Ассистент-преподаватель кафедры № 5
НУЦ СНБ РА, майор Н. Айрапетян

ИЗ ИСТОРИИ ПРИМЕНЕНИЯ КИБЕРОРУЖИЯ

Современные информационные технологии постепенно становятся неотъемлемой частью арсенала террористов. Глобальное информационное пространство стало для них не только средством передачи информации или пропаганды своих преступных идей. С его помощью террористы:

- вербуют новых сторонников в террористические структуры;
- проводят теоретическую, военную, религиозную подготовку;
- координируют деятельность отдельных первичных ячеек и групп;
- осуществляют финансовые операции и сделки по снабжению оружием;
- обеспечивают приобретение финансовых средств для подготовки и проведения террористических актов и т. д.

Отмеченная активность террористов в киберпространстве направлена на совершение террористических актов, с нанесением, по возможности, максимального ущерба. Ее выявление, постоянный контроль (наблюдение) и, по возможности, полное раскрытие и нейтрализация - актуальная проблема сегодня для любого государства, искренне нацеленного на эффективную борьбу с терроризмом.

Реальная угроза сегодня главным образом обусловлена тем, что кибертерроризм рассматривается террористическими организациями как альтернативная форма так называемых традиционных методов преступной деятельности. Постоянное совершенствование глобальных систем противодействия и последовательное укрепление национальных контртеррористических структур, затрудняют деятельность террористов. Соблазн осуществления террористических посягательств в киберпространстве связан с возможностью, без больших затрат и с минимальным риском для исполнителей, нанесения крупного физического ущерба объектам атак и значительного психологического воздействия на население. Кибертерроризм считается более опасным, особенно для тех стран, которые имеют мощную информационную инфраструктуру.

Следовательно, можно предположить, что количество посягательств кибертеррористического характера в обозримом будущем будет увеличиваться. Эффективно противодействовать использованию информационных технологий в террористических целях можно только в случае всестороннего научного

исследования этого явления и разработки глобальной стратегии борьбы с кибертерроризмом.

В настоящее время международное сообщество, параллельно с разработкой средств и методов по борьбе с кибертерроризмом, пытается выработать также единый подход к вопросам юридической классификации.

Кибертерроризм считается так называемым технологическим видом терроризма. Термин «кибертерроризм» был введен в оборот предположительно в 1997 году, когда специалист Федерального бюро расследований (ФБР) США М. Полит охарактеризовал этот вид терроризма как «нападение в политических целях со стороны националистических групп и тайных агентов на гражданские объекты, информационные, компьютерные программы и данные с угрозой насилия»[1].

Кибертерроризм можно охарактеризовать как незаконное уничтожение, блокирование (изоляцию) либо повреждение информации или программ (а также угроза этих действий) с помощью проникновения в компьютер, компьютерную систему или сеть, которое создает опасность возникновения человеческих жертв, значительного имущественного ущерба либо других общественно опасных последствий, если эти действия совершены с целью нарушения общественной безопасности, запугивания населения или воздействия на принятие решения государственным органом или должностным лицом либо исполнения преступного требования.[2].

Нижеприведенные примеры использования так называемого кибероружия свидетельствуют о том, что, попав в руки террористов, оно может привести к катастрофическим последствиям.

1988г. - По интернету стал распространяться вирус, разработанный аспирантом университета Корнелла Робертом Морисом, который не только вывел из строя работу компьютеров многих университетов и исследовательских центров, но и нацелился на системы управления Агентства национальной безопасности, стратегического командования, а также космических кораблей (шаттлов) НАСА. Это был первый вирус, который был удостоен внимания СМИ, а также привел к первому осуждению в США в соответствии с Законом «О компьютерном мошенничестве и злоупотреблениях» (Computer Fraud and Abuse Act, 1986). За свою разрушительную силу вирус получил название «Большой червь».

