Курс “Комп’ютерна вірусологія“

Класифікація комп’ютерних вірусів і шкідливого програмного забезпечення. Історія комп’ютерних вірусів і шкідливого програмного забезпечення.

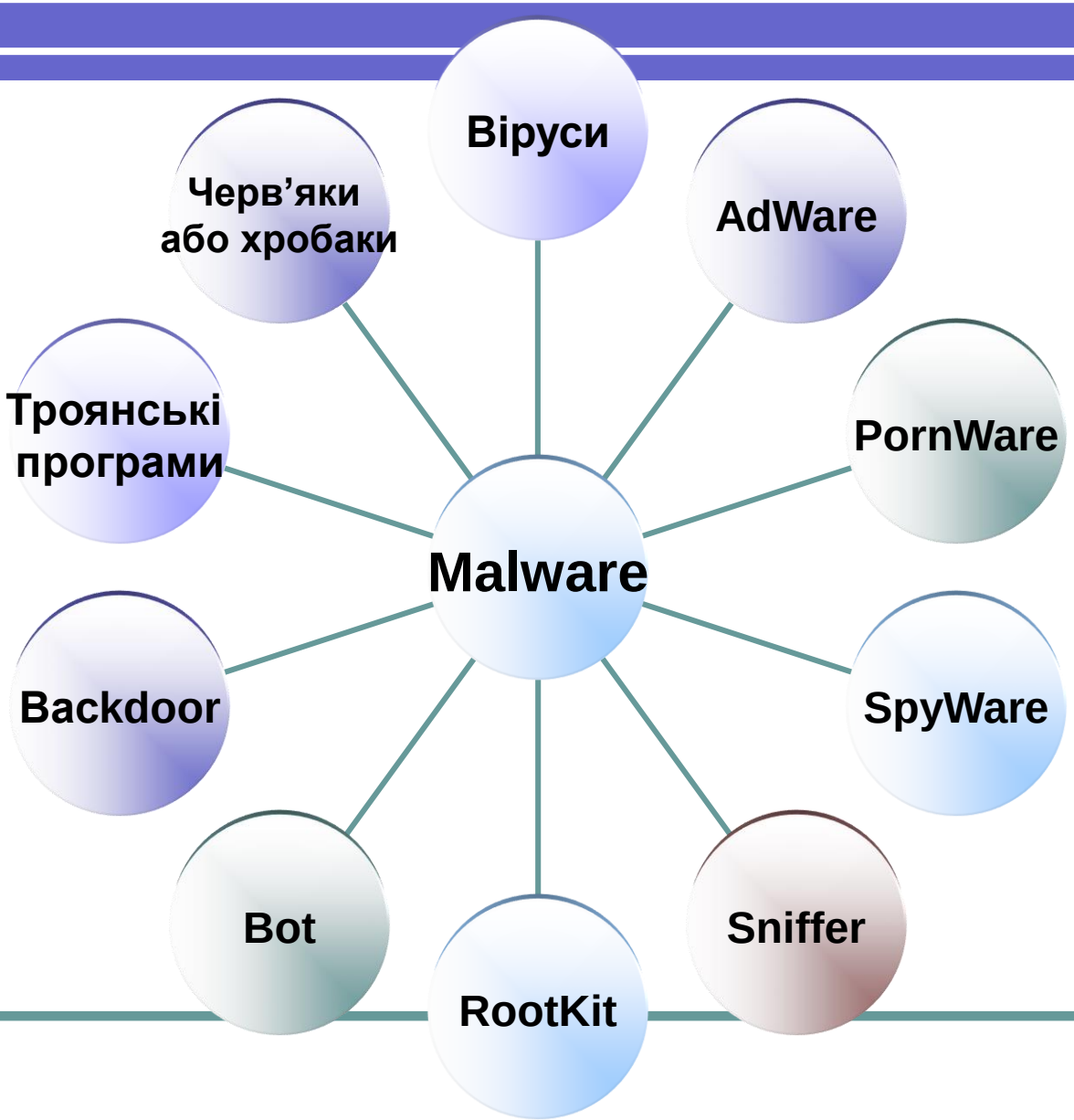
Ст. викладач
каф. Інформатики ФІ
Кирієнко Оксана Валентинівна

ok.kyrienko@gmail.com

"Комп'ютерна вірусологія"

Поняття інформаційної безпеки є вельми широким, воно охоплює і надійність роботи комп'ютера, і збереження цінних даних, і захист інформації від внесення до неї змін не уповноваженими персонами (конфіденційність), і збереження таємниці листування в електронному зв'язку.

ВІДОМІ ШКІДЛИВІ ПРОГРАМИ



Комп'ютерний вірус -

1. **це невелика програма, що здатна до саморозмноження й виконання різних деструктивних дій.**
2. **це комп'ютерна програма (сукупність програмних кодів), здатна без відома користувача комп’ютера створити свої копії та впровадити програмні коди у різноманітні файли або ресурси комп’ютерних систем.**

Хробаки – це шкідливі програми, які **здатні відтворювати себе** через комп'ютерні мережі:

Хробаки поширюються у такі способи:

- у формі файлу, надісланого у вкладенні електронного листа **Email-Worm**;
- у формі посилання, переданого через повідомлення сервіси миттєвих повідомлень **IM-Worm**;
- у формі посилання на на копію хробака або відсилання зараженого файлу якомусь користувачеві Internet Relay Chats **IRC-Worm**;
- саморазмноження в комп'ютерних мережах використовуючи критичні вразливості ПЗ **Net-Worm**;
- через пірингові мережі обміну даними P2P (peer-to-peer) **P2P-Worm**.

Троянські програми

Бекдори
Троянська програма бекдор дає зловмисникам змогу віддалено керувати зараженими комп'ютерами. Такі програми дають автору можливість виконувати на зараженому комп'ютері будь-які дії, зокрема надсилання, отримання, відкриття і видалення файлів, відображення даних і перезавантаження комп'ютера. Троянці-бекдори часто використовуються для об'єднання групи комп'ютерів-жертв у ботнет або зомбі-мережу для використання з кримінальною метою.

Експлойти – це програми з даними або кодом, що використовують уразливість програм, які працюють на комп'ютері.

Руткіти – це програми, призначені для приховування в системі певних об'єктів або дій. Часто основна їхня мета – запобігти виявленню шкідливих програм, щоб подовжити час роботи цих програм на зараженому комп'ютері.

Банківські троянці (Trojan-Banker) призначені для крадіжки облікових даних систем інтернет-банкінгу, систем електронних платежів і кредитних або дебетових карт.

Trojan-Downloader - здатні завантажувати і встановлювати на комп'ютер-жертву нові версії шкідливих програм, зокрема троянські та рекламні програми.

