Захист від клавіатурних шпигунів

Лекція 1(2)
дисципліна “ Захист інформації ”

Клавіатурний шпигун

- Кейлогер (клавіатурний шпигун) використовується для крадіжки паролів.
- Клавіатурні шпигуни погано (не більше 20%) виявляються антивірусами, антишпигунами (Anti-Spyware) та файрволами (за даними Network Intercept).
- Один із засобів протидії кейлогерам – віртуальна клавіатура.

Реалізація та розповсюдження кейлогерів

- Реалізуються кейлогери програмно і апаратно.
- Метою роботи цих програм є постійне відсилання віддаленому суб'єкту даних по натисненню клавіші.

- Способи зараження:

1) необережне натиснення на посилання, фото, відео (на неперевірених сайтах), які вміщують код вірусу;

2) погано організований захист ПК (найбільш розповсюджений злам сайту через крадіжку паролів з погано захищеного ПК).

Віртуальна клавіатура, захищена від кейлогерів

- Засобом боротьби з кейлогерами є **віртуальні клавіатури**, які спеціально захищені від клавіатурних шпигунів
- Посилання для скачування віртуальної клавіатури: http://narod.ru/disk/52935334001.15a16b625354b5441f3ae47f2dcb02a6/keyboard.exe.html
- Перевіряйте скачаний файл на наявність вірусів!!!

Небезпеки слабкого захисту

- “Просунуті” клавіатурні шпигуни мають можливість не тільки зчитувати й передавати коди натиснутих клавіш, а й захватувати переміщення курсору, а також робити знімки екрану в районі курсору.
- Тому потрібно використовувати спеціальні віртуальні клавіатури, які захищені від клавіатурних шпигунів, шпигунів буферу обміну та від ScreenLoggers.

Захист від кейлогерів

- Клавіатурні шпигуни, які реалізовані апаратно, можуть знаходитися в середині клавіш, корпусу клавіатури, у захисній заглушці між комп'ютером і клавіатурою (наприклад у PS2-адаптері чи USB-адаптері).
- Програмні клавіатурні шпигуни перехоплюють інформацію про натиснення клавіш через операційну систему. Вони можуть працювати

1) на рівні ядра Windows (з такими шпигунами дуже складно боротися),

2) на рівні Windows “hooks”. Windows заздалегідь попереджає кейлогера, основаного на “hooks”, про кожне натиснення клавіші до того, як повідомлення про це надійде до використовуваного додатку.

3) пасивними методами. Кейлогери постійно опитують Windows для виявлення моменту натиснення клавіші, після чого виявляють, яка клавіша була натиснута.

100%-го захисту від кейлогерів не існує, але є захисні програми які на високому рівні можуть забезпечити захист

- Їх функції основуються на блокуванні найбільш поширених шляхів перехвату паролів. Вони:

1) не допускають введення пароля з фізичної клавіатури,

2) не допускають копіювання пароля у буфер обміну та вставку з нього у віконце для пароля,

3) для протидії захвату інформації з віконця пароля використовують спеціальні програми (наприклад KeePass)

4) не допускають зйомку екрану (як повного екрану, так і екрану в районі курсору)

Програма для зберігання паролів KeePass*

- **KeePass Password Safe** – вільнорозповсюджувана програма для зберігання паролів, що розповсюджується за ліензією GPL– вільнорозповсюджувана програма для зберігання паролів, що розповсюджується за ліензією GPL. Програма розроблена Домініком Райхлом (нім. *Dominik Reichl*) для операційної системи Windows) для операційної системи Windows. KeePass підтримує алгоритми Advanced Encryption Standard) для операційної системи Windows. KeePass підтримує алгоритми Advanced Encryption Standard (AES (256-бит), Rijndael) та Twofish) для операційної системи Windows. KeePass підтримує алгоритми Advanced Encryption Standard (AES (256-бит), Rijndael) та Twofish для шифрування паролів своїх баз даних. Програма переведена більш чим на 40 мов. Keepass є переносимою програмою і встановлювати її не обов'язково. Вона забезпечує експорт у формати TXT) для операційної системи Windows. KeePass підтримує алгоритми Advanced Encryption Standard (AES (256-бит), Rijndael) та Twofish для шифрування паролів своїх баз даних. Програма переведена більш чим на 40 мов. Keepass є переносимою програмою і встановлювати її не обов'язково. Вона забезпечує експорт у формати TXT, HTML) для операційної системи Windows. KeePass підтримує алгоритми Advanced Encryption Standard (AES (256-бит), Rijndael) та Twofish для шифрування паролів своїх баз даних. Програма переведена більш чим на 40 мов. Keepass є переносимою програмою і

