

Како криминалците ја користат технологијата



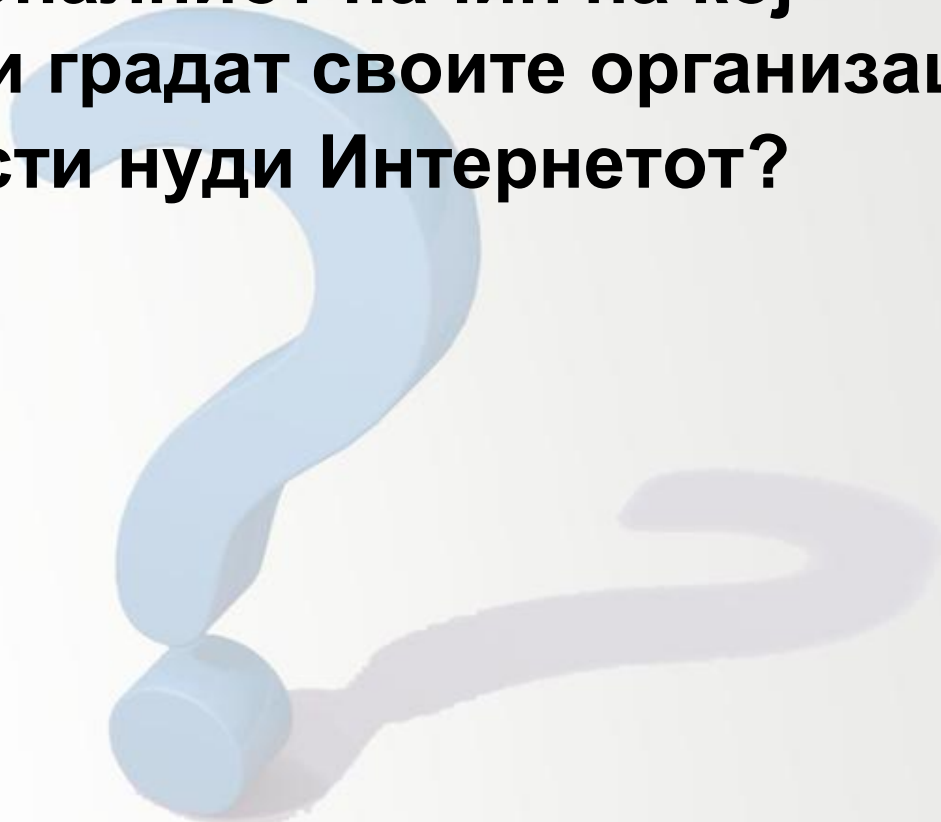
Цел на Модулот

- По завршетокот на презентацијата за овој модул, ќе знаете да опишете на кој начин терористите и другите криминалци го користат Интернетот и останатата технологија за целите на планирање и извршување кривични дела



Дискусија: Регрутација на терористи

- Кој е традиционалниот начин на кој терористите ги градат своите организации?
- Какви предности нуди Интернетот?



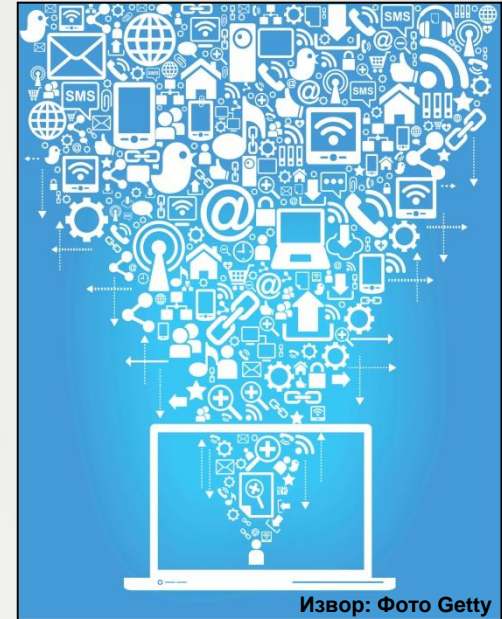
Зошто терористичките организации ја користат технологијата

- Дистрибуција на пропаганден материјал
- Регрутација
- Комуникација
- Собирање финансиски средства
- Обука
- Чување информации
- Споделување тактики
- Координација на нападите
- Идентификација на цели за напад
- Реализација на компјутерски упади
- Финансирање на операциите преку компјутерски криминал



