Історія одного вірусу,
на даний час дуже поширеного

(*із власного досвіду боротьби*)

П. Семенюк

Останнім часом в Інтернеті поширюються віруси, якими комп'ютер заражається при вході на якийсь сайт. Він копіюється на комп'ютер-жертву, прописується для завантаження у реєстрі і блокує роботу Windows. При цьому на екрані виводиться повідомлення від СБУ чи МВД, що ваш Windows блоковано через якесь порушення і вам необхідно заплатити штраф, причому у дуже короткий термін. Дається докладна інструкція щодо проплати штрафу. Проплата має проводитись на електронний гаманець, який вказується. В іншому випадку ви будете притягнуті до кримінальної відповідальності, дані про вас будуть передані у відповідні органи, дані із BIOS та вінчестера будуть знищені і т.д.

Про ці віруси розповідали по телебаченню, писали у пресі, адже, трапляються люди, які дзвонять у відповідні органи із запитаннями, люди, які перераховують чималі суми на електронні гаманці шахраїв.

Розмовляючи з одним директором профтехзакладу дізнався, - через подібне довелося переустановлювати Windows майже на всіх комп'ютерах закладу, при цьому багато потрібної інформації, напрацювань педпрацівників було втрачено, адже видалити вірус не вдавалось жодному антивірусу (*це із його слів*).

На час розмови справи із подібними вірусами я не мав; порадити щось конкретне на той час, звичайно, - не міг.

Однак, досить швидко – десь через тиждень, у мене трапилась зустріч з подібним вірусом-вимагачем. Два дні, після роботи, прийшлося вести боротьбу з цим непроханим гостем. Причому, Windows перевстановлювати мені не довелося…

Тому, хочу поділитися досвідом, своєї боротьби (*ну і вислів - подібно до назви праці великого фюрера*). Надіюсь, для багатьох він буде корисним.

Отже, про все по-порядку. Свого часу неодноразово відвідував сайт pclib.in.ua. На сайті розміщено дуже багато корисної літератури, навчальних відео тощо. Але десь із місяць тому мій Nod32 при спробі зайти на названий сайт почав видавати попередження про його небезпечність. Однак бажання виявилось сильнішим. Набрав в адресному рядку браузера Mozzila адресу бажаного сайту і натиснув Enter.

На диво сайт відкрився і душу огорнула радість… Але через кілька секунд вона змінилась тривогою: на екрані з'явився електронний документ із шапкою Міністерства внутрішніх справ України у якому повідомлялось, що мій

Windows заблоковано, і ви, себто я, маю заплатити 940 грн. штрафу за перегляд та поширення дитячого гей-порно.

Такого злочину я не вчиняв, але доводити це нашим провоохоронцям – процедура не з приємних. Розумію, чому декотрі з користувачів Інтернет в подібному випадку перераховували шахраям чималі кошти. Далі в документі, йшла детальна інструкція як перерахувати гроші, вказувалась адреса електронного гаманця. При сплаті я мав отримати код для розблокування Windows.

На документі були розміщені кнопки із цифрами і поле вводу, куди потрібно було вводити код розблокування.

Внизу документа повідомлялось, що у випадку несплати штрафу протягом 12 годин, або переустановлення операційної системи дані про мене (вас) будуть передані відповідним органам для притягнення до кримінальної відповідальності, а ПК (вінчестер та BIOS) буде виведено з ладу.

Розробникам-шахраям потрібно віддати належне – документ справляв враження. При цьому спроба закрити вікно документу не приносила успіху: Alt+F4 чи Ctrl+Alt+Del не діяли, а курсор переміщувався в межах документу і вийти за них не було можливості.

Кнопка для перезавантаження комп'ютера дозволила перезавантажити операційну систему, але після введення логіну і паролю спочатку з'являлися обої на Робочому столі (вміст стола не завантажувався), а за ними – знову „грізний" документ.

Те, що це вірус і шахрайство – сумніву не було. Але, як діяти? Як вирішити проблему? Переустановлювати Windows? Це вирішив залишити на крайній випадок. Адже, при перевстановленні може бути знищено чимало потрібної інформації, особливо, на Робочому столі. А встановлювати по-новому ОС, всі драйвери, програми, налаштувати пристрої, Інтернет… – аж неприємно стає, як подумаю.

