УДК 004.925.5

Лабунь Д.Л., *студент 4 курсу спеціальності «Інженерія програмного забезпечення»*
Романюк О.Н., *д.т.н., професор, завідувач кафедри програмного забезпечення*

РОЗРОБКА ПРОГРАМИ КОНТРОЛЮ ВИХІДНИХ ЗАПИТІВ КОРИСТУВАЧА

Вінницький національний технічний університет, Україна

Кейлоггер [1-5]– різновид ПЗ, яке застосовується для відстеження або логування всіх натискань клавіш на клавіатурі. Користувач електронного пристрою може навіть не підозрювати, що будь-які кліки і натискання записуються, а кейлоггер запам'ятовує абсолютно все - аж до листувань в соцмережах і чатах. Присутність такої програми практично неможливо помітити, оскільки вона функціонує у фоновому режимі, як складовий елемент операційної системи.

У багатьох подібні програми асоціюються з незаконною діяльністю і шкідливим ПЗ. Але, не дивлячись на те, що кейлоггери можна розглядати як вторгнення в особистий простір, все ж це жодним чином не порушує закон. Батьки, наприклад, можуть обзавестися таким ПЗ, щоб захистити своїх дітей в інтернеті, - і з'ясувати, з ким вони спілкуються в Facebook або Whatsapp. Додаток відстежує дані на ПК, Mac, iPhone і інших пристроях.

Роботодавець, в свою чергу, може зробити висновок про те, чим займаються його співробітники під час роботи. Система видає детальні онлайн-звіти про продуктивність персоналу [1].

За методом застосування. Тільки метод застосування кейлоґґерів (зокрема апаратних або програмних продуктів, що включають кейлоггер як модуль) дозволяє побачити грань між управлінням безпекою та порушенням безпеки.

Несанкціоноване застосування — встановлення кейлоггера (зокрема апаратних або програмних продуктів, що включають кілоґґер як модуль) відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Несанкціоновано вживані кейлоґґери (програмні або апаратні) іменуються як шпигунські програмні продукти або шпигунські пристрої. Несанкціоноване застосування, як правило, пов'язане з незаконною діяльністю (illegal activity). Як правило, несанкціоновано встановлювані шпигунські програмні продукти мають можливість конфігурації і отримання «скомплектованого» здійснимого файлу, який при інсталяції не виводить ніяких повідомлень і не створює вікон на екрані, а також мають вбудовані засоби доставки і дистанційної установки конфігурованого модуля на комп'ютер користувача, тобто процес інсталяції відбувається без безпосереднього фізичного доступу до комп'ютеру користувача і часто не вимагає наявності прав адміністратора системи;

Санкціоноване застосування — встановлення кілоґґера (зокрема апаратних або програмних продуктів, що включають кілоґґер як модуль) відбувається з відома власника (адміністратора безпеки) автоматизованої системи або з відома власника конкретного персонального комп'ютера. Санкціоновано вживані кейлоґґери (програмні або апаратні) називаються моніторинговими програмними продуктами, англ. employee monitoring software, parental control software, access control software, personnel security programs і тому подібне. Як правило, санкціоновано встановлені програмні продукти вимагають фізичного доступу до комп'ютера користувача і обов'язкової наявності прав адміністратора для конфігурації і інсталяції [2].

З огляду на, що як раніше, так і зараз подібні додатки досить широко застосовуються зловмисниками аж ніяк не в благих цілях, ставлення до даної категорії софта неоднозначне. З одного боку, кейлоггери зараховують до числа небезпечних програм, що не дивно, адже з їх

допомогою перехопити конфіденційну інформацію, що вводиться користувачем, - не проблема. А тому подібне ПО нерідко служить для здійснення комп'ютерних злочинів, пов'язаних з розкраданням грошових коштів, а також використовується як інструмент економічного і політичного шпигунства.

З іншого боку, велика частина існуючих сьогодні кейлогерів позиціонується розробниками як легальне ПЗ, яке можна використовувати для вирішення цілого класу задач. Зокрема, клавіатурні шпигуни можуть виявитися дуже корисними для батьків, а також для викладачів в комп'ютерних класах і адміністраторів в інтернет-кафе. Наприклад, батькам не завадить бути в курсі того, які сайти відвідує їх дитина, якими програмами користується і з ким веде переписку або спілкується в чаті, і чи дійсно він займається на комп'ютері в їх відсутність, а не грає в улюблену іграшку. А викладачам і адміністраторам обов'язково потрібно чітко знати, що відбувається на підвідомчих комп'ютерах, оскільки підростаюче покоління, експериментуючи, за дві секунди примудряється вивести останні з ладу. Правда, в обох випадках проводити подібний моніторинг потрібно вкрай ненав'язливо, не посягаючи на свободу особистості (підростаючої, а значить, і більш вразливою) і не порушуючи тонку грань взаєморозуміння.

У підсумку виходить, що одні й ті ж додатки можуть використовуватися і в благих, і в злочинних цілях. А це означає, що власникам комп'ютерів слід бути в курсі існування подібного ПЗ і вживати заходів для запобігання витоку конфіденційної інформації. Тим же, кому в силу батьківських обов'язків або за службовим обов'язком доводиться нести відповідальність за власне чадо або за групу комп'ютерів, краще заздалегідь потурбуватися про можливі проблеми і встановити відповідну програму для моніторингу комп'ютерної діяльності, щоб в разі необхідності виявитися у всеозброєнні.

