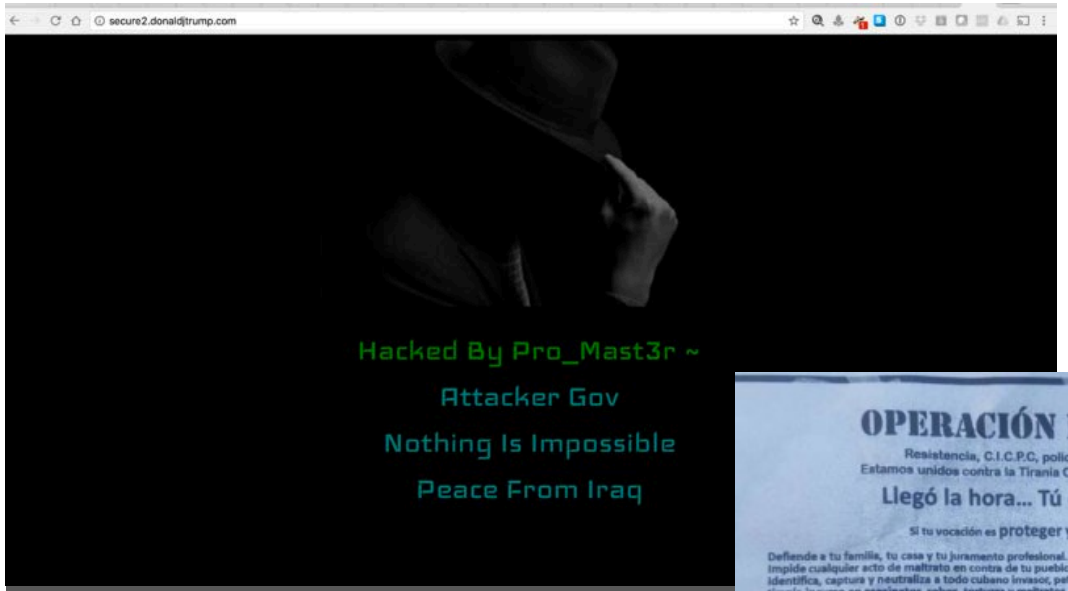
DDoS-атака на правительство Таиланда

DDoS-атака на правительство Испании

1. en.interfax.com.ua/news/general/441141.html
2. blog.radware.com/security/2017/04/opisrael-2017/
3. politica.elpais.com/politica/2017/10/21/actualidad/1508574710_898791.html?id_externo_rsoc=FB_CM
4. security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opsingle-gateway/

Дефейс государственных веб ресурсов

POSITIVE TECHNOLOGIES



Дефейс сайта предвыборной компании Дональда Трампа

Дефейс правительственных сайтов Венесуэлы

Дефейс малазийских сайтов

1. arstechnica.com/information-technology/2017/02/secure-trump-website-defaced-by-hacker-claiming-to-be-from-iraq/
2. dw.com/en/venezuela-cyberattack-targets-government-websites/a-40002475
3. thestar.com.my/tech/tech-news/2017/08/21/indonesian-hackers-defaced-malaysian-websites-following-flag-blunder/#0pDO5c6oApjlo7Oa.99

Прогнозы на 2019 год

POSITIVE TECHNOLOGIES

Масштабные вредоносные атаки

Майнинг криптовалюты за счет посетителей веб-сайтов может стать еще популярней

Масштабные DDoS-атаки за счет роста количества новых ботнетов и увеличения состава существующих

Ransomware as a service («вымогатель-как-услуга»)

POSITIVE TECHNOLOGIES

Хакера осудили за взлом учетных записей должностных лиц США[2] **5** лет лишения свободы	Взлом почты от **40 $**	Взлом сайта от **150 $**	Хакера осудили за проведение DDoS-атак[3] **2** года лишения свободы
Целевая атака на компанию от **4500 $**			DDoS-атака от **50 $** / день
Заражение трояном- майнером от **750 $**			Кража денег из банкоматов от **1500 $**
Программиста осудили за создание ВПО для обхода системы учета АЗС[4] **1,5** года лишения свободы	Заражение трояном-вымогателем (1000 узлов) от **300 $**	Кража денег со счетов (с помощью фишинга) от **270 $**	Мошенника осудили за кражу денег клиентов банка через систему ДБО[5] **6** лет лишения свободы

Стоимость целевой атаки на организацию в зависимости от сложности может составлять от 4500 $, включая наем специалиста по взлому, аренду инфраструктуры и покупку соответствующих инструментов.

Минимальная стоимость в долларах США при условии, что все необходимые средства и инструменты организатор атаки приобретет за деньги.

Защита от вредоносного ПО

- Своевременно обновлять используемое ПО
- Использовать средства антивирусной защиты
- Контролировать периметр сети
- Резервировать критически важные системы и ресурсы
- Повышать осведомленность сотрудников и клиентов в вопросах ИБ

Защита от атак с использованием уязвимостей ПО

POSITIVE TECHNOLOGIES

- Применять средства централизованного управления обновлениями и патчами
- Применять автоматизированные средства анализа защищенности и выявления уязвимостей в ПО
- Использовать WAF
- Регулярно проводить тестирования на проникновение

ГосСОПКА и методические рекомендации ФСБ

POSITIVE TECHNOLOGIES

Повышение осведомленности персонала и пользователей

PT Application Inspector

MaxPatrol 8

MaxPatrol SIEM

- **Инвентаризация информационных ресурсов**
- **Выявление уязвимостей**
- **Анализ угроз**

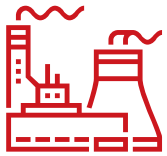
Рекомендации

- **Анализ данных о событиях безопасности**
- **Прием сообщений о возможных инцидентах**
- **Регистрация инцидентов**
- **Реагирование на инциденты и ликвидация их последствий**
- **Расследование инцидентов**
- **Анализ результатов устранения последствий инцидентов**

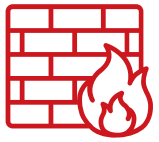
MaxPatrol SIEM

PT Ведомственный центр

Обнаружение компьютерных атак

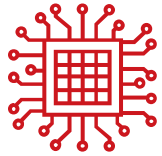


PT ISIM



PT Application Firewall

PT MultiScanner



PT Network Attack Discovery

Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.com