В такій ситуації важливо не панікувати, все обміркувати, можливо, відкласти дії на завтра. У росіян є гарна приказка „Утро вечера мудреней". (*Не подумайте, що перед ними схиляюся, просто, приказка неодноразово доводила свою правоту.*)

Перше, що виникає у думці користувача в такому випадку – перевірити персональний комп'ютер антивірусом. Оскільки, мій Nod32 зумів прогавити даний вірус, то потрібно шукати щось інше, а ще, - отримати потрібну інформацію на форумах в Інтернет, поспілкуватися з друзями, колегами.

Щодо друзів і колег, то в усіх випадках, при зустрічі з подібним – переустановлювали Windows. На форумах радили скористуватись антивірусними програмами, зокрема, антивірусною утилітою CureIt від Dr.Web.

Названа утиліта не раз виручала мене у подібних випадках; є безплатною, регулярно оновлюється (*пишуть – щодня*), скачати її можна за адресою

http://www.freedrweb.com/cureit/. Тому, на іншому комп'ютері (на роботі) скачав її нову версію. Названа утиліта постійно змінює назву виконуваного файлу. На час завантаження виконуваний файл мав назву 4d8ltm23.exe.

Оскільки, раніше я запускав CureIt із-під Windows, а вірус завантажити повністю Windows (зокрема, Explorer.exe) не дозволяє, виникло питання: „Як запустити CureIt?".

Пробую перезавантажити Windows у безпечному режимі. Перезавантажую ОС (кнопкою на системному блоці), тисну F8, вибираю Безпечний режим і чекаю завантаження.

Проходить певний час, Windows завантажується, … і знову виникає „грізне" повідомлення. Фокус не вдався.

Є ще один спосіб завантаження – Безпечне завантаження з підтримкою командного рядка. Цей режим, подібно до попереднього, вибирається з меню завантаження Windows, після натискання F8.

Однак, для того, щоб користуватись даним режимом потрібно знати команди MS DOS.

„Який MS DOS, адже ми маємо справу із Windows?! " - можливо хтось запитає. Для користувачів, які починали працювати з комп'ютером ще з часів зародження Windows, нічого дивного в цьому немає. Для більшості молодих та юних прийдеться дати роз'яснення.

Справа в тому, що з часів перший Windows (у мене – це 3.0, 3.1) відомо, що Windows – це операційна система, що являє собою графічну оболонку, побудовану на текстовій оболонці MS DOS. При завантажені Windows спочатку завантажується текстова оболонка MS DOS, а після неї графічна. В результаті отримуємо те, що називаємо Windows. Тому, якщо виникають проблеми з графічною оболонкою, – вирішити їх можна з допомогою текстової оболонки MS DOS. Для цього і потрібно знати команди MS DOS.

З історії від MS DOS до Windows відомо, що у зв'язку з тим, що командами MS DOS користуватись було незручно, програмісти придумали командні оболонки, – являли собою деякі таблиці із файлами і каталогами (підкаталогами або папками). В цих програмних оболонках можна було виконувати різні команди із файлами і каталогами, в тому числі, запускати програми. Щоб запустити програму, необхідно навести на неї курсор, виділити її і натиснути Enter.

Робота в цих оболонках нагадує роботу у Total Commander – програмі, яку багато користувачів і сьогодні використовують в останніх версіях Windows.

З тих часів я надавав перевагу програмі Volkov Commander. Програма подібна до свого іменитого конкурента Norton Commander, але має невеликий розмір – вміщується на дискеті, працює швидко, не лише в MS DOS, але і у Windows. Саме те, що потрібно…

Тому, перш ніж завантажувати Windows в режимі командного рядка, записав на DVD (можна – CD, або флешку) програму Volkov Commander (папка VC, у ній виконуваним є файл vc.com) та файл 4d8ltm23.exe (програма CureIt). Щоб простіше було вводити команди у командний рядок MS DOS (менше писати) записувати потрібно у кореневий каталог DVD-диску.