[1] Krasavin S. What is a Cyber-terrorizm? //http://rr.sans.org/infiwar

[2] Кинакцян А. Л., Киберпреступление и кибертерроризм: некоторые гносеологические и юридические вопросы / Юбилейный сборник научных статей «Гладзор - 20», Ереван, 2011.

1998г. - Убийство ключевого свидетеля, находящегося на лечении после тяжелого ранения в одной из больниц США под защитой ФБР. Интернет-хакер взломал сеть местной больницы и изменил график работы кардиостимулятора, убив пациента.

1998-2000г.г. - Операция Moonlight Maze. В следствие кибератак на Пентагон, НАСА, Департамент энергетики, научно-исследовательские компании и институты США были выявлены утечки информации и начато расследование, по окончании которого, стало известно, что первые атаки датируются 1996 г.

1999г. - Был активирован вирус «Чернобыль», стирающий все данные из полумиллиона зараженных компьютеров. Совпадение с годовщиной чернобыльской трагедии стало причиной названия вируса. В среде специалистов он известен также под названием «CIH». По разным оценкам, вирус уничтожил содержимое микросхем BIOS на многих из полумиллиона зараженных компьютеров. Вирус создал Чен Инхао, об аресте которого власти Тайваня сообщили 20 сентября 2000 года.

2000г. - По электронной почте из Филиппин стал распространяться вирус ILOVEYOU. Первоначально он искажал изображения, документы, программы, находящие в компьютере, скрывал музыку и видеоматериалы, а затем начал рассылать сам себя по всем адресам, найденным в электронной почте. В период своей активности, вирус ILOVEYOU успел заразить три миллиона компьютеров, причинив ущерб в 10-15 млрд. долларов, что сделало его самым разрушительным компьютерным вирусом Книги рекордов Гиннесса.

2001г. - Червь Code Red используя уязвимости в веб-сервере Microsoft IIS, просочился в компьютеры, работающие с помощью сервера и начал DoS-атаки. Вирус заменял всю информацию на веб-сервере следующей строкой: «HELLO! Welcome to http://www.worm.com! Hacked by Chinese!» Через 20-27 дней после заражения, зараженный сервер должен был начать DoS-атаку по нескольким IP адресам, один из которых принадлежал Белому дому. Были заражены 400.000 серверов, общий ущерб оценивается в 2.5 млрд. долларов США.

2004г. - Вирус My Doom, обновленная версия вируса ILOVEYOU, содержался в 30% всех электронных писем в Интернете, замедлил весь интернет-трафик на 10%. Ущерб оценивался в 38-40 млрд. долларов США. Вирус блокировал все антивирусные программы, а также веб-сайты компаний-

производителей, обеспечив хакерам доступ к зараженным компьютерам и превращая серверы Microsoft и SGO Group в зомби, атакующие спамом.

2003-2005г.г. – Операция Titan Rain. Кибератакам подверглись НАСА, компании Lockheed Martin, Sandia National Laboratories, Redstone Arsenal (предполагаемая геолокация атак - провинция Хуандун в Китае). В 2007г. подобной атаке подверглось также МИД Великобритании.

2006-2012г.г. - Хакерские атаки Shady RAt. В 2011 году специалисты по антивирусному программному обеспечению компании McAfee обнаружили «троянский конь», который распространялся по электронной почте. Пострадали около 50 организаций и компаний, в том числе правительства США, Тайваня, Южной Кореи, Вьетнама, Канады, Олимпийский комитет ООН, Ассоциация стран Юго-Восточной Азии, японские, швейцарские, индонезийские, датские, сингапурские, гонконгские, немецкие, индийские компании.

2007г. - Многочисленные хакерские атаки на государственные и военные структуры США, Германии, Индии. В апреле того же года Эстония подверглась масштабным DDoS-атакам, что побудило НАТО создать в Эстонии Европейский центр по борьбе с киберугрозами.

В сентябре Израиль разбомбил ядерный центр Сирии, во время которого использовал специально разработанную и заранее внедренную вредоносную программу по срыву работы радаров - операция Orchard.