Троянські програми

DDoS-троянці - призначені для здійснення атак типу «відмова в обслуговуванні» (Denial of Service, DoS) за цільовими веб-адресами. Унаслідок такої атаки із заражених комп'ютерів системі з певною адресою надсилається велика кількість запитів, що може спричинити її перевантаження і призвести до відмови в обслуговуванні

Trojan-Dropper - ці програми використовують хакери, щоб інсталювати троянські програми та/або віруси чи запобігти виявленню шкідливих програм. Не кожна антивірусна програма здатна виявити всі компоненти троянських програм цього типу.

Trojan-FakeAV - імітують роботу антивірусного програмного забезпечення. Створені, щоб вимагати гроші у користувача в обмін на обіцянку виявлення і видалення загроз, хоча загроз, насправді не існує.

Ігрові троянці - крадуть інформацію про акаунти учасників мережевих ігор.

IM-троянці - крадуть логіни й паролі до програм миттєвого обміну повідомленнями.

Trojan-Ransom - можуть змінити дані на комп'ютері таким чином, що комп'ютер перестає нормально працювати, а користувач позбувається змоги використовувати певні дані. Зловмисник обіцяє поновити нормальну роботу комп'ютера або розблокувати дані після сплати запитуваної суми.

Троянські програми

SMS-троянці - надсилають текстові повідомлення з мобільного пристрою на платні телефонні номери з підвищеним тарифом, витрачаючи ваші гроші.

Шпигунські програми - програми типу Trojan-Spy здатні приховано спостерігати за використанням комп'ютера, наприклад, відстежуючи введені з клавіатури дані, роблячи знімки екрана й отримуючи список активних програм.

Trojan-Mailfinder - здатні збирати на вашому комп'ютері адреси електронної пошти.

Також трапляються інші види троянських програм:

Trojan-ArcBomb

Trojan-Clicker

Trojan-Notifier

Trojan-Proxy

Trojan-PSW

Adware, Pornware і Riskware

Adware –програми, призначені для показу реклами на вашому комп'ютері, перенаправлення запитів пошуку на рекламні веб-сайти та збору маркетингової інформації про вас (наприклад, якого роду сайти ви відвідуєте), щоб реклама відповідала вашим інтересам.

Adware-програми, які збирають дані з вашої згоди, не слід плутати з троянськими програмами-шпигунами, які збирають інформацію без вашого дозволу і відома і вважаються шкідливими (наприклад, шкідливою є програма троянець-шпигун Trojan-Spy).

Pornware –програми, які відображають на пристрої порнографічний контент. До категорії Pornware також входять програми, встановлені зі зловмисною метою без повідомлення користувача про їх присутність. Зазвичай метою встановлення таких програм є рекламування платних порнографічних веб-сайтів і сервісів.

Adware, Pornware і Riskware

Riskware - легальні програми, які можуть завдати шкоди комп'ютеру, якщо використовуються зловмисниками для видалення, блокування, зміни або копіювання даних, а також для порушення роботи комп'ютерів і мереж.

До категорії Riskware входять такі типи програм:

- утиліти віддаленого адміністрування;
- програм-клієнти IRC;
- програми додзвонювання;
- програми для завантаження файлів;
- програмне забезпечення для моніторингу активності комп'ютерів;
- утиліти керування паролями;
- серверні веб-служби, наприклад FTP, Web, Proxy і Telnet.

За своїм призначенням це не шкідливі програми, але деякі їхні функції можуть бути знаряддям для зловживань.

До дій, які виконують комп’ютерні віруси, відносяться:

- вільні або мимовільні спроби порушити працездатність комп'ютерних систем,
- спроби злому захищених систем,
- використання і поширення програм, які порушують працездатність комп'ютерних систем та їх надійність.

Основними джерелами вірусів є:

- носії інформації, на яких знаходяться заражені вірусом файли;
- комп'ютерна мережа, в тому числі система електронної пошти та Internet;
- жорсткий диск, на який потрапив вірус в результаті роботи з зараженими програмами;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.

Вірусна атака

Процес порушення роботи програми і операційної системи, знищення інформації, яка зберігається на жорсткому диску.

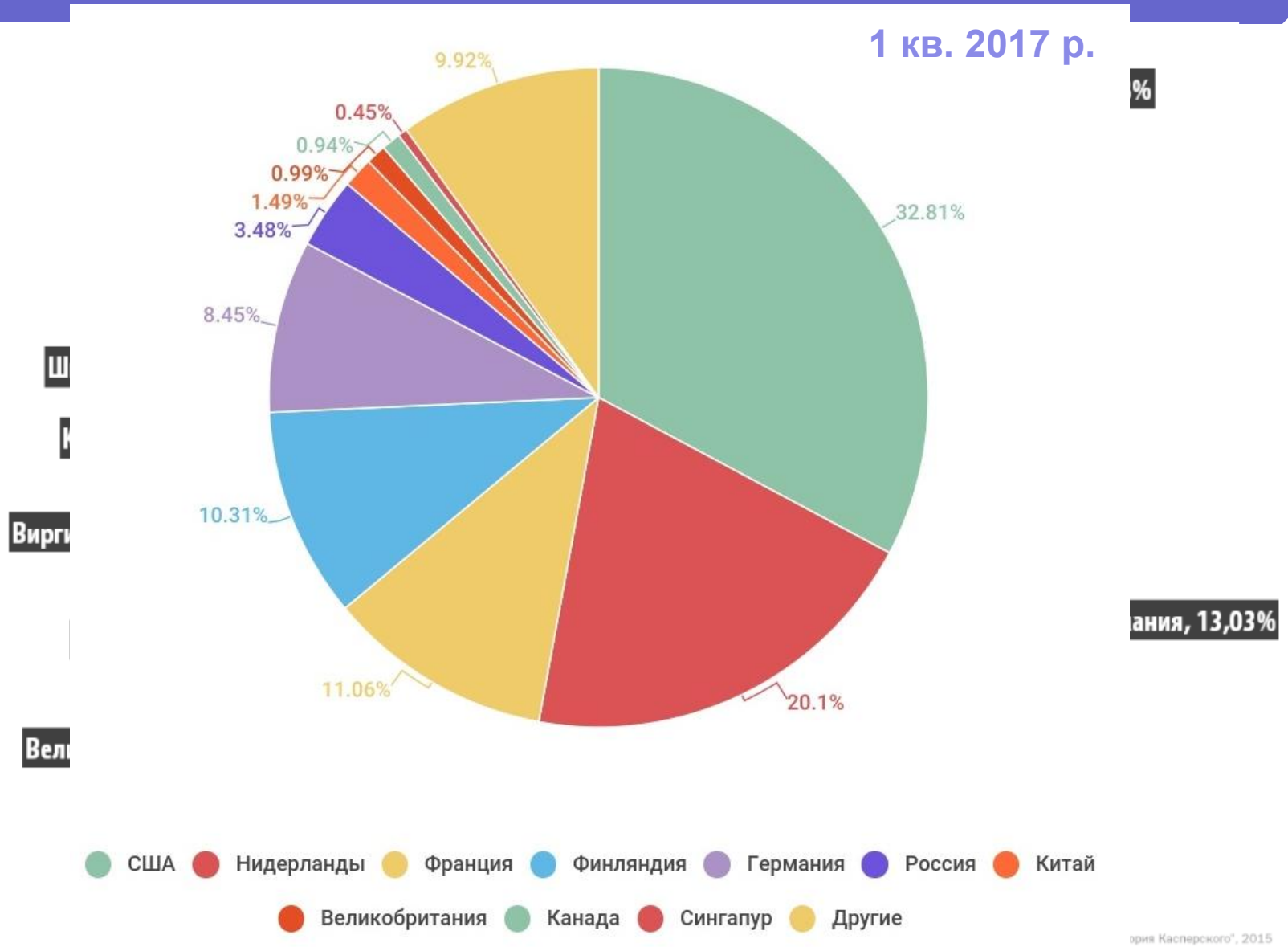
Ранні ознаки зараження комп'ютера вірусом.

