

#### Антон Дьяков

Руководитель направления развития решений информационной безопасности, AO «PHT»

## Кибероружие ТРОЯН КИБЕР ТЕРРОРИСТ ПОЛЬЗОВАТЕЛЬ Средства доставки Атакующая Вредонос головка

## Распространение кибероружия





РЕСУРСЫ СКРИПТ-КИДДИ

ОФИЦИАЛЬНЫЕ ЗАЯВЛЕНИЯ И НЕОФИЦИАЛЬНЫЕ ПУБЛИКАЦИИ

## Ресурсы скрипт-кидди



РЕСУРСЫ ДЛЯ СКАЧИВАНИЯ КИБЕР-ОРУЖИЯ

ПРОГРАММЫ ДЛЯ АУДИТА БЕЗОПАСНОСТИ

Сайты

Такие как: Softxaker и проч.

Такие как:

WinNuke Back Orifice

NetBus

Sub7

Metasploit

ProRat

PassJacker

iStealer

Snoopy

## Уязвимости как средство заработка



**2015 год** - начало повсеместного открытия бирж уязвимостей.

**2016 год** - открытие в России первой биржа EXPOCOD, где разработчики и хакеры могут официально продавать уязвимости в программном обеспечении Linux, Windows, OS X, Tor, iOS, Android, браузеров Chrome, IE и др.

Продавая уязвимость заинтересованному клиенту и сохраняя её в секрете, можно заработать **более 10 000 \$**. И это больше, чем по официальной программе выплаты вознаграждения за уязвимости, которая предусматривает раскрытие информации и выпуск патча.



## Неофициальные заявления







VS



**05.02.2018** «Фонтанка» со ссылкой на Женевскую конвенцию указала, что каждый пленный обязан сказать противнику личный номер, имя, фамилию, звание и дату рождения. Используя данные, которые опубликовали в интернете боевики «Исламского государства», журналисты получили доступ к личному кабинету летчика Романа Филиппова, погибшего в Сирии 3 февраля. Таким образом «Фонтанка» узнала размер заработной платы, историю службы, жилищные условия и другие персональные данные военного.

## Еще неофициальные публикации







# WikiLeaks

**В феврале 2017** Wikileaks опубликовывает материалы ФБР и ЦРУ, среди которых находится специализированная информация о вредоносах и атакующих головках кибероружия в прикладном виде.

Данная информация была оперативно зафиксирована и сохранена для дальнейшего использования киберпреступниками.

## Официальные заявления об уязвимостях





Многие гиганты современной IT индустрии, такие как Intel, AMD, Microsoft и прочие, публикуют информацию о собственных уязвимостях обновлениях.

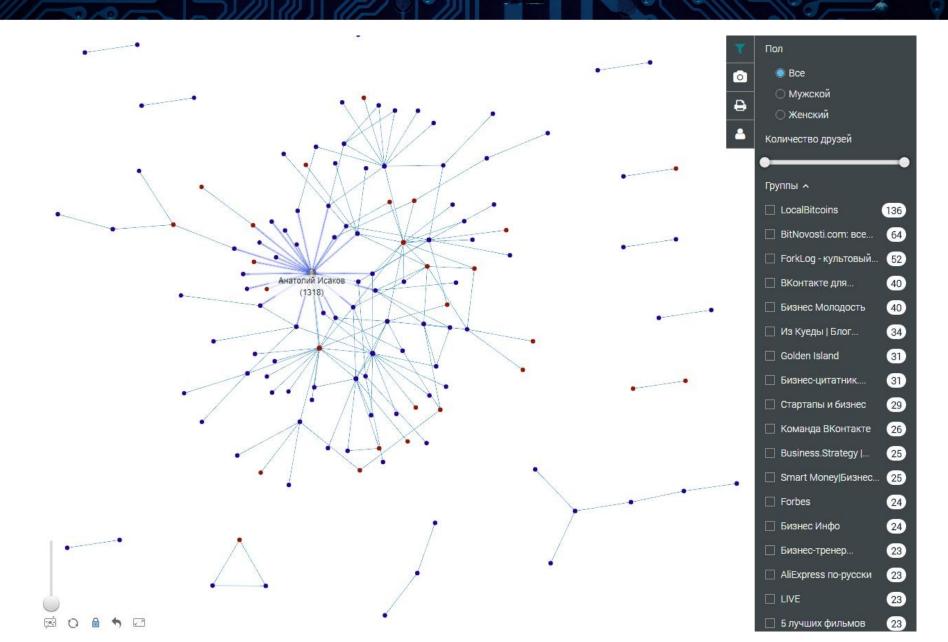
Порой, несмотря на заявления об уязвимостях, предлагаемые патчи не спасают, а выявленные закладки ждут своего дня, чтобы выстрелить.