Отже, приступаю…

Перезавантажуюсь. Тисну F8, вибираю Безпечний режим з підтримкою командного рядка, вводжу логін і пароль. Завантажується консольне вікно (темного кольору) із командним рядком MS DOS. На екрані бачу напис C:\Documens and Settings\Петро> _ .

Там, де стоїть нижня риска, знаходиться мигаючий курсор; з цього місця вводяться команди MS DOS. Текст зліва від курсора, який називають запрошенням MS DOS, вказує на якому диску і в якому каталозі (папці) перебуваємо у даний час.

Моє завдання: 1) перейти на диск DVD; 2) запустити Volkov Commander (файл vc.com); 3) з Volkov Commander запустити антивірусну утиліту CureIt (файл 4d8ltm23.exe).

Пункт 2 можна пропустити, але Volkov Commander дозволяє наочно бачити зміст дисків і каталогів комп'ютера, і працювати стає зручніше.

Вводжу команди: ***E:*** і тисну Enter. У мене DVD-дисковод позначається E:. Командний рядок змінюється: *E:*\>_ . Якщо у вас позначення DVD-дисковода інше – введіть іншу букву.

Щоб побачити вміст диску вводжу команду ***dir/p***. Вона виводить вміст каталогу (папки) з переривами: заповнюється назвами файлів і підкаталогів весь екран зверху до низу і виведення припиняється, до натискання будь-якої клавіші. Після чого вивід продовжується до виведення змісту всього каталога.

При виведеднні вмісту каталога навпроти його підкаталогів міститься напис ***DIR*** - від „директорій", тобто каталог (підкаталог каталога у якому перебуваємо).

Бачу, що я дійсно перебуваю на DVD-диску, а в ньому є папка VC і файл 4d8ltm23.exe.

Входжу у папку VC, для чого у командному рядку набираю: ***cd VC*** (ввійти в каталог VC; щоб вийти назад - команда ***cd..***). Рядок MS DOS змінився: ***E:*** **\VC\>_.**

Запускаю програму Volkov Commander, для чого у командний рядок вводжу ***vc*** і тисну Enter. Панелі Volkov Commander завантажились. Стрілками переміщення курсора на клавіатурі, або мишкою наводжу світлове поле (прямокутник) на файл 4d8ltm23.exe і тисну Enter. Антивірус запустився.

Для того, щоб ввійти у підкаталог (папку) на панелях Volkov Commander потрібно навести на нього світлове поле і натиснути Enter. Щоб вийти з

підкаталога: перевести світлове поле (його іноді називають курсором) на самий верх підкаталогу, де є дві крапки (..), і натиснути Enter.

При запуску CureIt програма працює у режимі швидкої перевірки.

Швидка перевірка вірусів не виявила.

