ПИРАТЫ XXI ВЕКА: КАК ХАКЕРЫ УГРОЖАЮТ ТОРГОВОМУ ФЛОТУ

Гаврилов Павел Олегович

курсант, МГУ им. Г.И. Невельского, Российская Федерация, Владивосток

Шмидт Игорь Анатольевич

курсант, МГУ им. Г.И. Невельского, Российская Федерация, Владивосток

В век цифровых технологий в нашем мире происходят такие события в которые бы раньше никто и не поверил, к примеру, киберпираты могут перехватить контроль над судном, изменить его курс и даже спровоцировать столкновение

Как же это возможно и как к этому быть готовым

Эксперты говорят, что атаки на компьютерные системы морских судов становятся все изощреннее и чреваты не только перебоями в мировой торговле и убытками коммерческого флота.

Киберпираты потенциально способны перехватить контроль над судном, изменить его курс и даже спровоцировать столкновение.

Тревожный сигнал

В июне сектор морских грузоперевозок серьезно пострадал от вируса NotPetya, основной удар которого пришелся на Украину, но пострадали и другие страны.

На этой неделе гигант грузового судоходства, датская компания Maersk, сообщила, что из-за данного вируса может недосчитаться 300 млн долларов прибыли.

Ларс Йенсен давно убежден, что хакеры угрожают морским перевозчикам. Три года назад он учредил CyberKeel и взял в бизнес-партнеры отставного лейтенанта датской армии Мортена Шенка - "одного из тех ребят, которые могут взломать почти всё что угодно".

Они начали предлагать перевозчикам проверку компьютерных систем на уязвимость, но на тот момент их услуги никого не заинтересовали.

"Ответ был довольно стандартным: Спасибо, не надо, не тратьте время зря, мы и так неплохо защищены", - вспоминает Йенсен.

Однако теперь всё иначе.

После атаки NotPetya, из-за которой Maersk на время пришлось даже закрыть часть портовых терминалов, транспортные компании на собственной шкуре почувствовали, как цифровой мир способен пагубно воздействовать на материальный.

Взламывая компьютерные системы, хакеры получают доступ к коммерчески важной информации. Так, недавно пиратам удалось спланировать нападение с хирургической точностью.

"Они поднялись на борт, по штрих-коду нашли интересовавший их ящик с ценностями,

вскрыли его - и только его - и удалились, не причинив других неприятностей", - описал преступление отдел кибербезопасности телекоммуникационной компании Verizon.

Уязвимы не только владельцы, но и собственно сам флот: управление грузовыми и пассажирскими судами все больше компьютеризируется.

Вирусы, подобные NotPetya, распространяются от одного компьютера к другому и потенциально угрожают всем подключенным к сети устройствам на борту судна.

"Нам, например, известен случай, когда из-за вируса-вымогателя на контейнеровозе отключился главный электрический распределительный щит", - рассказывает Патрик Росси из консультационной компании DNV GL.

Лишенное энергоснабжения обездвиженное судно некоторое время вынужденно простояло на приколе в одном из азиатских портов.

Дистанционный захват

Под удар попадают и навигационные системы. Один такой случай вспоминает Брендан Сондерс, отвечающий за морскую кибербезопасность в фирме NCC Group.

На этот раз дело происходило в азиатском порту, на борту танкера водоизмещением в 80 тысяч тонн.

Кто-то из команды принес на борт документацию на зараженной USB-флешке, а когда его коллега обновлял через USB-порт карты перед выходом в море, вирус поразил навигационную систему Ecdis.

Рейс пришлось отложить на время расследования.

"На Ecdis [Электронно-картографическая навигационно-информационная система] почти никогда не ставят антивирус, - говорит Сондерс. - Я не припомню ни одного коммерческого судна с антивирусом на Ecdis".

Подобные инциденты наносят существенный урон транспортному флоту, однако угроза может приобрести совсем иной масштаб, если хакеры решат вывести из строя или даже уничтожить судно, перехватив управление.

Возможно ли такое? Способен ли целеустремленный и хорошо оснащенный злоумышленник спровоцировать столкновение?

"В этом нет никаких сомнений, - говорит Сондерс. - Мы демонстрировали сценарии, при которых это возможно".

Тем временем эксперты находят все новые уязвимые места в судовых системах. Один из них, исследователь под псевдонимом x0rz, недавно взломал станцию спутниковой связи VSat на борту судна у берегов Южной Америки через приложение "Ship Tracker".

