

Что известно о масштабной хакерской атаке на Россию, Германию и Великобританию?

Чтобы предотвратить поражение тысяч подведомственных компьютеров надо было всего лишь обновить Windows.

Что случилось?

12 мая хакеры атаковали сервисы больниц в Великобритании, сервисы основного железнодорожного оператора Германии, серверы «МегаФон» и «ВымпелКом», а также МВД и Минздрава России. Одним из виновников атаки называют Агентство национальной безопасности (АНБ) США.

В «Лаборатории Касперского» зафиксировали 45 тысяч атак в 74 странах мира, основная часть пришлась на Россию. Во всех случаях кибератак хакеры использовали программу-шифровальщик WannaCry.

К обеду 13 мая атаку удалось отразить. Вирус-шифровальщик удалось остановить благодаря регистрации доменного имени iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Как выяснили специалисты по безопасности, этот адрес был зашит в коде вируса.

Как только зарегистрировали этот домен, распространение вируса замедлилось и почти остановилось.

Как проходила атака?

Как пишет Gizmodo, хакеры использовали уязвимость в операционной системе Windows под названием ExternalBlue, которая позволяет проникать в систему. Этот эксплойт был обнаружен еще прошлым летом, а пару месяцев назад Microsoft выпустила обновление, закрывающее дыру в безопасности. То есть заблокированными оказались те компьютеры, которые не были вовремя обновлены.

Важное уточнение: атака производилась не на компьютеры отдельной страны, а на вообще все компьютеры на Windows. Вовремя обновленные компьютеры программа-шифровальщик обошла стороной и задела только не обновленные. Карта, предоставленная «Лабораторией Касперского», хорошо иллюстрирует, в каких странах есть проблемы с систематической работой над безопасностью.

Что хотели хакеры?

Денег. Программа зашифровывает всю информацию на заблокированном компьютере и не отдает, пока владелец устройства не заплатит выкуп.



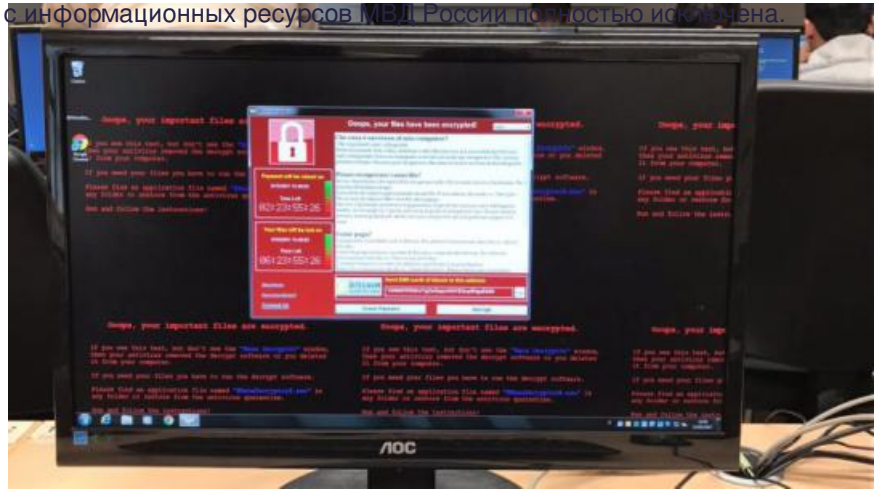
Если не заплатишь — останешься без данных. Как с проблемой справились в российских ведомствах и организациях — неизвестно. Возможно, на зараженных компьютерах не хранилось важной информации. Возможно, им пришлось заплатить злоумышленникам. Как сообщила официальный представитель МВД Ирина

Волк, утечка служебной информации с информационных ресурсов МВД России полностью исключена.

Кто виноват и что делать?

Виноваты, конечно, хакеры. Но не только. Виноваты службы безопасности всех пострадавших организаций. Там не проследили, чтобы критически важные обновления были установлены.

Один из выходов — переход на альтернативное программное обеспечение. В МВД, например, заявили, что им удалось избежать последствий благодаря использованию «иных операционных систем» и отечественных серверов с российским процессором «Эльбрус». Эксперт Иван Бегтин считает, что в будущем подобных проблем можно избежать, перейдя на открытое программное обеспечение.



При чём здесь АНБ?

Впервые об уязвимости ExternalBlue стало известно от группы хакеров The Shadow Brokers. Как заявляли сами хакеры, они выкладывают эксплойты известной группировки Equation Group, по некоторым данным связанной с АНБ. С высокой вероятностью Equation Group по заказу АНБ создавала такое известное кибероружие, как Stuxnet, Duqu, Regin, Flame и др.

Читайте также:

[Boom и еще пять мобильных приложений для меломанов](#)

[Четыре самых «горячих» иркутских стартапа](#)

[В августе на Байкале пройдет летняя школа программной инженерии](#)

[Ловил покемонов — поймал срок. Чем закончилось дело видеоблогера Руслана Соколовского](#)

Автор: Виктория Федосеенко © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3537
13.05.2017, 13:54 1

URL: <https://babr24.com/?IDE=272264> Bytes: 4660 / 3402 [Версия для печати](#)

[Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com



Автор текста: **Виктория Федосеенко**, журналист.

На сайте опубликовано **1274**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)