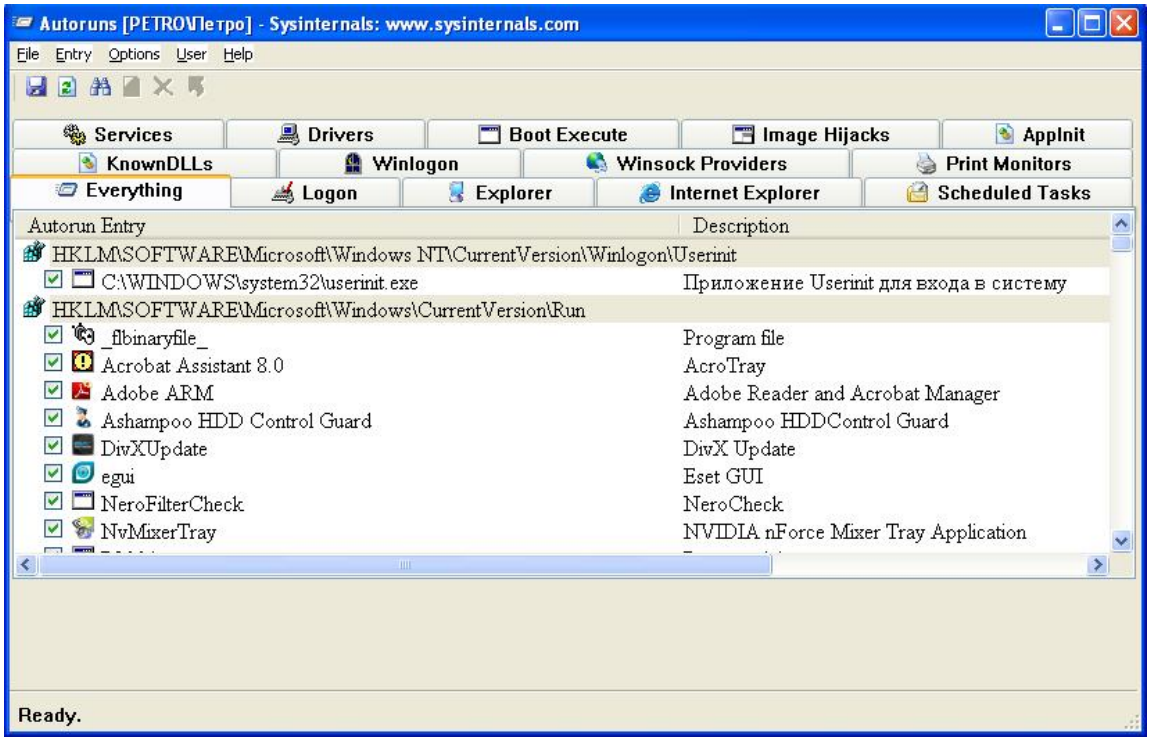
Вибрав режим вибіркової перевірки диска C:, запустив на перевірку. Програма почала виявляти віруси. За кілька годин, поки тривала перевірка, було виявлено десяток вірусів. Вилучив їх, перезапустив комп'ютер.

… І знову „грізне" вікно на екрані. Антивірусна програма, виявивши десяток інших вірусів, даного вірусу не виявила.

Знову перезавантажуюсь і запускаю Volkov Commander. Заходжу в папку Windows, для цього, якщо Windows на іншому диску, можна скористатись Alt+F1 або Alt+F2. Знаходжу Explorer.exe і запускаю Менеджер файлів. Працює. На екрані вікно Менеджера файлів. З нього можна запускати програми. Все працює! Роблю висновок: „Запуску віруса вдалося оминути. Отже, він запускається десь на етапі загрузки Windows, після вводу логіна і паролю користувача і перед запуском Менеджера файлів".

— „Звідки ж тоді він запускається?" І тут згадую, що у мене на ком'ютері встановлений Total Commander Podarok Edition, з якого кнопкою запускається програма Autoruns; вона показує, що стартує у системі. До речі, дану програму можна запустити і незалежно від Total; міститься вона у папці Program менеджера Total Commander.

Запускаю з Total Commander*a* програму Autoruns. Вид програми на малюнку.



На закладці Everything бачу у якому порядку, звідки і які програми запускаються. Після програми Userinit, - ініціалізації користувачів у системі, міститься вітка (*на малюнку не показано*)

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
у якій запускається програма C:\Documents and Settings\Петро\Local Settings\Temp\0.03545498714337891g8j8.exe.

Опис програми: Woods Bloom Adept Sleep Hiram.

Перший рядок у вітці вказує, що програма запускається із системного реєстра, тобто це є шлях до загрузки програми у реєстрі.

Другий рядок вказує на шлях розміщення програми та назву програми.