Активна фаза.

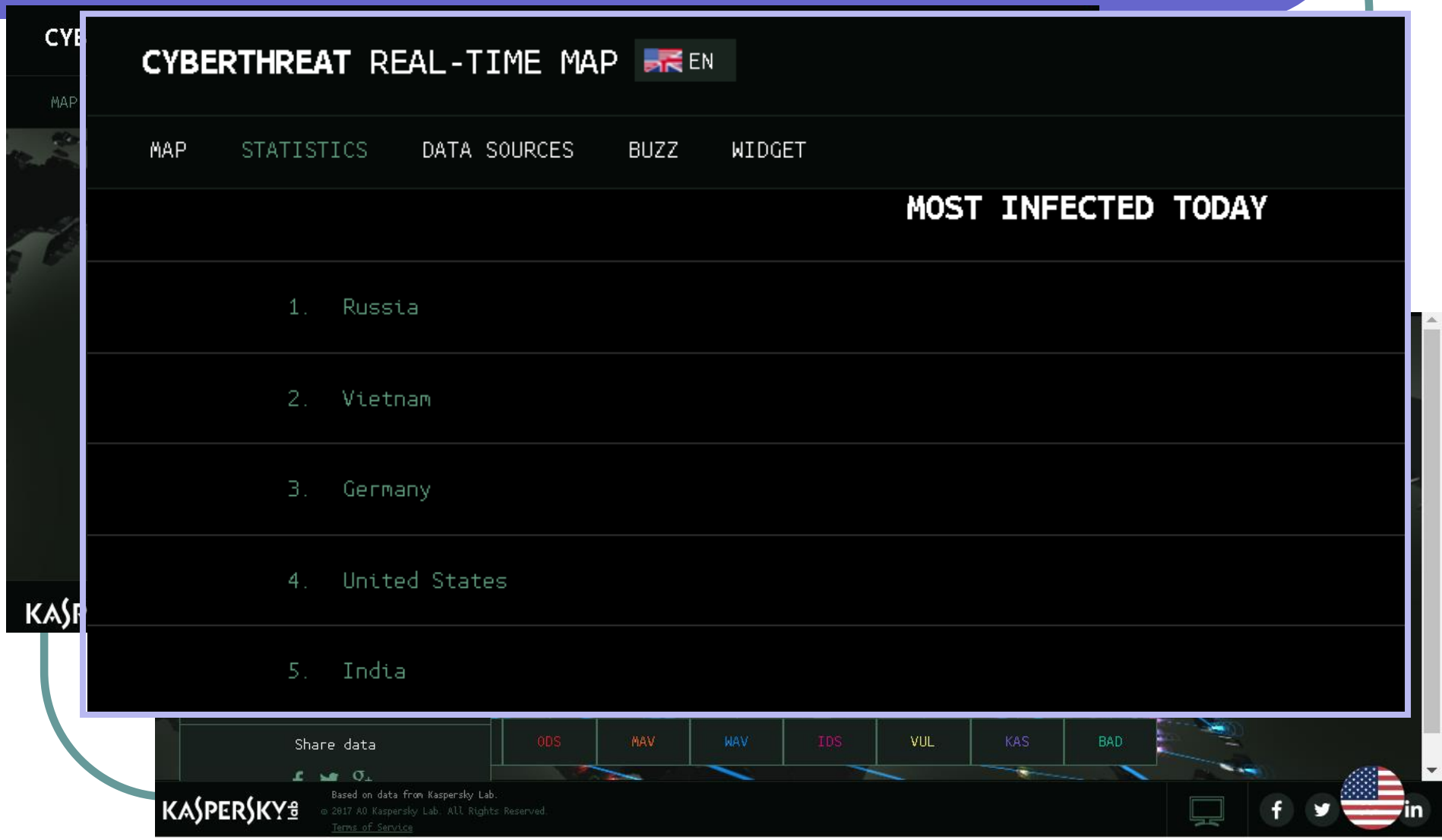
Класифікація комп'ютерних вірусів

- за середовищем мешкання;
- за способом зараження середовища мешкання;
- за деструктивними можливостями;
- за особливістю алгоритму вірусу;
- за способом знешкодження;
- за способом створення.

Звідки беруться віруси?



Інтерактивна карта інфікованих пристроїв (6 вересня 2017 року)

