



► **cybercrime section**

КРЪГЛА МАСА

"Състояние и проблеми на сигурността в киберпространството на България"

**"Организираната киберпрестъпност -
заплаха за националната
сигурност"**

Централен военен клуб

София 28.09.2010



► cybercrime section

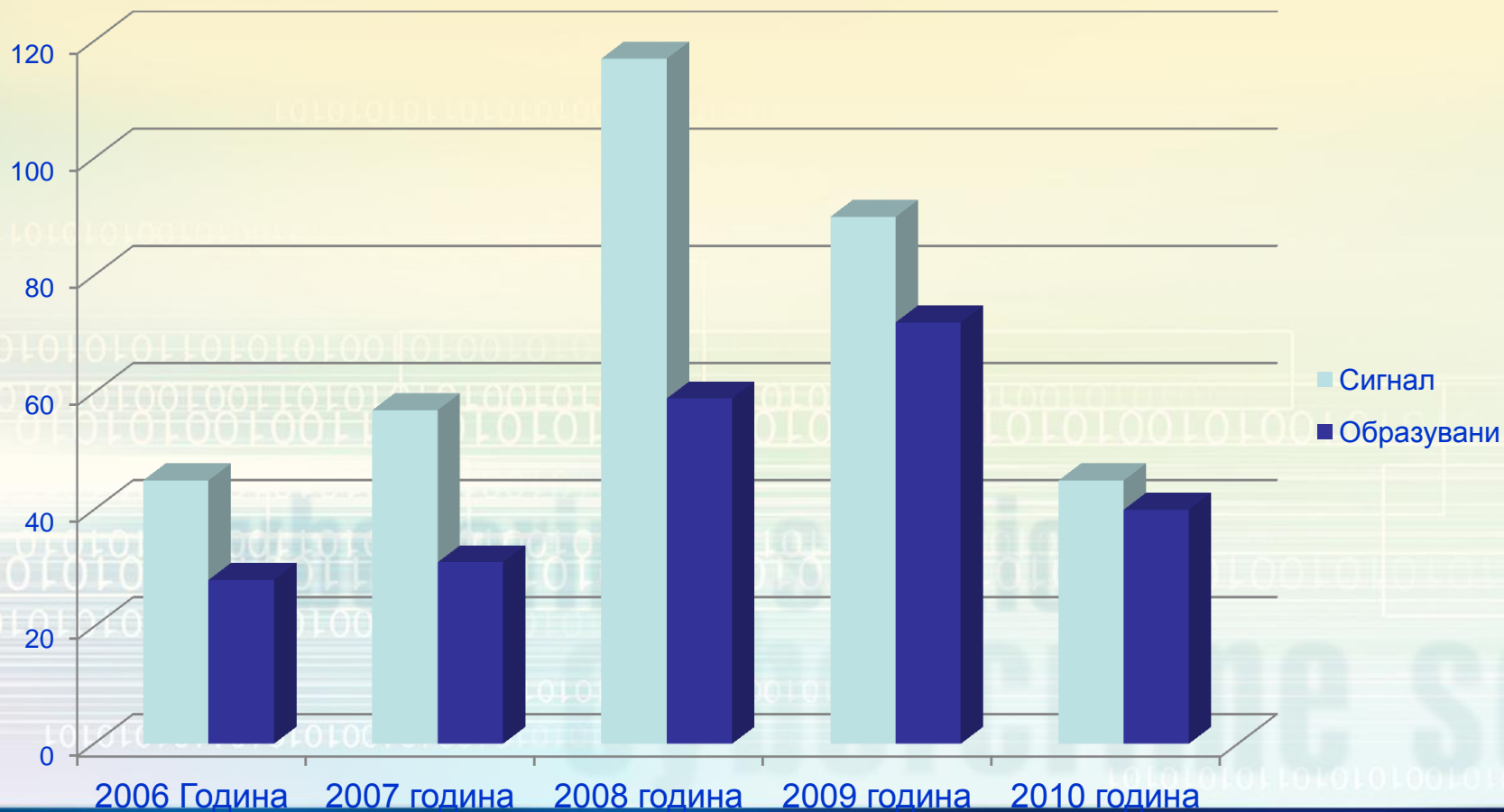
ТЕНДЕНЦИИ

- НАД 1 МЛРД. ДУШИ ИМАТ ДОСТЪП В СВЕТА
- Над 1 000 000 ТОЧКИ НА ДОСТЪП ДО ИНТЕРНЕТ В БЪЛГАРИЯ
- Над 40% ОТ НАСЕЛЕНИЕТО С ДОСТЪП ДО ИНТЕРНЕТ – Около 3 МЛН.
- УСТОЙЧИВО УВЕЛИЧАВАНЕ НА КИБЕРПРЕСТЪПЛЕНИЯТА



cybercrime section

ТЕНДЕНЦИИ





cybercrime section

Правна рамка

- **КОНСТИТУЦИЯ НА РЕПУБЛИКА БЪЛГАРИЯ**
- **КОНВЕНЦИЯ ЗА ПРЕСТЪПЛЕНИЯ В КИБЕРНЕТИЧНОТО ПРОСТРАНСТВО НА СЪВЕТА НА ЕВРОПА ОТ 23.11.2001 ГОДИНА**
- **НАКАЗАТЕЛЕН КОДЕКС**
- **НАКАЗАТЕЛНО – ПРОЦЕСУАЛЕН КОДЕКС**
- **ЗАКОН ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ**
- **ЗАКОН ЗА ЗАКРИЛА НА ДЕТЕТО**
- **ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**