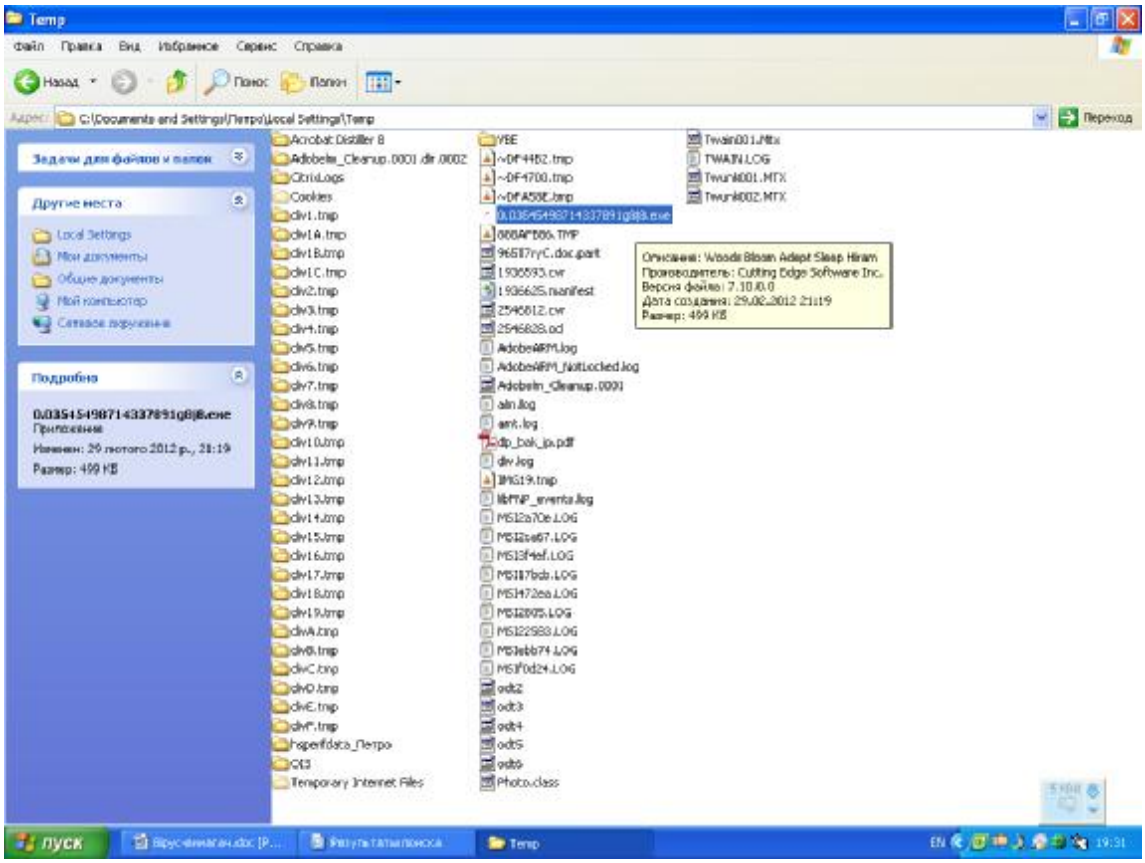
Включений зліва прапорець інформує, що програма активується при завантаженні.

Та чи вона це?

Знімаю прапорець, виходжу з Autorunsa і перезавантажую Windows.

Yes!!! Ось де „собака зарита“! Все працює нормально!

Заходжу у вказаний каталог і бачу її - „тепленьку“ (*див. мал.)*.



