Вредоносное (злонамеренное) программное обеспечение

MaliciousWare (Malware)

и

борьба с ним

ЦЕНТР СТРАТЕГИЧЕСКИХ И МЕЖДУНАРОДНЫХ ИССЛЕДОВАНИЙ (CSIS)

- УЩЕРБ, НАНОСИМЫЙ КИБЕРПРЕСТУПНОСТЬЮ ВАРЬИРУЕТСЯ ОТ $400 МЛРД ДО $600 МЛРД В ГОД).

Некоторые Гиператаки

•Уязвимость в **Foursquare** (социальная сеть с функцией геопозиционирования, предназначенная для работы с моб прил), позволяющуая получить доступ к любому профилю, и потенциально способная раскрыть 45 млн адресов электронной почты.

•Уязвимость в **Thunderbird (**бесплатная почтовая программа**)**, позволяющая внедрять вредоносный код в электронные письма. 10.02.2014

•Уязвимости в **GitHub** (веб-сервис для хостинга IT-проектов и их совместной разработки), позволяющая получить доступ к чужой учетной записи.

•Уязвимость в **CMS Joomla** (система управления содержимым) , позволяющая удаленно осуществить SQL-инъекцию и похитить важную информацию, хранящуюся в базе данных

13.03.2014	**Whatsapp** уязвимость, которая позволяет любому приложению, установленному на Android-устройстве, перехватывать и расшифровывать всю переписку пользователя.
17.02.2014	Взлом **Forbes (**финансово-экономический журнал**)**
22.02-03. 2014	Крупнейшая кибератака на онлайн-аукцион **eBay** с получением информации о поролях и других личных данных пользователя

18.04.2014	Взлом крупнейшей сотовой сети **Orange** во Франции с кражей около паспортных данных, телефонных номеров и адресов электронных почт около 1,3 миллиона пользователей.
28.04.2014	Стало известно об узявимости **Internet Explorer 6** позволяющей выполнять на ПК жертвы любой код.

21.05.2014	Google обнаружила и устранила 23 уязвимостей безопасности в браузере **Chrome**

Классификация вредоносного ПО

1. Вирусы (viruses) — это **саморазмножающиеся** программы путем дописывания собств-х кодов к **исполняемым файлам**. Вирусы могут содержать, а могут не содержать деструктивные функции.

Макровирусы - это файловые вирусы. Макровирусы заражают различные документы и электронные таблицы, такие, как, например, файлы редакторов Word и Excel. Код этих вирусов создается на макроязыках, отсюда и их название.

Большинство макровирусов обладают свойствами резидентов и действуют только во время работы с инфицированным документом.

Классификация вредоносного ПО

2. Черви (worms) — это программы, которые самостоятельно размножаются по сети и, в отличие от вирусов, не дописывают себя (как правило) к исполняемым файлам. Все черви съедают ресурсы компьютера, “нагоняют” интернет-трафик и могут привести к утечке данных с вашего компьютера.

3.Кейлоггеры (keyloggers) — программы, которые регистрируют нажатия клавиш, делают снимки рабочего стола, способом отслеживают действия пользователя во время работы за компьютером и сохраняют эти данные в скрытый файл на диске, затем этот файл попадает к злоумышленнику.

Классификация вредоносного ПО

4. Трояны (trojans), троянские кони — собирают конфиденциальную информацию с компьютера пользователя (пароли, базы данных и пр.) и тайно по сети высылают их злоумышленнику. Существует разновидность троянов под названием Trojan-Downloader, которая, осуществляет несанкционированную загрузку на компьютер пользователя программного обеспечения (обычно зловредного).

5 Боты (bots) — распространенный в наше время вид зловредного ПО, который устанавливается на компьютерах пользователей и используется для атак на другие компьютеры (сети bothet).

