МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ
ВИЩИЙ ПРИВАТНИЙ НАВЧАЛЬНИЙ ЗАКЛАД
МІЖНАРОДНИЙ ЕКОНОМІКО-ГУМАНІТАРНИЙ
УНІВЕРСИТЕТ ІМЕНІ АКАДЕМІКА
СТЕПАНА ДЕМ'ЯНЧУКА

О.М. ЧЕРКУН

СУЧАСНІ ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

Книга 7

Науковий керівник:
кандидат технічних наук,
доцент Р.М. Літнарович

Рівне 2012р.

УДК 614.2

Черкун О.М.. Сучасні технології комп'ютерної безпеки. Монографія. Науковий керівник Р.М.Літнарович. МЕГУ, Рівне, 2012. – 90с.
Cherkun O.M.. Modern technologies of computer safety. Monograph. Scientific leader R.M.Litnarovich. IEGU, Rivne, 2012. – 90p.
Рецензисти: В.Г.Бурачек, доктор технічних наук, професор
Є.С. Парняков, доктор технічних наук, професор
В.О. Боровий, доктор технічних наук, професор
Відповідальний за випуск: Й. В. Джунь, доктор фізико-математичних наук, професор.

Розглянуті особливості комп'ютерної безпеки, засоби та методи захисту комп'ютерних систем. Особлива увага приділяється шкідливим програмам, а саме комп'ютерним вірусам, черв'якам, троянським програмам. Подано методи їх виявлення та боротьби з ними. Докладно розглянуто віруси-вимагачі, їх види, класифікацію та подано способи їх видалення

Ключові слова: комп'ютерна безпека, комп'ютерний вірус, шкідлива програма, комп'ютерні черв'яки, троянські програми, віруси – вимагачі, Trojan.Winlock.

Рассмотрены особенности компьютерной безопасности, средства и методы защиты компьютерных систем. Особое внимание уделяется вредоносным программам, а именно компьютерным вирусам, червям, троянским программам. Подано методы их обнаружения и борьбы с ними. Подробно рассмотрены вирусы-вымогатели, их виды, классификацию и представлены способы их удаления

Ключевые слова: компьютерная безопасность, компьютерный вирус, вредоносная программа, компьютерные черви, троянские программы, вирусы - вымогатели, Trojan.Winlock.

Considered features of computer security tools and methods of protecting computer systems. Particular attention is paid to a malicious program, such as computer viruses, worms, Trojan horse. Methods of detection and control them. Considered in detail viruses extortionists, their types, classification and presented ways to remove them

Keywords: computer security, computer virus, malware, computer worms, Trojan horses, viruses - extortionists, Trojan.Winlock.

Черкун Оксана Мирославівна,
магістрант інформаційних технологій.

Зміст

Передмова

В даний час дуже широко використовується термін "комп'ютерна безпека". Насправді комп'ютер схильний лише кільком ризикам, якщо він по мережі не підключений до інших комп'ютерів. За останній час відсоток використання комп'ютерних мереж (особливо Інтернету) значно виріс, тому сьогодні термін «комп'ютерна безпека» використовується для опису проблем, пов'язаних з мережевим використанням комп'ютерів і їх ресурсів.

Основними технічними складовими комп'ютерної безпеки є:

- Конфіденційність;
- Цілісність;
- Аутентифікація;
- Доступність.

Конфіденційність, також відома як секретність, означає, що у неавторизованих користувачів не буде доступу до вашої інформації. Наслідки, які можуть бути викликані прогалинами в конфіденційності, можуть варіюватися від незначних до руйнівних.

Цілісність означає, що ваша інформація захищена від неавторизованих змін, що не відноситься до авторизованим користувачам. Загрозу цілісності баз даних і ресурсів, як правило, представляє хакерство.

Аутентифікація - це сервіс контролю доступу, який здійснює перевірку реєстраційної інформації користувача. Іншими словами це означає, що користувач - це є насправді той, за кого він себе видає.

Доступність означає те, що ресурси доступні авторизованим користувачам.

Іншими важливими компонентами, яким велика увага приділяється професіоналами в області комп'ютерної

безпеки, є контроль над доступом і суворе виконання зобов'язань. Контроль над доступом має на увазі не тільки факт, що користувач має доступ тільки до наявних ресурсів і послуг, але й той факт, що у нього є право доступу до ресурсів, які він законно очікує. Що стосується суворого виконання зобов'язань, то це має на увазі неможливість відмови користувачам того, що він відправив повідомлення і навпаки.

Концепція комп'ютерної безпеки дуже велика, тому до даних технічних аспектів є й інші додатки. Коріння комп'ютерної безпеки закладені в дисципліні. Основними питаннями, пов'язаними з цим терміном, є комп'ютерний злочин (спроби запобігти, виявити атаки) та конфіденційність / анонімність в кіберпросторі.

Хоча конфіденційність, цілісність, аутентифікація є важливими компонентами комп'ютерної безпеки, для користувачів Інтернету найбільш важливою складовою є конфіденційність, тому що більшість користувачів думають, що їм нема чого приховувати або інформація, яку вони надають при реєстрації на сайті, не є секретною.

В Інтернеті інформація дуже швидко поширюється серед компаній і потроху зібрана інформація з різних джерел може багато чого сказати про людину. Тому можливість контролю інформації, для чого вона збирається, хто і як може нею скористатися є дуже серйозним і важливим питанням в контексті комп'ютерної безпеки.

1. Комп’ютерна безпека

Особливості захисту персональних комп'ютерів (ПК) обумовлені специфікою їх використання. Як правило, ПК користується обмежене число користувачів. ПК можуть працювати як в автономному режимі, так і у складі локальних мереж (сполученими з іншими ПК), можуть бути підключені до віддаленого ПК або до локальної мережі.

Стандартність архітектурних принципів побудови, обладнання та програмного забезпечення персональних комп'ютерів, висока мобільність програмного забезпечення і ряд інших ознак визначають порівняно легкий доступ професіонала до інформації, що знаходиться в ПК. Якщо персональним комп'ютером користується група користувачів, то може виникнути необхідність в обмеженні доступу до інформації різних споживачів.

Несанкціонованим доступом (НСД) до інформації ПК будемо називати незапланованe ознайомлення, обробку, копіювання, застосування різних вірусів, а також модифікацію або знищення інформації. У захисті інформації ПК від НСД можна виділити три основні напрямки:

- Перше орієнтується на недопущенні порушника до обчислювального середовища і ґрунтується на спеціальних технічних засобах розпізнавання користувача;
- Друге пов'язане з захистом обчислювального середовища і ґрунтується на створенні спеціального програмного забезпечення по захисту інформації;
- Третій напрям пов'язаний з використанням спеціальних засобів захисту інформації ПК від несанкціонованого доступу.

1.1. Види вторгнення. Класифікація

Залежно від мети вторгнення, існує можливість визначити їх класи, які діляться на п'ять основних типів:

- апаратні засоби. Сервери, робочі станції, периферійні пристрої (принтери, сканери), мережеві кабелі і різноманітні дискові накопичувачі. У тому числі і мережеве устаткування: комутатори, маршрутизатори, мости;
- програмне забезпечення. Те або інше програмне забезпечення, встановлене на будь-якому з комп'ютерів, який включений в мережу, може стати можливим «ключем» для проникнення недоброзичливця. І не має значення, чи куплені ці програми у сторонніх розробників, або створені власним IT-відділом. Важливо відзначити, що операційні системи, що є базою для роботи всіх необхідних програмних продуктів, потребують регулярного оновлення (установка «патчів»);
- інформація. Найважливішою цінністю володіють дані, операція якими відбувається в комп'ютерній мережі. Якщо будь-яке програмне забезпечення і самі операційні системи можна відновити (або переустановити), то цілісність даних, як правило, не підлягає відновленню. Наприклад, список клієнтів, що потрапив до рук недоброзичливців, може вилитися в справжню катастрофу для всього бізнесу;
- люди. Користувачі, що працюють в єдиній мережі, завжди знаходяться в зоні ризику. Про це варто пам'ятати завжди;
- документи. Статистика показує, що різні паролі, дані і значну конфіденційну інформацію дуже часто переносять на паперовий носій (роздрук, записи на листах паперу і багато що інше). І, як правило, рано чи

пізно вся подібна «паперова» інформація потрапляє в сміття і просто викидається. Недоброзичливець може цим скористатися і оволодіти закритою для нього інформацією. Слід знати, що будь-які паперові носії, перш ніж бути викинуті, мають бути знищені. Наприклад, за допомогою спеціального утилізатора паперу.

Політика безпеки, яку дійсно можна назвати хорошою і ефективною, повинна, перш за все, бути зрозуміла всім користувачам. Проте, не все так просто, адже далеко не всі можуть все зрозуміти досконально. Для вирішення цієї проблеми рекомендується проводити постійні повторні ознайомлення робочого персоналу з наявною політикою безпеки. Це може бути виконано не тільки на спеціальних інструктажах, але і безпосередньо на самому робочому місці. І найголовніше - не розцінювати подібні дії як просту формальність. Користувачі повинні розуміти всю узяту на себе відповідальності і сприяти збереженню інформації.[34]

1.2. Спеціальне програмне забезпечення для захисту інформації ПК

Для захисту персональних комп'ютерів використовуються різні програмні методи, які значно розширюють можливості по забезпеченню безпеки інформації, що зберігається. Серед стандартних захисних засобів персонального комп'ютера найбільше поширення отримали:

- Засоби захисту обчислювальних ресурсів, що використовують парольну ідентифікацію і обмежують доступ несанкціонованого користувача;
- Застосування різних методів шифрування, що не залежать від контексту інформації;

- Засоби захисту від копіювання комерційних програмних продуктів;
- Захист від комп'ютерних вірусів і створення архівів.

1.3. Засоби, що використовують парольну ідентифікацію

У найпростішому випадку завжди можна скористатися апаратними засобами встановлення пароля на запуск операційної системи ПК з допомогою установок в CMOS Setup. При запуску ПК на екрані монітора з'являється повідомлення (залежно від типу встановленого BIOS) види: «Press DEL if you want to run Setup» або «Press CtrlAltEsc if you want to run Setup» (для деяких видів BIOS).

Якщо натиснути клавішу DEL або (Ctrl + Alt-Esc), на екрані з'явиться меню CMOS Setup. Вибравши опцію Password Checking Option, потрібно ввести пароль, зберегти нові установки Setup (F10, Y) та перезапустити комп'ютер. Таким чином перед кожним запуском комп'ютера на екрані монітора буде з'являтися повідомлення з вимогою ввести пароль.

На жаль, використання подібної парольної ідентифікації не є надійним. Досить ввести універсальний пароль (AWARD_SW) або відключити акумуляторну батарею, розташовану на материнській платі, і комп'ютер забуде всі налаштування CMOS Setup.

Захист вбудованого накопичувача на жорсткому магнітному диску становить одну з головних завдань захисту ПК від стороннього втручання. Існує кілька типів програмних засобів, здатних вирішити проблему захисту: захист від будь-якого доступу до жорсткого диска, захист диска від запису / читання; контроль за зверненням до диска; засоби видалення залишків секретної інформації.

Захист вбудованого жорсткого диска зазвичай здійснюється шляхом застосування спеціальних паролів для ідентифікації користувача (так звана парольна ідентифікація). У даному випадку доступ до жорсткого диску можна отримати при правильному введенні пароля під час завантаження операційної системи. В іншому випадку завантаження системи не відбудеться, а при спробі завантаження з гнучкого диска, жорсткий диск стає невидимим для користувача. Ефект захисту жорсткого диску в системі досягається видозміною завантажувального сектора диска, з якого видаляється інформація про структуру диска. Такий захист досить ефективний, і він надійно захищає жорсткий диск від звичайного користувача.

1.4. Використання криптографії

Можливість використання персональних комп'ютерів в локальних мережах (при сполученні їх з іншими ПК) або застосування "модемів" для обміну інформацією по телефонних дротах пред'являє більш жорсткі вимоги до програмного забезпечення щодо захисту інформації ПК. Споживачі ПК в різних організаціях для обміну інформацією все ширше використовують електронну пошту, яка без додаткових засобів захисту може стати надбанням сторонніх осіб.

Найнадійнішим захистом від несанкціонованого доступу до передаваної інформації та програмних продуктів ПК є застосування різних методів шифрування (криптографічних методів захисту інформації).

Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту,

безумовно, найбільш надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм, що розширюють можливості стандартної операційної системи. Захист на рівні операційної системи, частіше за все, повинен доповнюватися засобами захисту на рівні систем управління базами даних, які дозволяють реалізовувати складні процедури управління доступом.

В даний час не існує загальноприйнятої класифікації криптографічних методів захисту інформації. Проте, коли піддається перетворенню (шифровці) кожен символ передаваного повідомлення ("симетричний" метод закриття інформації), можна умовно виділити чотири основні групи:

- Підстановка - символи тексту, що шифрується, замінюються символами того ж або іншого алфавіту відповідно до заздалегідь визначеного правила;
- Перестановка - символи тексту, що шифрується переставляються по деякому правилу в межах заданого блоку передаваного тексту;
- Аналітичне перетворення – текст, що потрібно зашифрувати, перетворюється за деяким аналітичним правилом;
- Комбіноване перетворення - вихідний текст шифрується двома або великим числом способів шифрування. Існує велика кількість програмних продуктів шифрування інформації, що розрізняються за ступенем надійності. [1]

1.5. Безпека з фізичної точки зору

Несанкціонований доступ, а точніше його запобігання - це, перш за все, фізичне блокування доступу

до мережі, що захищається. Плюс позбавлення доступу до комп'ютерів і серверів мережі, кабелів повідомлень і різних периферійних пристроїв. У тому випадку, коли мережа і підключення до неї виходять за рамки контрольованої зони (наприклад, вихід в Інтернет через провайдера), необхідні особливі заходи, такі як організація віртуальних тунелів або шифрування. На додаток до цього, все устаткування, яке так чи інакше бере участь в обміні даними, повинне завжди знаходитися під контролем.

Банальним, але в той же час надзвичайно дієвим засобом подібного контролю може стати надійний дверний замок. Всі сервери і сховища даних повинні знаходитися в закритих приміщеннях. У них повинні мати доступ тільки компетентні особи із строгим рівнем допуску. Подібними заходами захисту мають бути забезпечені і пристрої функціонування мережі (концентратори, маршрутизатори і інші пристрої). Всі комп'ютери повинні знаходитися в приміщеннях, що закриваються на замок, за якими здійснюватиметься спостереження. Існує багато способів організації контролю і спостереження за приміщеннями, наприклад - реєстраційний журнал і вказівка в нім всіх відвідувачів. Різні резервні копії даних, розміщені на носіях (лазерні диски, стрічки, касети), повинні зберігатися в закритих місцях без загального доступу, наприклад - в сейфах.[34]

1.6. Антивірусне програмне забезпечення

Для захисту комп’ютерів від вірусів, часто доводиться користуватися антивірусним програмним забезпеченням. Встановлювати антивіруси потрібно обов’язково самої останньої версії, та постійно оновлювати вірусні бази та саму програму. Без цього комп’ютер залишається беззахисним від вірусних атак.

Жодна область індустрії програмного забезпечення не розвивається так швидко і не відрізняється такою жорсткою конкуренцією, як розробка антивірусних програм. Їх розробки діють в зоні постійних «бойових дій». Вони зобов'язані постійно оновлювати антивірусне програмне забезпечення, відповідаючи на нову загрозу з Інтернет, розроблювати нові версії програм, щоб дати відсіч останнім вірусним «розробкам». Крім того, кожен з них намагається бути першим: першим знайти новий вірус, першим назвати його і т.д.

Існує більше десятка високоякісних антивірусних програм, що розрізняються по ціні і набору виконуваних функцій.[33]

Антивірусне програмне забезпечення можна розглядати як імунну систему організму. Так, якщо організм піддаєтеся «нападу» хвороби, то його імунна система намагається затримати (і знешкодити) збудника інфекції, перш ніж людина захворіє. Основна ціль антивірусної програми також полягає в тому, щоб захистити комп'ютер від зараження вірусами. Вона аналізує в оперативному режимі все, що робиться на комп'ютері, і намагається не дати шансу вірусам «прижитися» в ньому.

Існує багато модифікацій вірусу, які використовують різні способи атаки. Саме тому не знайдено універсальний метод захисту від будь-якого вірусу. За час свого існування антивірусне програмне забезпечення набуло спеціальних функцій, які часто не залежать один від одного. Тому при виборі антивірусної програми слід шукати таку, яка підтримує всі описані функції.

Оперативна перевірка

З моменту завантаження системи антивірусна програма неперервно виконується у фоновому режимі,

перевіряючи систему на віруси. Перевірка відбувається кожен раз при збереженні файлу або виконанні програм, або коли користувач вставляє ком пакт – диск у CD-привід. Відбувається перевірка програм, які виконуються в пам'яті системи, - чи нема серед них підозрілої? Ціль оперативної перевірки полягає в тому, щоб запобігти інфікування файлів на комп'ютері або зразу виявити інфікований файл, що потрапив на нього, до того як вірус нанесе реальний збиток.

