Презентация к внеклассному занятию по информатике по теме

«Ложный антивирус: что такое и меры борьбы»

Автор материала:
Медведева Татьяна Александровна,
Учитель информатики
Высшей квалификационной категории
МБОУ Арбатская СОШ
Таштыпского района
Республики Хакасия

с.Арбаты – 2015г.

Что такое ложный антивирус?

- Ложные антивирусы (также известные как «scareware») – это программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты почти или совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции.

Ложный антивирус: что такое и меры борьбы

Как ложные антивирусы попадают на компьютер?

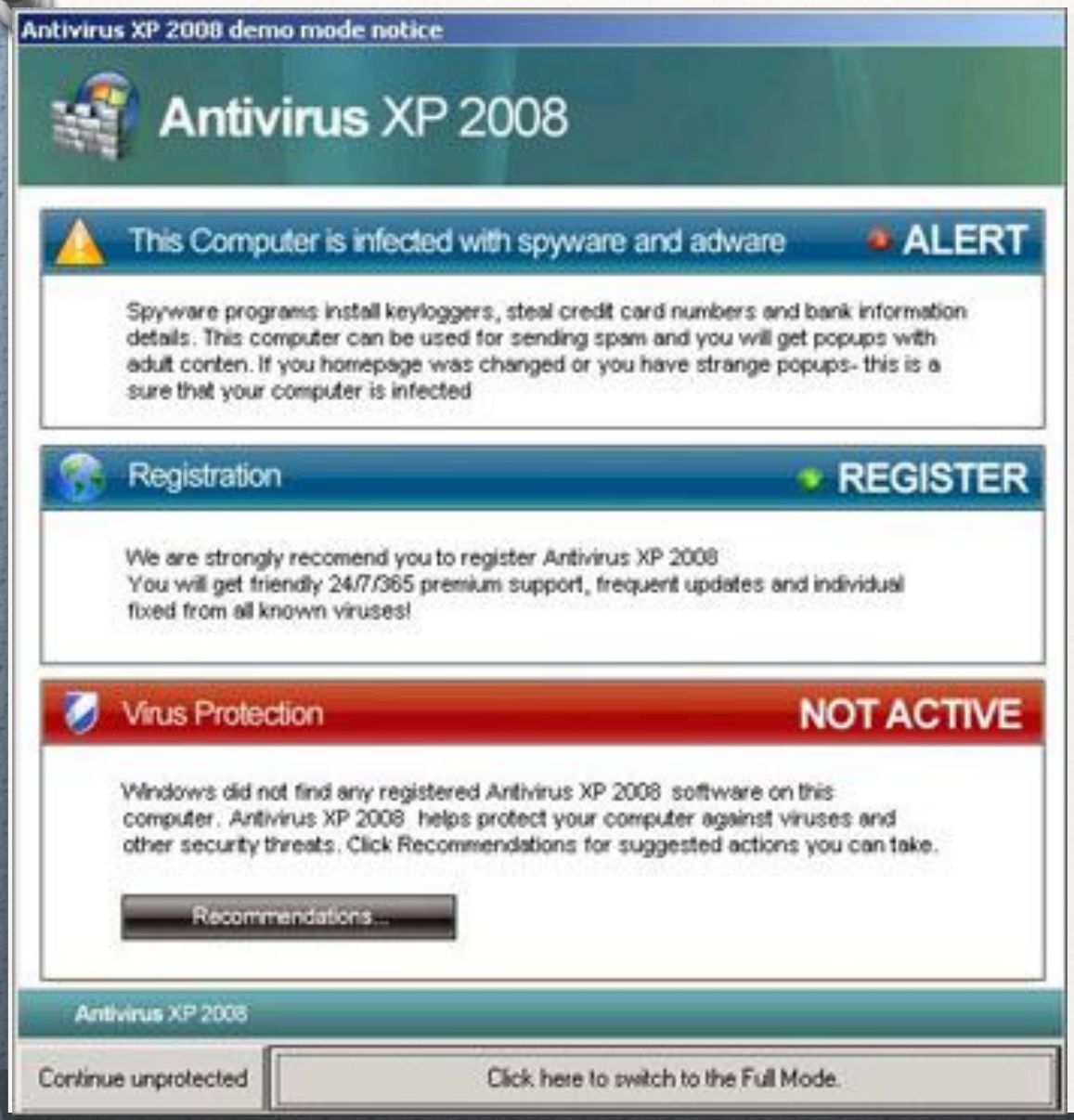
- Разработчики ложных антивирусов создают специальные рекламные окна, которые выглядят так, как будто они рекламируют легальное ПО для обеспечения безопасности или его обновления. Вы может увидеть их при посещении различных веб-ресурсов.
- «Сообщения» в таких окнах призывают пользователя выполнить некоторое действие, например, установить программу, загрузить рекомендуемые обновления или удалить вирусы и шпионское ПО. Если вы щелкните по такому объявлению, на ваш компьютер будет загружен и установлен ложные антивирус.
- Мошенническое программное обеспечение также может фигурировать в списке результатов при поиске легальных программ для обеспечения безопасности, поэтому важно обеспечить защиту компьютера заблаговременно.