- **ЗАКОН ЗА ЕЛЕКТРОННИЯ ДОКУМЕНТ И ЕЛЕКТРОННИЯ ПОДПИС**
- **ЗАКОН ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ**
- **ЗАКОН ЗА ЕЛЕКТРОННАТА ТЪРГОВИЯ**
- **ЗАКОН ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ**
- **ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА И ДР.**



cybercrime section

Структура на Сектора за противодействие на киберпрестъпността

Н-к Сектор

Екип I
"Компютърни измами финансови престъпления и хазарт"
Чл.212 а, 327 от НК

Екип II
"ПРИХВАЩАНА ЕЛЕКТРОННИ ДАННИ, НЕРЕГЛАМЕНТИРАН ДОСТЪП, ПРОМЯНА И УНИЩОЖАВАНЕ НА КОМПЮТЪРНО - ИНФОРМАЦИОННИ ДАННИ, ВЪВЕЖДАНЕ НА КОМПЮТЪРНИ ВИРУСИ, РАЗПРОСТРАНЕНИЕ НА СИСТЕМНИ ПАРОЛИ /чл.216 и гл.9 А от НК/

Екип III
Сексуално насилие , насаждане на расова и религиозна омраза в интернет
/чл.143;144;159;162;164;327 от НК/

Екип IV
Престъпления срещу интелектуалната собственост "
Чл.172А от НК

Екип V
"Информация и анализ и НКП 24/7"