Классификация вредоносного ПО

6. Снифферы (sniffers - *to sniff — нюхать*) — это анализаторы сетевого трафика. Могут использоваться в составе зловредного ПО, скрытно устанавливаться на компьютере пользователя и отслеживать данные, которые отправляет или получает пользователь по сети.

7. Руткиты (rootkits - наборы root'а) — сами по себе не являются зловредным ПО. Назначение — скрывать работу других зловредных программ (кейлоггеров, троянов, червей и т.д.) как от пользователя, так и от программ безопасности (антивирусов, файерволов, систем обнаружения атак и пр.).

Классификация вредоносного ПО

8. “Звонилка” (Dialer или Porn-Dialer) —может просто изменять настройки уже существующих соединений удаленного доступа на компьютере пользователя или создавать новое соединение.

9. Эксплоиты (exploits; от *exploit* - эксплуатировать)— это программы, которые через ошибку в программном обеспечении компьютера могут предоставить несанкционированный доступ машине или просто вывести ее из строя (завесить, перезагрузить).

Классификация вредоносного ПО

10. AdWare (приставка "Ad" является сокращением от английского слова "advertisement" — реклама, а слово "Ware" переводится как "продукт") — это приложение, которое показывает рекламу, доставляемую через интернет.

11. SpyWare (англ. Spy — шпион, Ware — продукт) — программа-шпион, которая собирает и передает посторонним лицам информацию о пользователе без его согласия. В основном, SpyWare используется для маркетинговых исследований, поэтому собранная информация обычно передается на серверы рекламных фирм.

Эксплойты (**эксплоит, сплоит,** англ. **exploit**, эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему;

это подвид вредоносных программ, которые содержат данные или исполняемый код, способный воспользоваться одной или несколькими **уязвимостями** в программном обеспечении на локальном или удаленном компьютере.

Особая проблема - эксплойты неизвестных уязвимостей, обнаруженных и использованных преступниками, — так называемые **уязвимости нулевого дня**.

Angler — один из самых сложных наборов эксплойтов на черном рынке. Обнаруживает антивирусы и виртуальные машины (часто используемые экспертами по безопасности как приманки) и задействует шифрованные файлы для затруднения исследования.

Nuclear Pack — поражает жертв эксплойтами Java и Adobe PDF.

Neutrino — набор эксплойтов от русскоязычных разработчиков для Java.

Blackhole Kit — наиболее распространенная веб-угроза (в 2012 году), нацеленная на уязвимости в старых версиях браузеров Firefox, Chrome, Internet Explorer и Safari, а также многих популярных плагинов, таких как Adobe Flash, Adobe Acrobat и Java.