2009г. - Канадские специалисты обнаружили крупную шпионскую сеть GhostNet, которая проникла в 1 миллион 295 тысяч компьютеров в 103 странах мира. Расследование началось с офиса Далай-Ламы, который, по всей видимости, был главной мишенью атаки кибертеррористов. Подверглись также атаке Министерства иностранных дел и посольства Ирана, Бангладеш, Индонезии, Индии, Южной Кореи, Таиланда, Германии и Пакистана. Правительство Китая отрицает свою причастность к данному инциденту.

2010 г. - Операция Myrtus. на заводе по обогащению урана в г. Натанз в Иране был обнаружен червь-Stuxnet, целью которого был срыв работы программирующихся контроллеров, регулирующих работу двигателей на сверхвысоких частотах. В Иране было заражено около 16 тысяч компьютеров.

Вирус обнаружил специалист белорусской компании «ВирусБлокАда» Сергей Уласень 17-го июня 2010г. Сетевой червь Stuxnet может быть использован для несанкционированного сбора (шпионажа) данных и диверсии против автоматических систем управления технологических процессов промышленных предприятий, электростанций, аэропортов и других инфраструктур.

В истории кибератак этот случай выделяется тем, что вирус впервые смог временно вывести из строя целую инфраструктуру. Об израильском происхождении вируса говорит наличие в его коде слова MYRTUS (на иврите

это звучит как «адас», которое, в свою очередь, похоже на имя «Адасса», которое принадлежит еврейке Эстер (Эсфир), спасшей от уничтожения свою нацию в Персидской империи). Кроме этого, в коде встречается число 19790509, которое совпадает с датой казни иранского бизнесмена еврейского происхождения Хабиба Элгханиана. Американский журналист Девид Сангер утверждает, что Stuxnet является частью американской антииранской операции «Олимпийские игры».

Расследование The New York Times в 2011 году подтвердило предположение, что нападение было совершено Израилем и было направлено против иранской ядерной программы. Обнаруженный в 2012 году «Лабораторией Касперского» вирус Flame являлся более усовершенствованной версией Stuxnet и также был нацелен против иранской ядерной программы. В опубликованных результатах журналистского расследования в сентябре 2019 года было отмечено, что заражение системы иранского центра по обогащению урана осуществил завербованный AIVD (Нидерландская служба разведки и безопасности) иранский специалист, по заказу ЦРУ и Моссада.

2011г. - Группа хакеров lulzsec, связанная с группировкой Anonymous взломала веб-сайты, в числе которых ЦРУ (CIA.gov), Sony PlayStation (утечка личных данных более миллиона пользователей), американской компании AT&T. В июле 2011 года, на Шетландских островах был арестован 18-летний молодой человек, который считается одним из главарей группы lulzsec. В целом, Anonymous ранее была более известена своими атаками на сайентологов и Fox News, однако в последнее время деятельность носит более политический характер. Например, в ответ на восстание против Хосни Мубарака, они заблокировали работу всех египетских государственных сайтов, а когда государство вообще отключило Интернет, наводнили государственные структуры факсами. В ответ на арест руководителя сайта по обмену файлами Megaupload Кима Даткома, Anonymous атаковала сайты Министерства юстиции США, ряда звукозаписывающих компаний, а также сайты их ассоциаций, офисы Конгресса.

2012г. - Более 35 тысяч компьютеров крупнейшей нефтедобывающей компании Saudi Aramco Саудовской Аравии были заражены вирусом Shamoon. ИТ-инфраструктуры компании понесли серьезные потери, однако, по официальным данным, вирус не подействовал на отрасль. Ответственность за кибератаку взяла на себя хакерская группа Cutting Sword of Justice, за которой, предположительно, стоит Иран.

В том же году, «Лаборатория Касперского» объявила об обнаружении вируса Gauss, который был направлен против крупнейших ливанских банков: Bank of Beirut, Blom, Bank, Byblos Bank, Credit Libanais, с целью выявить связи Ливана с террористами.