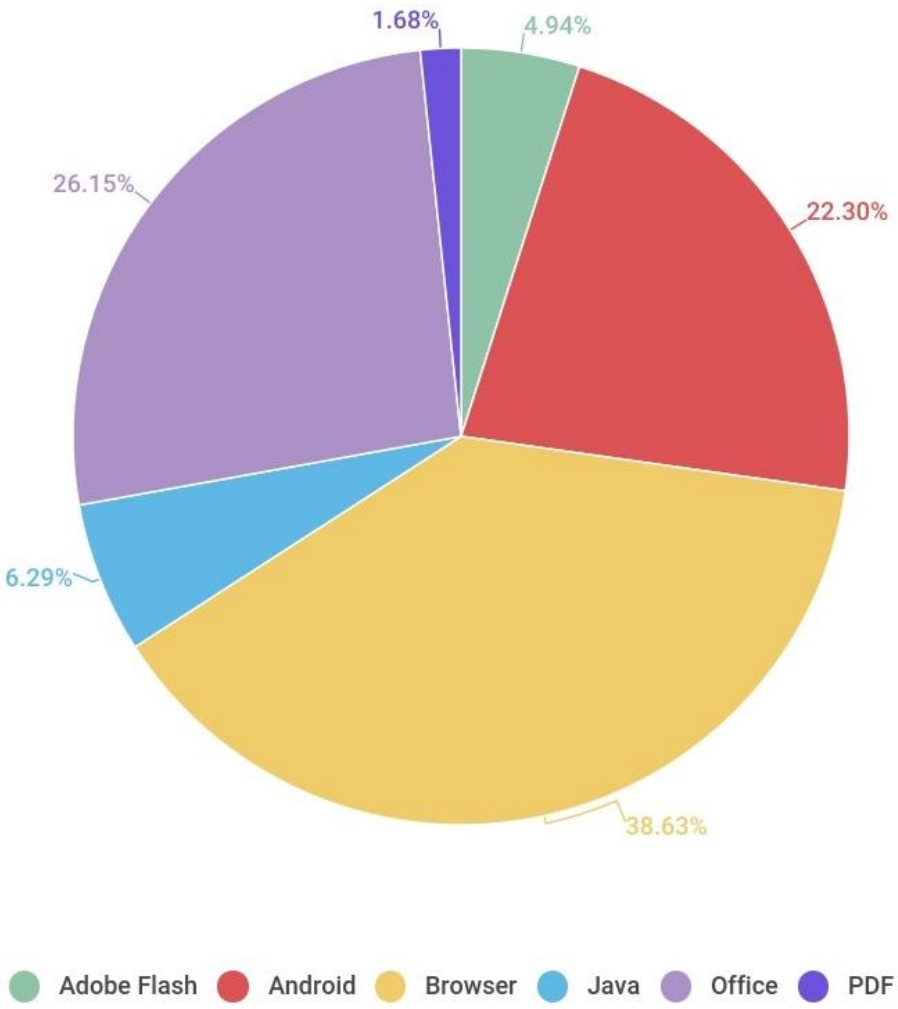


https://cybermap.kaspersky.com/

«Хіт-парад» шкідливих програм

10. *Псевдопослуги, фальшиві архіви. Trojan.SMSSend*
9. *Завантажувальні блокувальники. Trojan.MBRlock*
8. *Блокувальники запуску IM-клієнтів. Trojan.IMLock*
7. *Фальшиві антивіруси. Trojan.Fakealert*
6. *Редиректори на шкідливі сайти. Trojan.Hosts.*
5. *Редиректори на локальний веб-сервер. Trojan.HttpBlock*
4. *Блокувальник доступу до Інтернету* **Trojan.Mayachok**
3. *Блокувальники Windows. Trojan.Winlock*
2. *Банківські троянці. Trojan.PWS.Ibank, Trojan.PWS.Banker, Trojan.PWS.Multi*
1. *Шифрувальники даних. Trojan.Encoder, WannaCrypt*

Уразливі додатки, які використовуються зловмисниками



Загрози для операційної системи

- Сканування файлової системи
- Викрадення ключової інформації
- Підбирання паролів
- Збирання сміття
- Перевищення повноважень
- Програмні закладки
- Жадібні програми

Сканування файлової системи – це атака на політику безпеки

- Будь-який користувач в системі повинен отримати доступ лише до тих файлів, до яких він повинен мати доступ згідно політики безпеки
- Якщо порушник в результаті сканування отримує доступ до інших файлів, він порушує політику безпеки, тобто здійснює НСД
- При цьому порушник отримує можливість несанкціоновано ознайомитись з інформацією (порушення конфіденційності), або несанкціоновано модифікувати або видалити інформацію (порушення цілісності).

Сканування файлової системи

- Можливість НСД до об’єктів файлової системи визначається наявністю вбудованої ***системи розмежування доступу*** *і* ***коректністю її*** **адміністрування**.
- Джерелом атаки може бути будь-який легальний користувач системи. Атаку може здійснювати анонімний користувач (гість), якщо можливість анонімного входу в систему не заблокована

Викрадення ключової інформації

Найпоширеніший вид такої інформації – паролі доступу до системи. Типові способи викрадення паролів:

- викрадення пароля, що записаний на папері
- підглядання пароля в момент, коли користувач його набирає
- підглядання пароля на екрані
- зчитування пароля у командних файлах (сценаріях)
- отримання паролів, що ненадійно зберігаються

Підбирання паролів

- Підбирання паролів передбачає використання засобів аутентифікації для знаходження того пароля, який буде прийнятий як правильний

- Будь-яка система передбачає можливість того, що користувач під час введення пароля зробив помилку, тому введення пароля можна повторити

Підбирання паролів

В усіх сучасних системах аутентифікації вживаються заходи, які достатньо ефективно нейтралізують цю загрозу. Основні заходи:

- обмеження швидкості введення паролів шляхом введення штучних затримок в процедуру їх перевірки
- обмеження кількості спроб введення паролів (як правило до 3...5), після чого система аутентифікації на певний час блокує подальші спроби введення паролів з тієї консолі
- реєстрація спроб аутентифікації
- негайне повідомлення адміністратора про повторні невдалі спроби аутентифікації,

Збирання сміття

Збирання сміття - це отримання даних, які залишаються в об’єктах, що звільняються ОС після їх використання.

- У більшості файлових систем файли після їх видалення не знищуються фізично, а лише помічаються як знищені. **Сектори диску**, які були відведені для файлу, вважаються вільними, і на них можуть бути записані частини інших файлів. Але до нового запису вони продовжують містити дані, які знаходились у видаленому файлі.
- Копіювання і вивчення **тимчасових файлів**
- “**Файл підкачування**”, який створюється для реалізації механізму віртуальної пам’яті
- “**Кошик для сміття**” (trash bin)
- **Оперативна пам'ять**

Перевищення повноважень

Ця загроза полягає у тому, що ***порушник якимось чином отримує повноваження, що перевищують ті, які йому надані згідно політики безпеки***. Перевищення повноважень можливе

- або через помилки в розробці й реалізації політики безпеки (наприклад, невірні настроювання системи розмежування доступу),
- або шляхом використання наявних вразливостей в програмному забезпеченні, яке входить до складу ОС.

Отже, перевищення повноважень реалізується при будь-якому несанкціонованому переході користувача з нижчої категорії до вищої.

Програмні закладки

- До програмних закладок відносять програми або окремі модулі програм, які протягом тривалого часу функціонують в комп'ютерній системі, здійснюючи заходи щодо приховування свого існування від користувача.

- Програмні закладки можуть впроваджуватись вірусом, "троянським конем", мережним хробаком або безпосередньо користувачем-зловмисником.

Програмні закладки

Функції програмних закладок:

- перехоплення і передавання інформації: крадіжка паролів; шпигунські програми (*Spyware);*
- порушення функціонування систем (“логічні бомби”): знищення інформації; зловмисна модифікація інформації; блокування системи;
- модифікація програмного забезпечення: утиліти віддаленого адміністрування; Інтернет-клікери; проксі-сервера; дзвінки на платні ресурси; організація DoS і DdoS атак;
- психологічний тиск на користувача: реклама (*Adware);* злі жарти і містифікації.

Жадібні програми

Жадібні програми – це шкідливі програми, які захоплюють значну частину ресурсів комп'ютера, внаслідок чого робота інших користувачів та/або процесів помітно утруднюється або взагалі стає неможливою. Часто жадібні програми можуть призводити до краху ОС.

Здебільшого, жадібні програми належать до класу "троянських коней".

Жадібні програми можуть бути Web-застосунками, які запускаються при вході браузером на певні Web-сторінки.

Безпека WWW. Типові вразливості клієнтського ПЗ (браузерів)

- ***бінарні вразливості***, наприклад, помилки переповнення буферу або можливість використання посилання на вже видалений об'єкт у пам'яті;
- ***помилки, що дозволяють здійснити НСД до файлів на комп'ютері користувача***;
- ***помилки, що дозволяють підробляти чужі веб-сайти***;
- ***помилки контролю коректності коду сторінок***.