Основні прийоми кейлогерів

- Дистанційне керування клавішею Print Screen (практично використовується рідко, оскільки приводить до мерехтіння екрану, у буфері обміну з’являється копія екрану),
- Програмним способом роблять скріншоти елементів управління (кнопка, текстове поле і т.і.), які знаходяться під курсором за допомогою команд Windows API,
- Роблять програмним способом за допомогою команд Windows API знімки повного екрану

Neo’s SafeKeys v3

- відключає клавішу Print Screen під час своєї роботи,
- утворює невидимий захисний шар (слой) під вказівником миші, що не дозволяє проводити локальні фото екрана під курсором,
- SafeKeys зберігає прозорість екрану мінімум на 1%, що не дозволяє проводити фотографування екрану,
- Прихований режим миші не дозволяє локалізувати спостереження за вводом пароля

Реєстрація курсору миші

- Перед тим, як реєстрація екрану стала стандартною функцією, реєстрація розташування курсору миші іноді застосовувалася проти людей, що використовували екранні клавіатури на банківських сайтах,
- Механізм роботи можна описати так: щоразу, як Ви натискаєте координати курсору вашої миші захвачуються вірусом/трояном. На банківських сайтах екранна клавіатура завжди має однакову висоту/ширину, тому зловмисники, що пишуть віруси/трояни з великим ступенем достовірності можуть дізнатися, які клавіші Ви натискали на екрані.

- При використанні Neo's SafeKeys v3 кожного разу екранна клавіатура з'являється в іншому місті екрану і має різну висоту/ширину
- Кнопка "Resize SafeKeys" також дозволяє перевантажити висоту/ширину і розташування Neo's SafeKeys, кожен раз, коли вона натискається.

Захист від скальпування поля

- “Скальпування поля” – термін, що застосовується для опису методики, що використовується багатьма комерційними клавіатурними шпигунами для захвату Ваших паролів безпосередньо з поля введення,
- Через команди API Windows програми можуть запросити у Windows список засобів управління у програмі (таких, як кнопки, текстові вікна та графічні засоби управління). Завдяки цьому, вони дізнаються про текстові вікна у програмі. На наступному етапі вони запитують у Windows, чи є у текстових вікон маска пароля (пароль, прихований за *****). Саме небезпечне у цьому випадку, це те, що вони можуть навіть заставити Windows видати їм пароль, що приховується під маскою.

- Neo’s SafeKeys ніколи не зберігає ваш реальний пароль під маскою пароля *****. Він утримує Ваш пароль безпечно закритим “за кулісами”. Клавіатурні шпигуни / віруси/ трояни можуть колись отримати тільки перелік зірочок.

Перетягування паролів

- Neo’s SafeKeys передає пароль, коли Ви перетягуєте його з Neo’s SafeKeys у вікно програми (наприклад, Internet Explorer), де цей пароль має бути введений.
- Як би Ви не вводили пароль, Ви не використовуєте буфер обміну чи методи вирізання та вставки, клавіатурні шпигуни не можуть захватити Ваш пароль у процесі перетаскування.

- http://bezopasnostpc.ru/antivirusi/virtualnaya-klaviatura-i-keylogger-klaviaturnyiy-shpion-ch3 Я

NEW – режим “инъекция”

Некоторые программы не принимают пароли перетаскиванием – к ним относятся некоторые большие программы, как KeePass, Roboform, Opera, Excel и World Of Warcraft.

Однако Neo’s SafeKeys v3 имеет теперь режим “инъекция”, который позволяет перемещать Ваши пароли в эти программы методом тащить-и-опустить вполне безопасно. Обратите внимание на то, что более безопасно, если Вы не используете режим “инъекция” Мы были проинформированы, что некоторые клавиатурные шпионы могут при этом захватывать текст. Однако если вы используете режим “инъекция” в сочетании с программой такой, как KeePass, Вам по-прежнему предоставляется хорошая защита.