2013г. - Операция Red October, которая развивалась до этого 5 лет и достигла своего пика в 2013г. В качестве мишени были выбраны государственные структуры, посольства и другие представительские учреждения, научно-исследовательские институты, торговые и финансовые структуры, атомные и энергетические программы, космическая сфера, военные учреждения и организации, связанные с созданием оружия. Атаки, в основном, были направлены на бывшие страны СССР: Россия - 35 атак, Казахстан - 21, Азербайджан - 15, Армения - 10, а также Бельгия -15, Индия -14, Афганистан - 10. В январе 2013г. масштабным атакам подверглась также Греция.

2014г. - «Лаборатория Касперского» совместно с компанией Symantec опубликовали информацию о кибершпионской платформе Regin, особенностью которой являлась возможность проникновения в сеть GSM. Самое большое количество компьютеров было заражено в России, Саудовской Аравии, Ирландии и Мексике, а в одной из ближневосточных стран, имя которой не отмечается, Regin смогла создать сеть P2P, которая включала в себя администрацию президента, исследовательский центр, университет и банк. Вирус был обнаружен также на USB-накопителе в офисе канцлера Германии Ангелы Меркель.

2017г. - В мае программа-вымогатель WannaCry заблокировала более 230 тысяч компьютеров в 150 странах. Преступникам удалось получить всего лишь 50 тысяч долларов США, однако ущерб достиг миллиардов (специалисты Trend Micro говорят о 4 миллиардах).

2017г. - массированная атака вируса NotPetya (модифицированная версия, созданного в 2016 году) на инфраструктуры Украины. Атака была запущена через украинскую бухгалтерскую программу M.E.Doc. Были атакованы веб-сайты энергетических компаний, банков, Харьковского аэропорта, Чернобыльской АЭС и правительственные сайты. Позже появились сообщения об атаках на российские банки. Вирус также был зарегистрирован в Италии, Израиле, Сербии, Венгрии, Румынии, Польше, Аргентине, Чехии, Германии, Великобритании, Дании, Нидерландах, Испании, Индии, Франции и Эстонии. Специалисты считают, что в отличие от WannaCry, целью NotPetya была не кража денег, а нанесение вреда, поскольку после шифрования содержимое жесткого диск безвозвратно уничтожалось.

Южнокорейская компания «Наяна» согласилась выплатить преступнику 1.1 миллионов долларов США в биткоинах за расшифровку 150 серверов, обслуживающих 3 тысячи веб-сайтов. Специалисты утверждают, что это было большой ошибкой, потому что хакеры, узнав об «успехах» коллег, могут активизировать атаки для получения легких денег. Сумма, выплаченная

компанией в 1000 раз превышает сумму, выплаченную кибервымогателям в 2016 году.

Программа-вымогатель Bad Rabbit атаковала российские СМИ, требуя заплатить в течение 48 часов 16000 рублей за разблокировку каждого из сотен тысяч поврежденных компьютеров. Анализ программного кода показал, что Bad Rabbit на 13% совпадает с NotPetya.

2018г. - В результате хакерской атаки была нарушена работа справочной британского аэропорта Бристоль. В течение двух дней сотрудникам приходилось вручную записывать расписание полетов на бумаге формата А3 или писать маркерами на досках. Руководство аэропорта отказалось заплатить преступникам, вместо этого они на два дня отключили систему для проведения восстановительных работ.

Как и предполагали специалисты, использование программ-вымогателей получило новый размах. Согласно данным ФБР, в США за 2018 год с помощью программ-вымогателей было совершено 1493 атаки, в результате которых преступникам было выплачено 3.6 миллионов долларов США.

В том же году, во время обострения эпидемии гриппа, хакерской атаке подверглась клиника Hancock Health американского города Гринфилд. Была парализована вся работа медицинского учреждения. Руководство клиники сочло целесообразным выплатить преступникам 4 биткойна, равные сумме 55 тысяч долларов США.

2019г. - Американские города Лейк-Сити, Ривиера-Бич, Джексон были вынуждены заплатить преступникам для разблокировки программ городских инфраструктур, а также приобретения нового технического оборудования.