Техники: Светска компјутерска мрежа

- **Овозможува:**
 - Лесна размена на информации
 - Евтина алтернатива на традиционалните медиуми
 - Глобална публика (предмет на примена на различни закони и начини на нивно спроведување во пракса)



Техники: Шифрирање

- Бесплатни онлајн софтверски пакети на располагање
- Речиси невозможни за дешифрирање доколку ја немате лозинката



Техники: VoIP и Video Chat (видео чет)

- Овозможуваат слободни и бесплатни комуникации на било која локација
- Комуникацијата е шифрирана и законското пресретнување на истата е многу тешко



Извор: Фото Getty

Техники: Застапници (прокси) и Тунели

- Пренасочување на комуникацијата преку друга локација, со што следењето на изворот оди потешко



Активност: Студија на случај за технологија

Погледнете:
Прилог 3.1

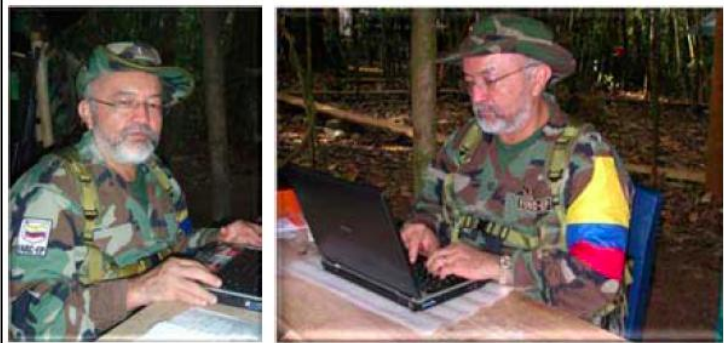


- **Упатство: Работејќи во поединечни тимови:**
 - Разгледајте ги клучните факти и информации во врска со заплената на преносниот компјутер на FARC (Револуционерни вооружени сили на Колумбија)
 - Одговорете на поставените прашања за потребите на дискусијата
 - Бидете подготвени своите одговори да ги споделите со останатите учесници по истекот на 10 минути

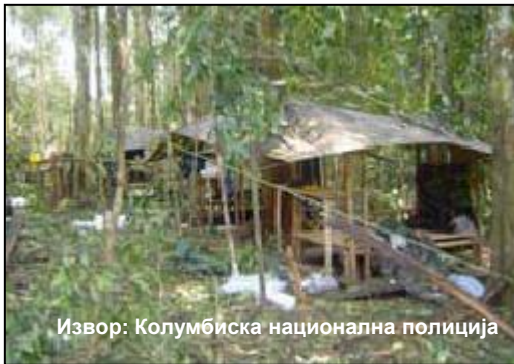
**Наод на ИНТЕРПОЛ број 3:
“не постојат докази дека биле создавани, модификувани
или бришени било какви фајлови”**



Активност: Заплена на преносниот компјутер на FARC



Luis Edgar Devia Silva *alias* Raúl Reyes working on a laptop computer.

