Расследование киберпреступлений: «виртуальная» реальность

Сушко Александр Евгеньевич

Начальник управления
по расследованию преступлений
против информационной безопасности и интеллектуальной собственности
ГСУ Следственного комитета Республики Беларусь

Следственный комитет Республики Беларусь

Развитие информационно-коммуникационных технологий

Масштаб и количество киберпреступлений, устройств, пользователей и потерпевших

Транснациональность и экстерриториальность, юрисдикция

Big data

Cloud

Интернет вещей

Следственный комитет Республики Беларусь

Приватность

Peer-to-peer/Virtual Private Networks/Darknet

?

Anonymizers (TOR, I2P)

?

Encryption/Bitcoin

VOIP

?

IPv4/IPv6

Безопасность, обучение, дети

Cybercrime and e-evidence

Следственный комитет Республики Беларусь

Беларусь поднялась в мировом рейтинге развития информационных технологий

30 ноября 2015 в 17:34

42.TUT.BY

Международный союз электросвязи представил ежегодный отчет по индексу развития информационно-коммуникационных технологий (ИКТ). Согласно его данным, Беларусь опередила Россию, Украину, Казахстан и заняла 36 место в рейтинге.

http://42.tut.by/474977

Следственный комитет Республики Беларусь

Microsoft

$ 407 000 000 000

Следственный комитет  Республики Беларусь

Alphabet

Google™

$ 500 100 000 000

Следственный комитет  Республики Беларусь

Apple

$ 586 000 000 000

Следственный комитет Республики Беларусь

Газпром

$ 57 100 000 000

Следственный комитет  Республики Беларусь

Wargaming.net

Следственный комитет  Республики Беларусь

Viber

Следственный комитет

Республики Беларусь

MSQRD

Следственный комитет Республики Беларусь

Хакеры украли у банков почти 2 млрд руб. с помощью «писем от ЦБ»

За последние полгода, с августа 2015 по февраль 2016 года, при помощи вируса Buhtrap хакеры совершили 13 успешных атак на российские банки, в результате которых похитили 1,8 млрд руб., сообщает в своем отчете компания Group-IB, которая занимается расследованием компьютерных преступлений.

Подробнее на РБК:
http://www.rbc.ru/finances/17/03/2016/56e97c089a794797e5b8e6b3

Следственный комитет Республики Беларусь

Ущерб от вируса Buhtrap

600 млн руб. — максимальная сумма хищения у российского банка в 2016 году

25,6 млн руб. — минимальная сумма хищения у российского банка в 2016 году

143 млн руб. — средняя сумма успешного хищения у банка

1 млрд руб. — сумма хищений, которые удалось остановить в январе 2016 года

Годовые затраты банков на эффективные средства предотвращения атак в 28 раз меньше, чем средний прямой ущерб от одной целенаправленной атаки.

Подробнее на РБК:
http://www.rbc.ru/finances/17/03/2016/56e97c089a794797e5b8e6b3

Следственный комитет Республики Беларусь

Российский "Металлинвестбанк", входящий в топ-100 крупнейших кредитно-финансовых учреждений страны, подвергся беспрецедентной хакерской атаке. Злоумышленникам удалось вывести из него рекордную сумму - более 677 миллионов российских рублей, что по курсу составляет 9,4 миллиона долларов, передает информагентство «РИА-Новости».

11:01 05.03.2016

Следственный комитет Республики Беларусь

Число хакерских атак на участников финансового рынка РФ будет расти в ближайшие годы, предупредил глава Сбербанка Герман Греф во вторник.

«Нападений, очевидно, станет больше на всех участников финансового рынка», — сказал Греф, пояснив, что рост числа кибератак на финансовые организации связан с глубоким проникновением Интернета на рынки.

Сейчас в мире действует примерно 40 млн. киберпреступников, потери от их деятельности составили около 500 млрд. долларов в 2015 году, 5 млрд. долларов из которых приходятся на Россию, указал Греф.

В 2018 году потери участников финрынков от действий кибермошенников могут возрасти до 1 трлн долларов, предупредил глава Сбербанка.

