# Cyber Attacks

In the real world, you only have to worry about the criminals in your city. But in the online world, you have to worry about criminals who may be located anywhere on the planet. Many hotbeds of online criminal activity are located in cities whose police forces are already overextended fighting “real-world” crimes and who lack the resources and expertise to investigate online activity. And in the past decade, the criminals themselves have changed. In 2003, all the malware was still being written for fun by hobbyists, but now it’s being produced by professional criminals, hacktivists, and governments who can invest big money to craft attacks that deliver massive payoffs.

What are the biggest threats?

***Bitcoins***

Bitcoins only have value when the transactions are confirmed by at least six members of the peer-to-peer network. Users who participate in transaction confirmations are rewarded with Bitcoins, a process that is called mining. As the value of a Bitcoin has increased, mining has become harder, because more people want to do it. Today, to make real money at mining Bitcoins, you need powerful computers — but those computers don’t necessarily have to be yours. Some of the largest botnets run by online criminals today are monetized by mining. So an infected home computer of a grandmother in Barcelona, for example, may be mining Bitcoins worth tens of thousands of dollars a day for a Russian cybercrime gang.

**Cyber-spies**

Companies and governments spend money on espionage. Cyber-spies use “trojans” and “back doors” to access data on their targets’ computer networks, remotely monitor them, and perform actions on them, such as keylogging to collect passwords or eavesdropping through the infected computer’s microphone.

The most effective method to protect data against cyber-spying is to process confidential information on dedicated computers that are not connected to the Internet. Critical infrastructure should be isolated from public networks.

**Exploits**

Cyber attacks rely on exploitation of “vulnerabilities” — bugs in the source code of commonly used software — to infect target computers. When professional criminals and governments got into the cyber attack game, demand for new “exploits” greatly increased, and boutique companies sprang up to find and sell these exploitable bugs. Some U.S.-based defense contractors are openly advertising positions for people with Top Secret/SCI clearance to create offensive exploits targeting iPhones, iPads, and Android devices. As the U.S. has engaged in offensive cyber attacks on other countries, other countries have followed suit, creating a cyber arms race that will continue to increase demand for exploits.

Кибер-атаки

В реальном мире вам нужно беспокоиться только о преступниках в вашем городе. Но в онлайн-мире вам нужно беспокоиться о преступниках, которые могут находиться в любой точке планеты. Многие очаги онлайн-преступной деятельности расположены в городах, полицейским силам, которые уже переполнены боевыми «реальными» преступлениями и которым не хватает ресурсов и опыта для изучения онлайн-активности. И за последнее десятилетие сами преступники изменились. В 2003 году все вредоносные программы все еще писали для забавы любители, но теперь они производятся профессиональными преступниками, хактивистами и правительствами, которые могут инвестировать большие деньги для создания атак, которые приносят массовые выигрыши.

Каковы самые большие угрозы?

**Биткоины**

Биткойны имеют ценность только тогда, когда транзакции подтверждены не менее чем шестью членами одноранговой сети. Пользователи, участвующие в подтверждениях транзакций, получают вознаграждение за биткойны, процесс, который называется «добыча». Поскольку стоимость биткойна увеличилась, добыча стала сложнее, потому что больше людей хотят это сделать. Сегодня, чтобы заработать реальные деньги на добыче биткойнов, вам нужны мощные компьютеры, но эти компьютеры не обязательно должны быть вашими. Некоторые из крупнейших бот-сетей, которыми управляют онлайн-преступники сегодня, монетизируются путем добычи. Так, например, зараженный домашний компьютер бабушки в Барселоне может добывать биткойны стоимостью десятки тысяч долларов в день для российской киберпреступной банды.

**Кибер-шпионы**

Компании и правительства тратят деньги на шпионаж. Кибер-шпионы используют «трояны» и «бэкдоры» для доступа к данным в компьютерных сетях своих целей, дистанционно контролируют их и выполняют на них действия, такие как кейлоггинг для сбора паролей или прослушивания через микрофон зараженного компьютера.

Наиболее эффективным методом защиты данных от кибер-шпионажа является обработка конфиденциальной информации на выделенных компьютерах, которые не подключены к Интернету. Критическая инфраструктура должна быть изолирована от сетей общего пользования.

**Бреши**

Кибер-атаки основаны на использовании «уязвимостей» - ошибок в исходном коде обычно используемого программного обеспечения - для заражения целевых компьютеров. Когда профессиональные преступники и правительства попали в кибер-атаку, спрос на новые «эксплойты» значительно увеличился, и возникли компании, чтобы найти и продать эти эксплуатационные ошибки. Некоторые американские оборонные подрядчики - это открытые рекламные позиции для людей с разрешением Top Secret / SCI для создания агрессивных эксплойтов, ориентированных на устройства iPhone, iPad и Android. Поскольку США занимались наступательными кибератаками в других странах, другие страны последовали этому примеру, создавая гонку кибербезопасности, которая будет продолжать увеличивать спрос на эксплойты.