Якщо програма виявила вірус, то з'явиться вікно з повідомленням, що знайдена проблема. Зазвичай існує опція вибору, хочете ви зупинити виконання вірусу і видалити його або продовжити процес перевірки, якщо виявиться що це була «фальшива тривога».[32]

Повна перевірка системи

Крім неперервної перевірки на віруси в фоновому режимі, антивірусне програмне забезпечення може також виконувати повну перевірку системи. При цьому вона перевіряє на віруси весь вміст жорсткого диску. В процесі цієї перевірки, яка може продовжуватися більше години, система намагається виявити будь-який інфікований файл, який міг «обійти» захист. Наприклад, якщо інфікований файл потрапив в систему при спільному використанні файлів, оперативна перевірка може його пропустити, однак повна повинна виявити.

Ця перевірка може проводитися вручну, хоча більшість антивірусних програм має опцію, що дозволяє автоматично проводити повну перевірку системи з тою чи іншою регулярністю. Зазвичай достатньо проводити її раз на тиждень.

Перевірка електронної пошти

Оскільки існують віруси, що розповсюджуються через електронну пошту, то природно, що розробники антивірусного програмного забезпечення уділяють цьому

увагу. Багато програм мають функцію перевірки електронної пошти і перевіряють кожне вхідне та вихідне повідомлення на наявність вірусів. Антивірусні програми «стоять» між поштовим сервером і програмою електронної пошти на комп'ютері, перехоплюючи будь-які потенційно загрозливі повідомлення, перш ніж вони потраплять у поштову скриньку чи будуть відправлені.

Перевірка макросценаріїв

Багато розповсюджувачів вірусів намагаються використовувати беззахисність макромов типу JavaScript, які використовуються для створення додаткових функцій і інтерактивних елементів для Web - сторінок, або VBScript, що може бути «вмонтований» у Web – сторінку, а також використовується для створення додаткових функцій в програмах Microsoft Office. Так як макросценарії достатньо просто писати та модифікувати,то антивірусні програми намагаються виявити підозрілі сценарії або їх виконання якщо навіть це не сценарій попередньо виявленого вірусу.

Перевірка архівів

Багато розповсюджувачів вірусів намагаються сховати результати своєї чорної праці, створюючи файл архіву типу .zip. Антивірусна програма повинна перевірити на віруси вміст цього архіву. На жаль вона не може перевірити архів, захищений паролем, так як «не знає» пароля. Розповсюджувачі вірусів намагаються це використати: вони додають пароль у повідомлення електронної пошти і вірусом, переконуючи легковірних користувачів розпакувати архів і запустити вірус.

Контроль над підозрілими процесами

Навіть якщо антивірусна програма не може виявити вірус, вона здатна виявити підозрілий процес, який вказує на роботу вірусу. Наприклад, якщо програма розсилає багато повідомлень електронної пошти за секунду або з'єднується зразу з сотнями Web – серверів, то це може

виявитися спробою вірусу розповсюдитися. Ця функція антивірусної програми часто називається евристичним аналізом.

Інтеграція з Microsoft Office

Багато вірусів розповсюджуються через документи Microsoft Office. Цьому сприяють недоробки захисту Office, особливо макрокоманди та макромови, що використовуються для автоматизації функцій. Тому компанія Microsoft вбудувала в програми Office можливість антивірусної перевірки. Кожен раз при відкритті файлу Office автоматично перевіряє його за допомогою встановленої на комп'ютері антивірусної програми.

Підтримка миттєвих повідомлень

Ще одна проста можливість для розповсюдження вірусів – це передача файлів через миттєві повідомлення, тим більше що таким чином легко відправити інфікований файл незнайомим людям. Інколи антивірусні програми мають спеціальну функцію вхідних та вихідних файлів, що відправляються через миттєві повідомлення. Однак, як і у випадку з документами Office, деякі антивірусні програми в змозі перешкодити збереженню або виконанню будь-якого інфікованого файлу навіть при відсутності спеціальних функцій підтримки визначення програм.

Завантажувальний диск

Деякі з найбільш небезпечних вірусів можуть зробити неможливим завантаження операційної системи. Деякі антивірусні програми мають опцію завантажувального диску, яка дає можливість завантажити заблокований комп'ютер і видалити вірус.

Однак навіть якщо на комп'ютері встановлена найкраща антивірусна програма з усіма необхідними функціями і для них встановлені оптимальні налаштування, то все рівно віруси в змозі обійти і цей

захист. Розповсюджувачі вірусів постійно створюють нові версії, використовуючи «дірки» в системі захисту – як в операційній системі, так і безпосередньо в антивірусному програмному забезпеченні.

Найбільш вразливе місце антивірусної програми – це база даних описів вірусів, яку програма використовує, щоб визначити, що ж являється вірусом. Розповсюдження нових вірусів відбувається дуже швидко, і описів вірусів, зроблених за останній тиждень, не достатньо, щоб запобігти небезпеці. Таким чином потрібно оновлювати програмне забезпечення.[2]

2. Комп’ютерні віруси та черв’яки

Комп'ютерний вірус (англ. *computer virus*) - комп'ютерна програма, яка має здатність до прихованого само розмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Слід зазначити, що помилково відносити до комп'ютерних вірусів також інші види шкідливих програм - програми-шпигуни чи навіть спам.

За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні створення і поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363).

Назва програми "комп'ютерний вірус" походить від однойменного терміну з біології за її здатність до само розмноження. [3]

Комп'ютерний черв’як - програма, що сама розповсюджується, яка долає всі три етапи розповсюдження самостійно (звичайний черв’як), або використовує агента-користувача тільки на 2-му етапі (поштовий черв'як).

Черв’яки можуть використовувати різноманітні механізми («вектори») поширення. Деякі черв’яки потребують певних дій користувача для поширення (наприклад, відкриття інфікованого повідомлення в клієнті електронної пошти). Інші черв’яки можуть поширюватися

автономно, вибираючи та атакуючи комп'ютери в повністю автоматичному режимі. Іноді зустрічаються черв'яки з цілим набором різноманітних векторів поширення, стратегій вибору жертви.

Одним з найбільш відомих комп'ютерних черв'яків є «Хробак Моріса», написаний Робертом Морісом-молодшим, який був в той час студентом Корнельского Університету. Поширення хробака почалось 2 листопада 1988, після чого хробак швидко заразив велику кількість комп'ютерів, під'єднаних до Інтернету. [4]

2.1. Історія виникнення вірусів

Історія замовчує багато фактів, пов'язаних із зародженням комп'ютерного шкідництва, але дещо все-таки дійшло до наших днів. Грудень 1949 можна вважати початком виникнення комп'ютерних вірусів. Саме тоді в Іллінойському університеті Джон фон Нейман читав серію лекцій «Теорія і організація складних автоматів», яка і лягла в основу теорії само відтворювальних автоматів. Однак це була теорія. Першим чинним вірусом можна назвати гру Darwin (http://www.cs.dartmouth.edu/ ~ doug / darwin.pdf), яку винайшли в 1961 році співробітники компанії Bell Telephone Laboratories В. А. Висоцький, Х. Д. Макілрой і Р. Моріс.

Наступний етап - програма Creeper, що сама переміщувалася, створена на початку 1970-х років співробітником компанії BBN Бобом Томасом для підсистеми RSEXEC з метою продемонструвати можливість самовільного переміщення програм між комп'ютерами. Creeper не приносив шкоди: попередня копія знищувалася, а вірус переміщався на наступний комп'ютер.

У цей час була розроблена ще одна програма - Reaper, яку можна вважати першим антивірусом.

Переміщаючись по мережі, Reaper відшукував діючі копії Creeper і припиняв їхню роботу.

У 1970 році відбулася ще одна знакова подія. У травні в журналі Venture було опубліковано фантастичне оповідання Грегорі Бенфорда, в якому наведено один з перших описів вірусних та антивірусних програм - Virus і Vaccine. Через два роки в фантастичному романі «Коли Харлі був рік» Девіда Герролда було описано програми, що захоплювали системи подібно до черв'яків. Сам термін «черв'як» був вперше використаний в романі Джона Браннера "На шоковій хвилі», опублікованому в 1975 році.

Термін «комп'ютерний вірус» був вперше використаний в 1973 році в фантастичному фільм Westworld. Дане словосполучення вживалося в значенні, звичному для сучасної людини, - «шкідлива програма, яка проникла в комп'ютерну систему».

Нарешті, 20 квітня 1977 року був випущений комп'ютер, призначений для масового використання. Умови для реалізації само відтворювальних програм помітно покращилися. У 1980-х роках комп'ютери значно подешевшали і їх кількість збільшилася. Крім того, машини стали більш продуктивними, а ентузіастів, які отримали до них доступ, стало набагато більше.

Подальший розвиток подій нагадувало лавину. У 1987 році з'явився перший вірус, котрий інфікував IBM PC-сумісні комп'ютери під управлінням MS-DOS, - Brain. Цей вірус був досить нешкідливим: його дія полягала в зміні мітки на дискетах в 360 Кбайт. Brain був написаний двома пакистанськими програмістами, власниками компанії Brain Computer Services (звідси і назва вірусу), виключно в рекламних цілях, але на його основі були створені менш миролюбні особини. У тому ж 1987 році з'явився Jerusalem («Єрусалимський вірус»), запрограмований на видалення заражених файлів по

п'ятницях 13-го. Перші його версії містили помилку, завдяки якій він повторно діяв на вже заражені файли. У наступних версіях помилка була виправлена.

Хоча на той час вже з'явилися матеріали, присвячені безпеці інформації, все це сприймалося не більше ніж іграшкою, експериментом. Прозріння настало несподівано, коли ця «іграшка» перестала коритися і повела себе як розумний організм, що заражає все на своєму шляху. Це сталося 2 листопада 1988 року, коли студент Корнельського університету Роберт Моріс - молодший запустив програму-хробак, яка збереглася в історії під ім'ям свого розробника. Хробак Моріса став першим мережевим хробаком, успішно поширився «на волі», і однією з перших відомих програм, що експлуатують таку вразливість, як переповнення буферу.

Комп'ютери ставали все доступнішими. З часом більшість платформ і операційних систем уніфіковано, на ринку стали переважати Intel-сумісні комп'ютери, які працювали під управлінням операційної системи, розробленої компанією Microsoft. Подальші події розвивалися з величезною швидкістю. У 1991 році з'явився поліморфний вірус, що видозмінював своє тіло. Операційна система Windows 95 була практично готова, і її beta-версію розіслали 160 тестерам. Всі диски виявилися зараженими завантажувальним вірусом Form, і лише один тестер не полінувався перевірити диск антивірусом. У прес-релізі, присвяченому виходу принципово нової операційної системи, було сказано, що вона повністю захищена від вірусів всіх типів. Через кілька місяців ці заяви були рознесені вщент несподіваним подарунком – першим макровірусом, який представляв собою незвичний виконуваний файл, а сценарій, який заражав документи Microsoft Word. Протягом місяця макровірус Concept облетів навколо земної кулі, впровадився в комп'ютери

користувачів Microsoft Word і паралізував роботу десятків компаній по всьому світу.

У січні 1996 року з'явився перший вірус для операційної системи Windows 95 - Win95.Boza, а резидентний вірус Win95.Punch, що з'явився пізніше, остаточно підірвав довіру користувачів до Windows 95. У березні цього ж року почалася перша епідемія вірусу Win.Tentacle, написаного для Windows 3.0/3.1. Він заразив комп'ютерну мережу в декількох установах Франції. До цього всі Windows-віруси зберігалися тільки в колекціях та електронних журналах вірусотворців, на волі гуляли лише написані для MS-DOS завантажувальні і макровіруси. У цьому ж році був спійманий макровірус Laroux, написаний для Microsoft Excel.

У 1997 році на світ з'явилися нові види вірусів – FTP і mIRC-черв'яки, в червні 1998 року - вірус Win95.CIH. Цей вірус активізувався 26 квітня (вперше - в 1999 році) і знищував інформацію на жорсткому диску, записуючи на нього сміття. Крім того, він перезаписував Flash BIOS, якщо перемикач знаходився в положенні, що дозволяло запис, і виводив з ладу материнську плату.

Хробак I love you, випущений на Філіппінах в травні 2000 року, завдав власникам комп'ютерів збитків на суму, за деякими оцінками перевищує $10 млрд. Наступний черв'як, який увійшов в історію як Code Red, за 14 годин зумів заразити більше 300 тис. комп'ютерів, підключених до Інтернету. Після них були й інші, часто - перші в певної категорії. Наприклад, Nimda (слово admin, прочитане навпаки), багатовекторний черв'як, поширювався відразу декількома способами, включаючи «чорні ходи», залишені іншими хробаками. MyDoom був визнаний найшвидшим хробаком, що поширювався по електронній пошті.

До цього велика частина вірусів була написана на мові низького рівня - асемблері, дозволяла створити невеликий оптимізований вірус. Автором хробака AnnaKournikova, який вразив Інтернет в лютому 2001 року, виявився голландський студент, який взагалі не вмів програмувати, навіть на такій простій мові, як Basic.

Сьогодні загальні річні втрати всіх комерційних організацій від дій вірусів можуть зрівнятися з бюджетом невеликої країни, і ця сума щороку подвоюється. Заяви деяких фахівців з безпеки свідчать про серйозність проблеми. [6]

2.2. Класифікація вірусів

На сьогодні не існує офіційної класифікації вірусів. Однак можна все ж розподілити віруси за такими ознаками:

- за середовищем існування
- за способом зараження
- за алгоритмом роботи
- за ступенем небезпеки

За середовищем існування віруси поділяються на:

- *файлові* – віруси, які або різними способами впроваджуються у виконувані файли (найбільш поширений тип вірусів), або створюють файли-двійники (компаньйони-віруси), або використовують особливості організації файлової системи (link-віруси).
- *завантажувальні* віруси записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, що містить системний завантажувач вінчестера (Master Boot Record), або ж змінюють покажчик на активний boot-сектор.
- *мережеві* віруси використовують для свого поширення протоколи та команди комп'ютерних мереж.

o *поштові* віруси можна також віднести до мережевих, але їх чисельність та особливості їх роботи дозволяють виділити їх як окрему групу. Такі віруси найчастіше поширюються через електронну пошту: вони розсилають за адресами, наявними в адресній книзі. Для передачі можуть використовуватися засоби операційної системи або невеликий вбудований поштовий сервер (функція такого сервера - відправлення листів).

o *Макровіруси* - це програмами, написаними на макросах – послідовностях команд, які використовуються у деяких системах обробки даних, наприклад текстових редакторах та електронних таблицях. Можливості макросів в таких системах дозволяють вірусу переносити свій код в інші файли, заражаючи їх. Найбільшого поширення набули макровіруси для Microsoft Word і Excel.

o існує велика кількість *комбінованих* вірусів - наприклад, *файлово-завантажувальні* віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему. Інший приклад такого поєднання - *мережний макровірус*, який не тільки заражає редаговані документи, але і розсилає свої копії по електронній пошті.

Файлові і макровіруси сьогодні практично вимерли, тому що швидкість їх поширення значно нижче, ніж швидкість розповсюдження мережевих вірусів.[6]

За способом зараження середовища комп'ютерні віруси діляться на:

o *резидентні*. Ці віруси після їх активізації повністю або частково переміщуються з довкілля (мережа, завантажувальний сектор, файл) в оперативну пам'ять ЕОМ. Ці віруси, використовуючи, як правило, привілейовані режими роботи, дозволені тільки операційній системі, заражають середовище існування і

при виконанні певних умов реалізують деструктивну функцію.

- *нерезидентні*. На відміну від резидентних нерезидентні віруси потрапляють в оперативну пам'ять ЕОМ тільки на час їх активності, протягом якого виконують деструктивну функцію та функцію зараження. Потім віруси повністю залишають оперативну пам'ять, залишаючись в середовищі існування. Якщо вірус поміщає в оперативну пам'ять програму, яка не заражає середовище проживання, то такий вірус вважається нерезидентом.

Відповідно до особливостей алгоритму функціонування віруси можна розділити на два класи:

- *віруси, що не змінюють середовище існування* (файли і сектори) при поширенні;
- *віруси, які змінюють місце існування* при розповсюдженні.