Различные методы ввода пароля

Как вы видите, есть несколько способов, Вы можете ввести пароли, используя Neo’s SafeKeys:

Стандартный ввод (Standard Entry) – кликайте на экране кнопки клавиатуры, набирая свой пароль, до перетаскивания в целевую программу.

Защита: Отлично.

Ввод наведения (Hover Entry) – наводите курсор мыши на экране на кнопки клавиатуры для набора своего пароля.

Защита: Бриллиант.

Скрытая мышь (Hidden Mouse) и ввод наведения (Hover Entry)- мышь будет превращена в маленькую точку серого цвета, в то время как Вы наводите курсор мыши на экране на кнопки клавиатуры для набора своего пароля.

Защита: безумно высока.

Пароль и видимый текст

Если Вы хотите, Вы можете использовать SafeKeys в качестве портативного “блокнота”. Если маска пароля отключена, Вы сможете видеть все, что Вы вводите, и Вы можете использовать Neo's SafeKeys, чтобы написать короткую записку с помощью экранной клавиатуры или с помощью скремблирования на клавиатуре. Это должно предоставить Вам некоторую защиту для записок, которые Вы пишете.

С помощью настройки в меню Keyboard Layout

можно импортировать новые экранные раскладки клавиатуры. Вы можете создать свою собственную раскладку.

Вы заметите, что Neo's SafeKeys v3 будет сохранить настройки (но НЕ ваши пароли) в файле NSKconfig.ini. Создайте копию этого файла (с новым именем), а затем редактируйте этот файл.

Кнопки отсортированы по ряду, слева направо, нижний и верхний регистр. Просто замените символы, которые Вы хотите изменить, а затем импортировать, используя опцию на “Keyboard Layout” меню.

Если Вы отправите нам по электронной почте раскладку для определенного языка, мы будем рады разместить это на сайте, чтобы другие люди могли использовать.

Предназначение кнопок на панели инструментов.

Возможности ввода с помощью мыши.

Стандартный ввод (Standard Entry)

Используя этот режим, с помощью мыши щелкайте по экранным клавишам, чтобы ввести пароль.

Ввод наведения (Hover Entry)

Используя этот режим, наведите курсор на экранную клавишу в течение времени, чтобы ввести пароль. Задержка при наведении может быть установлена – между 500 мс (0,5 секунды) и 2500 мс (2,5 секунды).

Некоторые клавиатурные шпионы способны делать скриншоты каждый раз, когда Вы щелкаете мышью. Используйте этот режим, чтобы победить этот вид кейлоггера.

Скрытая мышь (Hidden Mouse) и ввод при наведении (Hover Entry)

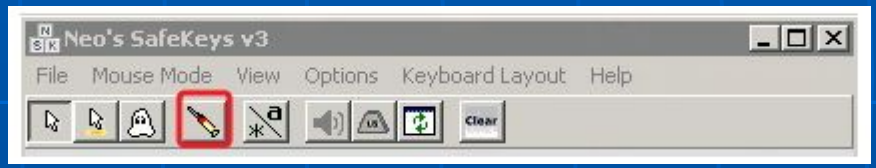
В этом режиме меняется курсор мыши на маленькую точку серого цвета. Используя этот режим, наведите курсор мыши в виде серой точки на экранную клавишу в течение двух секунд, чтобы ввести символ. Задержка при наведении запись может быть установлена – между 500 мс (0,5 секунды) и 2500 мс (2,5 секунды).

Некоторые клавиатурные шпионы могут делать скриншоты через определенные промежутки времени (щелкаете ли Вы мышью или нет), этот способ 'скрывает' курсор мыши при наведении его на символы клавиатуры на экране.