Рассмотрим на примере нашумевшего WannaCry



## Информационный портрет киберпреступника





### Безопасность российских учреждений и предприятий









#### WEBBEZ



#### Олимпиада

#### Сайт: www.olympic.ru

01.02.2018 15:27:40

Дата исследования: 2018-01-30 01:02:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/sochi...

#### Сайт: www.roc.ru

01.02.2018 15:27:14

Дата исследования: 2018-01-30 01:04:02 Статус; обнаружены проблемы

http://webbez.ru/1403rep/sochi.

#### Министерство Обороны

#### Сайт: archive.mil.ru

01 02 2018 15 33 20

Дата исследования: 2018-01-30 00:24:02 Статус: проблем не обнаружено

http://webbez.ru/1403rep/morfe

#### Сайт: www.oboronservice.ru

01 02 2018 15 32 55

Дата исследования: 2018-01-30 00:26:02 Статус: проблем не обнаружено

http://webbez.ru/1403rep/morfe\_

#### Госструктура

#### Сайт: www.cfopolpred.ru

08.02.2018 11:06:26

Дата исследования: 2018-02-08 08:02:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/govau...

#### Сайт: gub.rkursk.ru

08.02.2018 11:05:06

Дата исследования: 2018-02-08 08:22:02 Статус: обнаружены критические проблемы и уязвимости

http://webbez.ru/1403rep/govau...

#### Сколково

#### Сайт: community.sk.ru

01 02 2018 15 29 2

Дата исследования: 2018-01-30 00:36:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/skrfr...

#### Сайт: school.skolkovo.ru

01.02.2018 15:28:47

Дата исследования: 2018-01-30 00:38:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/skrfr...

#### Банк

#### Сайт: www.mtsbank.ru

07.02.2018 14:48:38

Дата исследования: 2018-02-06 00:58:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/mtsbd...

#### Сайт: rgsbank.ru

01.02.2018 15:30:23

Дата исследования: 2018-01-30 00:32:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/rgswe.

#### Коммерческая компания

#### Сайт: www.rosevrobank.ru

07 02 2018 14 47 50

Дата исследования: 2018-02-06 00:42:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/rebdi

#### Сайт: www.masterdata.ru

07.02.2018 14:47:26

Дата исследования: 2018-02-06 00:48:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/rebdi...

#### моэск

#### Сайт: www.moesk.ru

07.02.2018 14:47:53

Дата исследования: 2018-02-05 07:18:02

http://webbez.ru/1403rep/mskwe.

#### Сайт: mail.fsk-ees.ru

07.02.2018 14:47:41

Дата исследования: 2018-02-06 00:56:02 Статус: обнаружены проблемы безопасности

http://webbez.ru/1403rep/mskwe...

#### GreenPeace

#### Сайт: www.shelf-neft.gazprom.ru

29.01.2018 16:32.21

Дата исследования: 2018-01-27 15:22:02 Статус: проблем не обнаружено

http://webbez.ru/1403rep/gnshw...

