Компьютерный вирус: FLAME (2012)

FLAME

- Компьютерный червь-троянец, поражающий компьютеры под управлением операционных систем Microsoft W

- Программа, детектируемая защитными продуктами «Лаборатории Касперского» как Worm.Win32.Flame, разработана для ведения кибершпионажа.

Размер и загрузка

- 20 мегабайт исполняемого кода со всеми модулями и плагинами

  20-мегабайтная программа загружается на компьютер по частям: сначала базовый компонент размером 6 МБ с несколькими основными модулями в архивированном виде, затем подгружаются остальные модули по мере необходимости. Один из самых маленьких модулей Flame состоит из 70000 строк кода на СИ с более чем 170 зашифрованными строками.

Возможности FLAME

- Меняет параметры компьютера
- Запоминает нажатые клавиши на клавиатуре
- Фотографирует экран монитора
- Записывает разговоры пользователей с помощью встроенного микрофона
- Запоминает историю посещений
- Удаляет информацию с жесткого диска без возможности восстановления
- Создание Bluetooth-меток на зараженном компьютере

- В активом режиме Flame уничтожал важные данные, связанные с нефтяной промышленностью. Разрушительной деятельностью являлось затирание баз данных поставок нефти, номеров счетов, списков клиентов и другой важной для данной отрасли информации, в результате чего Ираном был остановлен главный терминал отгрузки нефти (так как не было понятно кому и сколько выдать).

Основные компоненты Flame

Windows\System32\mssecmgr.ocx — основной модуль, в реестре HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Authentication Packages
Windows\System32\msglu32.ocx
Windows\System32\nteps32.ocx
Windows\System32\advnetcfg.ocx
Windows\System32\soapr32.ocx

- **OCX** (OLE Custom eXtension) – элементы управления ActiveX, выполняющие примерно те же функции, что и файлы *.dll.
- **ActiveX** — программная платформа для определения программных компонентов, пригодных к использованию из программ, написанных на разных языках программирования.

- Flame использует библиотеки Zlib , libbz2 , PPMD для сжатия без потерь , встроенную СУБД sqlite3 , виртуальную машину Lua .

- **SQLite** - компактная встраиваемая - компактная встраиваемая реляционная база данных, т.е связанная СУБД.

- **Lua** - скриптовый язык программирования, разработанный в подразделении Компьютерная графика Technology Group в Бразилии.

  Интерпретатор языка является свободно распространяемым , с открытыми исходными текстами на языке Си .

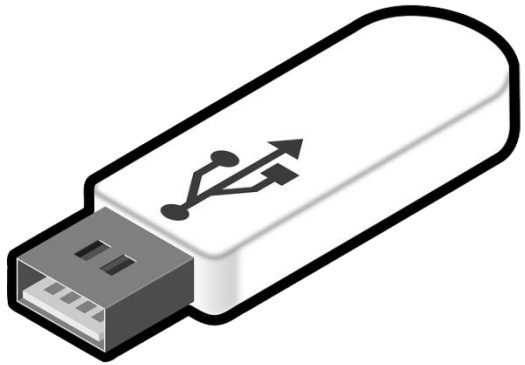
- Первоначально было инфицировано 1000 машин (начиная с 2010 года). Среди них правительственные организации, учебные заведения и некоторые частные лица

Обнаружение

- Был обнаружен по этому файлу ~ZFF042.TMP

Распространение

- Для распространения Flame использует уязвимость в службе диспетчера печати и через USB-устройства.
- Даже полностью пропатченной Windows 7 не защититься от этого вируса.



Пострадавшие страны


Иран


Израиль


Судан


Сирия


Ливан


Саудовская Аравия


Египет


Палестина

Искали Wiper, а нашли FLAME

- В мае 2012 года после того, как месяцем ранее неизвестная вредоносная программа удалила всю информацию с компьютеров ряда промышленных объектов нефтегазовой отрасли, расположенных в ближневосточном регионе Международный союз электросвязи (МСЭ)

  заказал исследование у “Лаборатории Касперского” .

Международный союз электросвязи

Международная организация, определяющая рекомендации в области телекоммуникаций и радио, а также регулирующая вопросы международного использования радиочастот. Учреждение ООН.

- Вредоносная программа уничтожала все данные, которые бы могли быть использованы для обнаружения вируса. Данные, находящиеся на жестком диске, удалялись без возможности их последующего восстановления.

- Имена ряда файлов, которых “Лаборатория Касперского” сумела восстановить с помощью системного реестра начинались с ~D, что схоже именами файлов, использованных в программах Duqu и Stuxnet.

- На 75% исследованных дисков данные были полностью удалены. Основной акцент был сделан на уничтожения первой половины дискового пространства. Затем происходило систематическое стирание оставшихся файлов, которые отвечали за работу системы, в результате чего она переставала функционировать.

- В ходе исследования выяснилось, что особое внимание удалялось уничтожению PNF-файлов.
- PNF- precompiled INF file. Создается на каждый INF файл для Windows.

- Как отмечают эксперты «Лаборатории Касперского», обнаруженный в апреле текущего года вредоносный код Wiper имеет очень много общего с вирусами Flame, Stuxnet и Duqu.