Сьогодні на ринку пропонується безліч клавіатурних шпигунів. У більшості випадків вони мають схожу базову функціональність, тобто перехоплюють натискання клавіш на клавіатурі, здійснюють моніторинг буфера обміну, фіксують відвідані веб-сторінки, запуск і закриття програм, а також ведуть запис знімків екрана. Подібні додатки забезпечують повну мультіпользовательской підтримку - це значить, що вести спостереження можна як відразу за всіма, так і тільки за обраними користувачами. А записана в ході проведеного ними моніторингу інформація зберігається в лог-файлах, і в подальшому її можна буде переглянути безпосередньо в додатках або перетворити в звіт (найчастіше в форматі HTML), який, як правило, може бути відправлений на вказану електронну скриньку, по FTP, а іноді і по локальній мережі. Розрізняються ж клавіатурні шпигуни деякими сервісними функціями і зручністю роботи зі звітами, а також якістю маскування в системі, тобто особливостями їх роботи в прихованому режимі. У найпростішому випадку під маскуванням мається на увазі відсутність додатків в списку програм меню Пуск, на робочому столі і в системному треї. А також приховування папки програми в директорії Program Files (в такому випадку для її запуску доведеться використовувати команду Пуск => Виконати або призначену для цієї мети функціональну комбінацію) і в списку програм, які видаляються панелі управління. В інших рішеннях теж передбачені можливості приховування в списку запущених процесів і в списку програм автозавантаження, а також є інструментарій для запобігання виявлення шпигунів антикейлоггерами [3].

Проникнення програмного кейлоггера в комп'ютер відбувається легко і непомітно. Шпигун може потрапити в систему разом з неліцензійним ПЗ, непомітно завантажитися при відвідуванні сайтів, при відкритті файлу, прикріпленого до електронного листа, і навіть бути вбудованим в інший додаток. Крім того, існують легальні кейлоггери, наприклад програма Punto Switcher від компанії «Яндекс». Вона не тільки автоматично перемикає розкладку клавіатури (що є її основною функціональністю), але і має опцію ведення щоденника, записуючи в текстовий файл всі натискання клавіш. Знаючи про це, зловмисники встановлюють її на комп'ютери жертв, так як Punto Switcher НЕ детектується антивірусними програмами. Кейлогери (keyloggers) втручаються в роботу комп'ютера, але не шкодять

операційній системі. Через відсутність деструктивних функцій, а також зважаючи на можливість легального використання їх відносять до небажаних програм, а не до шкідливим. Дійсно, реєстратор натискань клавіш може служити як хорошим засобом управління безпекою, так і результативним засобом її порушення. Побачити тонку грань між цими функціями допоможуть тільки цілі, з якими застосовувався кейлоггер. Отже, застосування клавіатурного шпигуна може бути санкціонованим і несанкціонованим. При санкціонованому використанні апаратного або програмного кейлоггера користувач ПК або ноутбука, інженер безпеки або власник автоматизованої системи ставиться до відома про його наявності. В такому випадку кейлоггери називаються моніторинговими продуктами і виконують ряд корисних функцій. Зокрема, реєстратори натискань клавіш санкціоновано застосовуються в державних установах, в приватних компаніях, на виробництвах і в інших різних організаціях. Установка кейлоггеров дає можливість визначити спроби передачі важливої інформації третім особам або набору паролів доступу, а також дослідити інциденти, пов'язані з комп'ютером. Клавіатурні шпигуни допомагають контролювати використання комп'ютерної техніки в особистих цілях або в неробочий час, а також отримати інформацію з жорсткого диска ПК, якщо з якоїсь причини немає пароля доступу. Кейлоггер дозволяє визначити, наскільки оперативно і грамотно персонал може реагувати на впливу ззовні. Крім того, кейлоггери вбудовуються в DLP-продукти з метою контролю листування персоналу для запобігання передачі секретної інформації. За допомогою реєстратора натискань клавіш можна відновити важливу інформацію після порушення роботи ОС. Несанкціоноване застосування кейлоггера полягає у впровадженні програми або апаратного пристрою без згоди і без відома власника або оператора. За допомогою кейлогерів здійснюється шпигунство в сфері політики і економіки, відкривається доступ до таємниць комерційних структур і державних установ, системам криптографічного захисту інформації, стає можливим заволодіння чужими грошовими коштами, використання облікових записів в своїх цілях. [4].

Щоб захиститися від розглянутого типу шкідливих програм, слід дотримуватися нескладних правил:

– Активуйте в вашому антивірусі функцію виявлення потенційно небезпечних програм (вона зазвичай відключена за замовчуванням);

– Для доступу до банківських даних користуйтеся двухфакторной ідентифікацією або одноразовим паролем.

– Використовуйте проактивний захист;

– Для введення важливих даних користуйтеся віртуальною клавіатурою [5].

Отже, сьогодні існує велика кількість програмних кейлоґґерів. Програмні продукти, що зберегли дану назву, виконують ще й багато додаткових функцій — це перехоплення інформації з вікон, перехоплення кліків миші, перехоплення буфера обміну, моніторинг файлової активності, моніторинг системного реєстру, моніторинг черги завдань, відправлених на принтер, перехоплення звуку з мікрофону та відеозображення з веб-камери, підключених до комп'ютера і так далі, тобто вони фактично відносяться до абсолютно іншого класу програмних продуктів, а саме до моніторингових програмних продуктів.

Література.

1. Кейлоггери [Електронний ресурс] // 2020. – Режим доступу до ресурсу: https://www.kickidler.com/ru/for-it/methods-of-working/10-luchshix-kejloggerov-dlya-slezhki-za-sotrudnikami.html

2. Застосування кейлоґґерів [Електронний ресурс] // Википедия. – 2020. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Keylogger.

3. Про клавіатурних шпигунів [Електронний ресурс] // 2020. – Режим доступу до ресурсу: https://compress.ru/article.aspx?id=18337

4. Об'єкт впливу [Електронний ресурс] // 2020. – Режим доступу до ресурсу: https://www.anti-malware.ru/threats/keyloggers