► **cybercrime section**

Регионални структури





► cybercrime section

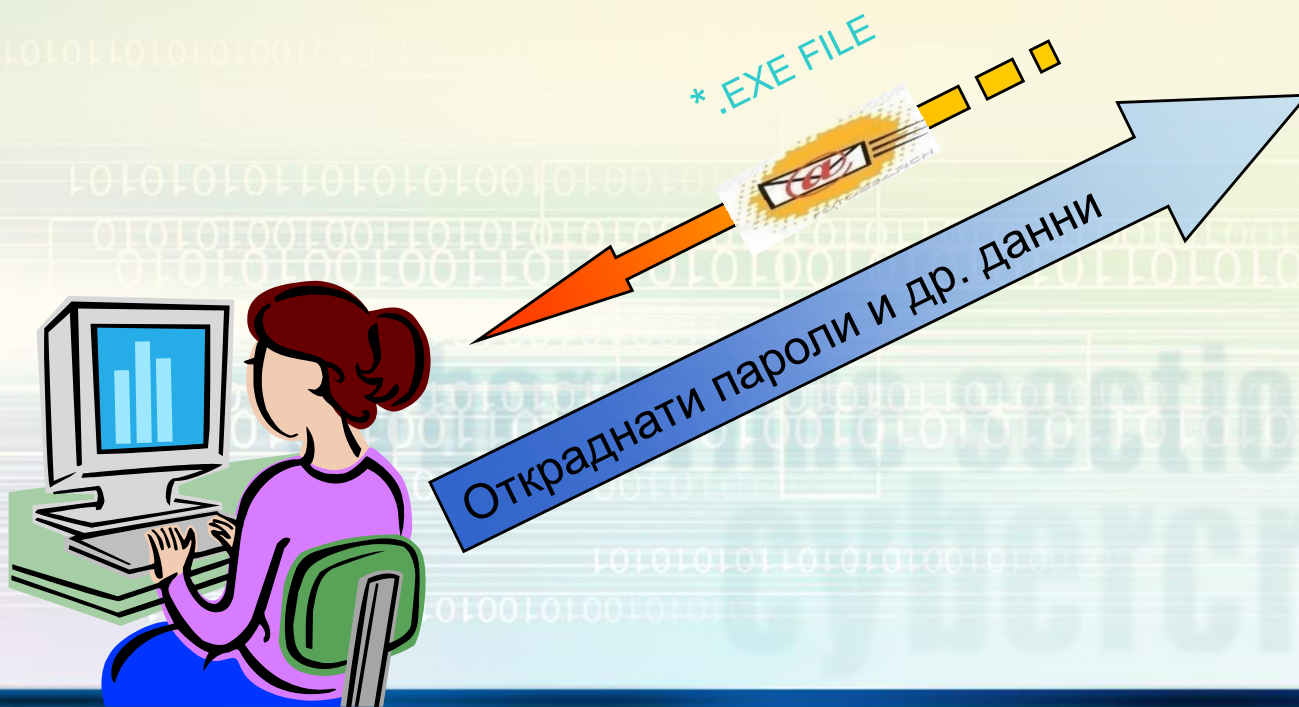
Кражба на банкови сертификати - Механизъм на атаката

- Заразяване на компютъра на жертвата с троянски кон например от типа - **Trojan.Pws.Sinowal**
- Изпращане на събраната информация, потребителски имена, пароли, сертификати и др. на сървър, контролиран от ОПГ
- Финансови агенти продават или използват събраната информация
- Наемане на "човешки проксита" или "мулета", които усвояват средствата и ги препращат на ОПГ чрез компании за международни валутни преводи /WU или MG/



cybercrime section

Схема на заразяване с Троянски кон





► **cybercrime section** ПРИМЕР

Анализ на компютъра на жертвата М. С.

Програмата е била активна в периода от 5 юни 2006г до 16 февруари 2007г.

През това време е събрана и изпратена следната информация:

- Адресна книга : 169 пъти
- Списък със запомнените пароли на браузъра: 169 пъти
- SSL сертификат: 402 пъти
- Номер на кредитна карта: 22 пъти
- Както и голям брой пароли за интернет сайтове, фрагменти от частна комуникация и т.н.



cybercrime section

Способи на заразяване

- Чрез спам мейли с прикачен файл.
- Сваляне на файлове /музика ,филми, софтуер/ посредством P2P /торенти/
- Чрез страници, които наподобяват сайтове – социални мрежи като Facebook. В момента в който потребителя щракне на линк обаче, получава съобщение да обнови Flash плейъра на браузера си и троянският кон се инсталира на компютъра му
- Чрез въвеждане на троянския кон от флаш-памет от лице имащо достъп до компютъра – служител на фирма за поддръжка или доставчик на интернет.





► cybercrime section

Набиране на човешки проксита

- По данни на Европол тази дейност отнема над 60 % процента от времето за подготовка на атаката
- Чрез обяви в сайтове за работа или сайтове за запознанства се предлага търговско представителство.
- Сключва се договор съдържащ реквизитите на истински договор за търговско представителство.
- Комисионната за мулето варира между 5 и 10 %.
- В България до момента няма осъдено муле.
- Тенденцията в 2010 год. към ограбване на сметки в чужбина/ основно Германия/ чрез бг мулета.