Что делает ложный антивирус?

- Ложные антивирусы могут сообщать вам об обнаруженных ими вредоносных программах, даже если ваш компьютер на самом деле не заражен.
- Естественно, такое «антивирусное» ПО вряд ли обнаружит настоящее заражение вашего компьютера вирусами и другими зловредными программами.
- Более того, мошеннические антивирусы могут специально загружать на компьютер вредоносные программы, чтобы им было чем вас «порадовать».

Некоторые мошеннические антивирусы также могут:

- Провоцировать вас на выполнение действий, нужных мошенникам (например, выполнить обновление до несуществующей платной версии программы).
- Красть ваши персональные данные, используя методы социальной инженерии.
- Устанавливать вредоносное ПО для кражи ваших данных.
- Отображать всплывающие окна с ложными уведомлениями о различных угрозах.
- Снижать производительность компьютера или повреждать файлы.
- Отключать обновления операционной системы или легальных антивирусных программ.
- Блокировать посещение веб-сайтов разработчиков антивирусных программ.



Лжеантивирусы также могут имитировать процесс обновления системы безопасности Microsoft. Вот пример того, как мошенническая программа имитирует уведомление от Microsoft, хотя на самом деле оно отправлено совсем другой «компанией».

Пример ложного антивируса, который известен как AntivirusXP.

- Чтобы получить дополнительные сведения об этой угрозе, включая поиск и способы предотвращения и восстановления, см.Trojan:Win32/Antivirusxp в энциклопедии Центра защиты от вредоносного ПО.
- Вот как выглядит настоящий Центр безопасности Microsoft Windows:

Центр безопасности Microsoft Windows

Рекомендации по защите от ложных антивирусов

- Установите брандмауэр и не выключайте его.
- Используйте автоматическое обновление для загрузки обновлений для вашего программного обеспечения.
- Установите антивирусное и антишпионское программное обеспечение, например,Microsoft Security Essentials и регулярно обновляйте его. Чтобы узнать ссылки на сайты других антивирусных программ, которые совместимы с решениями Microsoft, см. этот Список производителей антивирусного программного обеспечения.
- Если ваше антивирусное программное обеспечение не имеет антишпионских компонентов, следует установить отдельную антишпионскую программу, например, Защитник Windows(он входит в состав Windows Vista, а пользователи Windows XP могут загрузить его бесплатно).
- Относитесь с осторожностью к ссылкам, которые вам присылают по электронной почте или через сообщения в социальных сетях.
- Используйте стандартную учетную запись пользователя, а не учетную запись администратора.
- Ознакомьтесь с общими признаками фишинговых сообщений.

Что делать, если вы подозреваете, что у вас на компьютере установлен ложный антивирус?

- **Просканируйте компьютер.**Используйте для этого легальное антивирусное программное обеспечение или бесплатные утилиты, например, средство проверки безопасности. Этот сканер проверяет жесткий диск компьютера на наличие вирусов и удаляет их. Он также производит очистку диска от ненужных файлов, что улучшает производительность ПК.
- **Проверьте свои аккаунты.** Если вы думаете, что ввели конфиденциальную информацию, например, номер кредитной карты или пароль, во всплывающем окне или на сайте мошеннического антивируса, необходимо отслеживать, что происходит с соответствующими учетными записями. Чтобы получить дополнительную информацию, см. Защита от фишинга и других сетевых угроз.
- Если вы подозреваете, что ваш компьютер заражен ложной антивирусной программой, которая на данный момент не выявляется решениями безопасности Microsoft, вы можете отправить образцы ее файлов, используя эту форму на сайте Центра защиты от вредоносного ПО

Источники:

- Популярные фишинговые схемы - http://www.microsoft.com/ru-ru/security/online-privacy/phishing_scams.aspx
- Что такое ложный вирус - http://www.microsoft.com/ru-ru/security/pc-security/antivirus-rogue.aspx
- Рисунки взяты с сайта Office.com