Программы-вымогатели нарушили работу также компьютерной сети британской полиции, уничтожили резервные копии материалов, сделали недоступными электронную почту и файлы. Расследование, проведенное компанией BAE Systems, не обнаружило фактов утечки информации, однако не исключило такую возможность. Полиция распространила заявление о необходимости информировать правоохранительные органы обо всех фактах незаконного распространения такой информации среди граждан.

Российские компании также не остались без внимания со стороны программ-вымогателей. В 2019 году специалисты сообщили сразу о двух их разновидностях: Troldesh (впервые был обнаружен в 2015г.) и Shade (52% обнаруженных в России вредоносных вставок), которые распространялись с помощью спамов. Есть также данные о зафиксированных атаках в Германии, Японии и в Украине. По мнению специалистов компании Group-IB, вирус также производит криптовалюту и генерирует трафик веб-сайта, увеличивая посещаемость и доходы от онлайн-рекламы. Остановить распространение вируса очень сложно, так как центр управления находится в сети Tor и

постоянно перемещается. Он также активно продается на «черном» Интернет-рынке, что приводит к его различным модификациям, еще больше осложняя его обнаружение и обезвреживание.

Чтобы продемонстрировать опасность использования кибероружия, можно представить его суммарный ущерб в денежном выражении. В докладе правительства США за 2016 года, основанном на данных спецслужб, общий ущерб, нанесенный экономике страны от кибератак, оценивается от 57 до 109 миллиардов долларов. А организованную в 2017 году кибератаку вируса NotPetya Вашингтон квалифицировал как «самую дорогостоящую и разрушительную».

12 марта 2018 года компания «Лаборатория Касперского», занимающаяся антивирусной защитой, заявила об обнаружении вируса нового поколения. Он способен не только украсть любую цифровую информацию, но и одновременно следить за собственной безопасностью. Наличие такого рода вредоносных программ делает реальным возможность в ближайшем будущем генерацию и распространение подобных вирусов нейросетью[1].

ЛИТЕРАТУРА

1. Кинакцян А. JI., Киберпреступление и кибертерроризм: некоторые гнесеологические и юридические вопросы / Юбилейный сборник научных статей «Гладзор»-20, Ереван, 2011 г.

2. Krasavin S. What is a Cyber-terrorizm? / http://n-.sans.org/infowar.

3. https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_(шифровальщики)_Ransomware

4. https://iz.ru/885015/ivan-nosatov/istochnik-zarazv-shest-samvkh-zloveshchikh-vimsov-v-istorii-intemeta.

5. https://profile.ru/scitech/intemetygde-polzovatelei-interneta-segodnva-podst-eregayut- virusy-i-kak-ot-nix-zashhititsya-173995/.

[1] Согласно следующим интернет-источникам: https://www.iguides.ru/main/other/samye razrushitelnve kompyute-mye virusy nachala xxi veka/; https://iz.ru/885015/ivan-nosatov/istochnik -zarazv-shest-samykh-zloveshchikh-virusov-v-istorii-intemeta: https://technomode.ru/article/2018/05/04/samve-gromkie-kompvutemve-virusy-za-god/: https://www.computerra.ru/238843/virusnaya-ataka-vnov-maskiruetsva-pod-pisma/; https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_(шифровальщики)_Ransomware

6. https://ru.wikipedia.org/wiki/Stuxnet.

7. https://weekend.rambler.ru/read/411765_79-top-5-krupneyshih-virusnyh-ata-k-v-istorii/?updated.

8. https://technomode.ru/article/2018/05/04/samve-gromkie-kompvutemve-virusy-za-god/.

9. https://www.computerra.ru/238843/virusnava-ataka-vnov-maskimetsya-pod-pisma/.

10. https://www.gazeta.ru/tech/2019/06/24/12438187/ransomware rus.shtml.

11. https://www.iguides.ru/main/other/samye ra- zrushitelnye kompyutemye virusy nachal