Вразливості Java

Перевагою технології Java є вбудована модель безпеки, яка пропонує рішення проблеми безпеки вже на рівні архітектури. Але …

- У компіляторах і віртуальних машинах Java іноді виявляються помилки, що здатні негативно вплинути на безпеку комп'ютера. Це вимагає від адміністраторів і розробників систем контролю повідомлень про виявлені помилки і застосування нових виправлених версій.
- Завжди можна створити програму, яка не буде порушувати модель безпеки, але буде шкідливою з точки зору користувача. Наприклад, аплети Java можуть генерувати неприємні звуки з системного динаміка; не зупинятись при виході користувача з Web-сторінки, з якої аплет був завантажений; захоплювати значну частину системних ресурсів, наприклад, шляхом утворення великої кількості великих вікон на робочому столі, тощо.
- Аплети можуть взаємодіяти з іншими об'єктами, що завантажені у браузер

Небезпека сценаріїв JavaScript

Мова сценаріїв ***JavaScript*** була розроблена компанією ***Netscape*** і не має практично нічого спільного з ***Java*** крім співзвучної назви.

- Сценарії можуть бути вписані безпосередньо у сторінку, або завантажуватись як зовнішні об’єкти .
- Сценарії надають значні можливості для нападів на комп’ютери користувачів. А саме: звертатись до численних об’єктів ОС, відкривати нові вікна браузера, формувати веб-документи і демонструвати їх у вікнах, переадресовувати браузер з однієї сторінки на іншу, звертатись до змінних cookie (з міркувань безпеки вони не можуть читати і записувати cookie, які знаходяться не в тому домені, з якого був завантажений сценарій втім, час від часу виявляються деякі помилки або послідовності дій, які дозволяють ці обмеження обходити).
- Сценарії можуть використовуватись для розповсюдження шкідливих програм .
- Сучасні антивірусні програми переглядають веб-сторінки у кеші браузера і шукають відомі їм шкідливі сценарії за сигнатурами.

Основні загрози для сервера

- **Бінарні вразливості**:
  - Виконання зловмисником довільного коду на сервері
  - Підвищення привілеїв (наприклад, отримання прав зареєстрованого користувача або root)
  - DoS атаку
- **Специфічні веб уразливості**:
  - Ін’єкція вихідного коду - дуже поширена і одночасно одна з найнебезпечніших уразливостей сценаріїв, що виконуються на боці сервера характерна для сценаріїв на PHP і на Perl, полягає у тому, що порушник отримує можливість впровадити і виконати довільний код на відповідній мові сценаріїв.
  - SQL-ін’єкція - уразливість, при якій порушник може впроваджувати свої дані, не передбачені розробниками веб-програми, у SQL-запит.
  - Міжсайтове виконання сценаріїв (Cross-site scripting, XSS) - уразливість, яку можуть мати сторінки, частину вмісту яких користувачі можуть змінювати, і ці зміни потім виводяться іншим користувачам, що відвідують сторінку.

НАСЛІДКИ SQL-ІН’ЄКЦІЙ

- Можливі практично будь-які дії з базою даних. SQL-запити дозволяють не лише отримувати деяку вибірку інформації, але й видаляти або модифікувати окремі поля, записи, або навіть цілі таблиці

- У програмах, які доступні зовнішнім користувачам за протоколом HTTP, найчастіше зустрічаються такі SQL-запити:

  SELECT, INSERT, UPDATE, DELETE.

- Шляхом SQL-ін’єкції можна здійснити **DDOS-**атаку на сервер. Наприклад, в MySQL її можна здійснити, багаторазово викликавши функцію **benchmark(n,expr)**, яка **n** разів виконує заданий вираз **expr**. В MS SQL можливе виконання будь-якої системної команди шляхом виклику збереженої процедури **exec master..xp_cmdshell “cmd”**. Результат роботи команди при цьому порушнику не повертається, але сам факт виконання команди на сервері є надзвичайно небезпечним

ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТІ І ВИКОРИСТАННЯ SQL-ІН'ЄКЦІЇ ПОРУШНИКУ НЕОБХІДНО ПРОВЕСТИ ДОСЛІДЖЕННЯ:

- Реакції програми (у тому числі повідомлень про помилки) на різні варіації усіх параметрів, що передаються їй методами GET, POST, та через cookie
- Для використання вразливості необхідно також визначити тип сервера бази даних (MySQL, PostgreSQL, …)

Корисна книга:

Низамутдинов М. Ф. Тактика защиты и нападения на Webприложения. – СПб.: БХВ-Петербург, 2005. – 432 с

ЗАХИСТ ВІД SQL-ІН’ЄКЦІЇ:

Для унеможливлення цієї вразливості розробники Web-програм повинні включати ретельні перевірки типів усіх параметрів, що передаються

- Якщо очікуються дані числових типів, то необхідно або впевнитись, що передані дані саме таких типів, або жорстко привести дані до очікуваного типу.

- Якщо очікується рядок, необхідно ретельно контролювати, аби користувач не міг вийти у параметрі за межі рядка

МІЖСАЙТОВЕ ВИКОНАННЯ СЦЕНАРІЇВ:

Міжсайтове виконання сценаріїв (англ. – *Cross-Site Scripting,* XSS, іноді, також говорять «міжсайтовий скриптінг») є дуже поширеною вразливістю

- Цю вразливість можуть мати сторінки, частину вмісту яких користувачі можуть змінювати, якщо ці зміни потім виводяться іншим користувачам, що відвідують сторінку - Форуми, Чати, Системи обміну миттєвими повідомленнями, Соціальні мережі, Сторінки, що містять статті або мультимедійні об’єкти, до яких користувачі можуть додавати свої коментарі
- Вразливість виникає тоді, коли не проводиться достатня фільтрація даних, що передаються користувачами

МІЖСАЙТОВЕ ВИКОНАННЯ СЦЕНАРІЇВ:

- Через вразливу систему порушник отримує можливість виконати деякий сценарій на системі іншого користувача у контексті вразливої системи (сервера)
- ***Активна вразливість XSS*** — коли впроваджений зловмисником сценарій автоматично видається користувачам. Наприклад, код сценарію впроваджено в базу даних або у деякий файл, і він вставляється у сторінки, які сайт видає відвідувачам. Всі відвідувачі автоматично стають жертвами.
- ***Пасивна вразливість XSS*** вимагає, аби користувач сам виконав певні дії, наприклад пройшов по “отруйному” посиланню Приклад “отруйного” посилання:

http://www.site.com/page.php?var=<script>alert('працює!');</script>

МІЖСАЙТОВЕ ВИКОНАННЯ СЦЕНАРІЇВ:

Використовуючи вразливість типу XSS, порушник може:

- здійснити зміну вигляду сторінки з метою дискредитації її власника, введення в оману користувачів, або простого хуліганства);
- отримання параметрів (наприклад, cookie) від користувача;
- збирання статистики щодо дій користувачів: IP-адреси відвідувачів (навіть якщо сама система їх приховує); час відвідань (може допомогти у встановлені відповідності між умовними іменами користувачів та їхніми IP-адресами); тип і версія браузера, тип і версія ОС; з якої саме сторінки користувач звернувся до сайту порушника. Зібрана статистика може дозволити визначити конфіденційні дані окремих користувачів;
- виконання неявних дій адміністратором. Ідея полягає у надсиланні адміністратору веб-сторінку, модифіковану так, що адміністратор виконає деякі дії, потрібні порушнику. Наприклад, якщо вразливим ресурсом є форум, порушник у такий спосіб може руками адміністратора здійснити видалення повідомлень або цілих тем.