Иран, 2009

- Мировое сообщество высказало свое отношение к разработкам «мирного атома» Ираном, как к попытке создать ядерное оружие. После того, как Иран ответил запретом продаж нефти Европейским странам, в его системах был обнаружен тот самый Flame.

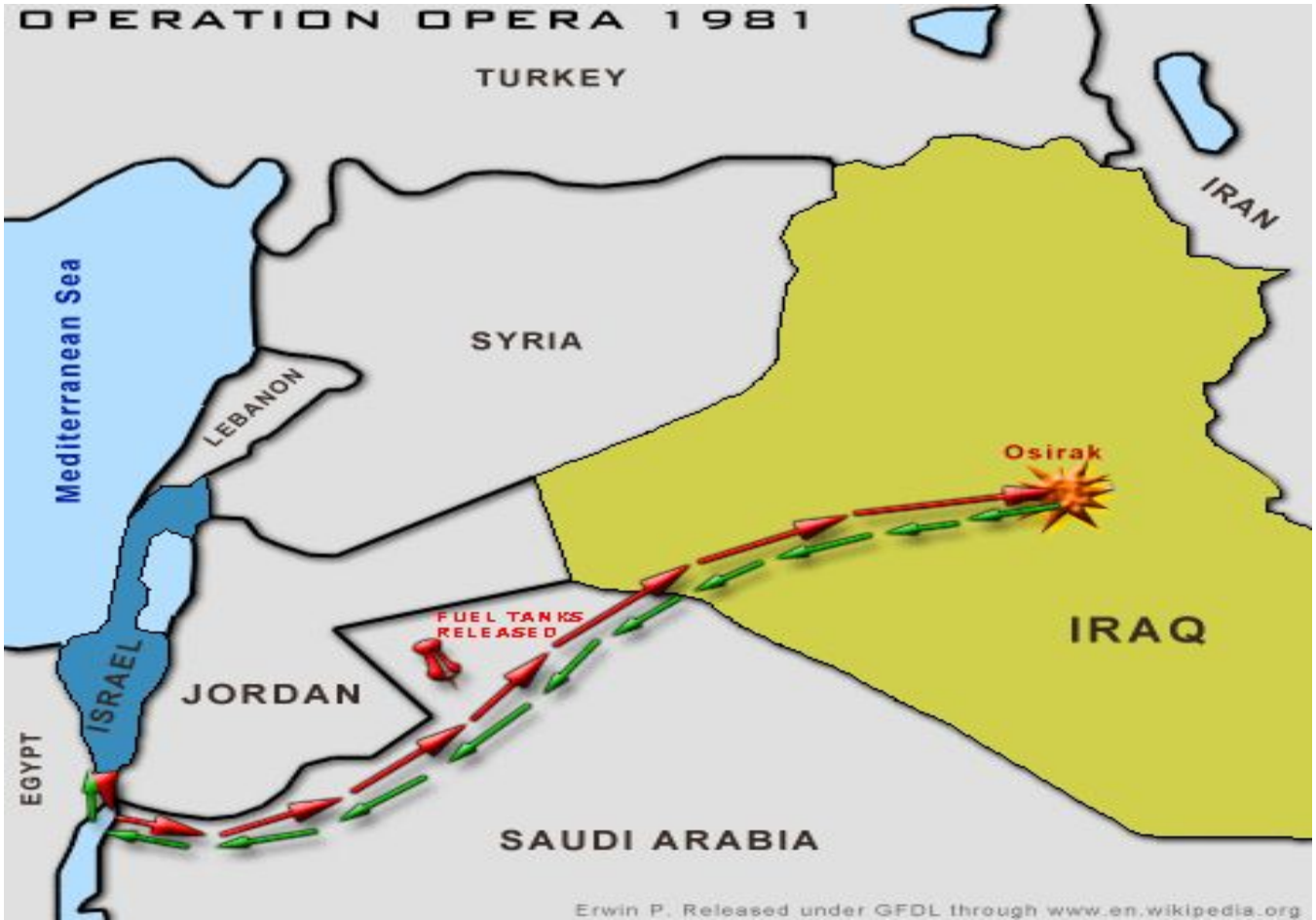
В июне 2012 года газета Washington Post со ссылкой на неназванных западных чиновников сообщила о том , что шпионский вирус Flame разрабатывался совместно специалистами США и Израиля для получения информации , которая могла бы быть полезна в срыве иранской ядерной программы.

Операция “Олимпийские игры”

- Операция кибервойны, направленная против иранских ядерных объектов со стороны США и, вероятно, Израиля. Начата была при президентстве Джорджа Буша в 2006 году, её проведение было ускорено при президенте Бараке Обаме, который внял совету Буша продолжать кибератаки на иранскую ядерную установку в Натанзе. Буш полагал, что данная операция была единственным способом предотвратить израильский удар по иранским ядерным объектам, подобный операции «Опера».

Операция « Опера »

Военная операция , проведённая ВВС Израиля для уничтожения ядерного реактора « Осирак » французского производства на территории Ирака в июне 1981 года .



- Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере. Вирус обнаружен в июне 2010 года.

Duqu - компьютерный червь , обнаруженный 1 сентября 2011 года

Распространяется через электронную почту .

Крадет конфиденциальную информацию , после чего удаляется через 36 дней .

Червь получил имя **Duqu** из-за префикса «~DQ», который использовался во всех именах файлов, создаваемых им.