Олександр КОСТИНСЬКИЙ

МАЙКРОСОФТ І ВІРУСИ

Аж подив бере, наскільки вкорінилися в масовій свідомості міфи про комп'ютерні віруси. Живучість цих міфів зумовлюється тим, що головні причини тотального поширення вірусів практично не обговорюються в засобах масової інформації. Показовою стала остання пошесть. На перший погляд, вона не має ніякого стосунку до антимонопольного процесу проти Microsoft, та насправді компанія Білла Гейтса створила чудове живильне середовище для розмноження й розвитку тисяч цифрових вірусів.

Новинні стрічки з 4 травня 2000-го року рясніли на драматичні повідомлення: «Комп'ютерні мережі в усьому світі зазнали атаки вірусa ILOVEYOU... Завдано збитків мало не на десять мільярдів доларів кільком серйозним організаціям, серед яких компанії "Форд", AT&T, ЦРУ, Міністерство оборони США... Деякі аналітики твердять, що вірус вразив понад половину американських комп'ютерів... Тільки у Великобританії постраждала третина бізнесу. Великі проблеми створено вірусом у Канаді, Німеччині, Франції, скандинавських та розвинутих азіатських країнах...».

Наче в бойовику, зачарована публіка стежила за розшуком та спійманням філіпінського «електронного пірата» Реонела Рамонеса на прізвисько «Бароко» та його найближчих друзів. Потім співробітники місцевих спецслужб та ФБР виявили, що в написанні вірусa брали участь до 40 чоловік із хакерської групи GRAMMERSoft та студентів комп'ютерного коледжу в Манилі.

Багато хто з оглядачів не без підстав убачають причину масового враження комп'ютерів у низькій цифровій культурі більшості користувачів та у вдало вибраному словосполученні «Я тебе кохаю» у заголовку листа, пояснюючи вірусну пошесть віртуозною грою «на схильності майже кожної людини вірити та ціпеніти, коли їй зізнаються в коханні». Але це достатня причина лише для поширення файлових вірусів, тобто вірусів, які активізуються при відкритті файлів, доданих до листів. Чимало ж інших вірусів уживають інші механізми експансії. І, звичайно ж, руйнівний ефект комп'ютерної пошесті зумовлюється не самою тільки довірливістю людей та загальним браком теплоти спілкування.

Наголосимо: необхідною передумовою для поширення вірусів є помилки в операційних системах комп'ютерів. Лаври всесвітньої слави разом із філіпінськими хакерами по праву поділяють і ті, хто написав і запровадив з недоробками і дірками операційні системи Windows, програми Microsoft Office та Microsoft Outlook. Саме завдяки їхнім численним хибам усередину комп'ютерів проникають і діють піратські підпрограми. А отже, цифрові епідемії не є чимось невід'ємним від комп'ютерних технологій. Вони — постійні супутники недостатньо захищених та недопрацьованих продуктів.

Трохи детальніше скажемо, що ж це таке — комп'ютерний вірус. Це — не жива істота, і сам по собі він не виникає. Комп'ютерний вірус — це спеціально написана підпрограма, яка вбудовується в прогалини встановленого до цього на комп'ютері програмного забезпечення і тимчасово бере на себе керування файлами, які виконуються. Головною особливістю вірусу є здатність примусити комп'ютер створювати вірусні копії та передавати їх іншим комп'ютерам різними способами: через дискети, магнітооптику, CD-ROMи та, звісно ж, через різні цифрові мережі. Віруси не обов'язково шкодять комп'ютерам. Деякі просто попереджають про помилки у програмному забезпеченні або вказують на них шляхом запуску якихось графічних або звукових ефектів.

Вірус, який проникає в мільйони комп'ютерів, — це оригінальна, глибоко продумана, добре написана і ретельно відладжена програма. Багато вірусів використовують складні механізми самошифрування, змінюючи власну структуру, за спроби їх виявлення підставляють замість зараженого файла незаражений тощо. З огляду на все сказане зрозуміло, що написати таку програму самостійно неспроможні ні хакер «Бароко», ані навіть сорок його друзів.

Тріумфальна хода вірусів є ще одним прикладом успіхів одного з типів вільно поширюваного програмного забезпечення. Поява вдалого вірусу починається з аналізу хиб операційної системи та методів використання цих хиб. Такий аналіз здійснюють талановиті, висококваліфіковані програмісти, які розміщують результати своїх досліджень на численних Інтернет-вузлах. Самі вони [програмісти. — **Ред.**] рідко коли доводять свої ідеї до кінцевого продукту. Їхні знахідки стають основою для майстрів написання конкретних витончених кодів. Цей процес давно автоматизовано. Уже понад десять років існують спеціальні програми — генератори вірусів, своєрідні вірус-редактори, на яких їх [коди. — **Ред.**] зручно писати. Ці коди, у свою чергу, стають громадським надбанням, зазнаючи при цьому поліпшень та модифікацій. І на останньому етапі вірус-програма потрапляє до рук починаючих програмістів — школярів та студентів (як це й сталося з філіпінцями з комп'ютерного коледжу). Вони звичайно вносять у первісний код вірусу невеликі зміни. Але саме студенти і школярі — маргінальна частина комп'ютерного співтовариства — запускають численні копії вірусів у живе середовище. Вони ж у більшості випадків надають їм руйнівних функцій, тоді як кодекс справжніх хакерів забороняє їм завдавати шкоди при проникненні в чужі системи.

