

## **Кибератаки, как угрозы глобальной безопасности на примере вируса "WannaCry"**

*Сильванский Юрий Юрьевич*

*E-mail: mr.hitrojop@mail.ru*

Сильванский Юрий Юрьевич

Кибератаки, как угрозы глобальной безопасности на примере вируса «WannaCry»

Студент (бакалавр)

Донецкий национальный университет, Исторический факультет, Кафедра международных отношений и внешней политики, Донецк, Украина

### **Кибератаки, как угрозы глобальной безопасности на примере вируса «WannaCry»**

Высокий уровень развития компьютерных технологий—одна из самых сильных сторон нашего современного общества, но она же и является возможной причиной глобальной катастрофы. Многие аспекты нашего социума сильно зависимы от работы ряда служб и компаний, которые играют далеко не последнюю роль в нашей жизни, а что-то и вовсе стало жизненно необходимым. На сегодняшний день очень остро стоит вопрос защиты глобальной безопасности от каких-либо угроз, так как способы взлома и распространения кибервирусов становятся все более продвинутыми, а способы защиты и решения последующих проблем просто не в состоянии противостоять огромному давлению со стороны кибертерраризма.

Всё, чего все службы и организации опасались, произошло 12 мая 2017 года. Компьютерный вирус «WannaCry» обрушился на все мировое сообщество и нанес непоправимый урон его аспектам, что кардинально изменило представление и значение понятия кибертерраризма. Вскоре, после глобальной кибератаки 12 мая стало известно, что в ходе крупной кибератаки пострадали больницы Великобритании, а вечером этого же дня, глава антивирусной компании Avast Якуб Кроустек заявил, что вирус атаковал и зашифровал свыше 55 тысяч компьютеров. Позже, российская Лаборатория Касперского установила более 47 тысяч атак кибервирусом «WannaCry» в 76 странах мира. Том Боссерт, советник президента безопасности США подтвердил, что 15 мая был осуществлен взлом свыше 280 тысяч компьютеров в 150 странах мира.

Как утверждают эксперты, только за первые трое суток вирус «WannaCry» взломал и заблокировал около 300 тысяч пользователей в 150 странах мира. Суммарная оценка ущерба составляет сумму 1 млрд долларов США и утраты продолжают расти. Что является не маловажным, в общую оценку ущерба вошли потеря данных, снижение производительности, простои в работе, судебные издержки, репутационные ущербы и другие факторы. Хочется отметить, что данная накопленная сумма образовалась в течении нескольких дней, а специалисты в области антивирусного обеспечения и по сей день не смогли полностью приостановить распространение вируса.

Вирус является главным аспектом кибератаки, именно червь-шантажист, именуемый «WannaCry». В ходе атаки и последующего заражения компьютера вирус-червь быстро распространяется по всей локальной сети, в которой производит шифрование файлов, а позже предлагает выплатить определенную сумму за разблокировку интернет-валютой (Bitcoin). Было отмечено, что вирус использует средства и инструменты, которые киберпреступники украли у хакеров из АНБ США еще в 2000-х годах.

Особое внимание стоит уделить тому факту, что высокая частота кибератаки вирусом «WannaCry» была установлена в таких странах как: Великобритания, Германия, Россия, Украина, Италия, Турция, Испания, Португалия, Япония, Тайвань. Серьезнейший урон получили Россия, США и Украина. В России пострадали сети «Мегафона», «Билайна», РЖД, Минздрава, Сбербанка, МВД и Следственного комитета. Также следует отметить, что атаке вируса «WannaCry» подверглись:

- **больницы Великобритании.** Огромное количество больниц осталось без каких-либо средств коммуникации, а пациенты, которые остро нуждались в медицинской помощи оказались тяжелейшем положении.

- **железнодорожный оператор Германии Deutsche Bahn.** В Ганновере были атакованы и заблокированы все диспетчерские системы управления. Вирус имел все возможности повлиять на режимы и графики движения поездов Deutsche Bahn.

- 12 мая множество российских СМИ сигнализировали о том, что была проведена атака **компьютерных сетей Следственного комитета и МВД РФ.** Поначалу шло опровержение информации о каких-либо вирусных атаках на сервера организаций, но через некоторое время представитель МВД РФ Ирина Волк подтвердила, что попытки шифрования и последующего блокирования информации на серверах были предотвращены.

- 15 мая **представитель МНБ США** заявил, что во время кибератаки **было осуществлено заражение компьютеров операторов объектов инфраструктуры США.**

Из всего вышперечисленного можно сделать вывод, что крушение безопасности в киберпространстве влечет серьезные последствия и в реальной жизни, что несомненно усложняет вопрос решения данной проблемы.

Как уже известно, вирус «WannaCry» за довольно короткий промежуток времени сумел сделать то, что многие террористические организации не смогли сделать на протяжении долгих лет, что несомненно заставляет задуматься о важности безопасности киберпространства. При этом заражаются компьютеры и сети различных государственных учреждений и служб, отчего их работа оказывается парализована, что может повлечь крайне негативные последствия.

Анализируя изложенное следует отметить, что каждая инфраструктура играет важную роль в работе основных служб и производственных систем в нашем современном обществе, что несомненно влияет на жизнь любого человека. Поэтому сбои, блокировка, технические неполадки или какие-либо ограничения в сферах киберпространства могут иметь необратимые последствия для нашего социума, что может привести к нарушению установленного порядка, влиянию органов правления, экономика и гос-безопасность и во все может рухнуть за считанные дни.

#### **Источники и литература:**

1. Анализ шифровальщика WanaDecrypt0r2.0. Nabrahabr 2017г.
2. Киселёв В. Костенко А. Кибервойна, как основа гибридной операции (рус.) // Армейский сборник: журнал. — 2015. — Ноябрь (т. 257, № 11). — С. 3-6.
3. Об атаке вируса Wannacry // «ФинЦЕРТ» Банка России 2017 г.
4. Сошников, Андрей. WannaCry: как работает крупнейшее компьютерное вымогательство. «Русская служба Би-би-си» 2017 г.
5. Статья УК РФ: ст. 159.6 "Мошенничество в сфере компьютерной информации".