У свою чергу, віруси, не змінюють середовище існування, можуть бути розділені на дві групи:

- *віруси-"супутники"* (companion). Віруси - «супутники» не змінюють файли. Механізм їх дії полягає в створенні копій виконуваних файлів. Наприклад, в MS DOS такі віруси створюють копії для файлів, що мають розширення. EXE. Копії присвоюється те ж ім'я, що і виконуваного файлу, але розширення змінюється на. COM. При запуску файлу з загальним ім'ям операційна система першої завантажує на виконання файл з розширенням. COM, який є програмою-вірусом. Файл-вірус запускає потім і файл з розширенням. EXE.
- *вируси-«черв`яки»* (worm) потрапляють в робочу станцію з мережі, обчислюють адреси розсилки вірусу по іншим абонентам мережі та здійснюють передачу вірусу.[7]

За ступенем небезпеки для інформаційних ресурсів користувача комп'ютерні віруси можна розділити на:

- *Нешкідливі* віруси. Деструктивний вплив таких вірусів зводиться до виведення на екран монітора невинних текстів і картинок, виконання музичних фрагментів і т. п. Однак такі віруси все ж завдають певної шкоди. По-перше, такі віруси витрачають ресурси комп'ютера, в тій чи іншій мірі знижуючи її ефективність функціонування. По-друге, комп'ютерні віруси можуть містити помилки, що викликають небезпечні наслідки для інформаційних ресурсів комп'ютера.
- *Небезпечні* віруси. До небезпечних відносяться віруси, які викликають істотне зниження ефективності комп'ютерної системи, але не призводять до порушення цілісності та конфіденційності інформації, що зберігається в запам'ятовувальних пристроях. Наслідки таких вірусів можуть бути ліквідовані без особливих витрат матеріальних і часових ресурсів
- *Дуже небезпечні* віруси. Дуже небезпечними вважаються віруси, що викликають порушення конфіденційності, знищення, необоротну модифікацію (у тому числі і шифрування) інформації, а також віруси, що блокують доступ до інформації, що призводять до відмови апаратних засобів і завдають шкоди здоров'ю користувачам. [7]

Використання в сучасних ПЕОМ постійної пам'яті з можливістю перезапису призвело до появи вірусів, що змінюють програми BIOS, що призводить до необхідності заміни постійних запам'ятовуючих пристроїв.

Можливий також вплив на психіку людини - оператора ЕОМ з допомогою підбору відеозображення, що видається на екран монітора з певною частотою (кожен двадцять п'ятий кадр). Вбудовані кадри цієї відеоінформації сприймаються людиною на підсвідомому рівні. У результаті такого впливу можливе нанесення серйозного збитку психіці людини. У 1997 році 700

японців потрапили до лікарні з ознаками епілепсії після перегляду комп'ютерного мультфільму по телебаченню. Припускають, що саме таким чином була випробувана можливість впливу на людину за допомогою вбудовування 25-го кадру.[8]

За складністю, ступенем досконалості і особливостям маскування алгоритмів віруси, які змінюють місце існування, діляться на:

- *Студентські*; До студентських відносять віруси, творці яких мають низьку кваліфікацію. Такі віруси, як правило, є нерезидентними, часто містять помилки, досить просто виявляються і видаляються.
- «*Стелс*» - віруси (віруси-невидимки) маскують свою присутність в середовищі проживання шляхом перехоплення звернень операційної системи до уражених файлів, секторів і переадресовують ОС до незаражених ділянок інформації. Вірус є резидентним, маскується під програми ОС, може переміщатися в пам'яті.
- *Поліморфні* віруси не мають постійних розпізнавальних груп. Звичайні віруси для розпізнавання факту зараження розміщують в зараженому об'єкті спеціальну двійкову послідовність або послідовність символів (сигнатуру), яка однозначно ідентифікує зараженість файлу або сектора. Сигнатури використовуються на етапі поширення вірусів для того, щоб уникнути багаторазового зараження одних і тих же об'єктів, оскільки при багаторазовому зараженні об'єкта значно зростає ймовірність виявлення вірусу. Для усунення демаскуючих ознак поліморфні віруси використовують шифрування тіла вірусу і модифікацію програми шифрування. За рахунок такого перетворення поліморфні віруси не мають збігів кодів.[6]

2.3. Загальний принцип дії вірусів

Будь-який вірус, незалежно від приналежності до певних класів, повинен мати три функціональних блоки: блок зараження (розповсюдження), блок маскування і блок виконання деструктивних дій. Поділ на функціональні блоки означає, що до певного блоку відносяться команди програми вірусу, що виконують одну з трьох функцій, незалежно від місця знаходження команд в тілі вірусу.

Після передачі управління вірусу, як правило, виконуються певні функції блоку маскування. Наприклад, здійснюється розшифрування тіла вірусу. Потім вірус здійснює функцію впровадження в незаражене середовище існування. Якщо вірусом повинні виконуватися деструктивні дії, то вони виконуються або безумовно, або при виконанні певних умов.

Завершує роботу вірусу завжди блок маскування. При цьому виконуються, наприклад, такі дії: шифрування вірусу (якщо функція шифрування реалізована), відновлення старої дати зміни файлу, відновлення атрибутів файлу, коректування таблиць ОС та ін..

Останньою командою вірусу виконується команда переходу на виконання заражених файлів або на виконання програм ОС.

Для зручності роботи з відомими вірусами використовуються каталоги вірусів. У каталог поміщаються такі відомості про стандартні властивості вірусу: ім'я, довжина, що заражають файли, місце впровадження в файл, метод зараження, спосіб впровадження в ОП для резидентних вірусів, що викликаються ефекти, наявність (відсутність) деструктивної функції і помилки. Наявність каталогів дозволяє при описі вірусів вказувати тільки особливі властивості, опускаючи стандартні властивості і дії. [7]

2.4. Методи боротьби з вірусами

Для боротьби з вірусами використовуються програмні та апаратно-програмні засоби, що застосовуються в визначеній послідовності і комбінації, створюючи методи боротьби з вірусами. Можна виділити методи виявлення вірусів і методи видалення вірусів.[9]

2.4.1. Методи виявлення вірусів

Відомі такі методи виявлення вірусів:[9]

- сканування;
- виявлення змін;
- евристичний аналіз;
- використання резидентних сторожів;
- вакцинування програм;
- апаратно-програмний захист від вірусів.

Сканування - один з найпростіших методів виявлення вірусів. Сканування здійснюється програмою-сканером, яка переглядає файли в пошуках пізнавальної частини вірусу - сигнатури. Програма фіксує наявність вже відомих вірусів, за винятком поліморфних вірусів, які застосовують шифрування тіла вірусу, змінюючи при цьому кожен раз сигнатуру. Програми-сканери можуть зберігати не сигнатури відомих вірусів, а їх контрольні суми. Програми-сканери часто можуть видаляти виявлені віруси. Такі програми називаються поліфагами.

Метод виявлення змін базується на використанні програм-ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких зазвичай розміщуються віруси. При періодичному виконанні програм-ревізорів порівнюються характеристики, що зберігаються і характеристики, одержувані при контролі областей дисків. за результатами

ревізії програма видає відомості про орієнтовну наявності вірусів.

Зазвичай програми-ревізори запам'ятовують в спеціальних файлах образи головного завантажувального запису, завантажувальних секторів, логічних дисків, характеристики всіх контрольованих файлів, каталогів та номери дефектних кластерів. Можуть контролюватися також об'єм встановленої оперативної пам'яті, кількість підключених до комп'ютера дисків і їх параметри.

Головною перевагою методу є можливість виявлення вірусів всіх типів, а також нових невідомих вірусів.

Є у цього методу і недоліки. За допомогою програм-ревізорів неможливо визначити вірус в файлах, які надходять у систему вже зараженими. Віруси будуть виявлені тільки після розмноження в системі.

Програми-ревізори непридатні для виявлення зараження макровірусами, так як документи і таблиці дуже часто змінюються.

Евристичний аналіз порівняно недавно почав використовуватися для виявлення вірусів. Як і метод виявлення змін, даний метод дозволяє визначати невідомі віруси, але не вимагає попереднього збору, обробки та зберігання інформації про файлову систему.

Суть евристичного аналізу полягає у перевірці можливих середовищ існування вірусів та виявлення в них команд (груп команд), характерних для вірусів. Такими командами можуть бути команди створення резидентних модулів в оперативній пам'яті, команди прямого звернення до дисків, минаючи ОС. Евристичний аналізатори при виявленні «підозрілих» команд в файлах або завантажувальних секторах видають повідомлення про можливе зараження. Після отримання таких повідомлень необхідно ретельно перевірити імовірно інфіковані файли і

завантажувальні сектори. Евристичний аналізатор є, наприклад, в антивірусній програмі Doctor Web.

Метод використання *резидентних сторожів* заснований на застосуванні програм, які постійно знаходяться в оперативний пам'яті комп'ютера і відстежують всі дії інших програм.

У разі виконання якою-небудь програмою підозрілих дій (звернення для запису в завантажувальні сектора, розміщення у оперативній пам'яті резидентних модулів, спроби перехоплення переривань і т.д.) резидентний сторож видає повідомлення користувачеві. Програма-сторож може завантажувати на виконання інші антивірусні програми для перевірки «підозрілих» програм, а також для контролю всіх файлів, що поступають ззовні (зі змінних дисків, по мережі і т.д.).

Істотним недоліком цього методу є значний відсоток помилкових тривог, що заважає роботі користувача, викликає роздратування і бажання відмовитися від використання резидентних сторожів. Прикладом резидентного сторожа може служити програма Vsafe, що входить до складу MS DOS.

Під вакцинацією програм розуміється створення спеціального модуля для контролю її цілісності. Як характеристики цілісності файлу зазвичай використовується контрольна сума. При зараженні вакцинованого файлу, модуль контролю виявлення змін контрольної суми повідомляє про це користувачеві. Метод дозволяє виявляти всі віруси, у тому числі й незнайомі, за винятком «стел» - вірусів.

Найбільш надійним методом захисту від вірусів є *використовування апаратно-програмних антивірусних засобів*. На сьогодні для захисту ПЕОМ використовуються спеціальні контролери та їх програмне забезпечення. Контролер установлюється в роз'єм розширення і має

доступ до загальної шини. Це дозволяє йому контролювати всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких у звичайних режимах роботи не допускається. Таким чином, можна встановити захист на зміну головного завантажувального запису, завантажувальних секторів, файлів конфігурації, виконуваних файлів та ін..

При виконанні заборонених дій будь-якою програмою контролер видає відповідне повідомлення користувачеві і блокує роботу ПЕОМ.

Апаратно-програмні антивірусні засоби мають низку переваг перед програмними:

• працюють постійно;

• виявляють всі віруси, незалежно від механізму їх дії;

• блокують недозволені дії, що є результатом роботи вірусу або некваліфікованого користувача.

Недолік один - залежність від апаратних засобів ПЕОМ. Зміна останніх веде до необхідності заміни контролера.

Прикладом апаратно-програмного захисту від вірусів може служити комплекс Sheriff.[7]

2.4.2. Методи видалення наслідків зараження вірусами

У процесі видалення наслідків зараження вірусами здійснюється видалення вірусів, а також відновлення файлів і областей пам'яті, в яких знаходився вірус. Існує два методи видалення наслідків впливу вірусів антивірусними програмами.

Перший метод передбачає відновлення системи після впливу відомих вірусів. Розробник програми-фага,

яка видаляє вірус, повинен знати структуру вірусу і його характеристики розміщення в середовищі існування.

Другий метод дозволяє відновлювати файли і завантажувальні сектори, заражені невідомими вірусами. Для файлів програма відновлення повинна завчасно створити і зберігати інформацію про файли, отриману в умовах відсутності вірусів. Маючи інформацію про незаражені файлі і використовуючи відомості про загальні принципи роботи вірусів, здійснюється відновлення файлів. Якщо вірус піддав файл незворотним змінам, то відновлення можливе лише з використанням резервної копії або з дистрибутива. При їх відсутність існує тільки один вихід - знищити файл та відновити його вручну.

Якщо антивірусна програма не може відновити головний завантажувальний запис або завантажувальні сектори, то можна спробувати зробити це вручну. У разі невдачі слід відформатувати диск і встановити операційну систему.

Існують віруси, які, потрапляючи в ЕОМ, стають частиною його ОС. Якщо просто видалити такий вірус, то система стає непрацездатною.[7]

2.5. Профілактика зараження вірусами комп'ютерних систем

Щоб убезпечити ЕОМ від впливу вірусів, користувач, перш за все, повинен мати уявлення про механізм дії вірусів, щоб адекватно оцінювати можливість і наслідки зараження комп’ютерної системи. Головною ж умовою безпечної роботи в комп’ютера є дотримання ряду правил, які апробовані на практиці і показали свою високу ефективність.

Правило перше. Використання програмних продуктів, отриманих законним офіційним шляхом. Імовірність наявності вірусу в піратської копії у багато

разів вище, ніж в офіційно отриманому програмному забезпеченні.

Правило друге. Дублювання інформації. Слід особливо подбати про збереження робочої інформації. Переважно регулярно створювати копії робочих файлів на знімних машинних носіях інформації.

Правило третє. Регулярно використовувати антивірусні програми. Перед початком роботи доцільно виконувати програми-сканери та програми-ревізори (Aidstest і Adinf). антивірусні засоби повинні регулярно оновлюватися.

Правило четверте. Особливу обережність слід проявляти при використанні нових знімних носіїв інформації та нових файлів. Нові диски обов'язково повинні бути перевірені на відсутність завантажувальних і файлових вірусів, а отримані файли - на наявність файлових вірусів. Перевірка здійснюється програмами-сканерами та програмами, що виконують евристичний аналіз (Aidstest, Doctor Web, AntiVirus). При першому виконанні виконуваного файлу використовуються резидентні сторожі. При роботі з отриманими документами і таблицями доцільно заборонити виконання макрокоманд засобами, вбудованими в текстові й табличні редактори (MS Word, MS Excel), до завершення повної перевірки цих файлів.

Правило п'яте. При роботі в розподілених системах або в системах колективного користування доцільно нові змінні носії інформації та файли перевіряти на спеціально виділених для цієї мети ЕОМ. Доцільно для цього використовувати автоматизоване робоче місце адміністратора системи або особи, яка відповідає за безпеку інформації. Тільки після всебічної антивірусної перевірки дисків і файлів вони можуть передаватися користувачам системи.

Постійне дотримання всіх наведених рекомендацій дозволить значно зменшити ймовірність зараження вірусами і захистити користувача від безповоротних втрат інформації.

В особливо відповідальних системах для боротьби з вірусами необхідно використовувати апаратно-програмні засоби (наприклад , Sheriff).[7]

2.6. Дії при виявленні зараження ЕОМ вірусами

Навіть при скрупульозному виконанні всіх правил профілактики можливість зараження ЕОМ комп'ютерними вірусами повністю виключити не можна. І якщо вірус все-таки потрапив до комп'ютерної системи, то наслідки його перебування можна звести до мінімуму, дотримуючись певної послідовності дій.

Про наявність вірусу в комп'ютері користувач може здогадатися за наступними подіям:

• поява повідомлень антивірусних засобів про зараження або про передбачуване зараження;

• явні прояви присутності вірусу, такі як повідомлення, що видаються на монітор або принтер, звукові ефекти, знищення файлів та інші аналогічні дії, що однозначно вказують на наявність вірусу в комп'ютерній системі;

• неявні прояви зараження, які можуть бути викликані й іншими причинами, наприклад, збоями або відмовами апаратних і програмних засобів комп'ютера.

До неявних проявів наявності вірусів в комп'ютері можна віднести «Зависання» системи, уповільнення виконання певних дій, порушення адресації, збої пристроїв тощо.

Отримавши інформацію про ймовірне зараження, користувач повинен переконатися в цьому. Вирішити таке

завдання можна за допомогою всього комплексу антивірусних засобів. переконавшись у тому, що зараження відбулося, користувачеві слід виконати наступну послідовність кроків:

Крок 1. Вимкнути ЕОМ для знищення резидентних вірусів.

Крок 2. Здійснити завантаження еталонної операційної системи зі змінного носія інформації, в якій відсутні віруси.

Крок 3. Зберегти на змінних носіях інформації важливі файли, які не мають резервних копій.

Крок 4. Використовувати антивірусні засоби для видалення вірусів і відновлення файлів, областей пам'яті. Якщо працездатність ЕОМ відновлена, то здійснюється перехід до кроку 8.

Крок 5. Здійснити повне стирання і розмітку (форматування) незнімних зовнішніх запам'ятовуючих пристроїв.

Крок 6. Відновити ОС, інші програмні системи і файли з дистрибутивів і резервних копій, створених до зараження.

Крок 7. Ретельно перевірити файли, збережені після виявлення зараження, і, при необхідності, видалити віруси та відновити файли;

Крок 8. Завершити відновлення інформації всебічною перевіркою ЕОМ за допомогою всіх наявних у розпорядженні користувача антивірусних засобів.