В этом случае владелец аппарата спутниковой связи сильно упростил ему задачу: к имени пользователя "admin" подошел пароль "1234".

По мнению x0rz, подобным образом можно обновить на устройстве программное обеспечение и захватить управление судном.

Теоретически можно даже изменить координаты, передаваемые судном, чтобы скрыть его истинное местоположение. Впрочем, ранее эксперты в этой области утверждали, что подобную подмену быстро обнаружат диспетчеры морских путей.

Очевидно одно: как и многим другим отраслям, торговому флоту придется адаптироваться к новой реальности.

Балтийский и международный морской совет и Международная морская организация недавно выпустили рекомендации, цель которых - помочь судовладельцам защититься от хакеров.

Однако задача это не из простых: в мире более 51 тысячи коммерческих судов, и экипажи на них постоянно меняются.

Впрочем, цена перебоев в морских перевозках тоже высока, ведь на них приходится более 90% мировой торговли.

Со всего мира приходят тревожные сообщения о проблемах с глобальными системами позиционирования (GPS), которые могут возникнуть в результате электронного «подавления» спутниковых сигналов со стороны недоброжелателей. Такие атаки формируют «поддельные» сигналы GPS, принимаемые бортовой аппаратурой.

К таким случаям можно привести в пример столкновение контейнерного судна ACX Crystal с военным кораблем USS Fitzgerald, который произошёл в июне 2017 года. Сообщалось, что внутри командования военно-морского флота США были подняты важные вопросы о серии столкновений еще до аварии с ACX Crystal. Одной из главных проблем, поднимаемых в данных вопросах является маневры военных и гражданских судов, включая такие смертельные для кораблей финты, как "штопор".

Такие повороты очень опасны для торговых судов, особенно контейнерных, которые следуют прямым маршрутом, чтобы сэкономить время и деньги и имеют мало технических возможностей для резкого маневра. Однако контейнеровоз врезался в американский военный корабль после несчетного количества поворотов". Чем это можно объяснить?

"ACX Crystal направлялось на восток к Токио из Нагои, и, сделав резкий правый поворот ударил в бок эсминцу.

Считается, что контейнерное судно, которое в три раза больше американского военного корабля, развернулось целенаправленно, чтобы столкнуться с эсминцем ВМФ. Существует также любопытный факт, что ACX Crystal крутилось, совершая одну и ту же серию поворотов, непосредственно перед встречей с американским военным судном.

По этой нелепой ситуации возникает масса вопросов. Например, почему американский USS Fitzgerald не знал о непосредственной близости контейнеровоза через оповещение автоматической идентификационной системы (AIS)? Иногда корабли ВМС США отключают ее при выполнении особых миссий. Тем не менее, корабли ВМФ регулярно используют свои AIS, когда находятся в зоне контроля местных служб отслеживания судов (СДС). Это тем более было актуально в условиях интенсивного судоходства в Токийском заливе.

"Системы AIS установлены на почти 400 000 кораблях, навигационных буях, маяках и морских нефтяных буровых платформах по всему миру. Если AIS эсминца была активирована, то должна была предупредить о близости гражданского корабля.

Вместе с тем, AIS контейнеровоза сама искала (!) свое местоположение во время столкновения, о чем свидетельствует трек его движения, передаваемый на различные сайты, включая Marinetraffic.com".

Допускается, что ACX Crystal , возможно, стал жертвой взлома его автоматической системы идентификации, электронных карт и информационной системы (ECDIS).

Ранее некоторые хакеры демонстрировали проникновение в системы AIS, в результате чего судна прекращали передачу сигнала о своем месте нахождения.

Система ECDIS заменяет бумажные морские карты и подвержена атакам, поскольку ее компоненты AIS, Navtex (навигационный телекс), радар и глубиномеры имеют слабую защиту от манипуляций с данными.

Спутниковый GPS уже стал жертвой подобных кибер-хакерских атак. В июне этого года 20

судов, находясь недалеко от российского города Новороссийска в Черном море, сообщили, что их системы GPS показали, что они дрейфуют примерно в 20 милях в дали от моря - непосредственно на территории аэропорта города Геленджик (Россия).

В таких условиях следует признать наличие серьезной опасности, существующей как для военного, так и для гражданского судоходства.

Данные случаи следует тщательно исследовать, поскольку перехват систем управления суднами может привести к очень серьезным последствием, особенно если в авариях будут участвовать пассажирские гражданские корабли.