Огляд вірусної активності за серпень 2017 року

Головні тенденції серпня

- Зростання числа шахрайських поштових розсилок
- Поява нового троянця-майнера
- Виявлення завантажувачів Linux.Hajime для MIPS і MIPSEL

Linux.Hajime - Мережеві черв'яки цього сімейства відомі з 2016 року. Для їх поширення зловмисники використовують протокол Telnet. Після підбору пароля і авторизації на атакується пристрої плагін-інфектор зберігає знаходиться в ньому завантажувач, написаний на асемблері. З комп'ютера, з якого здійснювалася атака, той завантажує основний модуль троянця, а вже він включає інфіковану пристрій в децентралізований P2P-ботнет.

Trojan.Inject - Сімейство шкідливих програм, що вбудовуються шкідливий код в процеси інших програм.

Trojan.DownLoader - Сімейство троянців, призначених для завантаження на атакується комп'ютер інших шкідливих додатків.

Trojan.InstallCore - Сімейство установників небажаних і шкідливих додатків.

Огляд вірусної активності за серпень 2017 року

Шкідливі програми в поштовому трафіку:

JS.DownLoader - Сімейство шкідливих сценаріїв, написаних на мові JavaScript. Завантажують і встановлюють на комп'ютер інші шкідливі програми.

VBS.DownLoader - Сімейство шкідливих сценаріїв, написаних на мові VBScript. Завантажують і встановлюють на комп'ютер інші шкідливі програми.

Trojan.Encoder.13570 - Представник сімейства троянців-вимагачів, шифруючих файли на комп'ютері і вимагають від жертви викуп за розшифровку.

Троянець-майнер для ОС Linux **Linux.BtcMine.26**. Ця шкідлива програма призначена для добування криптовалюти Monero (XMR) і поширюється аналогічно Linux.Mirai: зловмисники з'єднуються з пристроєм, який атакується по протоколу Telnet, підібравши логін і пароль, після чого зберігають на ньому програму-завантажувач. Потім кіберзлочинці запускають цю програму з терміналу за допомогою консольної команди, і на пристрій завантажується троян.

ТОП-10 шкідливих програм: серпень - початок вересня, 2017

Dr.WEB® АНТИВИРУС

Выберите страну: Rus

Решения | Купить | Скачать | Информация | Партнёры | Поддержка | Форум | О компании

Статистика обнаружения вирусов

Статистика Dr.Web®

Статистика

Дата начала: 1 Aug 2017 , 00:00

Дата окончания: 6 Sep 2017 , 16:00

Топ: 10 Запросить

Почта

Файлы

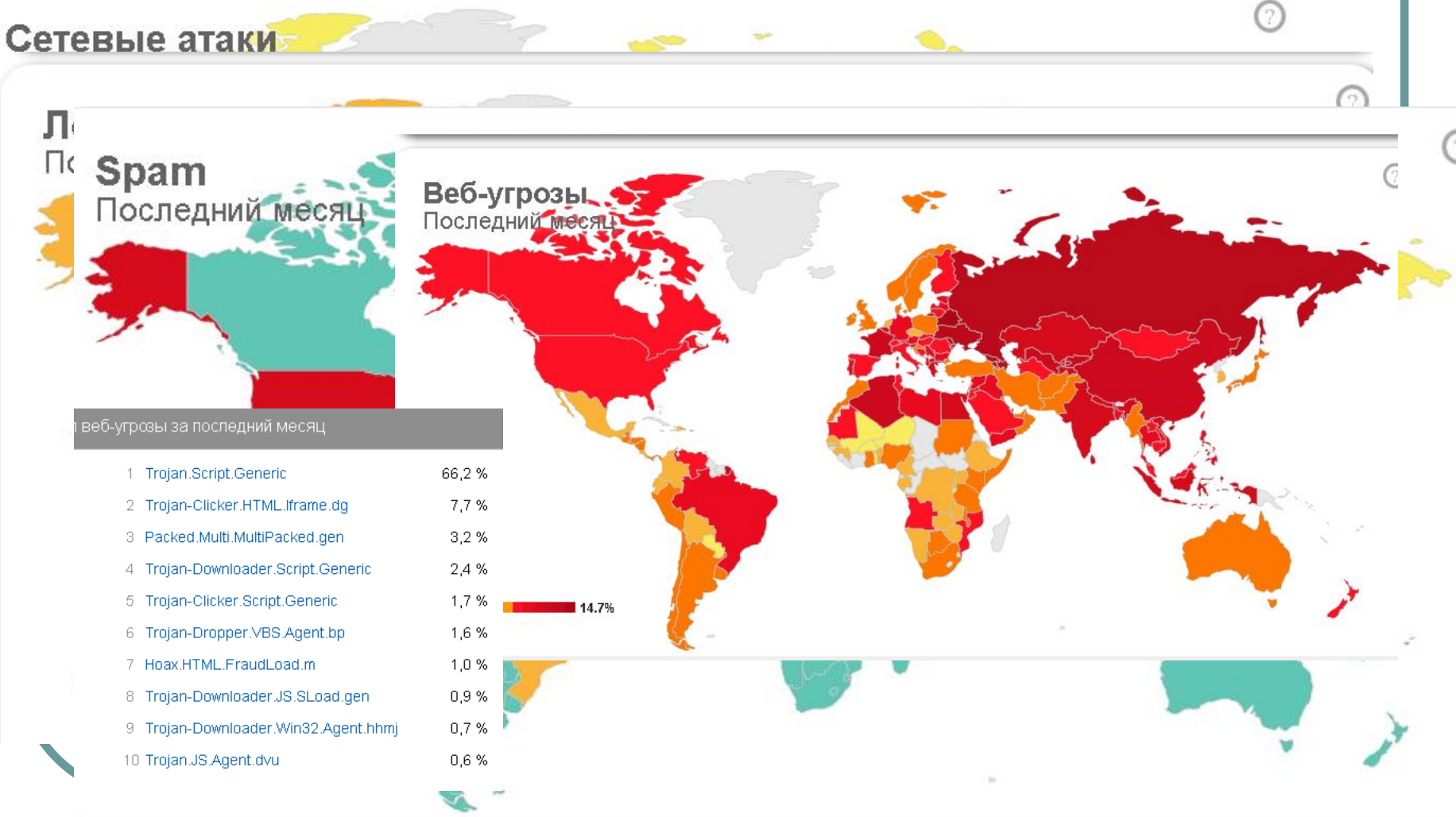
01.08.2017 00:00 - 06.09.2017 16:00		
1	SCRIPT.Virus	4.30%
2	Trojan.DownLoader25.21178	1.95%
3	JS.Inject.3	1.14%
4	BackDoor.PlugX.19	1.04%
5	Adware.Downware.17838	0.93%
6	Trojan.Inject2.58387	0.91%
7	JS.DownLoader.1225	0.79%
8	Trojan.InstallCore.2896	0.65%
9	Tool.FakeSLIC.2	0.51%
10	Adware.OpenCandy.152	0.51%