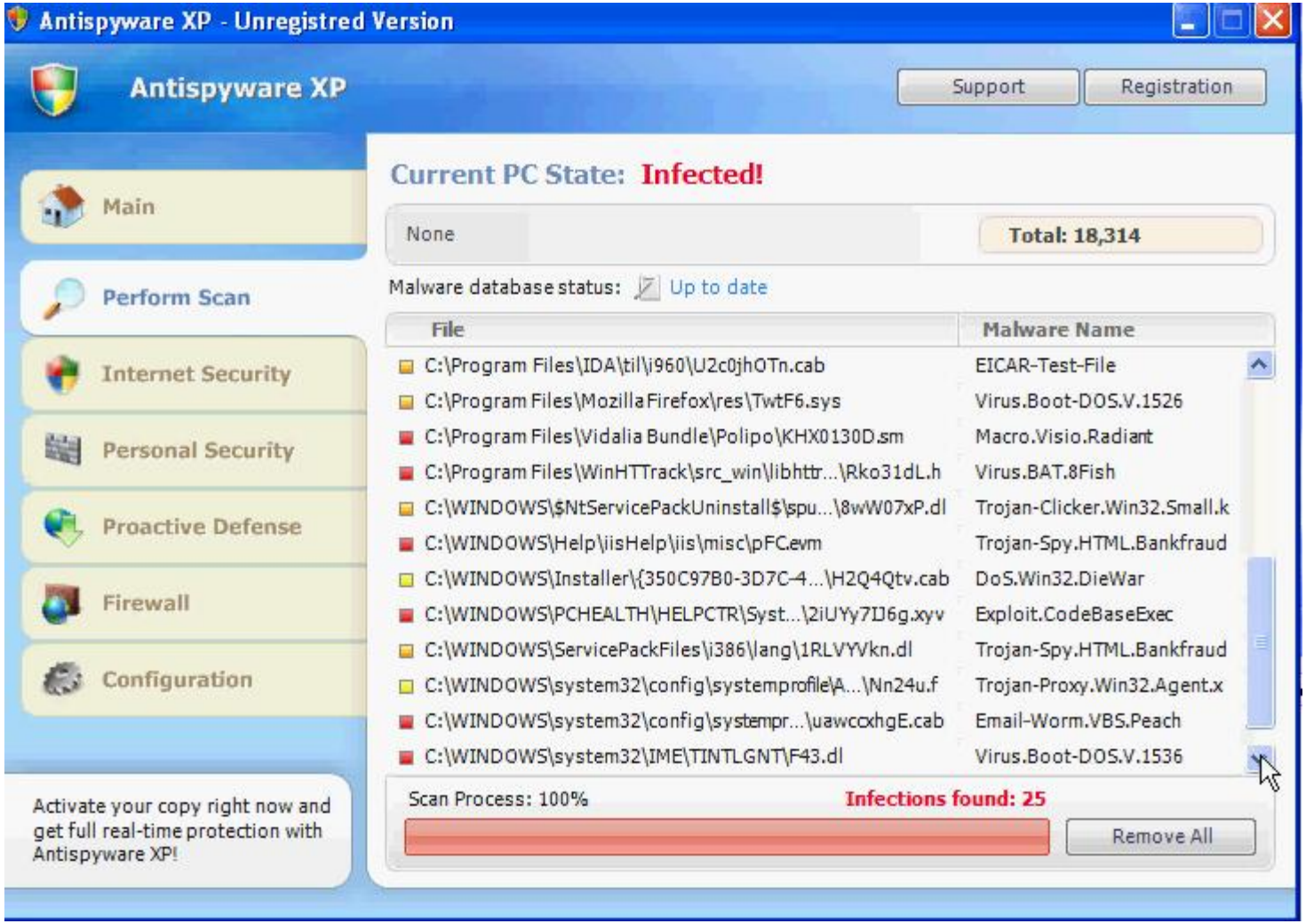
12.04.2016 15:35
http://www.banki.ru/news/lenta/?id=8849344