При виконанні рекомендацій з профілактики зараження комп'ютерними вірусами, а також при умілих і своєчасних діях у разі зараження, вірусами, збитки інформаційних ресурсів комп’ютерної системи можуть бути зведені до мінімуму.[7]

3. Троянські програми

Троянська програма. (також - троян, троянець, троянський кінь) - шкідлива програма, яка використовується зловмисником для збору інформації, її руйнування або модифікації, порушення працездатності комп'ютера або використання його ресурсів в непристойних цілях. Дія троянської програми може і не бути насправді шкідливою, але трояни заслужили свою погану славу за їх використання в інсталяції програм типу Backdoor. За принципом розповсюдження і дії троян не є вірусом, тому що не здатний поширюватися само розмноженням.[10] Троянська програма розповсюджується людьми. На відміну від вірусів і черв'яків, які поширюються мимовільно.[11]

Назва «троянська» походить від легенди про «троянського коня» - дарованому дерев'яному коні, що послужило причиною падіння Трої. У коні, подарованому в знак лже - премії, ховалися грецькі воїни, які вночі відкрили ворота армії завойовника. Велика частина троянських програм діє подібним чином - маскується під нешкідливі або корисні програми, щоб користувач запустив їх на своєму комп'ютері. Вважається, що першим цей термін у контексті комп'ютерної безпеки вжив Деніел Едвардс, співробітник NSA, у своєму звіті «Computer Security Technology Planning Study». [11]

Троянська програма запускається користувачем вручну або автоматично - програмою або частиною операційної системи, що виконується на комп'ютері-жертві (як модуль або службова програма). Для цього файл програми (його назву, іконку програми) називають службовим ім'ям, маскують під іншу програму, файл іншого типу або просто дають привабливе для запуску назву, іконку і т. п. Простим прикладом трояна може бути програма waterfalls.scr, чий автор стверджує, що це

безкоштовна заставка. При запуску вона завантажує приховані програми, команди і скрипти з або без згоди та відома користувача. Троянські програми часто використовуються для обману систем захисту, внаслідок чого система стає вразливою, дозволяючи таким чином неавторизований доступ до комп'ютера користувача. [2]

Троянська програма може в тій чи іншій мірі імітувати (або навіть повноцінно замінювати) завдання або файл даних, під які вона маскується (програма установки, прикладна програма, гра, прикладної документ, картинка). У тому числі, зловмисник може зібрати існуючу програму з додаванням до її вихідного коду троянські компоненти, а потім видавати за оригінал або підміняти його.[10]

Трояни - найпростіший вид шкідливих програм, складність яких залежить виключно від складності істинної задачі і засобів маскування. Найпримітивніші екземпляри (наприклад, що видаляють вміст диска при запуску) можуть мати вихідний код в кілька рядків.[11]

3.1. Розповсюдження

Троянські програми поширюються людьми - як безпосередньо завантажуються в комп'ютерні системи зловмисниками-інсайдерами, так і спонукають користувачів завантажувати або запускати їх на своїх системах.

Для досягнення останнього, троянські програми розміщуються зловмисниками на відкриті або індексовані ресурси (файл-сервери та системи файл обміну), носії інформації, надсилаються за допомогою служб обміну повідомленнями (наприклад, електронною поштою), потрапляють на комп'ютер через проломи безпеки або завантажуються самим користувачем з адрес отриманих одним з перерахованих способів.[11]

3.2. Типи тіл троянських програм

Тіла троянських програм майже завжди розроблені для різних шкідливих цілей, але можуть бути також нешкідливими. Вони розбиваються на категорії, засновані на тому, як трояни проникають в систему і завдають їй шкоди. Існує 6 головних типів[11]:

1. Віддалений доступ;
2. знищення даних;
3. завантажувач;
4. сервер;
5. дезактиватори програм безпеки;
6. DoS-атаки.

3.3. Цілі троянів

Метою троянської програми може бути[11]:

- закачування і скачування файлів;
- копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чати або інші сайти з реєстрацією;
- створення перешкод роботі користувача (жартома або для досягнення інших цілей);
- викрадення даних, що представляють цінність чи таємницю, в тому числі інформації для аутентифікації, для несанкціонованого доступу до ресурсів, викрадення деталей щодо банківських рахунків, які можуть бути використані в злочинних цілях, криптографічної інформації
- шифрування файлів при вірусній атаці;
- поширення інших шкідливих програм, таких як віруси. Троян такого типу називається Dropper;
- вандалізм: знищення даних (стирання або переписування даних на диску, важкопомітні пошкодження файлів) та обладнання, виведення з ладу

або відмови обслуговування комп'ютерних систем, мереж і т. п., в тому числі у складі ботнета (організованої групи зомбованих комп'ютерів), наприклад , для організації DoS-атаки на цільовий комп'ютер (або сервер) одночасно з безлічі заражених комп'ютерів або розсилання спаму. Для цього іноді використовуються гібриди троянського коня і мережевого черв'яка - програми, що мають здатність до швидкісного поширення по комп'ютерних мережах і захоплюючи заражені комп'ютери в зомбі-мережі;

- збір адрес електронної пошти і використання їх для розсилки спаму;
- пряме управління комп'ютером (дозвіл віддаленого доступу до комп'ютера-жертви);
- шпигунство за користувачем і таємне повідомлення третім особам відомостей, таких як, наприклад, звичка відвідування сайтів;
- реєстрація натисків клавіш (Keylogger) з цілю крадіжки інформації такого роду як паролі і номери кредитних карток;
- отримання несанкціонованого (і/або дарового) доступу до ресурсів самого комп'ютера або третім ресурсів, доступних через нього;
- установка Backdoor;
- використання телефонного модему для здійснення дорогих дзвінків, що тягне за собою значні суми в телефонних рахунках;
- дезактивація або створення перешкод роботі антивірусних програм і файервола.

3.4. Принцип дії трояна

Трояни зазвичай складаються з двох частин: Клієнт і Сервер. Сервер запускається на машині-жертві і стежить

за з’єднаннями від Клієнта, використовуваного атакуючою стороною. Коли Сервер запущено, він відслідковує порт або декілька портів в пошуку з'єднання від Клієнта. Для того, щоб атакуюча сторона під'єдналася до Серверу, вона повинна знати IP-адресу машини, на якій запущений Сервер. Деякі трояни відправляють IP-адресу машини-жертви атакуючої сторони по електронній пошті або іншим способом. Як тільки з Сервером відбулося з'єднання, Клієнт може відправляти на нього команди, які Сервер буде виконувати на машині-жертві. В даний час завдяки NAT-технології отримати доступ до більшості комп'ютерів через їх зовнішню IP-адресу неможливо. І тепер багато троянів з'єднуються з комп'ютером атакуючої сторони, який налаштований на прийом з'єднань, замість того, щоб атакуюча сторона сама намагалася з'єднатися з жертвою. Багато сучасних троянів також можуть безперешкодно обходити файерволи на комп'ютері жертви.[10]

3.5. Симптоми зараження трояном

Кілька загальних симптомів зараження трояном:

- поява в реєстрі автозапуску нових програм;
- показ фальшивого завантажування відео-програм, ігор і тд., які не завантажувалися і сайтів, які не відвідувалися;
- створення знімків екрану;
- відкривання і закривання консолі CD-ROM;
- програвання звуків і/чи зображень, демонстрація фотознімків;
- перезапуск комп'ютера під час старту інфікованої програми;
- випадкове і/або безладне вимкнення комп'ютера.

3.6. Способи розпізнавання троянських програм

Більшість програмних засобів, призначених для захисту від троянських програм, в тій чи іншій мірі використовує так зване узгодження об'єктів. При цьому в якості об'єктів фігурують файли і каталоги, а узгодження є спосіб відповісти на питання, чи змінилися файли і каталоги з моменту останньої перевірки. У ході узгодження характеристики об'єктів порівнюються з характеристиками, якими вони володіли раніше. Береться, наприклад, архівна копія системного файлу і її атрибути порівнюються з атрибутами цього файлу, який зараз знаходиться на жорсткому диску. Якщо атрибути розрізняються і ніяких змін в операційну систему не вносилося, значить в комп'ютер, швидше за все, проник троянець.

Одним з атрибутів будь-якого файлу є відмітка про час його останньої модифікації: щоразу, коли файл відкривається, змінюється і зберігається на диску, автоматично вносяться відповідні поправки. Однак позначка часу не може служити надійним індикатором наявності в системі троянця. Справа в тому, що нею дуже легко маніпулювати. Можна «підкрутити» назад системний годинник, внести зміни в файл, потім знову повернути годинник в початковий стан, і відмітка про час модифікації файлу залишиться незмінною.

Можливо, справа з розміром файлу має інший вигляд? Аж ніяк. Нерідко текстовий файл, який спочатку займав, скажімо, 8 КБ дискового простору, після редагування та збереження має той самий розмір. Трохи інакше поводяться двійкові файли. Вкласти в чужу програму фрагмент власного коду так, щоб вона не втратила працездатності і у відкомпільованому вигляді

зберегла свій розмір, досить непросто. Тому розмір файлу є більш надійним показником, ніж відмітка про час внесення до нього останніх змін.

Зловмисник, який вирішив запустити в комп'ютер троянця, зазвичай намагається зробити його частиною системного файлу. Такі файли входять в дистрибутив операційної системи та їх присутність на будь-якому комп'ютері, де ця операційна система встановлена, не викликає жодних підозр. Проте будь-який системний файл має цілком визначену довжину. Якщо цей атрибут буде якимось чином змінений, це стривожить користувача.

Знаючи це, зловмисник постарається дістати вихідний текст відповідної програми і уважно проаналізує його на предмет присутності в ньому надлишкових елементів, які можуть бути видалені без жодного відчутного збитку. Тоді замість знайдених надлишкових елементів він вставить у програму свого троянця і перекомпілює її заново. Якщо розмір отриманого двійкового файлу виявиться менше або більше розміру початкового, процедура повторюється. І так до тих пір, поки не буде отримано файл, розмір якого найбільшою мірою близький до оригіналу (якщо вихідний файл досить великий, цей процес може розтягнутися на кілька днів).

Отже, у боротьбі з троянцями покластися на відмітку про час останньої модифікації файлу і його розмір не можна, оскільки зловмисник може їх досить легко підробити. Більш надійною в цьому відношенні є так звана контрольна сума файлу. Для її підрахунку елементи файлу підсумовуються, і отримане в результаті число оголошується його контрольною сумою. Наприклад, в операційній системі SunOS існує спеціальна утиліта sum, яка виводить на пристрій стандартного виводу STDOUT контрольну суму файлів, перелічених у рядку аргументів цієї утиліти.

Однак і контрольну суму в загальному випадку виявляється не так вже й важко підробити. Тому для перевірки цілісності файлової системи комп'ютера використовується особливий різновид алгоритму обчислення контрольної суми, звана одностороннім хешуванням.

Функція хешування називається односторонньою, якщо задача відшукання двох аргументів, для яких її значення збігаються, є важко розв'язуваною. Звідси випливає, що функція одностороннього хешування може бути застосована для того, щоб відстежувати зміни, внесені зловмисником у файлову систему комп'ютера, оскільки спроба зловмисника змінити будь-який файл так, щоб значення, отримане шляхом одностороннього хешування цього файлу, залишилося незмінним, приречена на невдачу.

Історично склалося так, що більшість утиліт, що дозволяють боротися з проникненням в комп'ютерну систему троянських програм шляхом односпрямованого хешування файлів, було створено для операційних систем сімейства UNIX. Однією з найбільш зручних в експлуатації і ефективних є утиліта TripWire. Вона дозволяє робити односпрямоване хешування файлів за допомогою декількох алгоритмів, в тому числі - MD4, MD5 і SHA. Обчислені хеш-значення файлів зберігаються в спеціальній базі даних, яка, в принципі, є найбільш уразливим ланкою утиліти TripWire. Тому користувачам TripWire пропонується в обов'язковому порядку приймати додаткові заходи захисту, щоб виключити доступ до цієї бази даних з боку зловмисника (наприклад, поміщати її на знімному носії, призначеному тільки для читання).

Засоби боротьби з троянцями в операційних системах сімейства Windows традиційно є частиною їх антивірусного програмного забезпечення. Тому, щоб

відловлювати троянські програми, необхідно обзавестися одним із сучасних антивірусів.[12]

3.7. Методи видалення

В цілому, троянські програми виявляються і видаляються антивірусним і антишпигунським ПО так само, як і інші шкідливі програми.

Троянські програми гірше виявляються контекстними методами антивірусів (заснованих на пошуку відомих програм. Однак евристичні (пошук алгоритмів) і проактивні (стеження) методи для них настільки ж ефективні.

Приклади троянських програм: Adware Sheriff, Alpha Cleaner, AntiVirGear, Back Orifice, Brave Sentry, NetBus, Pest Trap, Pinch, Prorat, SpyAxe, SpyShredder, TDL-4 SpyTrooper, SpywareNo, SpywareQuake, Trojan.Genome.BUY, Trojan.Winlock, Vundo, Zlob, CyberGate, Wishmaster.[11]

Оскільки трояни мають безліч видів і форм, не існує єдиного методу їх видалення. Найбільш просте рішення полягає в очищенні папки Temporary Internet Files або знаходженні шкідливого файлу і видалення його вручну (рекомендується Безпечний Режим). Якщо антивірус не здатний відшукати троян, завантаження ОС з альтернативного джерела може дати можливість антивірусній програмі виявити троян і видалити його. Надзвичайно важливо для забезпечення більшої точності виявлення є регулярне оновлення антивірусної бази даних.[10]

3.8. Звідки беруться троянські програми?

Троянська програма - це плід праці програміста. Ніяким іншим способом створити її неможливо.

Програміст, що пише троянську програму, чудово усвідомлює, що він хоче отримати, і у своїх намірах він дуже далекий від альтруїзму.

Більшість троянських програм призначено для збору конфіденційної інформації. Їх завдання, частіше за все, полягає у виконанні дій, що дозволяють отримати доступ до даних, які не підлягають широкому розголосу. До таких даних відносяться паролі користувача, реєстраційні номери програм, відомості про банківські рахунки і т. і. Решта троянців створюються для заподіяння прямих збитків комп'ютерній системі, приводячи її у неробочий стан.

До останніх можна віднести, наприклад, троянську програму PC CYBORG, яка заманювала користувачів обіцянками надати їм новітню інформацію про боротьбу з вірусом, що викликає синдром набутого імунодефіциту (СНІД). Проникнувши в комп'ютерну систему, PC CYBORG відраховувала 90 перезавантажень цієї системи, а потім ховала всі каталоги на її жорсткому диску і шифрувала файли, що на ньому знаходилися.

Інша троянська програма називалася AOLGOLD. Вона розсилалася по електронній пошті у вигляді заархівованого файлу. У супровідному листі, що додається до цього файлу, йшлося про те, що AOLGOLD призначена для підвищення якості послуг, які надає своїм користувачам найбільший американський Internet-провайдер America Online (AOL). Архів складався з двох файлів, один з яких іменувався INSTALL.BAT. Користувач, що запустив INSTALL.BAT, ризикував стерти всі файли з каталогів C:, C: DOS, C: WINDOWS і C: WINDOWSSYSTEM на своєму жорсткому диску.

Подібного роду троянські програми, як правило, створюються підлітками, які хоч і одержимі пристрастю до руйнування, але не мають глибоких пізнань в

програмуванні. Наприклад, програма AOLGOLD видаляла себе з жорсткого диска, будучи запущена з будь-якого іншого дискового розділу за винятком C.

Інша справа - троянські програми, авторами яких є професійні програмісти, які займаються розробкою програмного забезпечення в солідних фірмах. Троянці, що входять до поширених комп'ютерних програми, утиліт та операційних систем, представляють значно більшу загрозу комп'ютерам, на яких вони встановлені, оскільки їхні дії носять не деструктивний характер, а мають на меті збір конфіденційної інформації про систему. Виявити такі троянські програми вдається, як правило, чисто випадково. А оскільки програмне забезпечення, частиною якого вони є, в більшості випадків використовується не тільки певною компанією, що закупила це програмне забезпечення, але також на великих Internet-серверах і, крім того, поширюється через Internet, наслідки можуть виявитися жахливими.

Трапляється й так, що троянці вбудовуються в деякі утиліти програмістами, які не мають ніякого відношення до розробки цих утиліт. Наприклад, в дистрибутив сканера SATAN, призначений для установки на комп'ютери з операційною системою Linux, що поширювалася через Internet, потрапила троянська програма, яка "влаштувалася" в утиліті fping. При першому ж запуску модифікованої утиліти fping в файл / etc / passwd додавався запис для користувача з ім'ям suser, який в результаті міг увійти в Linux і таємно отримати там повноваження адміністратора. Проте у автора цієї троянської програми були явні прогалини в комп'ютерній освіті. Зокрема, зберігання паролів в операційних системах сімейства UNIX. В результаті постраждали тільки два комп’ютери. [12]

4. Віруси - вимагачі

Метою дій програм-вимагачів є блокування доступу користувача до даних або обмеження можливостей роботи на комп'ютері та вимогу викупу за повернення до вихідного стану системи. Відмінність шкідливих програм полягає в їх початковій комерційній спрямованості. Кожна програма цієї поведінки є інструментом для отримання грошей кіберзлочинцями.