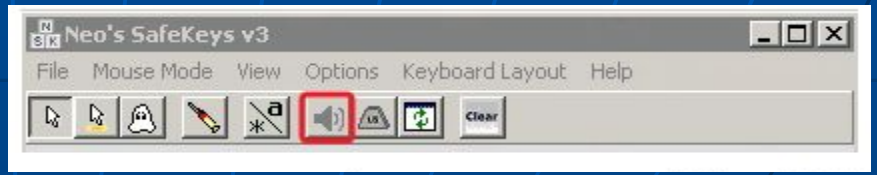
Этот режим также поможет защитить Вас от "серфинга плеча " (люди, подсматривающие через плечо, чтобы увидеть то, что Вы набираете).

Опції Neo’s SafeKeys v3 (частина 1)

- Режим ін'єкції (Injection Mode). В цьому режимі можливо використовувати Neo’s з програмами, які не приймають перетаскування (майстер паролів KeePress та Roboform, додатки Opera, Excel та інші)

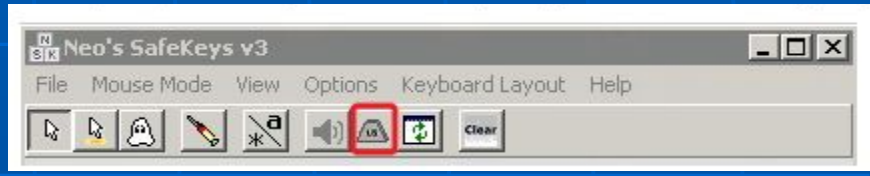


- При використанні режимів “ввід при наведенні” (Hover Entry) чи “прихована миша і ввід при наведенні”, комп'ютер подасть звуковий сигнал, коли вибраний на екрані символ буде введений

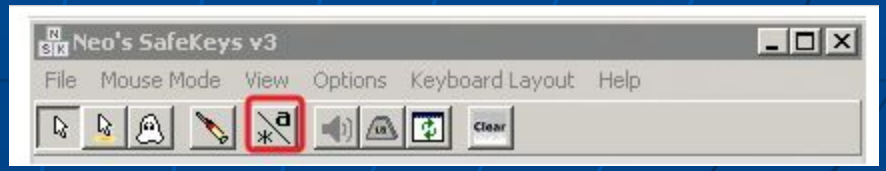


Опції Neo’s SafeKeys v3 (частина 2)

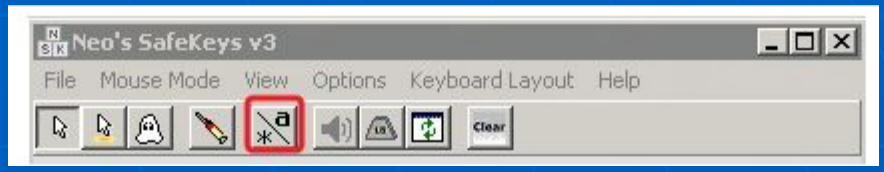
- Опція “Зберігати пароль після перетаскування” (Keep password after drap-drop) залишає весь текст в полі пароля після перетаскування пароля в інший додаток. Якщо це не дозволено, то текст буде видалений після кожного перетаскування.



- Вид: маска пароля (Password Mask). Якщо маска пароля увімкнена, то він буде приховуватися за символами *, інакше пароль буде видимим (у більшості випадків це небезпечно – він може бути викрадений методом “скальпування поля”).