Следственный комитет Республики Беларусь

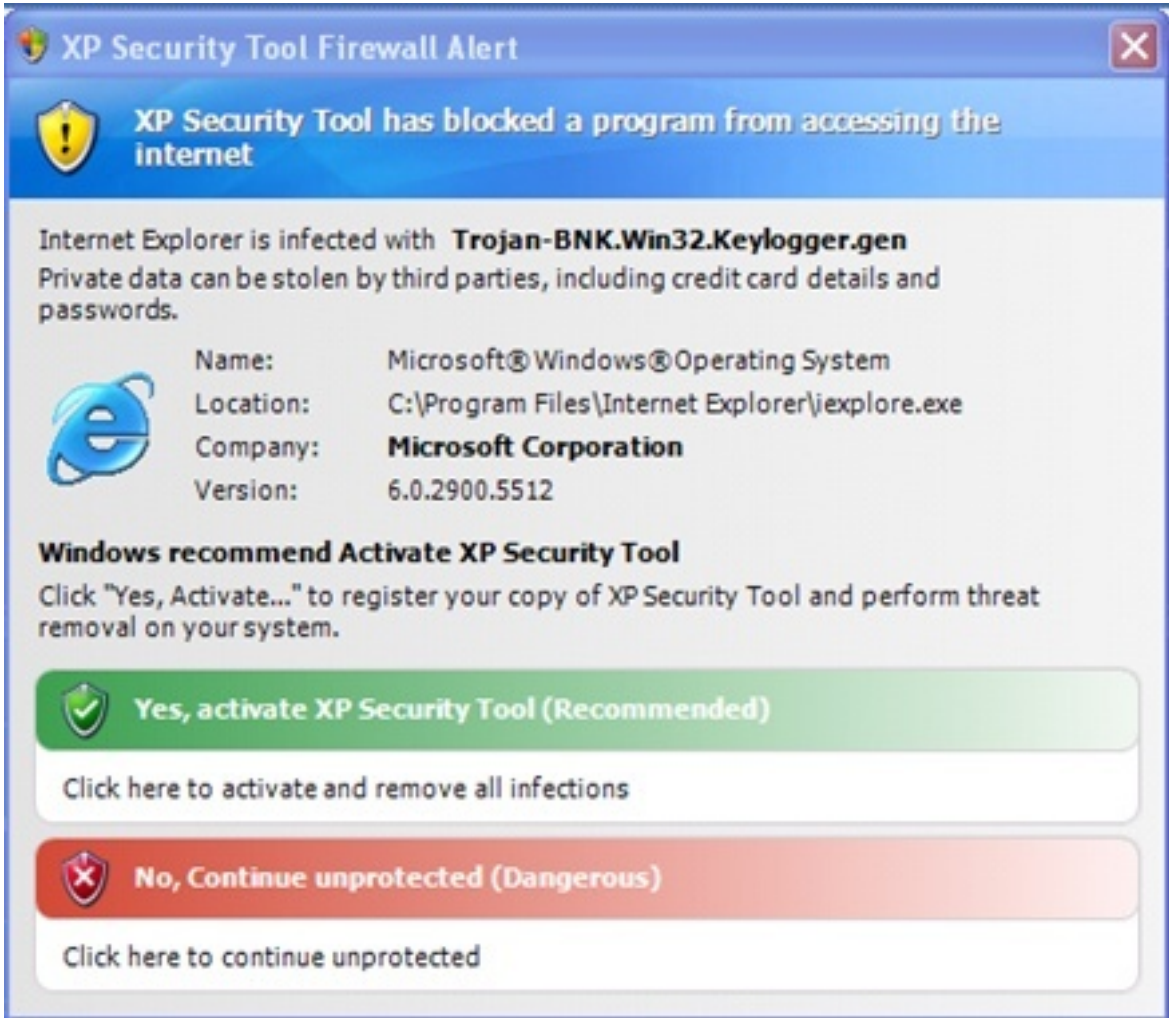
CASE
Фальшивый антивирус

Следственный комитет

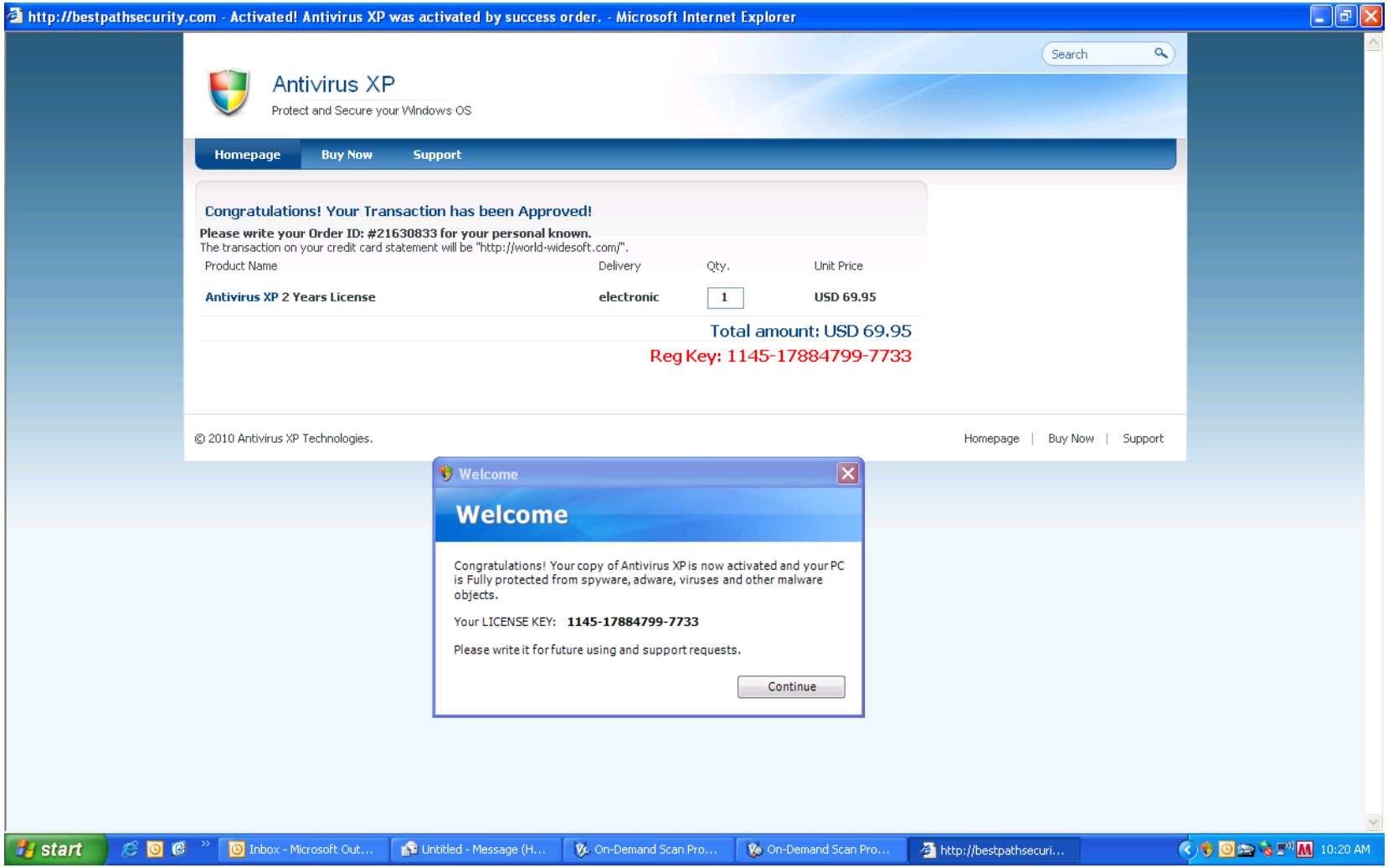
Республики Беларусь



Следственный комитет Республики Беларусь



Следственный комитет Республики Беларусь



Следственный комитет Республики Беларусь

ОСНОВНОЙ СЕРВЕР (ГЕРМАНИЯ)

БОЛЕЕ **500** СЕРВЕРОВ РАЗМЕЩЕНИЯ ВЕРСИЙ ВРЕДОНОСНОЙ ПРОГРАММЫ

БОЛЕЕ **170** САЙТОВ ОНЛАЙН-МАГАЗИНОВ ПО «ПРОДАЖЕ» «ФАЛЬШИВОГО АНТИВИРУСА»

БОЛЕЕ **40** САЙТОВ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

БОЛЕЕ **35** СЕРВЕРОВ ХРАНЕНИЯ РЕКВИЗИТОВ ПЛАТЕЖНЫХ КАРТ

Следственный комитет Республики Беларусь

БОЛЕЕ **2,5 МЛРД.**

ЗАРАЖЕННЫХ КОМПЬЮТЕРОВ

БОЛЕЕ **260.000** ПОСТРАДАВШИХ ЛИЦ,

ПРОЖИВАЮЩИХ В **125** ГОСУДАРСТВАХ МИРА

У КОТОРЫХ ПОХИЩЕНО

БОЛЕЕ **18 МЛН.** ДОЛЛАРОВ США

Следственный комитет Республики Беларусь

Следственный комитет Республики Беларусь

1 (Минск)

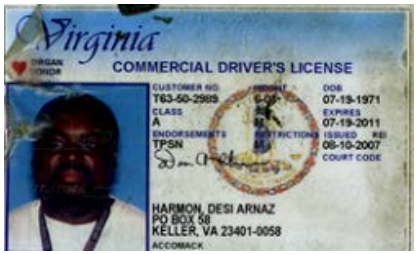
Вебмани,
ICQ(РФ)

2(Киев)

3 (Прага)

карта,
Канада

Skype(Люксембург)



Штат Филадельфия
США

apple.com
(Нью-Йорк США)

Gmail.com(штат
Калифорния США)

Почта (Литовская
Республика)

Следственный комитет Республики Беларусь

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Начальник управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности ГСУ Следственного комитета Республики Беларусь
Александр Сушко

Контактный телефон: +375 17 3895061
email: cybercrime@sk.gov.by

Следственный комитет Республики Беларусь