Програма-вимагач може вимагати від вас таких дій:

- Переказати гроші на телефонний рахунок
- Відправити SMS на короткий номер
- Поповнити кошти облікового запису Вконтакте
- Перерахувати гроші через термінал експрес-оплати

Творці програм-вимагачів постійно впроваджують нові способи отримання грошей від користувачів заражених комп'ютерів.[13]

Зазвичай необхідність виплати грошової суми пояснюється використанням неліцензійного програмного забезпечення або переглядом порнофільмів. В більшості випадків зараження відбувається саме з порно-сайтів. Досить часто причини необхідності оплати або способи отримання коду звучать абсурдно, наприклад, «Ваш комп'ютер заблокований за перегляд порнографії з неповнолітніми та зоофілією. Для розблокування комп'ютера необхідно поповнити баланс телефону в будь-якому терміналі оплати. Після оплати код розблокування повинен з'явитися на чеку оплати». Більше того практично на всіх банерах написано попередження, про те, що спроба обдурити «систему оплати» призведе до порушення роботи комп'ютера або знищення даних. У деяких з них навіть вбудований таймер зворотного відліку, після закінчення часу якого вірус обіцяє знищити всі дані користувача. Найчастіше, це проста загроза, для

переконання користувача віддати зловмисникові гроші. Однак, деякі версії дійсно забезпечуються інструментами для знищення даних, але по «кривизні» рук авторів, особливостями установки або з інших причин вони найчастіше не спрацьовують належним чином. Також зараження може статися під час запуску програм, що маскуються під установники додатків чи саморозпаковуючогося архіву. При цьому в ліцензійній угоді обмовляється, що користувач згоден встановити на комп'ютер додаток «рекламного характеру», яке він зобов'язаний переглянути 1000 разів, або відмовитися від перегляду, відправивши SMS.

Вид «інтерфейсу» троянів дуже барвистий і різноманітний. Але в більшості своїй їх об'єднує або схожість зі стандартними меню Windows, або наявність порнографічного матеріалу (фото, набагато рідше анімації і відео), а також вікно для введення коду розблокування. Є різновиди, дуже схожі на синій екран смерті або стандартне вікно привітання Windows. Також не рідкісні випадки, коли вони маскуються під антивірусну програму (наприклад Антивірус Касперського).

Trojan.Winlock умовно можна розділити на 3 типи, залежно від того, наскільки вони ускладнюють роботу користувача.

- 1 тип - це банери або порно-інформери, що з'являються тільки у вікні браузера. Найбільш легко видаляється. Зазвичай вони видають себе за додаткові плагіни або оновлення для браузера.
- 2 тип - це банери, які залишаються на робочому столі після закриття браузера і при цьому закривають більшу його частину. Але у користувачів зазвичай залишається можливість відкривати інші програми, у тому числі диспетчер завдань і редактор реєстру.

- 3 тип - це тип, що найбільш важко видаляється тип банерів, які закривають практично весь робочий стіл, блокують запуск диспетчера завдань, редактора реєстру, а також завантаження в безпечному режимі. Деякі різновиди повністю блокують клавіатуру, надаючи користувачеві лише цифрові клавіші зі свого «інтерфейсу», і робочий маніпулятор для введення коду.

Лабораторія Касперського поділяє Trojan-Ransom.Win32.Digitala(Trojan.Winlock) наступним чином:

- програми, що обмежують доступ до веб-сайтів
- програми, що обмежують роботу з оглядачем
- програми, що блокують доступ до ресурсів операційної системи
- програми, що обмежують дії користувача в операційній системі
- програми, що шифрують файли користувача.[14]

4.1. Історія вірусів-вимагачів

Перша програма-вимагач з'явилася 20 років тому, в грудні 1989 року. Користувачі отримали поштою дискети з програмою, що надає інформацію про СНІД. Після встановлення система приводилася в неробочий стан, і за її відновлення з користувачів вимагали грошей.

Поширення подібних шкідливих програм почалося в 2005 році. З того часу пішло поширення троянців, які за допомогою різних алгоритмів шифрували документи користувачів, а для розшифровки пропонували зв'язатися з авторами програми. Пізніше в повідомленнях, що вбудовуються в дані програми, явно повідомлялося про розмір викупу і про способи його відправлення. За класифікацією Dr.Web дані шкідливі програми мають назви Trojan.PGPCoder, а також Trojan.Encoder з його численними модифікаціями.

Перші зразки подібних програм (Trojan.Winlock) з'явилися одночасно з програмами-шифрувальника в тому ж 2005-му. Так, один з перших екземплярів Trojan.Winlock запитував відправку викупу через платіжну систему «Яндекс.Гроші». Перший SMS-блокер був зареєстровано 25 жовтня 2007. Вимагач інсценував збій системи (синій екран смерті). Практично повністю блокував управління системою.

Наступним кроком у спрощенні зловмисниками методів незаконного отримання грошей став вибір на користь платних SMS-повідомлень, які могли б відправляти жертви з різних країн світу, використовуючи різних операторів зв'язку.

На цій хвилі, починаючи з 2008 року з'явилося безліч реалізацій порно-банерів (Trojan.Blackmailer), для видалення яких з браузерів була потрібна відправка SMS-повідомлень. Переважна кількість таких троянців створюється для браузера Internet Explorer. Втім, останнім часом з'явилися реалізації і для Mozilla Firefox, а також Opera.

З листопада 2009 року така схема відбирання грошей користується все більшим успіхом у зловмисників - нові модифікації Trojan.Winlock стають все більш небезпечними. За зняття повідомлення про блокування Windows, яке вискакує поверх всіх вікон і унеможливлює нормальну роботу на комп'ютері, злочинці вимагають значно більше грошей. Троянці вже не видаляються автоматично з системи після деякого часу, але набувають додатковий функціонал. Зокрема, вони перешкоджають запуску деяких програм в зараженій системі (файлових менеджерів, утиліт збору інформації, яка може допомогти в лікуванні системи).[15]

Тільки за січень 2010 кількість постраждалих в Росії від блокувальників Windows склало кілька мільйонів

користувачів. З урахуванням того, що середня вартість SMS-повідомлення - 300-600 рублів, приблизні втрати росіян від цього виду шкідливого ПЗ тільки в першому місяці 2010 року склали сотні мільйонів рублів.[16]

Дизайн модифікацій Trojan.Winlock став більш агресивним. У нього вбудовується таймер зі зворотнім відліком, також повідомляється про те, що спроба перевстановити систему призведе до втрати даних (рис.1).

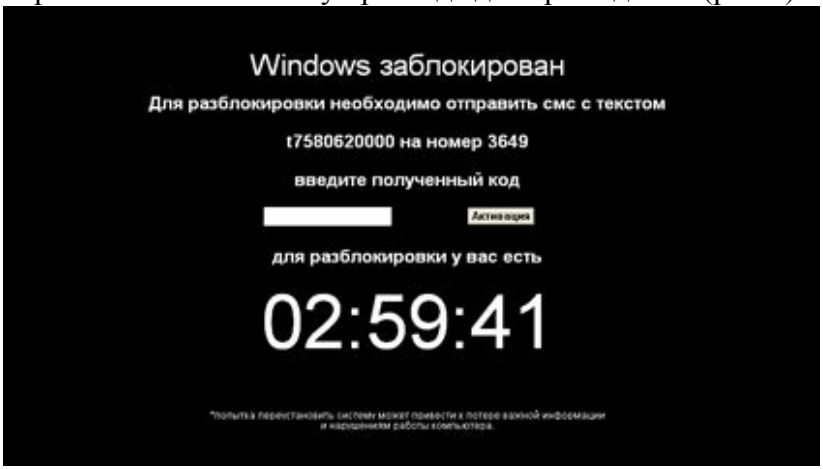

рис. 1. Trojan.Winlock з таймером

Нова хвиля Trojan.Winlock почалася 18 травня - в цей день число детектив троянця сервером статистики «Доктор Веб» зросла в 110 разів у порівнянні з середньодобовими показниками місячної давності.

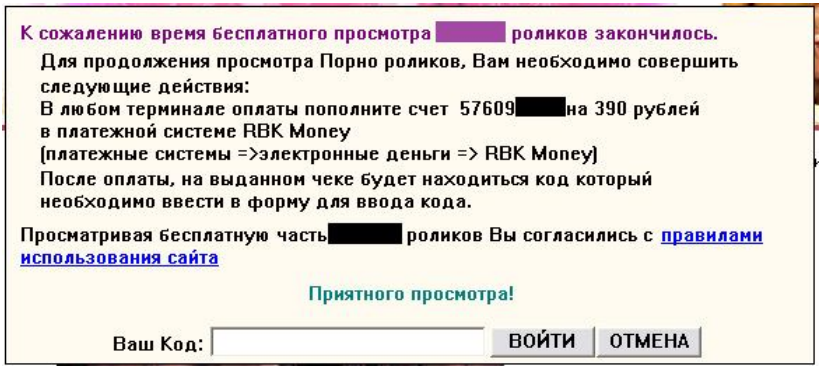

рис. 2.Trojan.Winlock, що зустрічався в 2010 році

У березні та квітні 2010 р. спостерігалося зниження рівня поширення Trojan.Winlock, який за цей період упав приблизно вдвічі. Однак травень вніс свої корективи (рис.3).[17]

рис. 3. Графік заражень комп'ютерів Trojan.Winlock - ом за травень 2010 року

Серед нових модифікацій Trojan.Winlock, які і стали каталізатором цього зростання, виділяється Trojan.Winlock.1678, а також ті види, які вже не вимагають відправки платних SMS, а змушують своїх жертв для переказу коштів користуватися різними платіжними системами.

З'явилося також і безліч наслідувачів Trojan.Winlock, що відрізняються низькою якістю. Часто для розблокування системи в цьому випадку потрібно ввести прописаний в коді троянця пароль. Крім того, в деяких випадках функція розблокування може взагалі не входити до складу такого шкідливого ПЗ.

Одним з останніх кроків авторів подібних шкідливих програм стало створення конструкторів троянців, які блокують Windows. Тепер для створення нової модифікації Trojan.Winlock достатньо лише встановити новий текст відповідного конструктору.[18]

4.2. Trojan Winlock

Trojan.Winlock (від англ. Lock - замок, win - Віндоус, Вінлокер) - сімейство шкідливих програм, які блокують або ускладнюють роботу з операційною системою, і вимагають перерахування грошей зловмисникам за відновлення працездатності комп'ютера. Вперше з'явилися в кінці 2007 року. Широке поширення віруси-вимагачі отримали взимку 2009-2010 року, за деякими даними виявилися заражені мільйони комп'ютерів, переважно серед користувачів російськомовного Інтернету. Другий сплеск активності такого зловмисних програм припав на травень 2010 року. (рис.4)

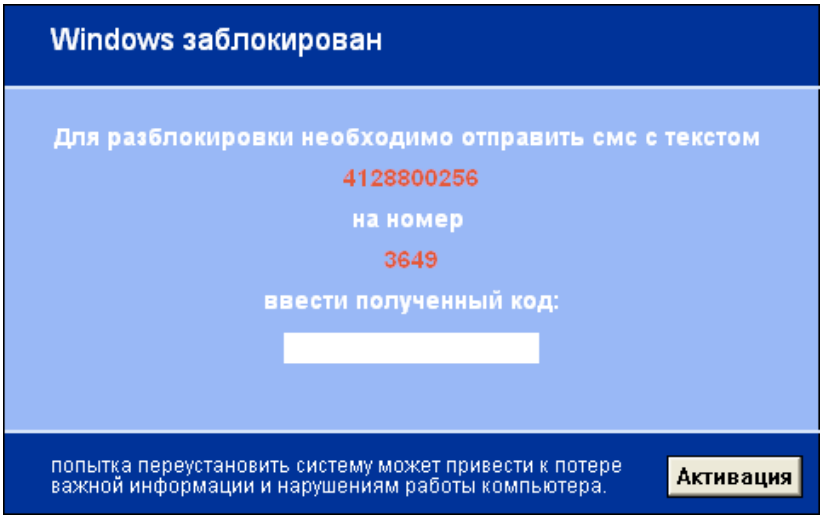

рис. 4. поширений вірус-вимагач

Раніше для переказу грошей зазвичай використовувалися короткі SMS-номери, в даний час подібні програми також можуть вимагати перерахування грошей на електронні гаманці (наприклад, «Яндекс.Гроші»), або баланс мобільного номера. Необхідність перевести гроші часто пояснюється тим, що «Ви отримали тимчасовий безкоштовний доступ до сайту для дорослих, необхідно сплатити продовження його використання», або тим, що «на Вашому комп'ютері виявлена неліцензійна копія Windows». Шляхи поширення Trojan.Winlock і подібних вірусів різноманітні, в значній частині випадків інфікування відбувається через уразливості браузерів при перегляді заражених сайтів.

Класифікація різних вендорів:

Trojan.Winlock - за класифікацією компанії Доктор Веб.
Trojan-Ransom - за класифікацією компанії Лабораторія Касперського.

На даний період часу співробітниками різних антивірусних компаній зафіксовано кілька тисяч різних

видів вінлокерів. Найбільш ранні типи вимагали за розблокування не більше 10 рублів, а якщо користувач залишав комп'ютер увімкнутим на деякий час, то вони самознищувалися (наприклад Trojan.Winlock 19 сам видалявся без сліду через 2 години.) Однак пізніше з'явилися більш небезпечні різновиди, які не видалялися самі по собі і вимагали за розблокування вже від 300 до 500 рублів.[19]

4.3. Боротьба з Trojan Winlock

Перш за все ні в якому разі не можна виконувати вимоги зловмисників. Слід пам'ятати, що вартість SMS може доходити до декількох десятків доларів незалежно від зазначеного в «інтерфейсі» вірусу. Практично у всіх випадках після відправки SMS обіцяний код розблокування не приходить.

У разі пропонованої оплати по SMS можна подзвонити в службу підтримки контент-аггрегатора, якому належить номер. Інколи вони можуть повідомити код розблокування.

При можливості можна скористатися онлайн-сервісами підбору коду розблокування на сайтах виробників антивірусного ПЗ (Dr.Web, Лабораторія Касперського) а також провести повне сканування комп'ютера антивірусною утилітою зі свіжими оновленнями антивірусної бази (наприклад, «одноразовим» антивірусом Dr.Web CureIt або Kaspersky Virus Removal Tool, скачати його бажано з «здорового» комп'ютера, навіть у разі успішного розблокування системи підбором коду).[20]

4.3.1. Розблокування за допомого сервісу деактивації Trojan Winlock від Лабораторії Касперського

Даний сервіс пропонує компанія Лабораторія Касперського. Знайти його можна за адресою: http://sms.kaspersky.ru/.

Для того щоб розблокувати комп'ютер за допомогою цього сервісу перш за все потрібно відкрити його у своєму браузері. Однак деякі вінлокери можуть блокувати доступ до цієї сторінки або до Інтернету. В цьому випадку слід скористатися іншим комп'ютером або телефоном з доступом до Інтернету. В пусте поле потрібно ввести номер рахунку, телефону чи облікового запису Вконтакте и натиснути на кнопку «Получить код» (рис.5).

рис. 5. Сервіс деактивації Trojan Winlock від Лабораторії Касперського

Після цього з'явиться поле «Зображення» і «Коди розблокування». Скріншот в полі «Зображення» допоможе визначити, який саме блокер знаходиться на комп'ютері і який код з поля «Коди розблокування» необхідно ввести для видалення банера. Для збільшення картинки потрібно клацнути лівою кнопкою миші по зображенню (рис.6).

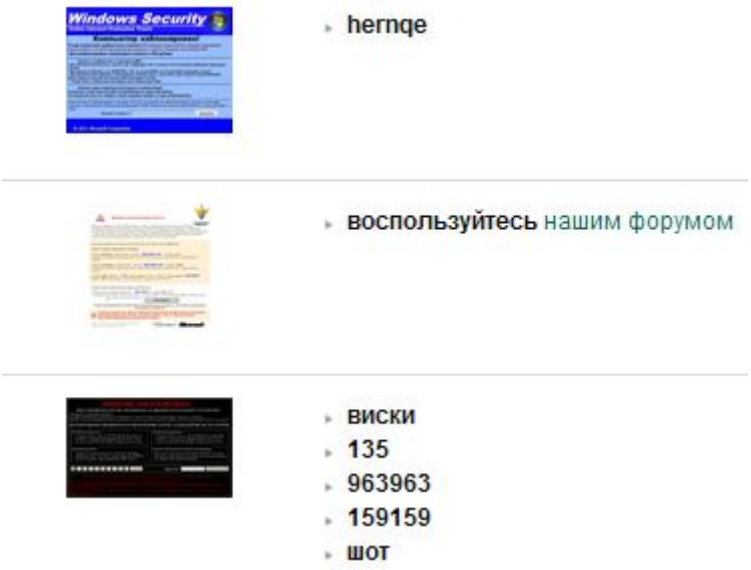

рис. 6. Сервіс деактивації Trojan Winlock від Лабораторії Касперського

У деяких випадках шахраї після введення одного коду можуть вимагати поповнити інший рахунок для видалення банера. Тому в полі Коди розблокування можуть бути представлені кілька кодів. Слід вводити в поле банера коди по черзі, поки банер не буде видалений з Робочого столу.