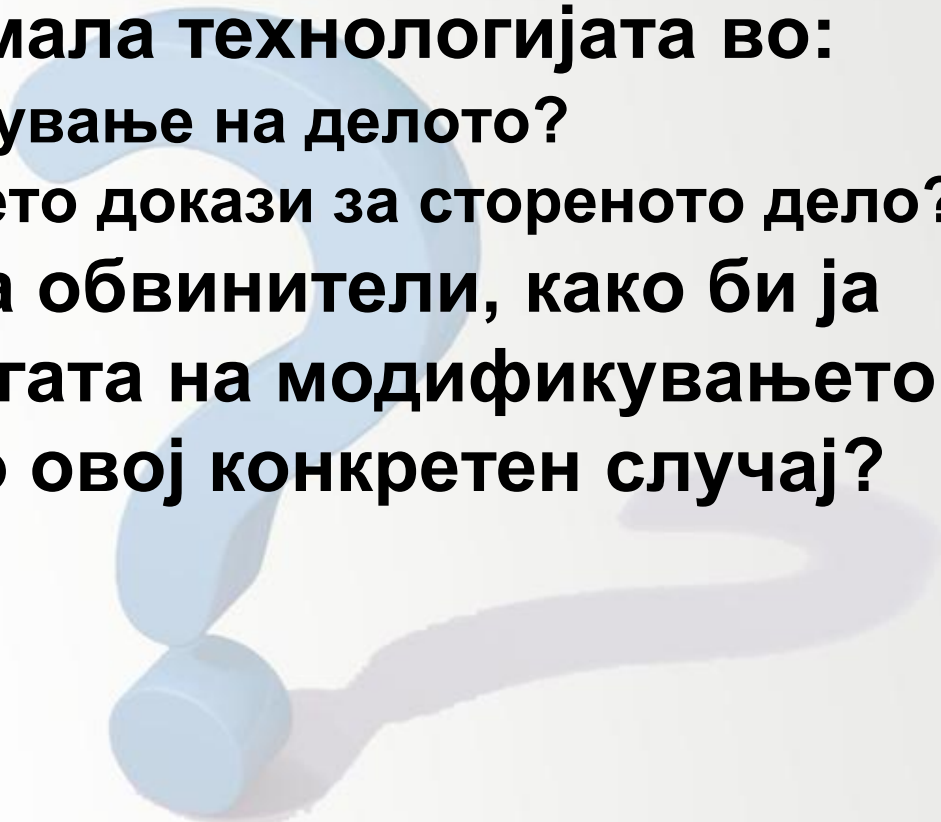


Извор: Колумбиска национална полиција



Активност: Финална дискусија за студијата на случај

- **Каква улога имала технологијата во:**
 - Самото извршување на делото?
 - Обезбедувањето докази за стореното дело?
- **Во својство на обвинители, како би ја објасниле улогата на модификувањето на податоците во овој конкретен случај?**



Зошто криминалците користат технологија

- Криминал со помал ризик
- Помали пречки за влез или пристап
- Вршење кривични дела на територии со друга кривична надлежност
- Голем број потенцијални жртви
- Поголем поврат на инвестициите
- Анонимна комуникација
- Лесна команда и контрола



Техники: Отворен лов - “Фишинг”

- Криминалецот испраќа бројни електронски пораки:
 - Тврдејќи дека истите доаѓаат од извор на кој може да му се верува
 - Барајќи доверливи информации
- Криминалецот потоа ги користи украдените информации за вршење измами



Source: Getty Images



Техники: Лов со копје

- Криминалците вршат истражувања во однос на потенцијалните жртви и ги бираат оние на кои ќе им пратат електронски пораки:



Извор: Фото Getty

- Наводно од некој кого жртвата го познава
- Барајќи информации или одредена постапка од жртвата со која во нејзиниот компјутер се инсталира штетен софтвер



Техники: Штетен софтвер



Source: Getty Images

- Вклучува вируси, црви и Тројанци
- Софтверот инфицира и делува без знаење на жртвата
- Може да се користи за неовластен пристап, пренос на пари, таргетирање специфични податоци или за заразување други компјутери



Техники: Измами со платежни картички

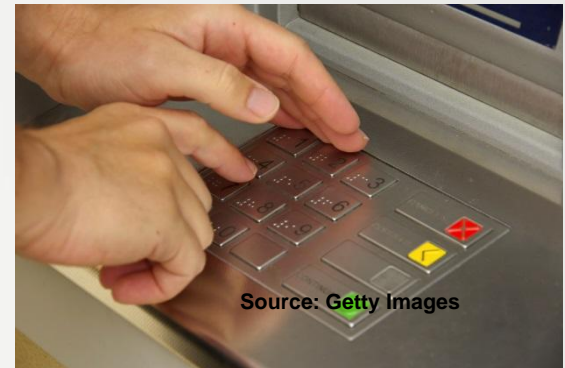
- Собирање украдени финансиски податоци за вршење измами
- Примерите го вклучуваат следново:
 - Снимање на податоците од картичките на банкомати
 - Неовластени упади во компјутерски мрежи, компјутери или веб страници
 - Тргување со украдените податоци
 - Фалсификување картички



Извор: Град Лафајет, Индијана

Пример за измами со платежни картички

- Платежни картички издадени во Обединетите арапски емирати (ОАЕ) биле незаконски копирани и потоа истите се користеле за вадење пари во готово во странски држави
- Неколку банки од своите клиенти побарале да ги сменат нивните шифри за лична идентификација (пиновите)



Техники: Хакирање

- Криминалците ја искористуваат ранливоста на софтверите за остварување незаконски пристап до компјутерските системи
- Потоа криминалците можат да крадат информации или да вршат понатамошни компјутерски напади



Техники: Ботнетови

- Криминалците создаваат ботнетови преку заразување на голем број компјутери со еден конкретен штетен софтвер
- Ботнетовите можат да се користат за собирање финансиски податоци или за вршење на понатамошни компјутерски напади



