

Отвъд страшния свят на "RATTERS"

Публикувано от **nicky931** на **2013-04-07**

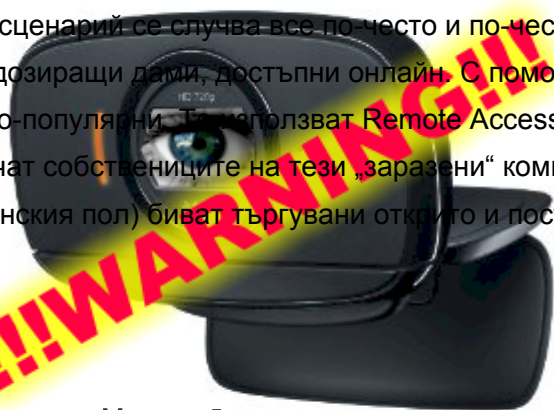
Отвъд страшния свят на "RATTERS"

-

Мъж стои пред монитора си и наблюдава, от хиляди мили разстояние, нищо неподозираща жена, която стои съблечена пред компютъра си и е готова за сън. В този момент тя няма ни най-малка представа, че бива наблюдавана. Хакер е инсталирал софтуер на нейния компютър, чрез който може да контролира камерата и. Най-лошото е, че той е записал всички нейни действия и е качил тези видеота в youtube или ги е изтъргувал.

Инструменти за отдалечен достъп.

Този сценарий се случва все по-често и по-често; има безброй подобни снимки и видеота, на нищо неподозиращи дами, достъпни онлайн. С помощта на онлайн общността „Ratters“ тези истории стават все по-популярни. Те използват Remote Access Tools, за да активират уеб камерата на компютъра. Те наричат собствениците на тези „заразени“ компютри „роби“ и видеотата (най-вече на потребителите от женския пол) биват търгувани открито и поставяни в YouTube.



Онлайн форуми на „Ratters“

Практиката за завземане на компютъра не е никак нова. Още преди години хакерите са произвели софтуер, който дава пълен контрол на хакера върху компютъра ви. Но това, което е непознато за нас е общността на нападателите, които с помощта на хакерските форуми са станали многоброен колектив от хора, който говори за подвизите на хората, чийто компютри са поробени.

В подробно описана статия в „Arts Technica“ журналистът Нейт Андерсон, който разследва членовете на hackforums.net, казва, че има повече от 134 страници с постове на заснети снимки и клипове на

женски „роби“. Някои са записани от уеб камерите, а други са лични клипове или снимки намерени на хард диска на компютъра на жертвата.

Трудности за полицията

Докато този тип на неоторизирано компютърно проникване е очевидно незаконно, борбата срещу „Ratting“ е предизвикателство. Нападателят обикновено не са местни или в непосредствена близост до жертвите. А дори и ако един от форумите на „Ratters“ бъде закрит, ще се появи друг на неговото място.

Как можем да се превърнем в жертви?

Компютрите на жертвите се заразяват чрез инструменти за отдалечен достъп. По същия начин се разпространяват и всички останали вируси. Отваряйки или теглейки различни файлове от непознати сайтове, а дори и само чрез едно щракване върху някой линк, ние правим нашите компютри лесна плячка за хакерите.

Как да се защитим?

Добрите новини са, че тези програми (вируси) могат да бъдат открити и отстранени. Първо, обръщайте внимание на малката лампичка точно до вашата уеб камера. Ако тази лампичката свети, а вие не използвате камерата си, може да сте станали жертва на „Ratters“. Чрез включване на антивирусна програма или чрез натискане на клавишите ctrl-alt-del, имате възможност да разберете кои от процесите на вашия компютър са активни. Ако видите нещо подозрително, изключете интернета си и отстранете проблема, като направите проверка с някакъв антивирусен софтуер.