Даний сервіс можна використовувати і при відновленні зашифрованих блокером файлів . На сторінці сервісу Deblocker (деблокер) http://sms.kaspersky.ru в порожньому полі введіть розширення створеного здирником файлу (рис.7). Це може бути одне з наступних розширень:. Encrypted,. Korrektor,. Bloc,. Gggg,. Cool,. Exe,. Mmm,. Vhd,. Vscrypt,. Infected,. Kis,. Popadalovo,. Mis,. Web, або якесь інше. Далі після натиснення на кнопку «Получить код» на екрані з'явиться назва трояну (наприклад, Trojan-Ransom.Win32.Rector) і посилання на утиліту для розшифровки файлів.[21]

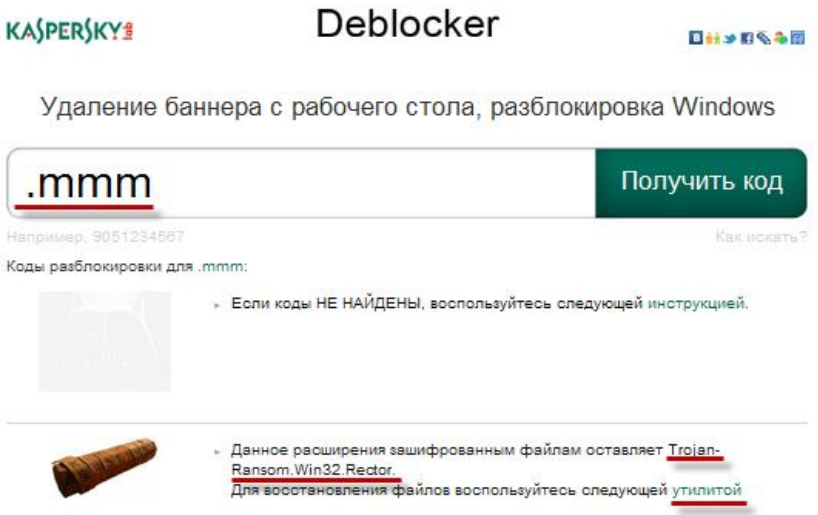

рис. 7. Сервіс від Лабораторії Касперського для розблокування зашифрованих файлів

4.3.2. Сервіс розблокування комп'ютера від компанії DrWeb

Сервіс розблокування комп'ютера від компанії DrWeb можна знайти за адресою: https://www.drweb.com/xperf/unlocker/?lng=ru.

Отримати код розблокування, можна скориставшись формою, що дозволяє ввести номер гаманця чи телефону, на який троянець вимагає перевести гроші (рис.8). Ввівши в поле дані, натисніть Шукати коди, вся знайдена інформація буде розташована нижче форми введення. Для полегшення сприйняття можна налаштувати формат виводу, використовуючи меню в лівій частині екрана. З його допомогою можна вказати число результатів на сторінці, включити / відключити відображення пов'язаних з даним троянцем гаманців і телефонів, а також приховати / відобразити дані по вірусам, інформація з яких в базі відсутня.

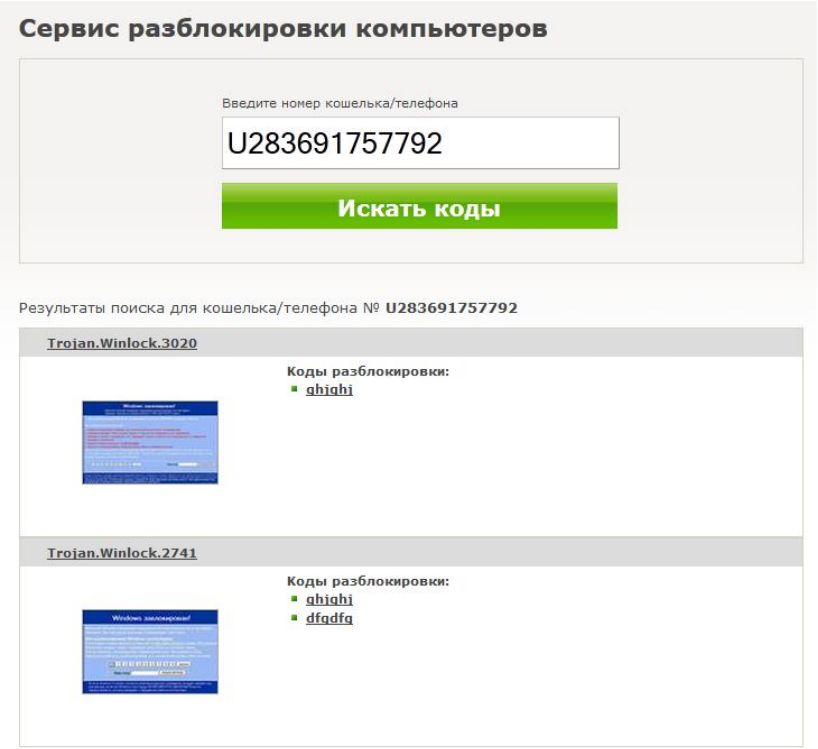

рис. 8. Сервіс розблокування комп'ютера від компанії DrWeb

Якщо відповідних кодів розблокування не знайдено або згенеровані коди не підійшли – можна спробувати підібрати код за допомогою пошуку по зображеннях. Дані в ньому представлені в наступному форматі.

У лівій частині вікна розташовано аналогічне описаному вище меню, з тим винятком, що є присутнім пункт Показувати тільки без телефонів / гаманців, який показує тільки троянці, не відображають ніяких даних і не потребують грошей. Права частина представляє собою таблицю з назвами і зображеннями троянців, а також кодами розблокування до них. При включенні відповідної опції додатково виводиться колонка з номерами пов'язаних

з троянцями гаманців і телефонів. У цій таблиці можна виконати наступні дії:

- При натисканні на скриншот зображення збільшується до повного розміру, що дозволяє звірити її з троянцем, які заблокували ПК.
- При натисканні на ім'я троянця відкривається сторінка з його описом.
- При натисканні на код розблокування відкривається вікно з пов'язаними з ним гаманцями / телефонами. [20]

Оскільки даним сервісом можна користуватися у випадку коли вірус не блокує Інтернет чи Операційну систему, інакше потрібен інший комп’ютер то у компанії DrWeb існує мобільна версія розблокувальника. Для того щоб скористатися нею потрібно за допомогою телефону з підключеним Інтернетом зайти на адресу http://www.drweb.com/unlocker/mobile/ та заповнити форму відповідно підказкам.

4.3.3. Сервіс розблокування Windows від NOD32

Щоб отримати код для розблокування ПК за допомогою цього сервісу компанії NOD32, в формі на сторінці http://www.esetnod32.ru/.support/winlock/ потрібно заповнити дані, які вказані в повідомленні зловмисників. У полі «Номер телефону» вкажіть номер, на який пропонується відправити SMS. В полі «Текст повідомлення» вказується текст, який пропонується відправити на цей номер (рис.9). Далі, після натиснення кнопки "Підібрати код», на сайті з'явиться код розблокування, який необхідно ввести у вікно троянця.

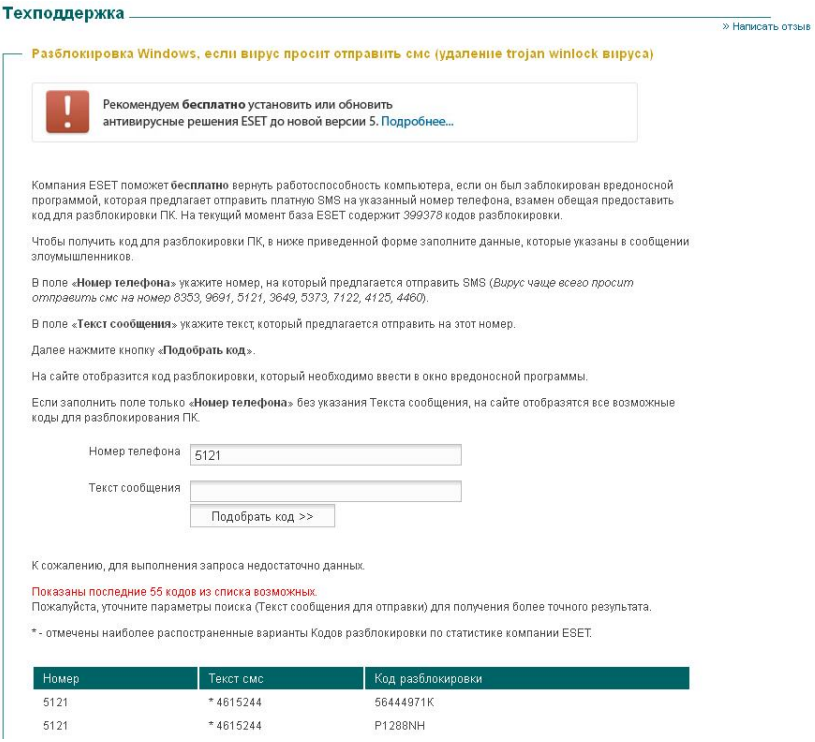

рис. 9. Сервіс розблокування Windows від NOD32

Якщо заповнити поле тільки «Номер телефону» без вказівки Тексту повідомлення, на сайті з'являться всі можливі коди для розблокування ПК.

4.3.4. Видалення Trojan Winlock за допомогою Live CD

У технічному плані трояни блокувальники Windows спочатку були виконані у вигляді. Tmp файлу, при інсталяції він записував своє тіло в тимчасову папку і прописувався в автозапуск через хвіст системного файлу userinit.exe. Перші екземпляри даних смс-блокувальників містили в собі технічну вразливість, що дозволяла у

кінцевому підсумку добратися до робочого столу через спеціальні засоби можливостей Windows. Виклик спеціальних можливостей на етапі вітання операційної системи дозволяв надалі дістатися до провідника Windows і провести відносно нескладне видалення здирника за допомогою антивірусів або безкоштовних антивірусних утиліт. Але в пізніших версіях троянця автори усунули можливість виклику вікна «спеціальних можливостей» в момент появи вікна з вимогою викупу. Ось тут IT-фахівцям і системним адміністраторам вперше довелося зіткнутися з необхідністю лікування зараженої системи за допомогою Live CD або шляхом підключення жорсткого диска зараженого комп'ютера до іншої системи.

Live CD являє собою завантажувальний диск, з якого вантажиться операційна система без своєї установки на жорсткий диск ПК. Досить завантажити комп'ютер безпосередньо з Live CD, в процесі чого вміст диска підвантажується в оперативну пам'ять комп'ютера, що в результаті дозволяє працювати з файлами на диску, з мережею і навіть запускати програми, які не потребують інсталяції, а також робота з реєстром вихідної системи. Правда, необхідно відзначити, що роботу з реєстром підтримують не всі Live CD, а тільки ті, які базуються на Windows Bart PE і містять у своїй збірці редактор реєстру - regedit.exe.

Тут Вам і можуть знадобитися такі лікувальні утиліти, як AVZ або Dr.Web CureIt!, за допомогою яких можна здійснити пошук на диску файлів троянця-здирника. Ці утиліти не вимагають установки і запустити їх можна разом з Live CD. Їх потрібно тільки завантажити, вкрай бажано найостаннішої версії, записати на флешку і підключити її до системи, завантаженої з Live CD. Також можна спробувати скористатися Live CD від DRWeb, який виконаний на базі Linux і має на борту антивірусний

сканер від DRWeb. Хоча знайти вірус таким чином не завжди вдається.

Видалити троян-блокувальник за допомогою Live CD зазвичай не складало труднощів, оскільки достатньо було лише почистити тимчасові папки вихідної зараженої системи і видалити ключ автозапуску троянця через реєстр зараженої системи. Для цього досить у редакторі regedit відкрити один з файлів реєстру вихідної ОС (розташований він в папці WINDOWS \ system32 \ config і має назву Software) через операцію «Загрузить куст» в меню Файл, а після здійснення необхідних змін «Выгрузить куст» назад. Якщо ж не почистити реєстр при видаленні самого файлу вірус, який прописався в хвіст до userinit.exe, то неминуче доведеться зіткнутися з неможливістю завантаження операційної системи, тому що вхід в обліковий запис буде просто неможливий. Windows після вибору облікового запису буде тут же завершувати сеанс поточного користувача і повертатися до вибору облікових записів.

Якщо варіант з Live CD Вам не допоміг, то залишається останній засіб перед переустановлення Windows.

4.3.4.1. Утиліта Kaspersky Rescue Disk та WindowsUnlocker для боротьби з програмами-вимагачами

Утиліта Kaspersky WindowsUnlocker дозволяє проводити лікування реєстру всіх операційних систем, встановлених на комп'ютері (у тому числі встановлених на різних розділах, в різних папках одного розділу), а також лікування гілок реєстру. Знайти дану уліту можна за адресою: http://utils.kaspersky.com/Distr/WindowsUnlocker/KWU_1.0.3.upd2.iso. Цей iso-образ потрібно записати на порожній CD / DVD за допомогою будь-якої програми для запису оптичних дисків (наприклад, Nero Burning ROM,

ISO Recorder, DeepBurner, Roxio Creator або іншої програми). Також можна записати образ на USB- носій, скориставшись улітою для запису образу на USB від Лабораторії Касперського, яку знаходиться за адресою: http://rescuedisk.kaspersky-labs.com/rescuedisk/updatable/ rescue2usb.exe.

Для того щоб вилікувати комп'ютер від вірусу-вимагача за допомогою Kaspersky WindowsUnlocker потрібно:

- Завантажитися з диску на якому знаходиться Kaspersky WindowsUnlocker, після чого потрібно натиснути будь-яку кнопку та вибрати мову.
- Вибрати один з наступних режимів завантаження:
  - Kaspersky Rescue Disk. Графічний режим - завантажує графічну підсистему (рекомендований більшості користувачів)
  - Kaspersky Rescue Disk. Текстовий режим - завантажує текстовий інтерфейс користувача, який представлений консольним файловим менеджером Midnight Commander (MC).
- Прочитайте текст ліцензійної угоди на використання Kaspersky Rescue Disk 10 і, якщо ви згодні з його умовами, натисніть клавішу C на клавіатурі.
- Якщо Kaspersky Rescue Disk завантажився в графічному режимі, натиснути на кнопку Пуск в лівому нижньому кутку екрану і в меню вибрати пункт Kaspersky WindowsUnlocker.
- Якщо Kaspersky Rescue Disk завантажився в текстовому режимі, в меню користувача за допомогою кнопок-стрілок вгору / вниз вибрати Kaspersky WindowsUnlocker і натисніть Enter на клавіатурі.
- Утиліта автоматично запуститься і проведе лікування реєстру. Результат роботи утиліти відобразиться у вікні root. Якщо у вікні з'явилися повідомлення про

успішне відкритті гілок регістра виду Registry hive%*ім'я гілки регістру*% opened successfully і про видалення підозрілих значень виду %*ім'я значення параметра регістра*% - suspicious value, deleted, значить, утиліта спрацювала успішно.

- Після очищення реєстру необхідно видалити залишки вимагача-блокера з комп'ютера. Для цього потрібно запустити повну перевірку комп'ютера за допомогою Kaspersky Rescue Disk. [21]

4.4. Видалення банера-вимагача з браузера

З весни-літа 2008 року користувачі активно почали стикатися з раптовою появою в своєму браузері (спочатку в Internet Explorer, а потім і Mozilla Firefox разом з Opera) огидного спливаючого вікна поверх улюблених сайтів, в якому демонструвалося порно-зображення із супроводжуючим текстом типу: «*щоб видалити інформер, відправте смс на номер .... в результаті чого у відповідь Ви отримаєте код розблокування*». Даний інформер не блокував роботу операційної системи та її компонентів, а лише заважав подорожувати по Інтернету своїм постійним присутністю в нижній частині екрана. (рис.10)

Функціонал даного трояна-вимагача звичайно мав процедуру самостійного видалення із системи після місяця «проживання» на зараженому комп'ютері. Логіка зловмисників-вимагачів тут була достатня проста - якщо інформер (по суті троян вимагач) просить відправити повідомлення на платний номер протягом місяця, а користувач ніяк не реагує на це прохання, то користувачеві на даний інформер, швидше за все, начхати, а значить - вимагати відправити смс від такого користувача далі марно.

