КИБЕРПРЕСТУПНОСТЬ

Выполнила раянова.А. ДД-103

Киберпреступность

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации (клеветы, порнографических материалов) через Интернет

КИБЕРПРЕСТУПНОСТЬ В УГОЛОВНОМ КОДЕКСЕ РФ

- В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства

- киберпреступления как правовую категорию
- киберпреступность как социальное явление.

ПРИЧИНЫ ПОРАЖДАЮЩИЕ КИБЕРПРЕСТУПНОСТЬ

- Это прибыльно. 9 млн. долларов за 30 мин.- такова «добыча» киберпрестпников от одной глобальной атаки на банкоматы;
- Взломы автоматов для обмены валюты ;
- Взлом компьютерной системы.

- Это легко выполнимо. Это технически просто;
- Отсутсвие физического контакта;
- Архитектура современных операций систем гибка и небезопасна.

- Это бизнес с минимальным риском.
- Серьёзные пробелы в законодательстве;
- Жертвы редко сообщают в правоохранительные органы о престеплении;
- Киберпреступность не имеет государственных границ.

Принципы реализации атак

- Современные киберпреступники выбрали своим оружием троянские программы, с помощью которых они строят ботнеты для кражи паролей и конфиденциальной информации, проводят DoS атаки и шифруют данные, чтобы затем шантажировать своих жертв. Характерной и опасной чертой сегодняшних вредоносных программ является то, что они стремятся сохранить свое присутствие на инфицированной машине. Для достижения этой цели киберпреступники используют различные технологии.

Первый шаг любого киберпреступления

- доставка и установка вредоносной программы.

спам-рассылки и зараженные веб-страницы

Второй шаг

- после доставки вредоносной программы - как можно дольше сохранить ее необнаруженной.

РУТКИТЫ

- Чем менее видима программа для систем антивирусных радаров раннего оповещения, тем дольше ее можно будет использовать для получения доступа к зараженным компьютерам и сбора информации. Стандартные технологии сокрытия программы на компьютере включают применение руткитов, блокирование системы извещений об ошибках и окон предупреждений, выдаваемых антивирусом, сокрытие увеличения размеров файлов, использование множества разнообразных упаковщиков.

ПОЛИМОРФИЗМ

- Во избежание обнаружения вредоносных программ вирусописатели широко используют технологию умышленного запутывания. Полиморфизм - одна из таких технологий, он был популярен в 90-х годах, но затем фактически исчез. Сегодня вирусописатели вернулись к полиморфизму, но они редко предпринимают попытки изменять код на компьютерах жертв. Вместо этого применяется так называемый «серверный полиморфизм» - изменение кода на веб-серверах с включением в него «пустых» инструкций, изменяющихся с течением времени, что существенно затрудняет обнаружение новых вредоносных программ, размещенных на веб-сервере.

«Троянского конь» в современных киберпреступлениях

- Троянская программа - программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. По принципу распространения и действия троян не является вирусом, так как не способен распространяться саморазмножением.

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере:

- Backdoor -- троянские утилиты удаленного администрирования;
- Trojan-PSW -- воровство паролей;
- Trojan-Clicker -- интернет-кликеры;
- Trojan-Downloader ;
- Trojan-Dropper ;
- Trojan-Proxy;
- Trojan-Spy;
- Trojan-Notifier .

Основные тенденции развития троянских программ:

- Значительный рост числа програ… крадущих конфиденциальную банковскую информацию;

- Стремление к получению тотального контроля над зараженными компьютерами. Это выражается в объединении их в зомби-сети, управляемые из единого центра;

Trojan-Dropper и Trojan-Downloader

- Конечные цели у них абсолютно идентичны -- установка на компьютер другой вредоносной программы, которая может быть как червем, так и «троянцем». Отличается только принцип их действия. «Дропперы» могут содержать в себе уже известную вредоносную программу или наоборот -- устанавливать новую ее версию. Также «дропперы» могут устанавливать не одну, а сразу несколько вредоносных программ, принципиально отличающихся по поведению и даже написанных разными людьми.

1	Heur.Trojan.Generic	248857	7,08%
2	Trojan-Downloader.Win32.Small.aacq	228539	6,50%
3	Trojan-Clicker.HTML.IFrame.wq	177247	5,04%
4	Trojan-Downloader.SWF.Small.ev	135035	3,84%
5	Trojan-Clicker.HTML.IFrame.yo	121693	3,46%
6	Trojan-Downloader.HTML.IFrame.wf	107093	3,05%
7	Trojan-Downloader.Win32.Small.abst	78014	2,22%
8	Trojan-Downloader.JS.Agent.dau	73777	2,10%
9	Trojan-Downloader.JS.IstBar.cx	68078	1,94%
10	Trojan-GameThief.Win32.Magania.gen	66136	1,88%
11	Trojan-Downloader.JS.Iframe.yv	62334	1,77%
12	Trojan.HTML.Agent.ai	60461	1,72%

Заключение

- Атаки злоумышленников становятся все масштабнее и изощреннее. А действия игроков способствуют росту черного рынка виртуальных ценностей, на чем зарабатывают деньги хакеры и вирусописатели.
- «Троянский конь» является наиболее опасной из всех вредоносных программ

РЕКОМЕНДАЦИИ

- Результаты данного исследования могут стать полезными всем пользователям персональных компьютеров, заботящихся о сохранности своих документов и об информационной безопасности.

- Также их можно применить на уроках информатики, для ознакомления учеников с вредоносными программами. Важно еще со школы осознавать наносимый вред киберпреступлениями.