Техники: Дистрибуирано негирање услуги

- Голем број компјутери испраќаат штетни податоци и барања истовремено
- Во тој случај, жртвата:
 - Не може да ги обработи сите барања поради огромниот број
 - Блокирана е поради постапувањето по легитимните барања и задолженија



Извор: Фото Getty



Активност: Студија на случај за компјутерски криминал

Погледнете:
Прилог 3.2



- **Упатство: Работејќи во поединечни тимови:**
 - Разгледајте ги клучните факти и информации во врска со случајот [ShadowCrew.com](https://www.shadowcrew.com)
 - Одговорете на поставените прашања за потребите на дискусијата
 - Бидете подготвени своите одговори да ги споделите со останатите учесници по истекот на 10 минути



Активност: Истрага

■ 2002-2004

- Хостирањето е во Хонг Конг, а потоа во САД
- Само за регистрирани членови (4,000 членски сметки)
- Место на кое може да се тргува со украдени податоци од кредитни картички и лажни документи за лична идентификација
- Над \$4 милиони загуба од кредитни картички

Shadowcrew
For Those Who Wish To Play In The Shadows!

Classic Gold Platinum
@purchasing@business@corporate@world
[click to order]

FAQ Search Memberlist Register
Profile Log in to check your private messages Log in

The time now is Mon Nov 01, 2004 9:38 am
Shadowcrew Forum Index

Forum	Topics	Posts	Last Post
Global Forum All topics from all forums *DO NOT POST IN THIS FORUM*	6425	49931	Thu Oct 28, 2004 6:15 pm dawgman →
Discussion Forums			
The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge or post news from the fraud world. Moderators disk, Mubon, carsen	1488	13303	Thu Oct 28, 2004 6:15 pm Big Frosty →
Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like. Moderators pythic, sigeep, carsen	1257	9270	Thu Oct 28, 2004 6:08 pm squiggles →
Cyberspace Discussion about hacking, SPAM, online anonymity tools and programs in general. Moderators cumbajohnny, menaste	618	3918	Thu Oct 28, 2004 3:26 pm riscphree →
Credit, E-Currencies, Checks, and Bank Accounts Discussion concerning credit cards, bank accounts, paypal, e-currencies, credit bureaus, credit reports, and credit services. Moderators JimB, Spookycat, Scylla	2599	19078	Thu Oct 28, 2004 6:15 pm dawgman →
Qualification Discussion of Diplomas, Employment References, Job searches, Transcript, Etc Moderators ShadowReview, macgyver	89	810	Thu Oct 28, 2004 9:29 am barto →
Auction Forum Buy and sell in the Auction forum. Moderator Volcur	27	182	Thu Oct 28, 2004 3:51 pm redslamp →



Активност: Истрага

- **Операција на Тајната служба на САД под назив Огнен ѕид**
 - **Есен 2003 година: Уапсен е администраторот на веб страницата Алберт Гонзалес, познат и како Кумба Џони и преземена е контролата на страницата**
 - **Пролет 2004 година: Употреба на виртуелна приватна мрежа (VPN) и судски налози за прислушување на различните членови за потребите на нивно следење и набљудување**