			Angler	Sweet Orange	Nuclear	Fiesta	Magnitude	Neutrino	Astrum	RIG	Archie
CVE 2011-3402	Windows	уязвимость в модуле шрифтов TrueType Win32k					+				
CVE 2013-7331	Windows	ошибки в XMLDOM ActiveX компоненте			+						
CVE 2014-6332	Windows	неправильный доступ к объектам, хранящимся в памяти		+							+
CVE 2013-0074	Silverlight	ошибка двойного разыменования указателя в Silverlight	+		+	+			+	+	+
CVE 2013-3896	Silverlight	некорректная обработка объектов памяти в Silverlight	+			+			+		
CVE 2012-0507	Java	уязвимость в реализации класса AtomicReferenceArray			+	+	+			+	
CVE 2012-1723	Java	коллизии в JIT-компиляторе		+	+			+			
CVE 2013-0431	Java	уязвимость, позволяющая запускать неподписанные Java-апплеты						+			
CVE 2013-2424	Java	ошибка в компоненте ImageIO		+							
CVE 2013-2460	Java	ошибка в компоненте Deployment		+				+			
CVE 2013-2463	Java	ошибка в компоненте JMX					+	+			
CVE 2013-2465	Java	ошибка в компоненте Libraries			+	+		+		+	
CVE 2013-2471	Java	ошибка в компоненте Serviceability		+	+		+				
CVE 2013-2551	IE	использование ранее освобожденной памяти	+	+	+	+	+	+	+	+	+
CVE 2014-0322	IE	ошибки использования памяти при обработке CMarkup-объектов	+	+						+	
CVE 2014-1776	IE	ошибки при обработке доступа к объектам в памяти в библиотеке VGX.DLL	+								
CVE 2013-0634	Flash	уязвимость из-за неизвестной ошибки					+				
CVE 2013-5329	Flash	повреждение памяти приложения	+								
CVE 2014-0497	Flash	ошибка потери значимости целочисленных данных	+	+		+			+	+	+
CVE 2014-0515	Flash	уязвимость, позволяющая вызвать переполнение буфера	+	+	+				+		+
CVE 2014-0556	Flash	уязвимость, позволяющая вызвать переполнение буфера			+	+					
CVE 2014-0569	Flash	ошибка целочисленного переполнения памяти		+		+			+		+
CVE 2014-8439	Flash	ошибки в работе с указателями	+		+		+				
CVE 2014-8440	Flash	баг повреждения памяти во Flash	+								
CVE 2015-0310	Flash	обход ограничений безопасности в Adobe Flash Player	+								
CVE 2015-0311	Flash	уязвимость во Flash версий до 16.0.0.287 для Windows и OS X	+							+	
CVE 2013-2883	Chrome	ошибки использования после освобождения в MutationObserver			+						
CVE 2010-0188	Adobe PDF	PDF-сплойт LibTiff			+	+			+		

Кто создает вредоносное ПО

1. Подростки для самоутверждения.

2. Профессиональные программисты под заказ.

3. Сотрудники компаний по разработке антивирусного ПО с целью получения прибыли.

Пути проникновения вредоносного ПО

1. Ошибки в операционной системе и установленном ПО.

2. Безграмотность пользователей в области компьютерной безопасности.

- ***Пиратские CD (DVD) - диски***

- ***Флеш-накопители (флешки)***

- ***Электронная почта***

- ***Системы обмена мгновенными сообщениями***

- ***Веб-страницы***

- ***Интернет и локальные сети***

Меры борьбы с вредоносным ПО

- регулярное обновление операционной системы;

- использование безопасного браузера (Opera, Mozilla Firefox) и почтового клиента (The Bat!, Mozilla Thunderbird , Sylpheed) ;

- установка надежного файервола (Outpost Firewall Pro, ZoneAlarm Free Firewall, Gomodo Firewall);

Файервол (англ. firewall — огненная стена) — это браузер типа программный фильтр (существуют и программно-аппаратные файерволы), который отслеживает входящий и исходящий сетевой трафик компьютера и блокирует потенциально опасные соединения.

Меры борьбы с вредоносным ПО

- установка антивируса и антишпионского ПО

Существует два режима работы антивируса:

•Режим сканера — это основной режим.

•Режим резидентного монитора — в этом режиме антивирус работает постоянно в оперативной памяти, пока работает операционная система, и налету проверяет всё файлы, с которыми осуществляются какие-нибудь действия в системе (запуск, открытие, копирование и т. п.).

- Частое обновление антивирусных баз

- Проверка файлов в архивах

Наиболее популярные в нашей стране антивирусы: Dr.Web, антивирус Касперского. Avira AntiVir PersonalEdition Classic , avast! 4 Home Edition.

Превентивные меры борьбы с вредоносным ПО

Проверка на вредоносное ПО с помощью
- антишпионов (AVG Anti-Spyware Free Edition),
- антируткитов (Rootkit Unhooker),
- антикейлоггеров (Advanced Anti Keylogger).

- отключение неиспользуемых служб

Службы (Services) — это приложения, которые запускаются в фоновом режиме и обеспечивают многие важные функции ОС. При стандартной установке Windows XP Professional в систему устанавливается около 80-и системных служб.

- ручная диагностика системы

- Проверка автозагрузки файлов
- Просмотр списка процессов