

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](http://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 Vuhtrap 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

Antispyware XP - Unregistered Version

Antispyware XP

Support Registration

Main

Perform Scan

Internet Security

Personal Security

Proactive Defense

Firewall

Configuration

Activate your copy right now and get full real-time protection with Antispyware XP!

Current PC State: Infected!

None **Total: 18,314**

Malware database status: Up to date

File	Malware Name
C:\Program Files\IDA\ti\i960\U2c0jhOTn.cab	EICAR-Test-File
C:\Program Files\Mozilla Firefox\res\TwtF6.sys	Virus.Boot-DOS.V.1526
C:\Program Files\Vidalia Bundle\Polipo\KHX0130D.sm	Macro.Visio.Radiant
C:\Program Files\WinHTTrack\src_win\libhtr...\Rko31dL.h	Virus.BAT.8Fish
C:\WINDOWS\$NtServicePackUninstall\$\\$pu... \8wW07xP.dl	Trojan-Clicker.Win32.Small.k
C:\WINDOWS\Help\iisHelp\iis\misc\pFCevm	Trojan-Spy.HTML.Bankfraud
C:\WINDOWS\Installer\{350C97B0-3D7C-4... \H2Q4Qtv.cab	DoS.Win32.DieWar
C:\WINDOWS\PCHEALTH\HELPCTR\Syst... \2iUYy7D6g.xyv	Exploit.CodeBaseExec
C:\WINDOWS\ServicePackFiles\j386\lang\1RLVYvkn.dl	Trojan-Spy.HTML.Bankfraud
C:\WINDOWS\system32\config\systemprofile\A... \Nn24u.f	Trojan-Proxy.Win32.Agent.x
C:\WINDOWS\system32\config\systempr... \uawcoxhgE.cab	Email-Worm.VBS.Peach
C:\WINDOWS\system32\IME\TINTLGNT\F43.dl	Virus.Boot-DOS.V.1536

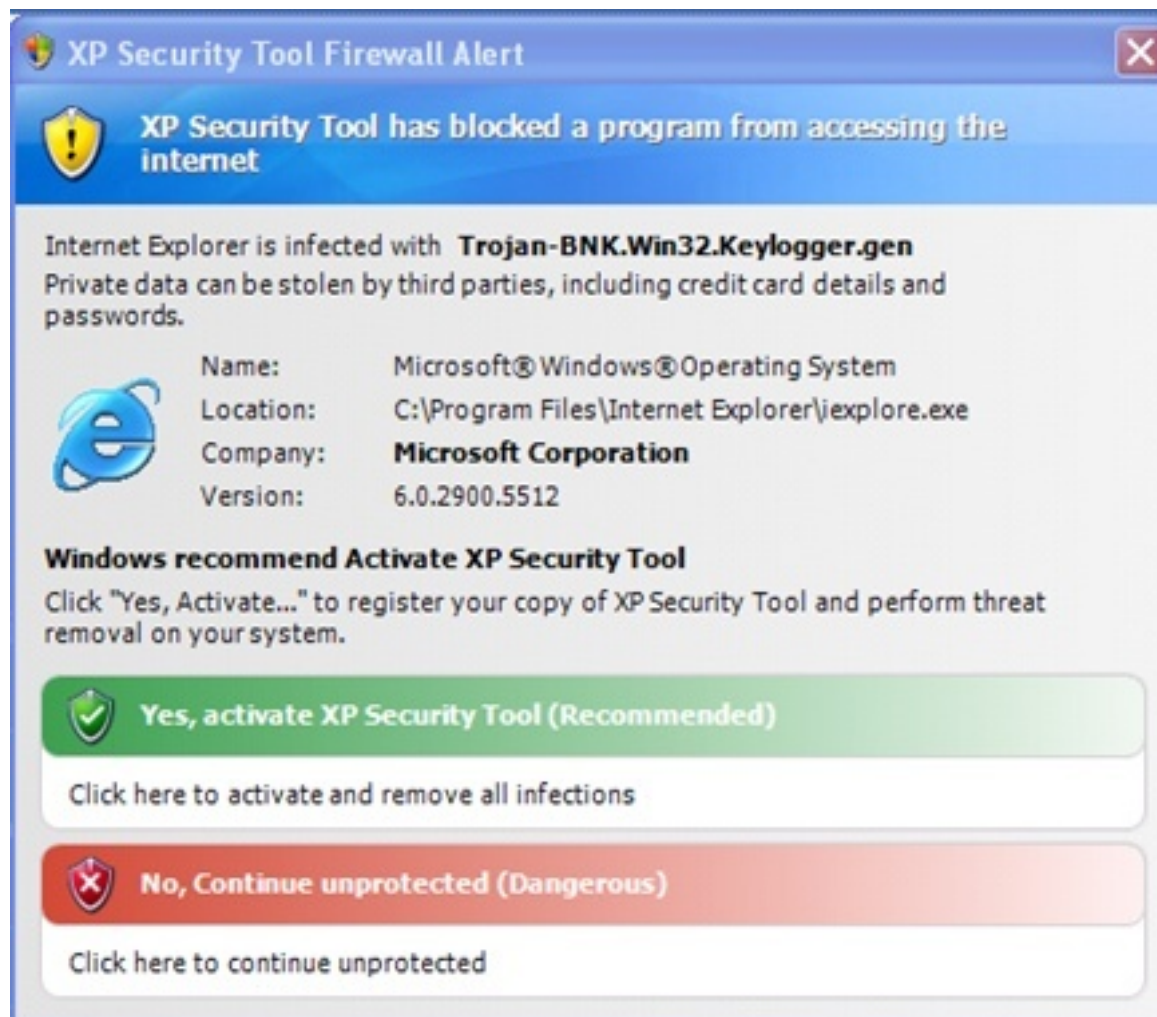
Scan Process: 100% **Infections found: 25**

