Аннотация – В этом документе представлен анализ хакерской группы Cyber Toufan Al-Aqsa, которая быстро приобрела известность благодаря кибератакам, нацеленным в первую очередь на израильские организации.

В анализе рассматриваются различные аспекты деятельности группы, включая её предысторию и возникновение, методы работы, заметные атаки и нарушения, предполагаемое государственное спонсорство и последствия её деятельности для специалистов по кибербезопасности и других специалистов в различных отраслях. Он также направлен на то, чтобы подчеркнуть его значительное влияние на практику кибербезопасности и более широкий геополитический ландшафт.

Анализ служит ценным ресурсом для профессионалов в области кибербезопасности, ИТ-специалистов и лидеров отрасли, предлагая понимание проблем и возможностей, связанных с меняющимся ландшафтом киберугроз.

I. Введение

Cyber Toufan Al-Aqsa – хакерская группировка, возникшая в конце 2023 года и взявшая на себя ответственность за серию кибератак против израильских компаний и организаций.

Группа участвовала в различных типах кибератак, включая порчу веб-сайтов, несанкционированный доступ к учреждениям, предприятиям и частным резиденциям, взлом камер видеонаблюдения и утечку данных. Одна из атак была направлена против Signature-IT, израильской компании, специализирующейся на размещении международных веб-сайтов для бизнеса, в ходе которой удалось украсть примерно 16 гигабайт файлов данных. Также в фокусе внимания оказались Radware, фирма по кибербезопасности, Израильское управление инноваций и Ikea в Израиле. Деятельность группы не ограничивалась утечкой данных; они также использовали домены корпоративной электронной почты своих жертв для распространения хактивистских сообщений. Некоторые даже предполагают потенциальную связь с Ираном из-за стиля и продемонстрированных в атаках возможностей.

II. Последствия атак

Деятельность группы привела к увеличению числа кибератак в Израиле на 20%, при этом количество атак на государственный сектор увеличилось более чем на 50%.

Операция поставила под угрозу более 150 целей, разбросанных по правительству, производству, электронной коммерции, кибербезопасности и другим секторам. Группировка утверждала, что уничтожила более 1000 серверов и нанесла удары по 150 израильским целям. Атаки не нанесли ущерба израильской экономике, но они нанесли большой ущерб, и некоторые компании до сих пор расплачиваются за это.

Потенциальное воздействие кибератак осложнилось продолжающимся конфликтом между Израилем и различными организациями, включая ХАМАС и связанные с Ираном группировки, т.к. привёл к увеличению числа атак, направленных против израильской инфраструктуры, предприятий и государственных структур.

Эти атаки были нацелены на сектора, включая госсектор, электронную коммерцию, водоснабжение, энергетику, судоходство, и телекоммуникации. В атаках использовались различные методы, такие как распределённые атаки типа "Отказ в обслуживании" (DDoS), атаки с порчей данных, утечки данных и использование учётных данных по умолчанию в критически важных системах.

Однако, несмотря на рост числа кибератак, Израиль, похоже, уверен в своей способности справиться с этими угрозами, противопоставляя имеющиеся в стране надёжную инфраструктуру кибербезопасности и богатую экосистему стартапов.

III. Ключевые особенности атак

Группировка "Toufan Al-AqsaCyber" использовала различные тактики для проведения кибератак

- **Порча веб-сайтов**: изменение внешнего вида веб-сайта, часто для отображения политического сообщения или демонстрации того, что сайт был скомпрометирован
- **Несанкционированный доступ**: несанкционированный доступ к различным учреждениям, предприятиям и частным резиденциям. Это может быть связано с использованием уязвимостей в программном обеспечении, использованием фишинговых методов для кражи учётных данных для входа или других методов обхода мер безопасности
- **Компрометация камер наблюдения**: компрометация камер видеонаблюдения

потенциально позволяет отслеживать действия своих целей

- **Утечка данных**: группа умело извлекает большие объёмы данных из объектов, которые затем размещают публично. Это не только наносит ущерб целевым организациям, но и потенциально влияет на отдельных лиц, чья личная информация может быть включена во взломанные данные
- **Использование платформ социальных сетей**: группа активна на платформах социальных сетей, таких как Twitter и Telegram, где они распространяют информацию о своей деятельности и потенциально координируют атаки
- **Вредоносное ПО wiper**: Группа использовала вредоносное ПО wiper в своих атаках, которое предназначено для удаления данных или нарушения работы систем
- **Психологическая война**: группа выпустила публикации, оправдывающие их кибератаки на Израиль, ссылаясь на возмездие за те вещи, что они считают израильской жестокостью и преступлениями
- **Последующие атаки**: после первоначальных взломов группа проводит последующие атаки, потенциально используя скомпрометированные системы для дальнейшего проникновения в сеть цели или для атаки на другие связанные системы

IV. Цели и последствия

Цели кибер-атак были весьма разнообразными:

- **Правительственные структуры**: Группа поставила под угрозу цели, разбросанные по всему израильскому правительственному сектору
- **Промышленность**: Производственные фирмы оказались в числе пострадавших секторов
- **Электронная коммерция**: под прицелом оказались платформы онлайн-торговли и предприятия, которые могут включать данные клиентов и информацию о деловых транзакциях
- **Фирмы по кибербезопасности**: группа атаковала компании по кибербезопасности, такие как Radware, что указывает на сосредоточенность на организациях, которые являются неотъемлемой частью кибер-защиты Израиля

A. Государственные структуры

Последствия атак на государственные структуры:

- **Утечка данных**: Группа успешно взломала несколько государственных структур, что привело к существенной утечке данных. Это не только ставит под угрозу безопасность и конфиденциальность затронутых организаций, но и потенциально влияет на отдельных лиц, чья личная информация может быть включена во взломанные данные
- **Нарушение работы служб**: Атаки привели к нарушению работы служб, что повлияло на нормальное функционирование целевых правительственных организаций
- **Ущерб репутации**: публичный характер этих атак и последующие утечки данных могут нанести ущерб репутации целевых организаций, подорвав общественное доверие
- **Возможность последующих атак**: Первоначальные нарушения потенциально могут быть использованы для проведения последующих атак, используя скомпрометированные системы для дальнейшего проникновения в сеть цели или для атаки на другие связанные системы
- **Психологическое воздействие**: Атаки служат формой цифровой психологической войны, создавая атмосферу страха и неуверенности
- **Экономический эффект**: Атаки могут иметь экономические последствия, включая затраты, связанные с реагированием на инциденты, восстановлением системы, а также потенциальные штрафы регулирующих органов или судебные иски, связанные с утечками данных
- **Проблемы национальной безопасности**: Учитывая конфиденциальный характер государственных структур, эти атаки потенциально могут представлять угрозу национальной безопасности, в зависимости от характера взломанных данных и затронутых систем

B. Производство

Последствия кибератак на производственный сектор:

- **Сбои в работе**: Кибератаки, особенно программы-вымогатели, могут привести к остановке производственных линий, что приведёт к значительным сбоям в работе. Это может вынудить производителей переводить свои физические системы в автономный режим, иногда на длительные периоды, чтобы смягчить последствия атаки и восстановить нормальную работу
- **Финансовые потери**: Финансовые последствия кибератак для производителей существенны. Сообщалось, что средняя стоимость утечки данных в производственном секторе в 2022 году составила 4,47 миллиона долларов, что больше, чем годом ранее. Эти затраты включают расследование, устранение последствий и реагирование на кибератаки, а также потенциальные убытки от остановки производства и продаж
- **Утечка данных и кража интеллектуальной собственности**: Кибератаки могут привести к краже конфиденциальных данных, включая интеллектуальную собственность, коммерческие секреты и информацию о клиентах. Это не только влечёт за собой немедленные финансовые

последствия, но и может привести к долгосрочным недостаткам в конкурентной борьбе

- **Уязвимости цепочки поставок**: взаимосвязанный характер производственной цепочки поставок означает, что атака на одного производителя может иметь волновой эффект, затрагивающий поставщиков, партнёров и заказчиков. Атаки на цепочки поставок могут поставить под угрозу целостность продуктов и услуг, что приводит к более широким проблемам безопасности
- **Ущерб репутации**: Публичное раскрытие факта атаки может подорвать доверие к производителю, повлиять на отношения с клиентами и потенциально привести к потере бизнеса. Ущерб, нанесённый репутации компании, может быть, одним из самых сложных последствий, после которого приходится восстанавливаться
- **Комплаенс и юридические риски**: Производителям могут грозить штрафы регулирующих органов и судебные иски, если кибератаки приведут к потере защищённых или конфиденциальных данных. Это особенно актуально для производителей в отраслях с высоким уровнем регулирования или для тех, кто обрабатывает личные данные
- **Физический ущерб и риски для безопасности**: В случаях, когда целью являются операционные технологические системы (OT), кибератаки могут привести к физическому повреждению оборудования и создать угрозу безопасности для сотрудников. Манипулирование производственными процессами может привести к выходу из строя оборудования, нанесению ущерба окружающей среде и даже поставить под угрозу жизни людей
- **Психологическая война**: помимо ощутимых последствий, кибератаки могут также служить формой психологической войны, создавая атмосферу страха и неуверенности среди сотрудников, руководства и заинтересованных сторон

C. Электроннаякоммерция

Последствия атак на сектор электронной коммерции:

- **Операционные сбои**: Кибератаки могут серьёзно нарушить работу предприятий электронной коммерции, повлияв на их способность обрабатывать транзакции и обслуживать клиентов. Эти сбои могут привести к простоям, что напрямую влияет на продажи и доставку
- **Финансовые потери**: Финансовые последствия кибератак на предприятия электронной коммерции могут быть существенными. Сюда входят прямые затраты, связанные с расследованием, устранением последствий и реагированием на атаки, а также косвенные затраты, такие как потеря продаж во время простоя. Средняя стоимость утечки данных в 2022 году достигла 4,35 миллиона долларов, что подчёркивает значительную финансовую нагрузку, которую могут налагать эти инциденты
- **Утечка данных и потеря конфиденциальной информации**: Платформы электронной коммерции часто хранят большие объёмы личных и финансовых данных. Атаки могут привести к утечке данных, раскрывая конфиденциальную информацию клиентов, такую как данные кредитной карты, адреса и личную идентификационную информацию. Это не только нарушает конфиденциальность клиентов, но и подвергает бизнес санкциям регулирующих органов и судебным искам
- **Ущерб репутации и доверию клиентов**: Публичное раскрытие кибератаки может нанести значительный ущерб репутации бизнеса электронной коммерции, что приведёт к потере доверия клиентов. Восстановление такого доверия может быть долгим и сложным процессом, и некоторые предприятия, возможно, никогда полностью не восстановятся
- **Риски регулирования и соблюдения требований**: Предприятия электронной коммерции подчиняются различным нормативным актам и стандартам соответствия, связанным с защитой данных и конфиденциальностью. Кибератаки, приводящие к утечке данных, могут привести к несоблюдению требований, что влечёт за собой значительные штрафы и пени
- **Увеличение затрат на кибербезопасность**: после кибератаки предприятиям электронной коммерции часто приходится вкладывать значительные средства в улучшение своей системы кибербезопасности. Это включает в себя внедрение новых технологий, наем дополнительного персонала службы безопасности и внедрение более строгих мер безопасности. Эти возросшие издержки могут повлиять на прибыль бизнеса и могут быть переданы потребителям в виде более высоких цен
- **Уязвимости цепочки поставок**: Предприятия электронной коммерции являются частью более крупной цифровой и физической цепочки поставок. Кибератаки на одну платформу электронной коммерции могут иметь волновой эффект, затрагивающий поставщиков, партнёров и клиентов. Эта взаимосвязанность может усилить последствия атаки, затрагивая более широкую экосистему

D. Фирмы по Кибербезопасности

Последствия атак на ИБ-компании:

- **Операционные сбои**: Фирмы, занимающиеся вопросами кибербезопасности, как и любой другой бизнес, могут сталкиваться с операционными сбоями в результате кибератак. Это может повлиять

на их способность обслуживать клиентов и выполнять повседневные операции, потенциально приводя к временному сокращению услуг безопасности, которые они предоставляют

- **Финансовые потери**: Финансовые последствия для компаний, занимающихся кибербезопасностью, могут быть существенными, включая затраты на расследование, устранение последствий и реагирование на атаки. Кроме того, возможны финансовые потери из-за простоя в работе и потенциальных требований о компенсации от пострадавших клиентов
- **Утечки данных и кража интеллектуальной собственности**: Фирмы, занимающиеся вопросами кибербезопасности, часто владеют конфиденциальными данными, включая запатентованные инструменты и методы обеспечения безопасности, а также информацией о клиентах. Нарушение может привести к потере интеллектуальной собственности и конфиденциальных клиентских данных, подрывая конкурентные позиции фирмы и доверие клиентов
- **Ущерб репутации**: возможно, в большей степени, чем в других отраслях, кибератака на фирму, занимающуюся вопросами кибербезопасности, может нанести значительный ущерб её репутации. Клиенты ожидают, что эти фирмы будут наиболее безопасными, и взлом может привести к потере доверия, что затруднит удержание и привлечение клиентов
- **Регуляторные риски и риски соответствия требованиям**: Фирмы, занимающиеся кибербезопасностью, подчиняются строгим нормативным требованиям. Кибератака, приводящая к утечке данных, может привести к проблемам с соблюдением требований, штрафам и судебным действиям
- **Увеличение затрат на кибербезопасность**: после атаки фирме, занимающейся кибербезопасностью, вероятно, потребуется вложить значительные средства в укрепление своей защиты. Это может включать внедрение новых технологий, наем дополнительного персонала и внедрение более строгих мер безопасности, все из которых могут быть дорогостоящими
- **Уязвимости в цепочке поставок**: Фирмы, занимающиеся кибербезопасностью, являются частью более крупной цифровой экосистемы. Атака на одну фирму может иметь волновые эффекты, потенциально ставя под угрозу безопасность клиентов и партнёров
- **Психологическое воздействие и потеря морального духа**: Кибератаки могут создать атмосферу страха и неуверенности среди сотрудников и руководства. Для фирмы, занимающейся кибербезопасностью, стать жертвой атаки также может привести к падению морального духа, поскольку это напрямую ставит под угрозу основную миссию организации