рис. 10. Банер-вимагач

Підхоплювали даний банер спочатку лише користувачі Internet Explorer, в який інформер встановлювався під виглядом flash плагіна чи відсутнього кодека для відтворення відео. Часто при відвідуванні будь-якого ресурсу, на який натикалися користувачі з пошукових систем google або Яндекс, в браузері поверх сайту спливало нав'язливе вікно з пропозицією безкоштовно подивитися відео еротичного змісту. Якщо користувач кликав на віконце, то в силу вступали методи соціальної інженерії. Користувачеві демонструвалися завідомо цікаві кадри з порнографічного відео, а при виборі одного з них виводилося повідомлення, що в браузері користувача відсутня flash plugin, або ж система не має потрібний кодек для відтворення відео. При цьому «дбайливий» сайт тут же пропонував завантажити все необхідне прямо на місці, забувши згадати, що скачується зовсім не кодек або флеш-плагін, а знайомий нам інформер. За своїм виконанням даний троян був досить примітивний і вдавав із себе злобливий BHO (Browser Helper Object), який при установці в систему реєструвався в розширеннях Internet Explorer, а в подальшому автоматично запускався при відкритті інтернет-браузера.

Перший масовий банер представляв із себе звичайну динамічну бібліотеку (.dll файл), яка автоматично довантажувався в Internet Explorer при його відкритті. Цікавий інший факт - сама бібліотека троянця-здирника

містила лише структуру виведеного вікна, тоді як вміст вікна, виведене інформером, «підтягувалося» з мережі Інтернет. Запустивши вражений інформером браузер на комп'ютері без доступу в Інтернет, користувач замість квітчастого спливаючого вікна інформера міг побачити лише межі вікна «інформера» без його безпосереднього вмісту, яке, очевидно, зберігалося десь на сервері зловмисника.

Трохи пізніше автори вірусу доопрацювали цей інформер-блокувальник, після чого він став здатний заражати вже такі популярні браузери, як Mozilla Firefox або Opera. Причому найчастіше інформер встановлювався відразу в усі наявні в системі браузери при проникненні в систему.

Видалення інформера простіше всього відбувалося в браузері Mozilla, оскільки достатньо було лише відкрити меню розширень браузера і відключити там компонент інформера. У Mozilla це можна зробити в п. «Інструменти» - «Додатки» - «Розширення».

У випадку з Internet Explorer видалити інформер теж досить просто: для видалення інформера в IE 8.0 потрібно лише відкрити «Властивості оглядача» - «Програми» - «Налаштувати надбудови» - і тут вже відшукати той самий шкідливий вірус, після чого деактивувати шкідливий BHO через меню. Файли інформера переважно мають назву, що закінчується на * lib.dll. Опис і копірайти файлу інформера мають різні варіації, але по імені файлу досить легко виявити і видалити його.

Найважче виконати видалення вимагача в браузері Opera. У «Опері» інформер прописується в папку з призначеними для користувача java scripts, знайти його в якій для недосвідченого користувача виявляється не дуже просто. Не допомагає навіть переустановлення Opera в ту ж саму папку або чищення файлів конфігурації опери в

папці «documents and settings». Щоб видалити інформер в Opera, потрібно пройти в налаштуваннях за наступним шляхом: «Інструменти» - «Налаштування» - «Додатково» - «Вміст» - «Налагодження Java Script» - далі потрібно лише очистити все зайве в рядку «Папка користувальницьких файлів Java script», де і прописує свій автозапуск троянець-здирник.

У цілому, перші трояни-здирники доставляли не так багато клопоту при видаленні з системи. Якщо не справлявся антивірус, то без особливих проблем ранні банери-вимагачі можна було видалити через меню управління браузером. Видаленню таких вірусів «першої хвилі» також сприяли такі безкоштовні лікувальні утиліти, як avptool або DRWeb Cureit. Їх використання було можливе без видалення встановленого антивіруса із зараженої системи, що в більшості випадків дозволяло користувачеві позбавитися від шкідливого банера в браузері. Вартість смс рідко перевищувала 600 рублів, хоча вимагач зазвичай декларував ціну викупу - не більше 300 р. Правда, тут необхідно відмітити, що відкуп часто носив короткочасний характер, тому що після успішної відправки sms повідомлення, вірус показувався знову через якийсь час.[26]

4.5. Троян, що блокує доступ до Інтернету.

«*Доступ в Інтернет заблокований, відправте смс ...*». У листопаді 2009 року відбувся черговий концептуальний виток розвитку троянців-вимагачів. Троян позбавляв користувача доступу до Інтернету з зараженого комп'ютера. Безпосередньо після включення комп'ютера і завантаження робочого столу вірус sms викликав появу спливаючого вікна поверх всіх інших вікон операційної системи. У цьому самому вікні троян-вимагач вимагав від

користувача протягом трьох хвилин ввести код активації від якогось програмного забезпечення (Get Access або чогось подібного), ліцензія на який у користувача нібито закінчилася (рис.11.).

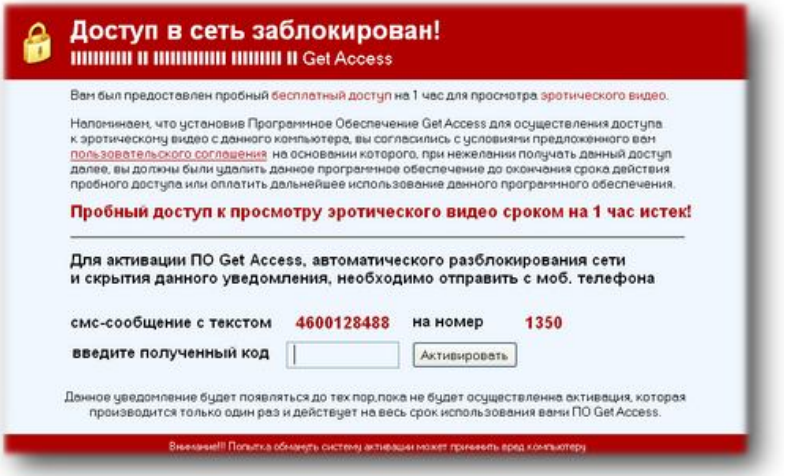

рис. 11. Троян-вимагач, що маскується під програму Get Access

Прикладом може стати шкідлива програма сімейства Trojan-Ransom.Win32.Digitala (Get Accelerator, Digital Access, Get Access, Download Manager v1.34, Ilite Net Accelerator) - це програма-здирника (рис.12). Шкідлива програма сімейства Trojan-Ransom.Win32.Digitala блокує доступ до Інтернету і виводить на екран повідомлення про порушення ліцензійної угоди. Повідомлення містить вимогу - відправити смс з певним кодом на вказаний в повідомленні номер, щоб розблокувати доступ до Інтернету. Ця програма на комп'ютері користувача може з'явитися: за участю користувача, тобто користувач може сам запустити установку з вигляду легальної програми, яка видає себе за Digital Access (рис.12). При запуску такої "замаскованої" програми виводиться ліцензійна угода.

Якщо користувач погоджується з цією угодою, то відбувається зараження комп'ютера. Також програма може проникнути без участі користувача, тобто шкідлива програма може завантажуватися з Інтернету і встановлюватися за допомогою інших шкідливих програм (Get Access)На екран буде виведено повідомлення з вимогою відправки смс-повідомлення для отримання коду активації, який дозволить активувати встановлену програму. Повідомлення може бути виведено як відразу після установки "замаскованої" програми, так і через 6 годин. [22]

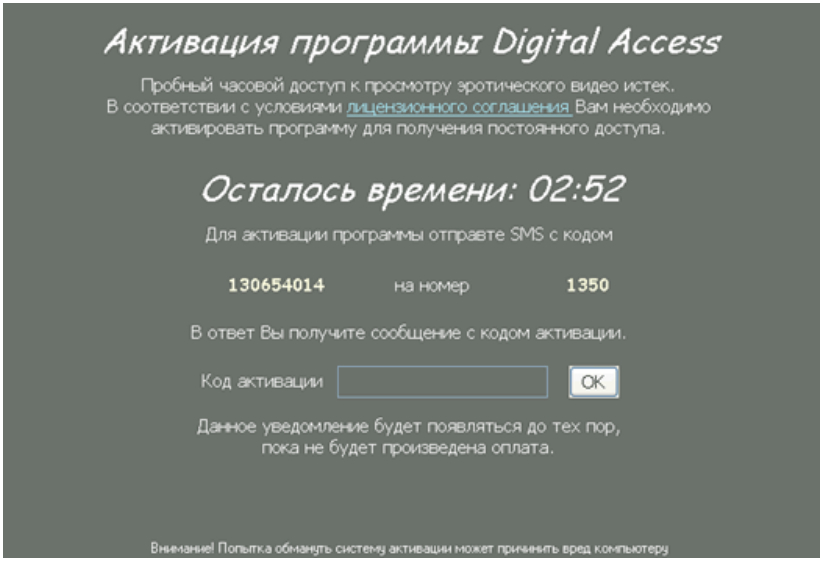

рис. 12. Троян-вимагач - Trojan-Ransom.Win32.Digitala

Якщо протягом трьох - п’яти хвилин користувач не вводив код, то слідувало перезавантаження комп'ютера (рис.13). Складність ситуації полягала в тому, що після інсталяції в систему подібний вірус завантажувався навіть в безпечному режимі роботи та відключав засіб відновлення системи (System recovery). Плюс до всього

вікно троянця-здирника вилазило поверх всіх активних вікон системи, що ускладнювало запуск і керування антивірусами на зараженій системі.

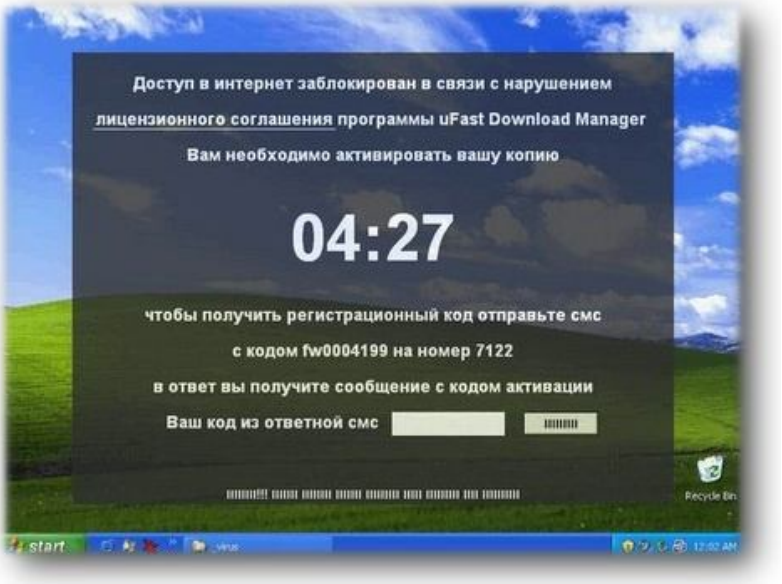

рис. 13. Вірус-вимагач, що блокує доступ до мережі Інтернет.

Для боротьби з вірусами такого типу призначена уліта **Digita_Cure.exe** її потрібно скачати та запустити, а після її роботи перезавантажити комп'ютер. Вона сама знайде вірус, видалить його та очистить файлову систему від нього. [23]

Також можна скористатися наступним алгоритмом:

- Запустити командний рядок, ввести "UninstallString" та натиснути Enter (з'явиться діалогове вікно про підтвердження видалення, але вірус буде закривати його)
- Оскільки скористатися діалоговим вікном неможливо потрібно зробити наступне

- викликати диспетчера задач, натиснувши Ctrl+Alt+Del
- встановити властивість «options» - «Always On Top»
- натиснути правою кнопкою миші на завдання «Видалити» та вибрати властивість «Розгорнути» (Maximize)

- Натиснути кнопку Yes та перезавантажити комп`ютер

Слід зазначити, що версії ОС Windows x64 не схильні до зараження шкідливими програмами сімейства Trojan-Ransom.Win32.Digitala.[22] .

Часто вірус блокує сайт або кілька сайтів, при цьому інші сайти завантажуються нормально. Найчастіше вірус блокує сайти: vkontakte.ru, www.odnoklassniki.ru і mail.ru. Рідше вірус блокує антивірус і оновлення антивіруса. Можливі різні комбінації блокування сайтів. Найостанніші модифікації такого вірусу блокують близько 100-200 найпопулярніших сайтів і складається враження, що Інтернет не працює зовсім. [23]

Прикладом програми такого виду може бути шкідлива програма Trojan-Ransom.BAT.Agent.c (за класифікаціїю Лабораторії Касперського), яка являє собою BAT-файл розміром 13 КБ (рис.14). Після запуску програми блокується доступ користувача до багатьох веб-сайтів, в тому числі, сайтам Лабораторії Касперського, пошукових засобів Google, Яндекс, соціальних мереж (усього близько 200 доменних імен). Ввівши адресу веб-сайту замість очікуваної початкової сторінки, користувач бачить вікно з вимогою викупу.[24]

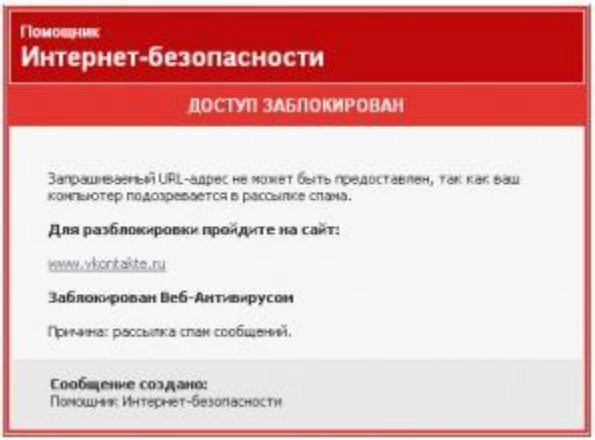

рис. 14. Trojan-Ransom.BAT.Agent.c

Для того щоб розблокувати сайти потрібно видалити записи (крім рядка «127.0.0.1 localhost») з файлу C: \ WINDOWS \ System32 \ drivers \ etc \ hosts. Якщо у файлі зайвих рядків немає, то потрібно увімкнути відображення прихованих файлів «Сервис» - «Свойства папки» - «Вид» і зняти галочки з пункту «скрывать защищенные системные файлы» і поставити «показать скрытые файлы и папки». Швидше за все у папці з'явиться ще один файл hosts, який і потрібно відредагувати.[25]

4.6. Трояни-вимагачі у вигляді помилкових антивірусів, модернізовані блокувальники

Початок 2010 року породило епідемію концептуально нових троянів-вимагачів, які, крім усього іншого були «навчені» блокувати роботу антивірусних програм на зараженій системі. Працювали такі блокувальники Windows по сигнатурах і спеціальним внутрішнім списками, в яких полягало до 90% всього антивірусного програмного забезпечення. Заразившись

таким трояном, користувач позбавлявся не тільки доступу До Інтернету, але і практично не мав можливості провести видалення вірусу із зараженої системи без використання Live CD. Крім усього іншого, вірус завантажувався в безпечному режимі (Safe mode), відключав редактор реєстру і видаляв точки відновлення системи. [33]

З перебігом часу змінився і спосіб функціонування блокувальника Windows в зараженій системі. Якщо раніше троян-вимагач працював як системний процес, то тепер блокувальник просунувся до рівня драйвера ядра або декількох динамічних бібліотек, що прикривають один-одного з сусідніх процесів. Незабаром смс віруси завдяки старанням своїх розробників почали записуватися в додаткові потоки, де їх не було видно навіть з Live CD через засоби провідника Windows. При запуску спеціалізованих лікувальних утиліт, наприклад, AVZ, яку часто використовували для лікування зараженої системи, вірус просто запускав вимкнення комп'ютера. Таким чином, в технічному плані у троянців-вимагачів в січні 2010 року стався справжній прорив.

Для видалення троянців цієї хвилі використання завантажувального Live CD стало звичайною справою. Також на допомогу приходили спеціальні утиліти для пошуку і видалення даних у додаткових потоках NTFS, що запускаються з під Live CD. В кінцевому підсумку проблема троянів-вимагачів привернула увагу не тільки правоохоронних органів і антивірусних компаній, але і стільникових операторів, які запустили спеціальні засоби для уточнення реальної вартості коротких sms-повідомлень на короткі номери. Всі ці заходи в підсумку призвели до скорочення числа заражень вимагачами trojan.winlock до рівня листопада 2009 року. [27]

Слід також виділити трояни, що імітують собою антивірусні продукти. Так, наприклад, при зараженні

«підробленим антивірусом» можна було спостерігати таку картину: відразу після запуску зараженої системи на екрані з’являлося повідомлення про те, що персональний комп'ютер інфікований однією або декількома троянськими програмами, причому виводився цілий список загроз, і виконувалася нібито швидка перевірка комп'ютера на віруси для більшої переконливості (рис.15). Після того троян-вимагач вимагав від користувача відправити sms-повідомлення на платний номер для видалення знайдених вірусів з системи, ввівши присланий у відповідь код активації. Нахабство зловмисників полягала в тому, що всі ці лжеантівіруси прикидалися продуктами відомих антивірусних компаній, наприклад, добре відомої Лабораторії Касперського. [28]

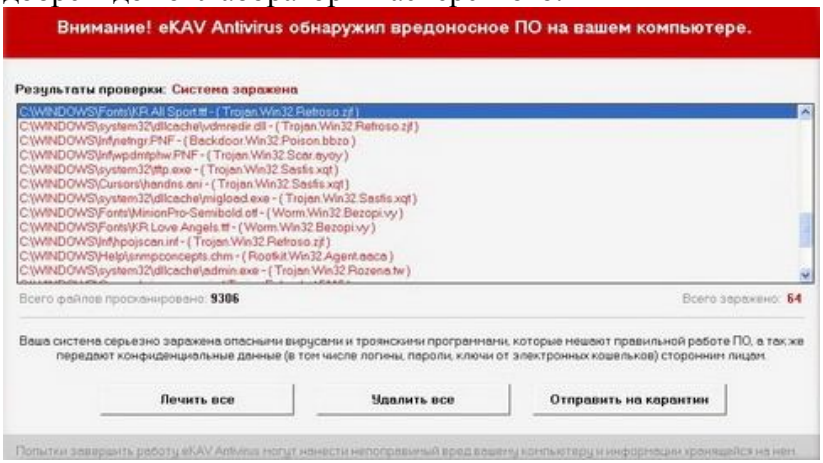

рис. 15. Маскування троянської програми під антивірусну.