Dr.WEB® www.drweb.com

SCRIPT.Virus
Tool.BtcMine.431
Adware.OpenCandy.152
Adware.Downware.17838
HLLW.Shadow

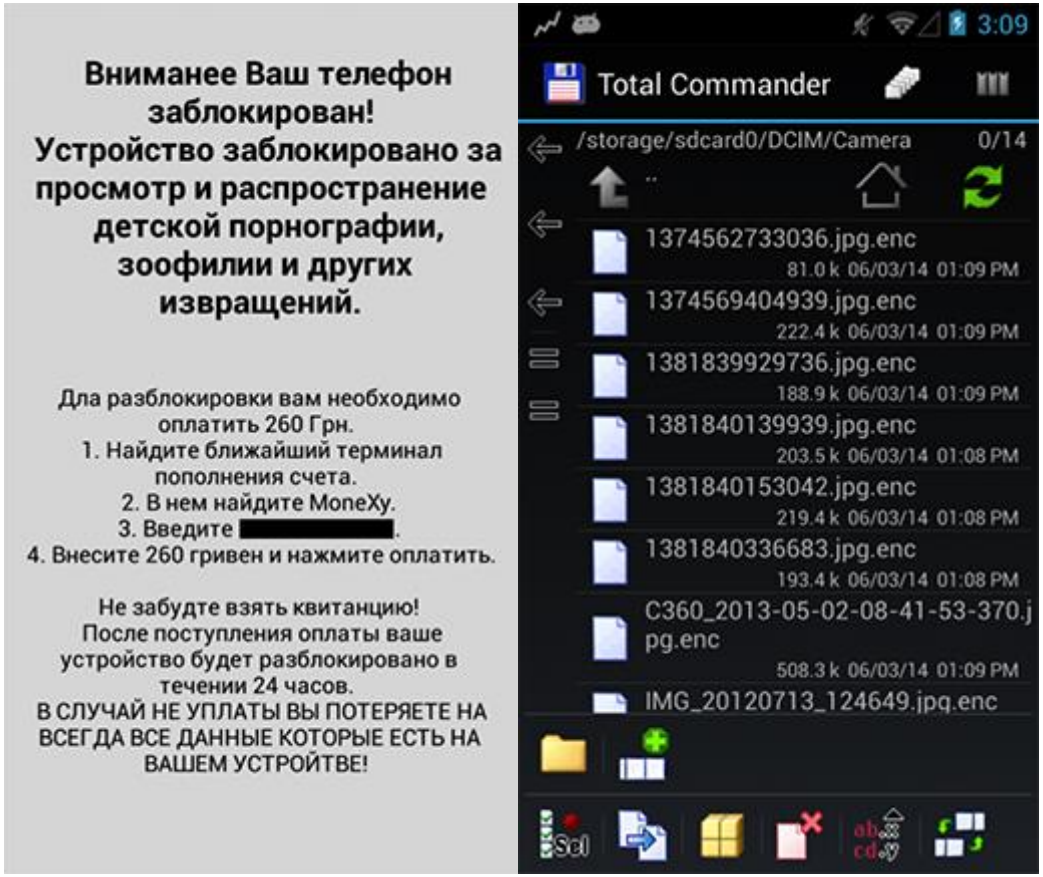
За даними компанії DrWEB: http://stat.drweb.com/

Загрози останнього місяця 17



За даними Securelist https://securelist.ru/statistics/

Simplocker, блокує мобільні пристрої і вимагає гроші за розшифровку даних.



Після завантаження даної загрози на Android смартфони або планшети здійснюється сканування SD карти на наявність документів, фото, відео у форматах * .doc, * .docx, * .jpeg, * .jpg, * .png, * .bmp, * .gif, * .pdf, * .txt, * .avi, * .mp4 та інших. Потім відбувається шифрування виявлених даних, а користувач отримує повідомлення з вимогою заплатити за розблокування 260 гривень.

Троян - спадкоємець Zeus і Carberp

Користувачів ПК атакує небезпечний поліморфний троян, який ***спеціалізується на крадіжці банківських даних і грошових коштів*** з рахунків жертв.

Новий банківський троянець (**Trojan.Agent.Win32.692577** в класифікації антивірусної лабораторії **Zillya!**) в першу чергу він шпигує за зараженим пристроєм. Крім того, він здатний перехоплювати дані і працювати у всіх поширених браузерах Microsoft Internet Explorer, Chrome, Opera і Mozilla Firefox. Така функція дозволяє «вірусу» ***красти дані, які вводяться в форми для заповнення на різноманітних сайтах.***

Також троян ***може робити знімки екрану монітора*** і виступати в ролі ***кейлогера*** - крадія паролів, які вводяться через клавіатуру. Таким чином, метою банківського троянця стають пари логінів і паролів до акаунтів інтернет-банку, що дає його господарям необмежений доступ до грошей жертви.

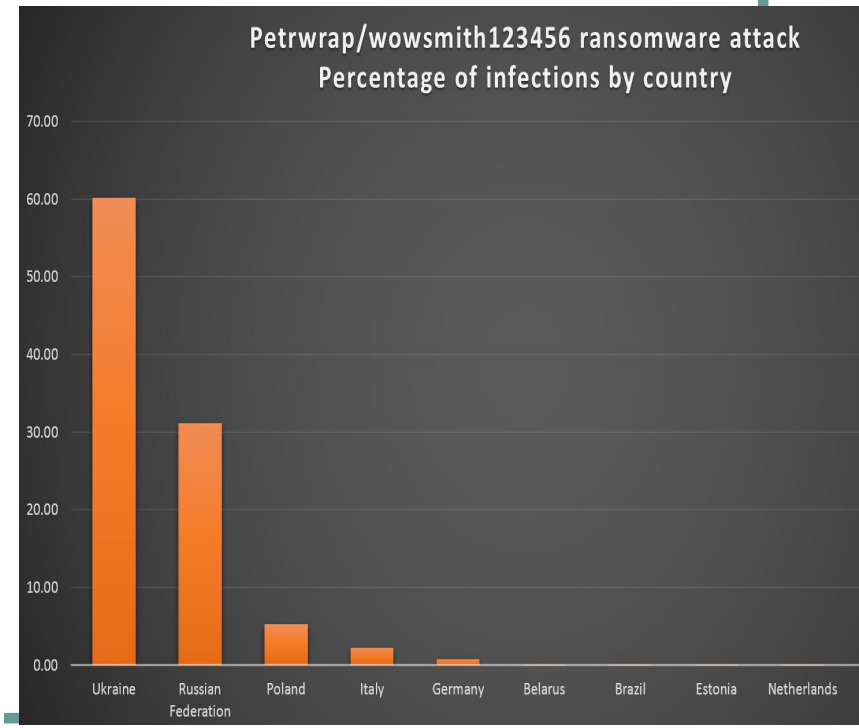
http://www.zillya.ua/u-merezhi-zyavivsya-troyan-spadko-mets-zeus-i-carberp

Вірус Petya

В кінці червня відбулися атаки нового вимагача-шифрувальника, який отримав назву ***ExPetr*** (aka Petya, Petrwrap і NotPetya), він був націлений в першу чергу на компанії в Україні, в Росії і в Європі.