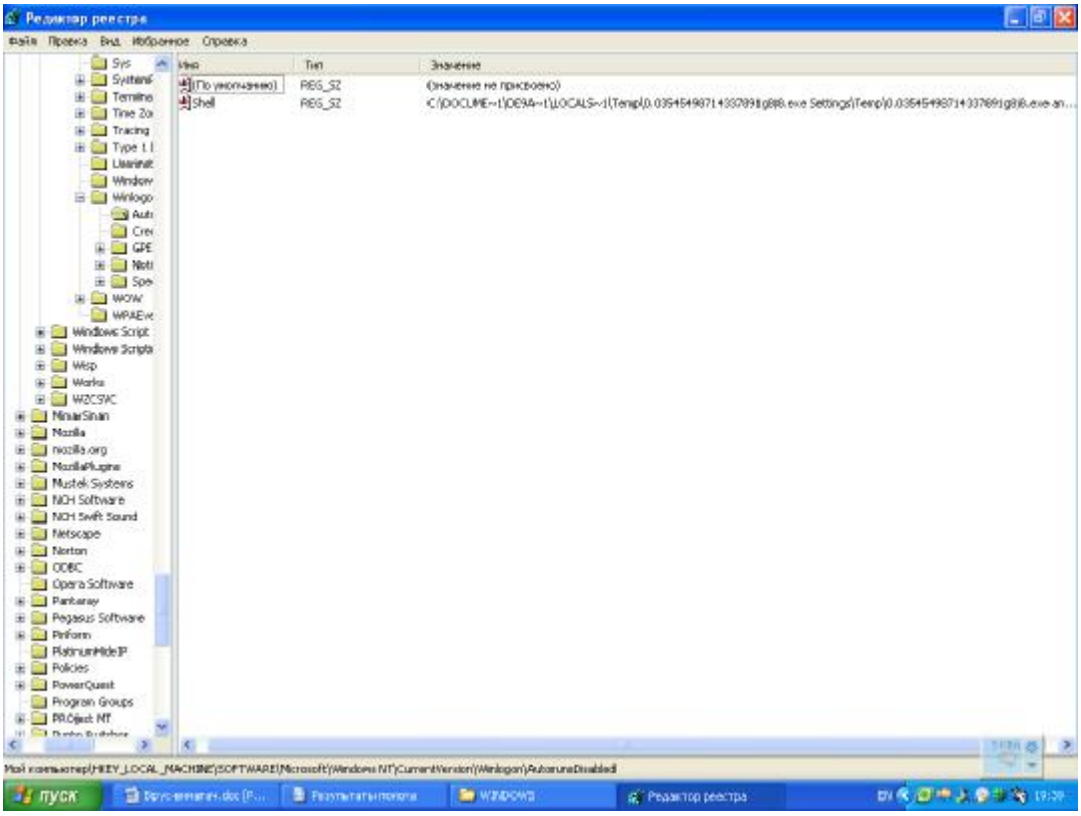
Щоб переконатись, що це дійсно той самий вірус, – запускаю подвійним кліком. Знову на екрані „страшне“ попередження, але тепер ми його не боїмося!

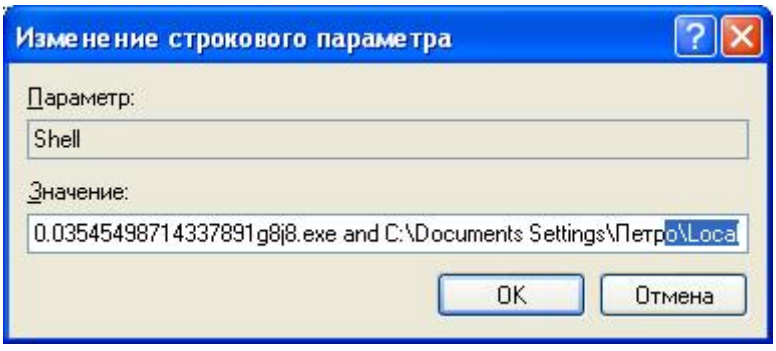
Що ж, пограємось і ми із тобою у „кошки-мишки“: запускаю CureIt у режимі вибіркової перевірки, вказую каталог із вірусом,… – антивірус мовчить. Потім виконую пошук файла вірусу через Меню ->Найти, ввожу його ім’я (скопіювавши). Пошук не дає результатів. Отже, вірус чудово маскується від антивірусів.

Замість злості до шахраїв-вимагачів, яка було на початку, виникло почуття поваги. Мабуть, розумні хлопці писали даний вірус; особливо, врахували

людську психологію, сучасний рівень користувачів персональних комп'ютерів, передбачили їх типові дії. А те, що вірус легко шукається з допомогою Autorunsa, так це не кожен додумається; а ще потрібно трішки знати MS DOS і принципи функціонування операційної системи. І нарешті, щоб показати користувачу документ (щоб він заплатив), ради чого і писався вірус, він (документ) мусить завантажитись в ОС, а отже від Autorunsa не сховається.

Залишилось поставити крапку у цій боротьбі: запускаю regedit.exe із каталога Windows, шукаю HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell і вилучаю рядковий параметр Shell (шлях до файла вірусу). *Див. малюнки.*





І нарешті, входжу у каталог із вірусом, виділяю, дякую за науку,… і тисну клавішу Delete.