► cybercrime section

СТАТИСТИКА

- 63 отработени сигнала в периода май – ноември 2007
- обща стойност на измамите около 1 400 000 лв.
- 400 000 лв. са блокирани от банките
- 200 000 лв. са предотвратени от ГДБОП
- 800 000 лв. са изтекли към ОПГ в страни от ОНД.



► cybercrime section

Мерки на банките за подобряване на сигурността

- Въвеждане на хардуерна защита на банковите сертификати /универсален електронен подпис/.
- Еднократни пароли чрез one-time password (OTP)
- Разяснителна кампания на сайтовете за интернет банкиране
- Използване на лицензирани ОС и антивирусен софтуер.
- SMS и e-mail известяване
- Контрол и строги проверки на новооткрити банкови сметки, по които има наредени еднократни преводи.
- Контрол на суми, близки по размер на сумите, за които се изисква потвърждение.



► cybercrime section

ПРЕДЛОЖЕНИЯ НА ЕКСПЕРТА

- Създаване на национални платформи и общоевропейска платформа за сигнализация на компютърни престъпления, свързана с националните.
- Създаването на различни мрежи за комуникация в реално време, с цел по – добро взаимно опознаване между конкретните участници и обмен на експертиза в конкретни области на киберпрестъпността, като напр. – мрежа на началниците на отдели за борба с компютърните престъпления; мрежа на техническите експерти, мрежа на полицаи работещи по противодействие на киберпрестъпността и др.
- Изработване на общоевропейски легални дефиниции на понятия от областта на киберпрестъпността.
- Въвеждане на задължения за сътрудничество и съдействие от страна на ДЕСУ и полицията.
- Създаване двустранни и с участие на повече от две страни /Европол/ на съвместни екипи за разследване на трансгранични киберпрестъпления.



cybercrime section

ПРОЕКТЪТ CYBERCRIME.BG

Борба с компютърни престъпления | Cyber Crime - Mozilla Firefox

http://www.cybercrime.bg/bg

Начало | Карта на сайта | Контакти

CyberCrime
Официален сайт за Борба с компютърните престъпления

Подий сигнал
за всяко киберпрестъпление

Какво е ФИШИНГ и как да се предпазим от него? Кои са другите дигитални заплахи в ИНТЕРНЕТ, как да ги разпознаваме и неутрализираме? [[Чакан повече](#)]

Интернет заплахи

Защитени ли са децата ни в глобалната мрежа? Какво трябва да знаеат децата и техните родители за безопасното използване на интернет? [[Чакан повече](#)]

Експлоатация на деца

Цели на сайта

Целта на този уебсайт е да предостави полезна информация при борбата с компютърни престъпления, фишинг, сексуална експлоатация на деца, престъпления срещу интелектуалната собственост и незаконен азарт. Тук можете да отпирете отговори как да процедираме ако интернет сайта?]

[Прочети повече](#)

Новини

Крадат милиони през мейла
25.05.2010
Статия на МОНИТОР от 25.05.2010 г. с автори Георги Ангелов и Йордан Йочев Никер[...]

[Прочети цялата новина](#)

1 2 3 [Други новини](#)

Последно видео [Всички клипове](#)

Интернет заплахи · Експлоатация на деца · ФИШИНГ · Незаконен азарт · Интелектуална собственост · Кибертероризъм · Новини · Видео · Благодарности · Контакти

© 2010 Cybercrime.bg · Всички права запазени · Карта на сайта

Уеб дизайн и оптимизация от СТЕНИК

https://www.linkedin.com/secure/login?trk=hb_signin

start | Борба с компютърн... | Kaspersky: Internet S... | Борба с компютърн... | P:\ | Microsoft PowerPoint

06:14



► **cybercrime section**

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!

Главен инспектор Явор Колев,
Началник сектор “Компютърни престъпления ,
интелектуална собственост и хазарт” при
Главна Дирекция “Борба с организираната
престъпност” - МВР

Сл.тел. : +35929828342

GSM : +359888795021

E-mail chief@cybercrime.bg

Web site www.cybercrime.bg

icq 48495113

Skype ID: javor.v.kolev