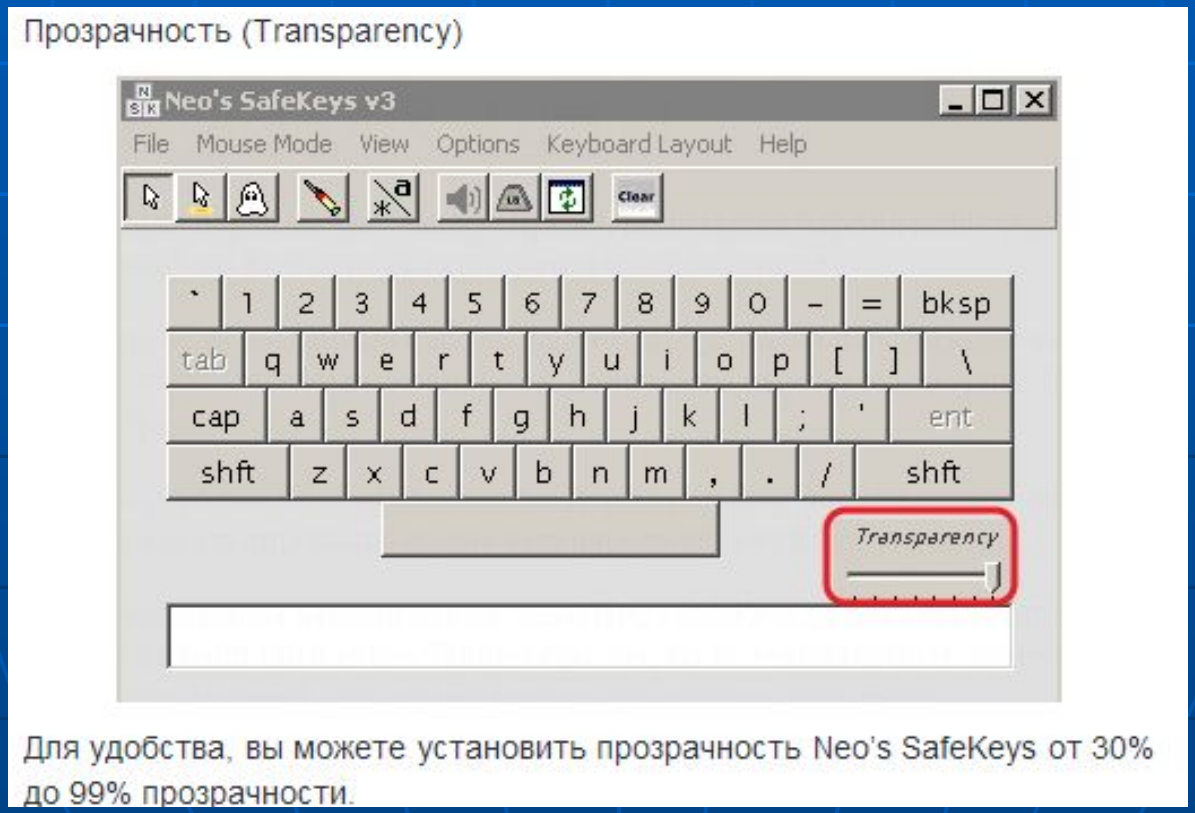
Маска пароля (Password Mask).



- Якщо маска пароля буде вимкнена, Neo’s SafeKeys буде реєструвати натиснення клавіш tab та enter, що дозволить за необхідності ввести невелику пам'ятку, використовуючи екранну клавіатуру,
- Якщо маска пароля буде вимкнена, та в полі пароля буде доступний більш ніж один рядок та символ табуляції. При ввімкненій масці пароля Neo’s SafeKeys відмовиться від всього тексту, окрім першого рядка, а також відмовиться від будь-яких символів табуляції, і сховає текст, що залишився, за символами *.

Зкачати Neo’s SafeKeys v3

- http://bezopasnostpc.ru/antivirusi/virtualnaya-klaviatura-i-keylogger-klaviaturnyiy-shpion-ch3



Технології MicroWorld

- У продуктах MicroWorld реалізовані інноваційні технології, які забезпечують захист не тільки від відомих, але також від нових загроз. Основні технології MicroWorld – це MWL (MicroWorld Winsock Layer), DIRC (Domain and IP Reputation Checker), NILP (Non-Intrusive Learning Pattern), а також складні евристичні алгоритми виявлення шкідливих програм.
- Технологія MicroWorld Winsock Layer (MWL) працює на рівні Windows Sockets (Winsock), блокуючи шкідливі програми ще до того, як вони можуть досягнути додатків.
- Технологія Non-Intrusive Learning Pattern (NILP), що використовує методи штучного інтелекту, дозволяє ефективно відсівати спамерські та фішингові електронні листи.
- NILP має механізм адаптації до поведінки користувача та аналіз того, які повідомлення для користувача є бажаними, а які небажаними.
- Технологія Domain and IP Reputation Checker (DIRC) перевіряє репутацію будь-яких підозрілих web-сайтів та IP-адрес, надійно захищаючи від фішинга, шкідливих програм, небажаного контенту, хакерських атак та інших загроз.

eScan Internet Security Suite для Домашніх користувачів та малого офісу

- http://www.avescan.ru/products/products/home-iss.php