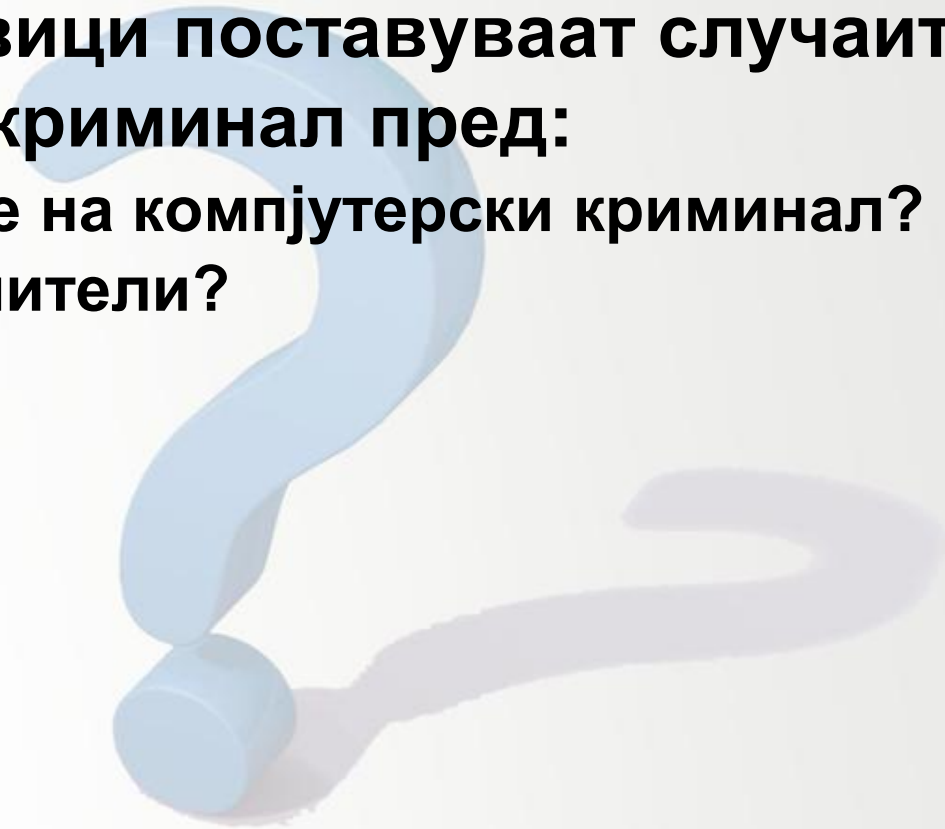
Активност: Меѓународна соработка

- Октомври 2004:
 - Паралелно лишување од слобода на 28 високо рангирани членови во 8 различни држави (19 во САД)
 - Веб страната е затворена



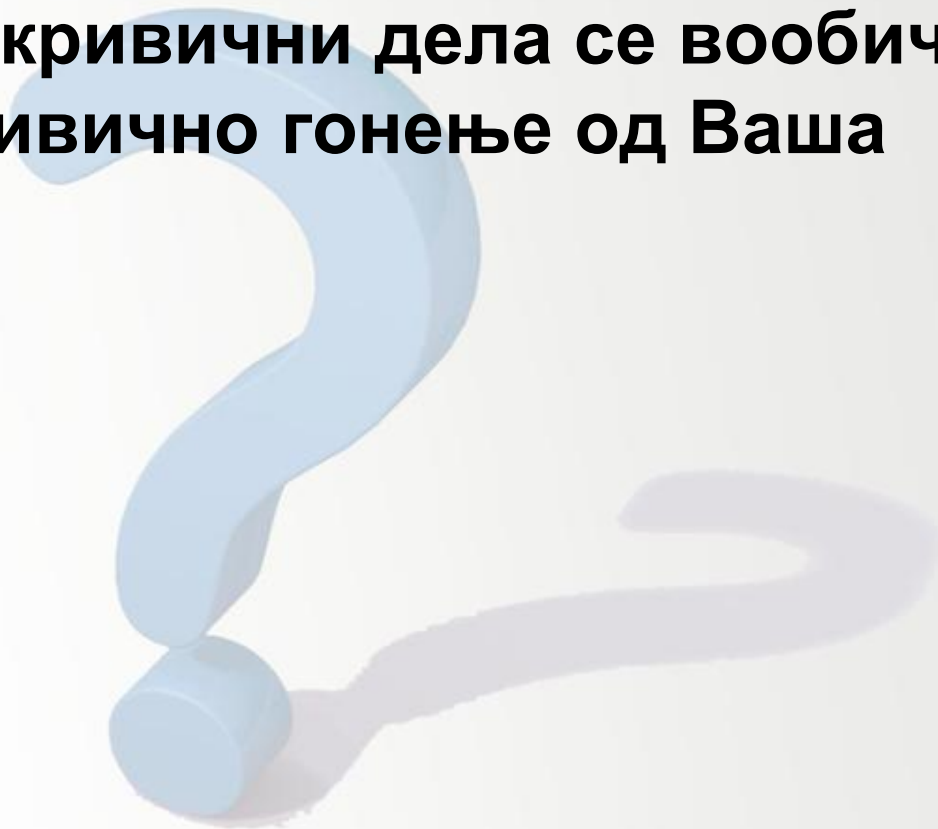
Активност: Конечна дискусија за студијата на случај

- **Какви предизвици поставуваат случаите на компјутерски криминал пред:**
 - Истражителите на компјутерски криминал?
 - Јавните обвинители?



Дискусија: Технологија во вообичаените случаи

- **Какви видови кривични дела се вообичаено предмет на кривично гонење од Ваша страна?**



Резиме на модулот

Погледнете:
Прилог 3.3



- Користење на Интернетот од страна на терористите
- Компјутерски криминал и напади