Процес поширення вірусу є подібним до імпульсного електричного розряду. Його природа — принципово статистична. Для гарантованого електричного пробою не тільки потрібно, щоб електричне поле перевищило певний поріг, а й необхідна достатня кількість початкових електронів. Так само і при розвитку вірусної пошесті. Недосить мати численні помилки й недоробки в масовому програмовому забезпеченні та якісні програми, які використовують ці дірки. Важливо постійно запускати в Мережу велику кількість близьких модифікацій одного й того ж самого виду вірусу, аж поки його характеристики не зрезонують з оточуючим комп'ютерно-людським середовищем, породивши вірусну лавину (що й сталося у випадку філіпінських студентів, котрі запустили кінцеву версію ILOVEYOU). До речі, співробітники спецслужб виявили на дискетах підозрюваних студентів величезну кількість схожих на вірус об'єктів. Їх спіткала доля більшості копій, які не «дотягують» до видатного вірусу і ланцюг розмноження яких є недосить довгим, через що й уривається. Отож 40 чоловік, що їх підозрюють у співучасті в комп'ютерному злочині, — це лише верхівка айсбергу причетних до народження вірусу.

Та повернімось до того ґрунту, на якому так рясно розквітає багатюща творчість «вірусописачів». **Уявляєте, скільки недоробок є у програмових продуктах Microsoft, якщо на них паразитують десятки тисяч вірусів?** ILOVEYOU — класичний приклад такого роду. Вірус вбудовується до поштового редактора Microsoft Outlook. Після відкриття файлу, доданого до листа, вірус, користуючись помилками у програмі, перехоплює керування та знищує або змінює не тільки деякі користувальні файли у зараженій машині, — завдяки незахищеності комп'ютера він псує саму операційну систему Windows, а вона відповідає за взаємодію всіх апаратних та програмних засобів комп'ютера. Після цього комп'ютер перетворюється на купу погано сполучених деталей і потребує нової установки операційної системи. Але, крім того, вірусна підпрограма ухитряється за допомогою Microsoft Outlook розіслати копію вірусу по всіх електронних адресах з адресної книги користувача.

Ще раз наголосимо — вірусні пошесті не є якоюсь фатальною і невід'ємною властивістю комп'ютерних систем. Середовищу Microsoft, де паразитують тисячі

вірусів, можна протиставити, наприклад, операційну систему Linux. Секрет Linux — у захищеності важливих вузлів паролями й пріоритетами та у відкритості вихідного тексту. Пріоритети не дають вірусам хазяйнувати всередині комп'ютера, а злам паролей при доступі до важливих файлів на мільйонах різних комп'ютерів — нерозв'язне завдання для будь-якого вірусу. Цілковита відкритість Linux дає змогу тисячам програмістів своєчасно знаходити недоліки в захисті та закривати їх латками. Те ж саме зробили після пошесті ILOVEYOU для Microsoft Outlook співробітники Білла Гейтса, — щоправда, вже після шоку всієї цифрової індустрії. Вихідні тексти програм Microsoft цілком або частково закриті, а система паролей та пріоритетів є надзвичайно слабкою. Зроблено це не зі злої волі чи з недбалості, а на догоду логіці дворічного циклу продаж нової версії масовому покупцеві.

На наш погляд, недоліки Windows є настільки серйозними, що вони ставлять під загрозу нормальний розвиток усієї цифрової індустрії. Windows — це фундамент для більшості прикладних програм, а фундамент будівлі повинен бути стійким навіть до малих збурень, хоч би звідкіля вони надходили. Якщо жменька філіпінських підлітків може струснути до основи комп'ютерні мережі, то зосередитися необхідно не на відомих недоліках підлітків і деталях злочину, а на докорінних хибах операційних систем, котрі перетворюють хуліганство на катастрофу.

На жаль, не можна сподіватися, що Windows буде замінена на Linux, але дає надію те, що американські законодавці натрапили на правильний напрямок у судовому позові до Microsoft. Це, звісно, не поділ компанії на дві частини, кожна з яких має одні й ті ж вади. Текст Windows повинен стати відкритим для всіх, повинен, як і текст Linux, стати громадським надбанням. Після цього необхідно терміново і спільними зусиллями захистити життєво важливі вузли операційної системи, спираючись на успішний досвід Unix-Linux-подібних систем. І не слід посилатися на зашкарубліть та лінощі рядового користувача. Та ж сама людина [тобто користувач. — **Ред.**] сумлінно вчить суворі правила шляхового руху і не ремствуючи складає іспити, несучи при цьому карну відповідальність за їхнє порушення. Більше того, при серйозних аваріях з вини шляхових служб, які відповідають за інфраструктуру, їхнє керівництво також несе пряму відповідальність. Чому ж тоді в комп'ютерній індустрії увесь вогонь зосереджується на стрілочниках, а не на тих, хто створив ненадійні залізниці?

Але справа полягає також і в тому, що хакери — не стрілочники. Їх можна уподібнити до вовків в екологічній системі. Вони успішно атакують лише хворих і слабких особин, посилюючи стійкість екосистеми в цілому. Спричинюючи своїми атаками постійну незручність, вони примушують егоїстичні фірми поліпшувати неякісний програмовий продукт і убезпечують тим самим комп'ютерну систему від глобальної катастрофи, що її цілком спроможні свідомо спровокувати розлючені на весь світ численні тоталітарні режими.

Що ж його робити зараз рядовим користувачам?

Можна вчинити радикально: знести продукцію Microsoft і запровадити вільно поширюваний швидкий і надійний софт. Якщо ж на це не стане духу, то треба бодай поставити безкоштовну програму PGP, яка на кожне вкладення в електронний лист ставить цифровий підпис, виключаючи тим самим запровадження вірусів. Якщо й це складно, то скористуйтеся хоча б слабеньким цифровим підписом у тому ж Microsoft Outlook та ні в якому разі не відкривайте механічно файли навіть від своїх знайомих, якщо вони не описані в самому електронному листі.

Джерело:

http://www.svoboda.org/programs/SC/2000/SC0523.shtml