Современный кибертеррорист: кто он и как его победить?

Антон Дьяков
Руководитель направления развития решений информационной безопасности, АО «РНТ»

Кибероружие

КИБЕР ТЕРРОРИСТ

ТРОЯН

Средства доставки

Вредонос

Атакующая головка

ПОЛЬЗОВАТЕЛЬ

Распространение кибероружия

БИРЖИ УЯЗВИМОСТЕЙ

РЕСУРСЫ СКРИПТ-КИДДИ

ОФИЦИАЛЬНЫЕ ЗАЯВЛЕНИЯ И НЕОФИЦИАЛЬНЫЕ ПУБЛИКАЦИИ

Ресурсы скрипт-кидди

РЕСУРСЫ ДЛЯ СКАЧИВАНИЯ КИБЕР-ОРУЖИЯ

Такие как:

Сайты

Softxaker и проч.

ПРОГРАММЫ ДЛЯ АУДИТА БЕЗОПАСНОСТИ

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

фонтанка.ру
www.fontanka.ru

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

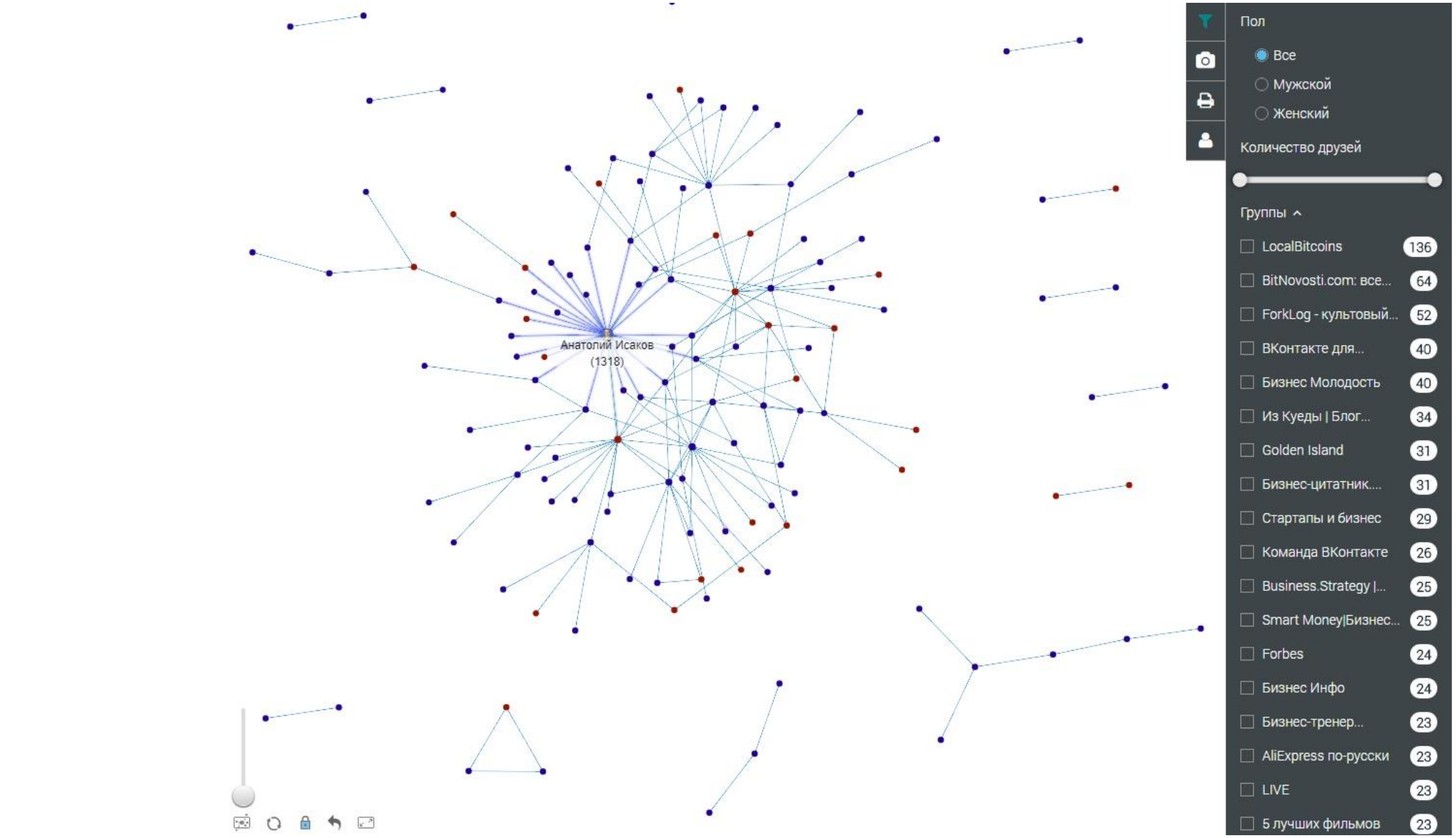
Многие гиганты современной IT индустрии, такие как Intel, AMD, Microsoft и прочие, публикуют информацию о собственных уязвимостях обновлениях.