Remove All

Следственный комитет



Республики Беларусь



Следственный комитет



Республики Беларусь

http://bestpathsecurity.com - Activated! Antivirus XP was activated by success order. - Microsoft Internet Explorer

Antivirus XP
Protect and Secure your Windows OS

Homepage Buy Now Support

Congratulations! Your Transaction has been Approved!
Please write your Order ID: #21630833 for your personal known.
The transaction on your credit card statement will be "http://world-widesoft.com/".

Product Name	Delivery	Qty.	Unit Price
Antivirus XP 2 Years License	electronic	1	USD 69.95

Total amount: USD 69.95
Reg Key: 1145-17884799-7733

© 2010 Antivirus XP Technologies. Homepage Buy Now Support

Welcome

Welcome

Congratulations! Your copy of Antivirus XP is now activated and your PC is Fully protected from spyware, adware, viruses and other malware objects.

Your LICENSE KEY: **1145-17884799-7733**

Please write it for future using and support requests.

Continue

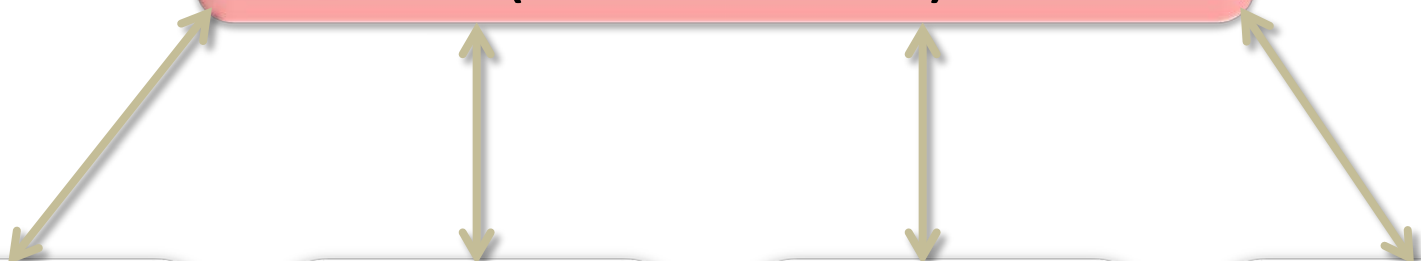
start | Inbox - Microsoft Out... | Untitled - Message (H... | On-Demand Scan Pro... | On-Demand Scan Pro... | http://bestpathsecu... | 10:20 AM

Следственный комитет



Республики Беларусь

ОСНОВНОЙ СЕРВЕР (ГЕРМАНИЯ)



БОЛЕЕ

500

СЕРВЕРОВ
РАЗМЕЩЕНИЯ
ВЕРСИЙ
ВРЕДНОСНОЙ
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

ОРГАНИЗАТОР ОПГ



АДМИНИСТРАТОРЫ
СЕРВЕРОВ

РАЗРАБОТЧИКИ
«ФАЛЬШИВОГО
АНТИВИРУСА»

ТЕХ. ПОДДЕРЖКА

РАСПРОСТРАНТЕЛИ
«ФАЛЬШИВОГО АНТИВИРУСА»
(ОКОЛО 100 ЛИЦ)

ПРОЦЕССИНГОВАЯ
КОМПАНИЯ

«МАСТЕРБАНК»

ФИРМЫ-
ОДНОДНЕВКИ

Следственный комитет



Республики Беларусь



1 (Минск)

Вебмани,
ICQ (РФ)



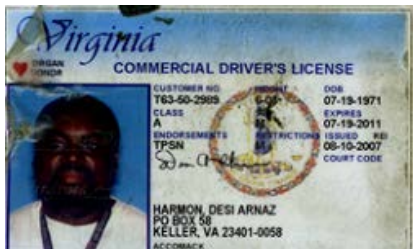
2 (Киев)

карта,
Канада



3 (Прага)

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