Сайт: www.918-999-81-81.ru

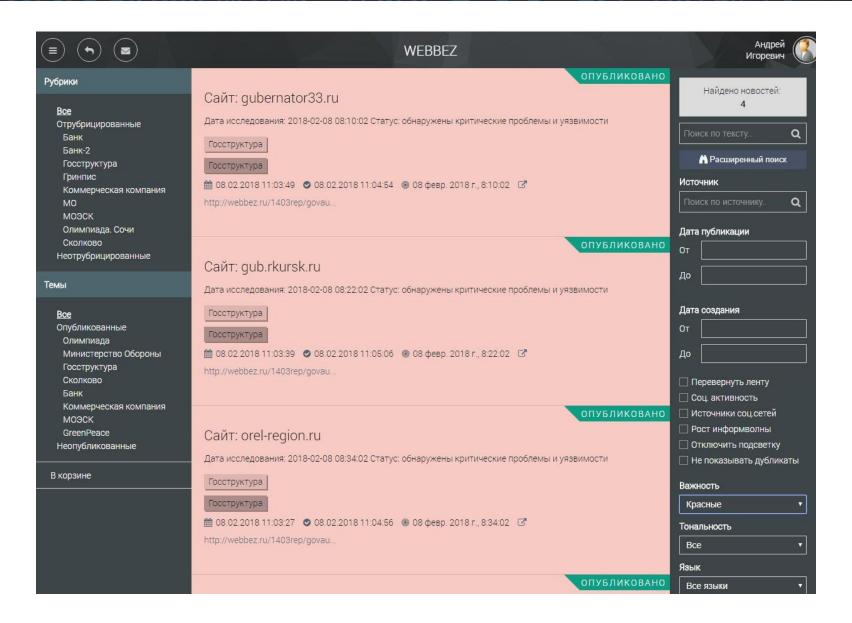
29 01 2019 16 31 57

Дата исследования: 2018-01-27 15:24:02 Статус: проблем не обнаружено

ttp://webbez.ru/1403rep/gnshw

## Пример «будущего пациента»





## Пример «красной» уязвимости







#### **WEBBEZ**





tsitaty/www.gubernator33.ru/deyatelnost/svetlana-oriova-neobkhodimo-navesti-poryadok-v-seiskikh-shkolakn/www.gubernator33.ru/deyatelnost/svetlana-oriova-regionalnaya-vlast-pomozi qus-khrustalnomu-stat-qorodom-masterov1

/deyatelnost/svetlana-orlova-gastroli-odnogo-iz-luchshikh-teatrov-strany-sovremennika-znakovoe-sobytie-v-kulturno~

/tsitaty/www.qubernator33.ru/deyatelnost/www.qubernator33.ru/deyatelnost/svetlana-orlova-regionalnaya-vlast-pomozhet-qus-khrustalnomu-stat-gorodom-masterovtest

Возможно, некоторые из них являются устаревшими или только тестируются.

Они могут представлять опасность.

Анализ robots txt

Время обнаружения: 2018-02-08 04:08:02

Проверка файла robots.txt.

Найдены следующие объекты, запрещенные для индексирования:

/dlya-smi/onlayn-translyatsiya/

Уязвимости системы управления сайтом Время обнаружения: 2018-02-08 06:48:31

Система управления сайтом: 1C-Bitrix.

Версию систему управления определить не удалось.

Резервные копии конфигурационного файла НЕ обнаружены.

Обратите внимание на следующие факты:

Панель администрирования доступна для всех по адресу:

http://gubernator33.ru/bitrix/admin/

Обнаружены следующие угрозы безопасности:

Для панели администрирования установлен типовой логин и пароль: admin 123456

Госструктура

http://webbez.ru/1403rep/govaushduihfu.php | Отредактировать новость | Снять новость с публикации | Отредактировать источник || Выгрузить отчет Уведомление поолучили: Borneo | Dasha |