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

Рассмотрим на примере нашумевшего WannaCry

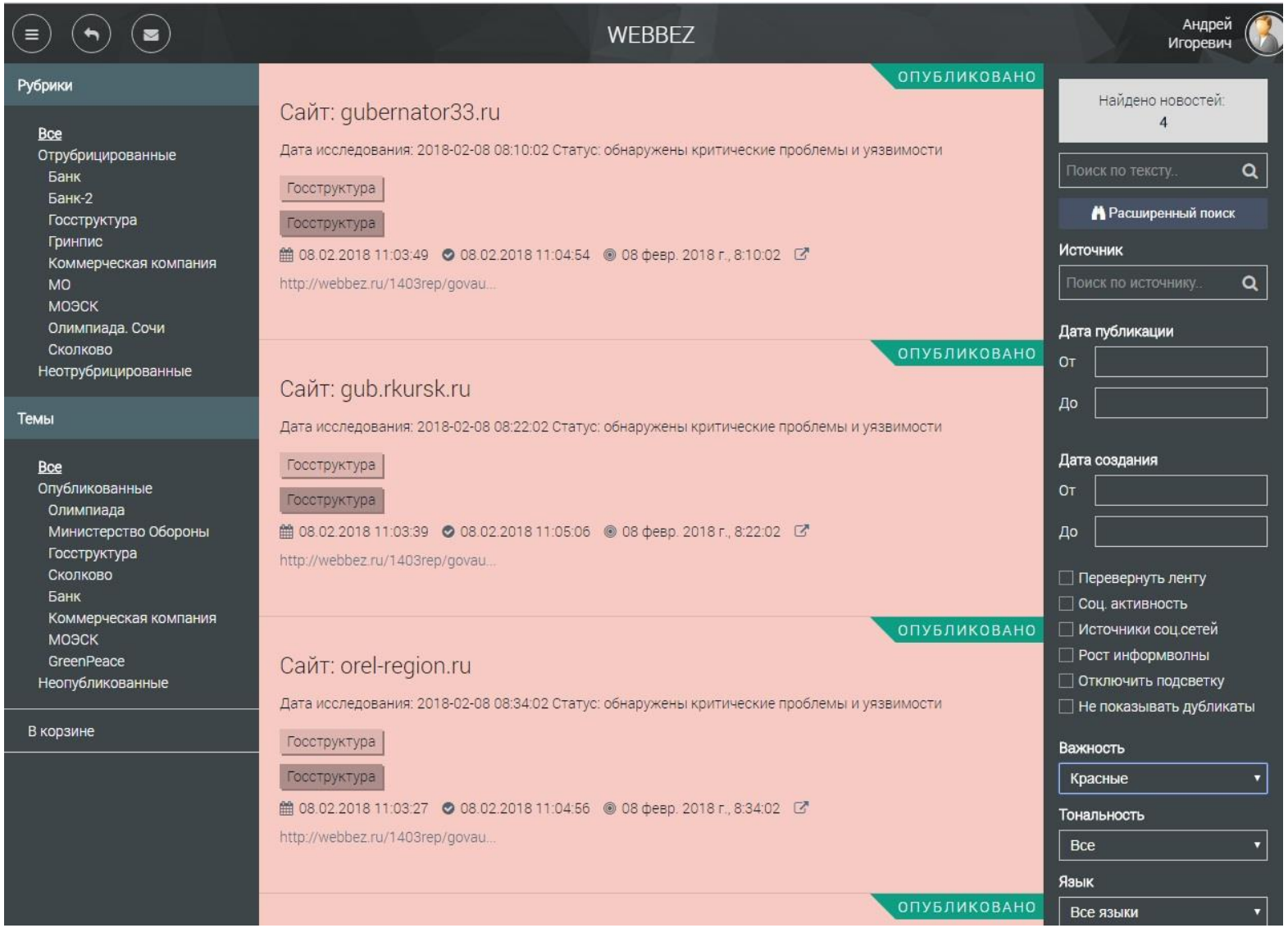
Хронология неминуемой угрозы

Информационный портрет киберпреступника

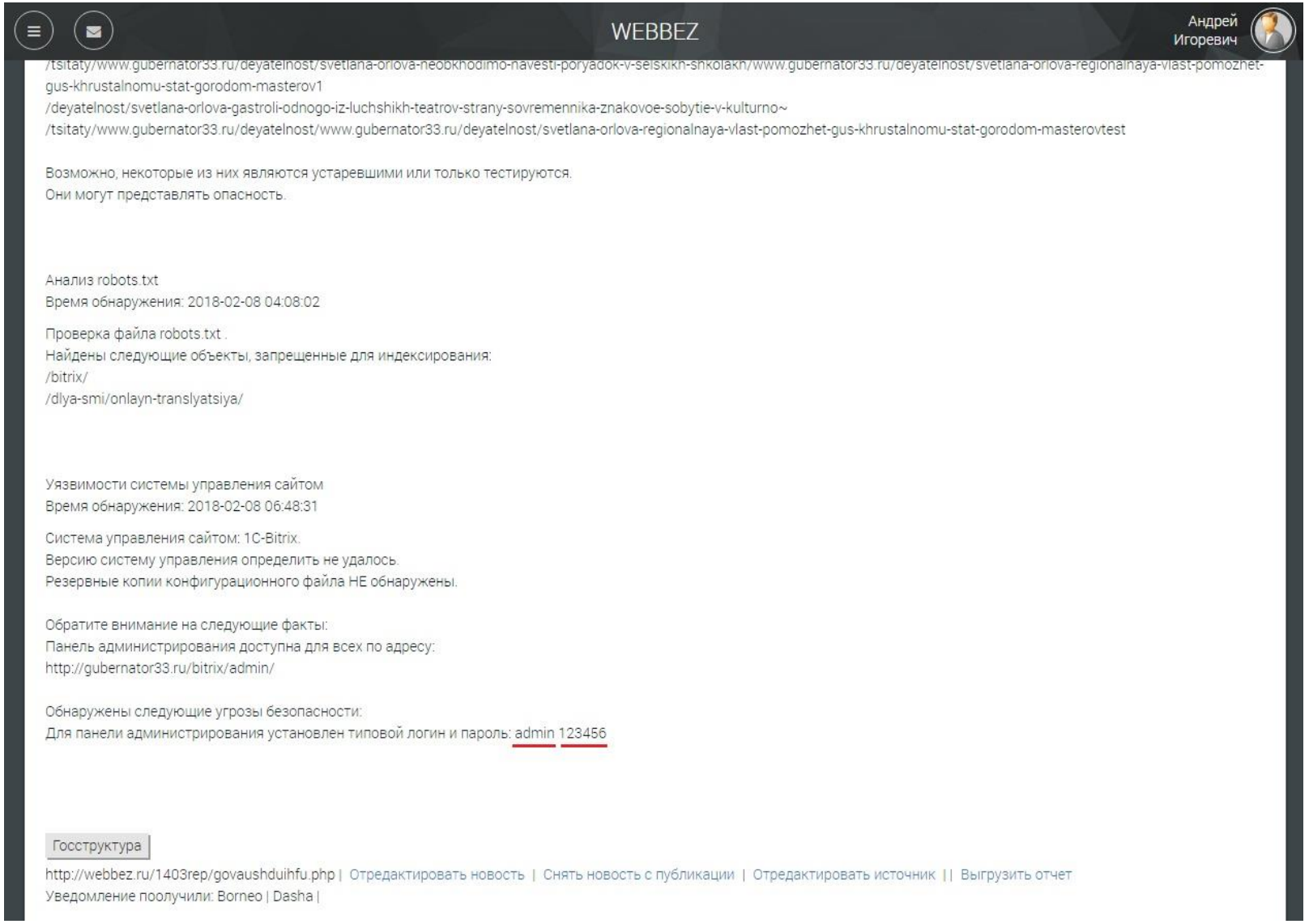


Безопасность российских учреждений и предприятий

Пример «будущего пациента»



Пример «красной» уязвимости



ТЕРРИТОРИЯ БЕЗОПАСНОСТИ

129515, Москва,
2-я Останкинская улица, д.6
+7 (495) 777 75 77
rnt@rnt.ru
www.rnt.ru

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