БЕЗПЕЧНИЙ ІТЕРНЕТ

Автор:
Барановська Анна

Шляхи розповсюдження вірусів

Розуміння того, як поширюються мережеві віруси, багато в чому може убезпечити користувача, який вміє захищатися від них. Знання – це не тільки сила, але і безпеку. Серед основних шляхів поширення можна згадати:

Електронну пошту.
Програмне забезпечення, отримане через FTP або Web.
Інфіковані сайти

Самозахист в мережі

Неможливо повністю убезпечити комп `ютер і операційну систему від проникнення шкідливих програм. Все що залишається користувачеві, це знизити потенційну небезпеку і по можливості попередити її. Для цього є деякі способи:

Не заходити на сторінки з потенційно небезпечним вмістом, контентом (+18) і по посиланнях, які надіслали невідомі люди через ICQ, Skype або Mail.

Не викачувати програми з невідомих джерел.

Не відкривати отриману пошту, якщо вона прийшла з невідомих адрес.

Поставити на систему хороший антивірус

Обережність і тільки обережність – головне правило при роботі, спілкуванні і розвазі через інтернет.

Чого побоюватися в Інтернеті.

Шкідливі програми. Вони можуть ховатися в скачуваних файлах, приходити до вас поштою і навіть «гніздитися» безпосередньо в коді електронного документа,
відкритого вами в браузері. Дуже часто трапляється, що потрапляння на ПК одного-єдиного «шкідника» непомітно для вас відкриває доступ до системи
безлічі інших програм — вони можуть не тільки частково або повністю знищувати дані, але також красти і пересилати своїм господарям конфіденційну
інформацію. Фальшиві антивіруси. Програма може називатися антивірусом, виглядати і працювати, як антивірус, але при цьому робити дещо ще. Вона стане виводити
попередження про шпигунський «софт» або вірусах, яких насправді немає на вашому ПК, а за лікування від цієї міфічної хвороби вимагати покупки повної версії або спеціалізованих «ліків».

Шкідливі програми

Сайти, що поширюють «троянців» та віруси
Такі сайти з'являються в Мережі часто. Щоб заманити на них користувачів, кіберзлочинці йдуть на різні хитрощі.
Наприклад, при появі яскравого новинного приводу — різкому висловлюванні публічної персони, вихід нового фільму, кліпу чи іншому подію, освітлюваному в різних ЗМІ, в блогах і т.д. — Кіберзлочинці публікують на популярних і відвідуваних сайтах явну або приховану рекламу, яка призводить нічого не підозрюють користувачів на сайти з шкідливим контентом.
При відвідуванні такого сайту «злоблива» програмне забезпечення може опинитися на комп'ютері користувача різними способами. Наприклад, відвідувачеві можуть запропонувати скачати розрекламований кліп або переглянути його прямо у вікні браузера. Але ось невдача — для перегляду необхідно встановити спеціалізований плеєр або плагін для браузера. Ті, хто скачав і встановив рекомендований кіберзлочинцями ПО, можливо, отримають доступ до бажаного контенту, але «в доповнення »до нього на комп'ютер абсолютно точно буде встановлено шкідливе програмне забезпечення.

Хто такі хакери

Технічні фахівці високої кваліфікації, здатні використовувати недокументовані можливості цифрового устаткування і програмного забезпечення. Слово «хакер» не є синонімом слова «кіберзлочинець», а «хакерство» само по собі не є злочин.На хакера не вчать ніде.

Більшість хакерів поєднує «стандартну» технічну підготовку з активним самоосвітою.

А ось недокументовані можливості програм і устаткування, особливості роботи вірусів, «больові точки» захисних структур, операційних систем і т.д. можна в тонкощах вивчити тільки самостійно.

Знання та інструменти хакера самі по собі не небезпечні (так само як і будь-які інші інструменти). Вони можуть виявитися вкрай корисними (наприклад, якщо ви забули пароль від архіву або облікового запису), а можуть стати знаряддям вчинення злочинів. Навіть набори вірусів і «троянці», які представлені на хакерських сайтах, можуть бути небезпечними, якщо «експонати» модифікувати і випустити у відкритий Інтернет, а можуть бути абсолютно нешкідливими, якщо використовуються для вивчення особливостей програмування.

Піратський контент

Шкідливі програми. Недобросовісні люди намагаються поширювати віруси і «троянці» і через «файлообмінники». Особливу небезпеку становлять собою програми для злому захисних систем пакетів і програм — «краки», генератори ключів і навіть архіви, що містять текстові файли з серійними номерами, так як всі вони можуть містити шкідливі коди. Втім, на популярних торрент-трекерах і файлообмінних ресурсах проводиться перевірка файлів на наявність інфікованих компонентів, і небезпечні посилання видаляються.

Переслідування за законом. У правоохоронних органах всіх країн (за винятком держав, в яких Інтернет заборонений в принципі) існують спеціальні відділи по боротьбі з кіберпіратством. Їх співробітники ведуть просту гру: вони пропонують нелегальні музичні файли і фіксують IP-адреси, куди вони завантажують.

The End