Шифрувальник поширювався під виглядом оновлень до MEDoc –програма електронного документообігу. Потрапивши в корпоративну мережу, це ШПЗ витягує облікові дані з процесу lsass.exe і передає їх інструментам PsExec або WMIC, які далі поширюють їх усередині мережі.
Вірус вичікує від 10 хвилин до години, потім перезавантажує комп'ютер, шифрує таблицю MFT в NTFS-розділах і перезаписує головний завантажувальний запис кастомними загрузчиком, який містить вимогу викупу.

Разом з таблицею MFT, ***ExPetr*** шифрує і файли. За ключ розшифровки зловмисники просили аналог $ 300 в біткоінах; викуп слід відправити на єдиний bitcoin-рахунок.

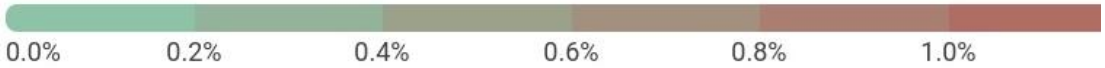


Географія мобільних банківських загроз за за II квартал 2017 року.

Топ 10 країн, атакованих **банківськими троянцями.** Кількість атак.

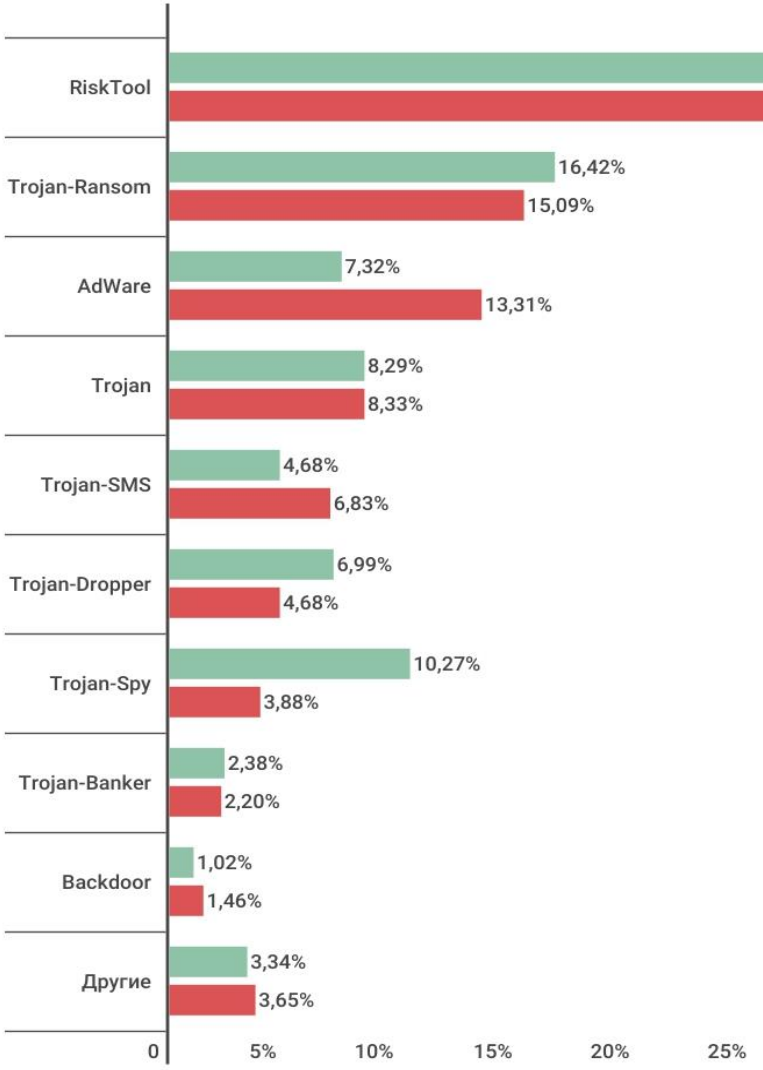
Страна*	% атакованных пользователей**
Германия	2,61
Того	2,14
Ливия	1,77
Палестина	1,53
Ливан	1,44
Венесуэла	1,39
Тунис	1,35
Сербия	1,28
Бахрейн	1,26
Тайвань	1,23

Найпопулярнішим мобільним банківським троянц
цьому кварталі став ***Trojan-Banker.AndroidOS.S***
активно поширюється через SMS спам. Основна
крадіжка грошей.



За даними Securelist https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/

Розподіл мобільних загроз в I та II кварталах 2017



TOP 20 мобільних шкідливих програм

1	DangerousObject.Multi.Generic	62,27%
2	Trojan.AndroidOS.Boogr.gsh	15,46%
3	Trojan.AndroidOS.Hiddad.an	4,20%
4	Trojan-Dropper.AndroidOS.Hqwar.i	3,59%
5	Backdoor.AndroidOS.Ztorg.c	3,41%
6	Trojan-Dropper.AndroidOS.Agent.hb	3,16%
7	Backdoor.AndroidOS.Ztorg.a	3,09%
8	Trojan.AndroidOS.Sivu.c	2,78%
9	Trojan-Dropper.AndroidOS.Lezok.b	2,30%
10	Trojan.AndroidOS.Ztorg.ag	2,09%
11	Trojan-Clicker.AndroidOS.Autosus.a	2,08%
12	Trojan.AndroidOS.Hiddad.pac	2,08%
13	Trojan.AndroidOS.Ztorg.aa	1,74%
14	Trojan.AndroidOS.Agent.bw	1,67%
15	Trojan.AndroidOS.Agent.gp	1,54%
16	Trojan.AndroidOS.Hiddad.ao	1,51%
17	Trojan-Banker.AndroidOS.Svpeng.q	1,49%
18	Trojan.AndroidOS.Agent.ou	1,39%
19	Trojan.AndroidOS.Loki.d	1,38%
20	Trojan.AndroidOS.Agent.eb	1,32%

https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/

Географія DDoS атак за II квартал 2017 року.

Розташування командних серверів