Кибербезопаснос

проект по информатике учениц 9 А класса Дмитриевой Софьи, Хомичук Татьяны

Цифровой мир кажется таким удобным, все становится отцифрованным, все подключается к интернету , но вместе с этим приходят новые угрозы, от которых приходится защищаться. Уже сейчас тостер и регистраторы используют в DDOX атаках. Мы хотим рассказать о том как защитить себя в интернете, где за нашей информацией разворачивается настоящая война.

Компьютерный вирус - вид вредоносного программного обеспечения, он способен создавать копии самого себя, внедрять я в код других программ, в системные области памяти, в загрузочные секторы, а также способен распространять свои копии по разнообразным каналам связи.

Пока мы пользуемся своими ноутбуками и телефонами за нашей информацией разворачивается настоящая охота. Хакеры придумывают все сложные вирусы, а те кто с ними борются наращивают все более сложную защиту.

Каждый хакер сам решает какую нашу он занимает и начинает бесконечно войну со специалистами по киберспециалистами.

Выглядит это вот так:


0.1%
9.9%
Целевые атаки, нацеленные на определенных людей или организаций
90%
Массовые угрозы-черви, трояны, фишинговые письма, и большинство атак в интернете

ФИШИНГ

```
fnum = FreeFile
fname = Environ("TMP") & "\vba_macro.exe"
Open fname For Binary As #fnum
```

Большая часть атак ни на кого отдельно не нацелена, это трояны или фишинговые письма которые просто так гуляют по сети. Их жертвами становятся как правило те, кто не позаботился о своей безопасности или киберграмотности. Разнообразия таких писем бесконечны.

Разновидности фишинговые атак:

Hamograph arrack построена на невнимательности людей. Раньше вы могли зайти на известный сайт, где например в URL первая а-русская. Когда социальные сети не были защищены зная Логин вы могли подобрать в специальной программе пароль. Сегодня уже не каждым будет кликать на подозрительные ссылки, киберграмотность растёт.
Как распознать такой вирус: вирус из смс может открываться поверх письма и просить ввести данные банковской карты.

Drive-by dowload

Теперь не нужно ничего скачивать, ты просто заходишь на веб-страницу и ты уже заражён. Так происходит если у вас не обновлены программы на компьютерах, например браузер. Хакер использует ошибки в них чтобы незаметно запустить свой код. Так что пользоваться приложениями безопаснее, в них сразу закладывают ряд проверок.

Bot net . Даже если все ваши данные уже у хакера, ваш телефон остаётся полезным. Хакер встраивается вас в сеть. Он пользуется вашей вычислительной мощностью, самое безобидное - манить с помощью вашего телефона криптовалюту. Но все деньги отправляются злоумышленнику.

DDOS атаки. Хакер через командный центр даёт приказ всем устройствам, и вся армия ботов стучится на этот сайт одновременно. Сайт не выдерживает и не работает. Из-за ботнета MIRAI в 2016 году перестали работать на некоторое время такие сайты как NETFLIX, REDDIT, TWITTER, AIRBNB. Этот БОТНЕТ объединит 300 тысяч устройств со всего мира.

САМОЕ КРУПНОЕ ЦИФРОВОЕ ОГРАБЛЕНИЕ CARBANAK

Самое крупное цифровое ограбление в истории - 1 200 000 000$. Руководил всем этим русской мужчина, который жил в Испании

Код вируса пакуется во вложение и рассылается Фишером на почту бухгалтерам банка . При открытии файла- вирус заражал всю систему в течении 2-4 месяцев. Проникая в сервера , отвечающие за управления банкоматами они давали им команды и точное время для выдачи денег. В это же время у банкомата появлялся мул, эти деньги мулы передавали посредникам , а те переводили их в криптовалюту и скрывались. После операции подключался чистильщик и очищал цифровые следы. Хакеры заработали миллиард используя человеческую уязвимость, зная, что бухгалтера банков будут открывать зараженные письма. Они не учли одного- их хакеры тоже будут ошибаться . Один из мулов в Тайване потерял свою карту у банкомата. Так, полиция установила его личность и начала задерживать