4.7. Блокувальники Windows, що інфікують завантажувальний сектор жорсткого диску

В кінці 2010 року з'явилися нові блокувальники Windows, які при інсталяції в систему заражали

завантажувальний сектор жорсткого диска. Це дозволило запускати тіло трояна ще до завантаження Windows. Справа в тому, що просто видалити завантажувальний блокер за допомогою команд відновлення завантажувального запису (fixboot, fixmbr) неможливо - у цьому випадку витиралася таблиця розділів жорсткого диска, що призводило до втрати даних. Звичайно, дані можна було спробувати потім відновити, але все одно це викликало чимало проблем. Вилікувати заражений mbr можна за допомогою DrWeb Cure it з під Live CD або ж за допомогою Kaspersky Rescue Disk 10, який має можливість поновлення своїх антивірусних баз після завантаження. Головне, щоб знайшлася потрібна сигнатура конкретно до даного різновиди блокувальника.

Також можна підключити заражений жорсткий диск до іншого комп'ютера і здійснити лікування завантажувального сектора вже з нього. За класифікацією DrWeb такі троянці отримали назву Trojan.MBRlock.

На момент середини літа 2011 року епізодично зустрічаються випадки зараження троянцями-вимагачами, які записують своє тіло в завантажувальний сектор жорсткого диска, в результаті чого лікування такої системи ускладнюється. Для лікування блокувальника в завантажувальному секторі можна спробувати завантажитися з інсталяційного диска Windows і виконати наступні команди в консолі відновлення:

- Fixmbr
- fixboot c:
- exit

За умови, що завантажувальний сектор був розташований на диску C (саме на ньому зазвичай встановлюється операційна система).[26]

4.8. Програми, що обмежують дії користувача в операційній системі.

В операційних системах сімейства Windows є гнучкий механізм політики безпеки, що дозволяє системним адміністраторам налаштовувати користувацьке оточення. Використовуючи системний реєстр, можна відключити пункти системного меню, Панель Завдань, змінити вид папок і т.і. Автори вірусів використовують функцію системи в своїх цілях. Зміна системних налаштувань, таких як заборона запуску редагування реєстру, заборона запуску Диспетчера завдань і т.і., вже давно використовується різноманітними шкідливими програмами. До цього виду програм-вимагачів можна віднести сімейства Trojan-Ransom.Win32.Krotten і Trojan-Ransom.Win32.Taras. Як правило, після запуску такої програми на комп'ютері можна запустити тільки Інтернет-браузер, щоб можна було заплатити викуп.[29]

Розглянемо деякі способи лікування.

Спосіб лікування № 1. Видалення профілю заблокованого користувача. Для цього потрібно:

- перезавантажити комп'ютер в Безпечному режимі
- увійти в систему під іншим користувачем, наприклад, користувачем «Адміністратор»
- у випадках деяких програм-вимагачів (наприклад, Trojan-Ransom.Win32.Taras.e) ви побачите, що можливості цього користувача нічим не обмежені, тому що дія троянської програми поширюється лише на того користувача, який запустив цю шкідливу програму
- скопіювати вміст робочого столу заблокованого користувача та інші потрібні файли, щоб не втратити важливу інформацію, а потім видаліть профіль заблокованого користувача

- створити нового користувача і увійти в систему під новим аккаунтом.

Спосіб лікування № 2. Деякі здирники (наприклад, Trojan-Ransom.Win32.Krotten.kq) змінюють системні налаштування, які надають ефект на всіх користувачів в системі. Наприклад, шкідлива програма запускається при старті Windows і застосовує налаштування для кожного нового користувача, крім того, забороняючи вхід в безпечному режимі Windows. У цьому випадку може допомогти лікування з використанням завантажувального диска LiveCD. Алгоритм дій:

- скачати архів з утилітою AVZ
- розпакувати архів
- скопіювати утиліту на flash-носій
- завантажитися з LiveCD. Як правило, шкідливі програми даного виду залишають можливість запуску на заблокованому комп'ютері лише декількох додатків: Internet Explorer, Outlook Express, щоб користувач міг відправити лист зловмисникам
- скопіювати вміст каталогу з утилітою AVZ на робочий стіл користувача заблокованого комп'ютера
- перейменувати виконуваний файл утиліти з AVZ.exe на iexplore.exe (назва файлу Internet Explorer)
- перезавантажити комп'ютер
- увійти в систему під заблокованим користувачем
- запустити з робочого столу утиліту AVZ під ім'ям iexplore.exe. Утиліта запуститься, тому що програмі Internet Explorer запуск дозволений.
- у вікні утиліти виберіть пункт меню «Файл» → «Відновлення системи»
- відзначте всі пункти, крім пунктів "Повне переналаштування SPI (небезпечно)" і "Очистити ключі MountPoints & MountPoints2"

- натиснути кнопку Виконати зазначені операції
- Перезавантажити комп'ютер. [14]

4.9. Програми, що шифрують файли користувача.

Цей вид програм-вимагачів непомітно шифрує дані користувача. Пізніше користувач виявляє, що не може отримати доступ до потрібних файлів. Умови викупу «даних-заручників» або поміщується в текстовий файл у кожному каталозі з зашифрованими файлами (наприклад, у випадку Trojan-Ransom.Win32.GPCode), або розміщуються на робочому столі (наприклад, так чинить Trojan-Ransom.Win32.Encore).

Зазвичай програми-здирники цього виду шифрують файли вибірково - з розширеннями doc, xls, txt і т.д., тобто ті, які потенційно можуть містити важливу для користувача інформацію. Найбільш відоме сімейство таких програм Trojan-Ransom.Win32.Gpcode.

Так як алгоритми шифрування даних варіюються від програми до програми, універсальних способів лікування привести не можна. Для розшифровки файлів, як мінімум треба мати примірник троянської програми, хоча і цього може бути недостатньо.[30]

4.10. Інші методи лікування

Наведемо ще деякі методи лікування комп'ютера від вірусів – вимагачів.

- В деяких випадках допомагає перестановка дати в BIOS на кілька років назад.

- Відкрити диспетчер задач (якщо це можливо). Переглянути процеси на предмет підозрілих. Спробувати завершити процес. Швидше за все, процес перезапуститься. Перезавантажитися в безпечному режимі та видалити програму вручну.[31]

- Якщо троян не блокує безпечний режим, то при натисканні клавіші F8 необхідно вибрати безпечний режим з підтримкою командного рядка. Після завантаження треба запустити редактор реєстру за допомогою команди regedit і шукати там підозрілі записи. У першу чергу необхідно перевірити гілку HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon, зокрема в параметрі Shell має бути написано explorer.exe, а в параметрі Userinit - C: \ WINDOWS \ System32 \ userinit.exe, (обов'язково з коми). Якщо там все в порядку, необхідно перевірити цей же шлях, але в гілці HKEY_LOCAL_USER. Також бажано перевірити гілки, в яких прописані автозавантажувальні програми, наприклад HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run. У разі виявлення підозрілих записів, їх необхідно замінити на стандартні значення (у випадку з автозавантаженням видалити). Після перезавантаження і входу в систему трояна можна видалити вручну по вже відомому шляху. Цей спосіб хоч і ефективний, але підходить тільки для досвідчених користувачів.[33]

- Деякі трояни замінюють собою один з файлів userinit.exe, winlogon.exe і explorer.exe у відповідних каталогах. Рекомендується відновити їх з дистрибутива або каталогу C: \ WINDOWS \ System32 \ DLLCACHE.

- Троян може створювати розділ HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Image File Execution Options \ userinit.exe, де може прописувати виклик свого виконуваного файлу (найчастіше debug.exe), для відновлення роботи системи необхідно видалити даний розділ. [10]

Завжди можна перевстановити Windows, але при цьому можуть постраждати дані, важливі для користувача а також це займе більше часу ніж видалення вірусу.

Висновок

Абсолютного захисту бути не може.

Повністю захищений комп'ютер - це той, який знаходиться під замком у броньованій кімнаті в сейфі, не підключений ні до якої мережі (навіть електричної) і виключений. Такий комп'ютер має абсолютний захист, однак використати його не можна. Використання постійних, що не розвиваються механізмів захисту небезпечно, і для цього є кілька причин.

Не можна забувати про розвиток й удосконалювання засобів нападу. Техніка так швидко міняється, що важко визначити, який пристрій новий або програмне забезпечення, використане для нападу, може обдурити ваш захист.

Комп'ютерний захист - це постійна боротьба з безпечністю користувачів й інтелектом хакерів. Навіть хакери найчастіше використають саме некомпетентність і недбалість обслуговуючого персоналу й саме останні можна вважати головною погрозою безпеки.

Кращий захист від нападу - не допускати його. Навчання користувачів правилам безпеки мережі може запобігти нападам. Захист інформації містить у собі крім технічних мір ще й навчання.

У цей час узагальнена теорія безпеки інформації поки не створена. Застосовувані на практиці підходи й засоби нерідко страждають істотними недоліками й не мають оголошену надійність. Тому необхідно володіти достатньою підготовкою й кваліфіковано орієнтуватися у всьому спектрі питань забезпечення інформаційної безпеки, розуміючи їх комплексний і взаємообумовлений характер.

Список використаних джерел:

1. Использование криптографии - Энциклопедия безопасности - [Цит. 2011 26 листопада] - Доступний з: <http://www.opasno.net/st832.html>
2. Фейнштайн К. Защита ПК от спама, вирусов, всплывающих окон и шпионских программ / Кен Фейнштайн; Пер. с англ. О.Б.Вереиной.-М.:НТ Пресс, 2005.-240 с.:ил.-(Самоучитель).
3. Компьютерный вирус. – Wikipedia. –[Цит. 2011 29 листопада]. – Доступний з: <http://ru.wikipedia.org/wiki/Компьютерный_вирус>
4. Сетевые черви. – Wikipedia. –[Цит. 2011 29 листопада]. – Доступний з: <http://ru.wikipedia.org/wiki/Компьютерный_червь>
5. http://ru.wikipedia.org/wiki/Компьютерный_червь
6. Яремчук С.А.Защита вашего компьютера / Сергей Акимович Яремчук; - Санкт-Петербург, Питер, 1-е издание, 2009. - 288 с.
7. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие.-М.:Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264с: ил.
8. . Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. - Серия «Информатизация России на пороге XXI века». - М.: СИНТЕГ, 1999.- 152 с.
9. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. -М.:ДИАЛОГ-МИФИ,1996. – 256 с.
10. Троянские программы – AnVir - [Цит. 2011 14 грудня] - Доступний з: <http://www.anvir.net/troyanskie-programmyi.htm>

11. Сетевые черви. – Wikipedia. –[Цит. 2011 21 грудня]. – Доступний з:
<http://ru.wikipedia.org/wiki/Троянская_программа>
12. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Перербург, 2000. - 384 с.: ил.
13. Как удалить баннер блокера-вымогателя с Рабочего стола? – Служба технической поддержки Лаборатории Касперского - [Цит. 2011 25 грудня] - Доступний з:
<http://support.kaspersky.ru/viruses/solutions?qid=208638485>
14. Способы борьбы с программами-вымогателями класса Trojan-Ransom – Служба технической поддержки Лаборатории Касперского - [Цит. 2011 25 грудня] - Доступний з:
<http://support.kaspersky.ru/faq/?qid=208637133>
15. Обзор вирусной обстановки за апрель 2009 года от компании «Доктор Веб» - Доктор Веб –[Цит. 2011 22 грудня]. – Доступний з:
<http://news.drweb.com/show/?i=324>
16. В России эпидемия Trojan.Winlock. Заражены миллионы компьютеров - Доктор Веб –[Цит. 2011 22 грудня]. – Доступний з:
<http://news.drweb.com/show/?i=874&c=5&lng=ru&p=5>
17. Новая волна Trojan.Winlock пришлась на середину мая 2010 - Доктор Веб –[Цит. 2011 22 грудня]. – Доступний з:
<http://news.drweb.com/show/?i=1136>
18. Вирусная активность за май 2009» - Доктор Веб –[Цит. 2011 23 грудня]. – Доступний з:
<http://www.comss.info/page.php?id=563>

19. Trojan.Winlock. – Wikipedia. –[Цит. 2011 21 грудня]. – Доступний з: <http://ru.wikipedia.org/wiki/Trojan.Winlock>
20. Разблокировка Trojan.Winlock - DrWeb - [Цит. 2011 27 грудня]. – Доступний з: <http://support.drweb.com/show_faq?qid=46452743&lng=ru >
21. Утилита Kaspersky WindowsUnlocker для борьбы с программами-вымогателями – Служба технической поддержки Лаборатории Касперского - [Цит. 2011 27 грудня]. – Доступний з: <http://support.kaspersky.ru/viruses/solutions?qid=208641245 >
22. Как бороться с вредоносными программами семейства Trojan-Ransom.Win32.Digitala Get Accelerator, Digital Access, Get Access, Download manager v1.34, Ilite Net Accelerator) – Служба технической поддержки Лаборатории Касперского - [Цит. 2012 5 січня]. – Доступний з: <http://support.kaspersky.ru/faq/?qid=208637303>
23. Вирус блокирует интернет - InHelp - [Цит. 2012 6 січня]. – Доступний з: <http://www.in-help.ru/articles/virus_blokiruet_internet>
24. Вирус блокирует компьютер - InHelp - [Цит. 2012 3 січня]. – Доступний з: <http://www.in-help.ru/articles/virus_blokiruet_computer/ virus_blokiruet_komputer>
25. Вирус. Помощник интернет безопасности доступ заблокирован. - HelpProfi - [Цит. 2012 7 січня]. – Доступний з: <http://www.helpprofi.ru/virus_info/pomoshhnik_internet_bezopasnosti_dostup_zablokirovan/>

26. Убрать порно информер в браузере – Золотое Руно - [Цит. 2012 5 січня]. – Доступний з: <http://goldfleece.com.ua/blogs/remont-kompyutora/ubrat-porno-informer-v-brauzere.html>
27. Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп,2008.-256с.:ил. – (Компьютер – это просто!)
28. Касперски К. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005. – 316с.:ил.
29. Касперски К. Компьютерные вирусы изнутри и снаружи.-СПб.: Питер, 2006. – 527с.:ил.
30. Гульев И. Компютерные вирусы, взгляд изнутри/Игорь Гульев – М.:ДМК,1998 – 304с., ил
31. Петров А.А. Компютерная безопасность. Криптографические методы защиты.- М.: ДМК, 2000. – 448с.: ил.
32. Гордрн Я. Компьютерные вирусы без сееретов. – ЗАО «Новый издательский дом», 2004 – 320с.:ил.
33. Белоусов С.А. Троянские кони. Принцыпы работы и методы защиты: Учебное пособие/Белоусов С.А., Гуц А.К., Планков М.С., - Омск% Издательство Наследие. Диалог-Сибирь, 2003. – 84с.
34. Комп'ютерна безпека - uasol.com - [Цит. 2012 20 січня]. – Доступний з: <http://uasol.com/index.php?aid=1385>
35. Как это работает? - DrWeb - [Цит. 2011 27 грудня]. – Доступний з: <http://www.freedrweb.com/livecd/how_it_works/?lng=ru>

СУЧАСНІ ТЕХНОЛОГІЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ

Книга 7

Оксана Мирославівна Черкун

Комп'ютерний набір, верстка і макетування та дизайн в редакторі Microsoft®Office® Word 2007 О.М. Черкун.

Науковий керівник Р.М.Літнарович, доцент, кандидат технічних наук.

Міжнародний Економіко-Гуманітарний Університет ім. акад. Степана Дем'янчука

33027,м.Рівне,Україна
Вул.акад. С.Дем'янчука,4, корпус 1
Телефон:(+00380) 362 23-73-09
Факс:(+00380) 362 23-01-86
E-mail:mail@regi.rovno.ua
E-mail: oksana077@list.ru