Аннотация – В этом документе представлен анализ компаний, занимающихся наступательной безопасностью". Анализ охватывает различные аспекты инвентаризации, включая характер компаний, включённых в список, типы возможностей, которые они предлагают, и геополитические последствия их услуг.

Предоставленная выдержка обобщает общедоступную информацию без раскрытия чувствительных или конфиденциальных данных. Она служит ценным ресурсом для специалистов по безопасности, предлагая представление об условиях участия частного сектора в наступательных кибер-операциях.

I. Введение

Ряд компаний участвовали в наступательных кибер-операциях на уровне национальных государств, и предоставили такие возможности, как программные имплантаты, наборы средств взлома (включая эксплойты нулевого дня, структуры эксплуатации, методы обхода безопасности) и продукты для перехвата коммуникаций. Список не касается утечки секретной или конфиденциальной информации, а скорее объединяет то, что уже общедоступно. В список включены действующие, ликвидированные или приобретённые компании из разных стран мира. Перечень представляет собой совокупность общедоступной информации и включает ссылки на разведывательные данные из открытых источников (OSINT), в которых упоминается участие этих организаций в такой деятельности.

II. Разница между частными и публичными компаниями

Разница между частными и публичными компаниями заключается, прежде всего, в их структуре собственности и доступе к капиталу.

Частные компании принадлежат избранной группе лиц, часто принадлежащих членам семьи, основателям или частным инвесторам. Их акции не торгуются на публичных биржах и не выпускаются посредством первичного публичного размещения акций (IPO). В результате частным фирмам не нужно соблюдать строгие требования Комиссии по ценным бумагам и биржам (SEC) к подаче деклараций. Акции этих предприятий менее ликвидны, и их оценку сложнее определить.

С другой стороны, акции публичных компаний котируются и торгуются на фондовых биржах, что делает их доступными для более широкого круга инвесторов. Это приводит к более децентрализованной структуре собственности. Публичные компании зачастую могут с большей лёгкостью продать акции или привлечь деньги посредством размещения облигаций. Они также подчиняются большему количеству правил и должны регулярно раскрывать информацию, публиковать свои финансы и действовать прозрачно.

В данном контексте частных компаний в сфере наступательной безопасности термин «частные» относится к компаниям, находящимся в частной собственности. В инвентаризации не проводится различие между частными и государственными компаниями; скорее, он фокусируется на компаниях, участвующих в наступательных кибер-операциях национальных государств. Термин «публичный» в этом контексте относится не к публичным компаниям, а к тому факту, что информация об этих компаниях является общедоступной.

III. Примеры частных компаний

Примеры частных компаний, которые участвовали в наступательных кибер-операциях на уровне национальных государств, перечисленные в Перечне частных компаний, занимающихся наступательной безопасностью, включают:

- **CyberPoint (США):** действует с 2015 года, есть ссылки в Википедии.
- **CyberRoot Risk Advisory (Индия):** действует с 2013 года, есть ссылки на IntelligenceOnline.
- **Cycura (Канада):** действует с 2013 года, есть ссылки на IntelligenceOnline.
- **DarkMatter Group (ОАЭ):** действует с 2014 года, есть ссылки в Википедии.
- **Cytrox Holdings Zrt (Венгрия):** действует с 2017 года, есть ссылки на CitizenLab.
- **STEALIEN Inc. (Южная Корея):** действует с 2015 года, отзывы на официальном сайте.
- **Synacktiv (Франция):** действует с 2012 года, есть ссылки на EX Files.
- **Syndis (Исландия):** действует с 2013 года, есть ссылки на DarkReading.

Эти компании были вовлечены, предоставляя такие возможности, как программные имплантаты, наборы средств вторжения (например, эксплойты 0day, платформы

эксплуатации, методы обхода безопасности, продукты для перехвата коммуникаций и т. д.).

A. Предлагаемые услуги

Частные компании по кибербезопасности, акции которых не торгуются на бирже, предлагают широкий набор услуг, направленных на защиту организаций от киберугроз. Эти услуги необходимы для защиты цифровых активов, обеспечения конфиденциальности данных и поддержания целостности информационных систем.

CyberPoint (США)

CyberPoint предлагает широкий набор услуг по кибербезопасности, включая:

- **Тестирование на проникновение:** моделируются кибератаки для выявления уязвимостей.
- **Управление уязвимостями:** непрерывный мониторинг/тестирование и политики управления уязвимостями.
- **Реагирование на инциденты:** инфильтрация, «захват и контроль» активной системы, судебная экспертиза и анализ после взлома.
- **Облачное проектирование и инфраструктура:** безопасные и быстрые процессы разработки.
- **Искусственный интеллект (ИИ) и машинное обучение (МО) в кибербезопасности:** использование ИИ и МО для обнаружения вредоносного ПО, обратного проектирования, и предотвращения атак.
- **Технологический консалтинг и стратегии ИТ/ОТ**: индивидуальный консалтинг по технологиям, политике и операциям на глобальном рынке.

CyberRoot (Индия)

CyberRoot Risk Advisory включала:

- **Сети фишинга и шпионского ПО:** создание поддельных учётных записей для фишинга и слежки за пользователями по всему миру. Они использовали поддельные домены крупных провайдеров электронной почты и других сервисов для кражи учётных данных.

Cycura (Канада)

Cycura предлагает такие услуги, как:

- Аудит кибербезопасности
- Криминалистика и реагирование на инциденты
- Анализ вредоносного ПО
- Обучение безопасности

Группа DarkMatter (ОАЭ)

DarkMatter принимал участие в:

- **Наблюдение и кибершпионаж:** заключён контракт на проект «Project Raven», чтобы помочь ОАЭ наблюдать за правительствами и активистами. Для этих операций они привлекли бывших сотрудников американской разведки.

Cytrox Holdings Zrt (Венгрия)

Cytrox включает в себя:

- **Разработка шпионского ПО:** известен разработкой шпионского ПО Predator, используемого в операциях по слежке за журналистами, политиками и другими людьми. Они были внесены в черный список Министерства торговли США за торговлю кибер-эксплойтами.

STEALIEN Inc. (Южная Корея), Synaktiv (Франция), Syndis (Исландия)

STEALIEN Inc., Synaktiv или Syndis. предоставлять широкий набор услуг в области кибербезопасности:

- Пентест
- Оценка безопасности
- Реагирование на инциденты
- Консультации по безопасности

B. Список предлагаемых услуг

Частные компании, занимающиеся кибербезопасностью, акции которых не торгуются на бирже, предлагают различные услуги по защите организаций от киберугроз

- **Оценка рисков:** выявление уязвимостей в сетях, данных и коммуникациях, а также рекомендации по их устранению и улучшению безопасности.
- **Услуги защиты:** реализация таких мер безопасности, как брандмауэры, системы обнаружения вторжений и антивирусное программное обеспечение.
- **Обнаружение угроз и реагирование:** мониторинг киберугроз, их обнаружение и реагирование для предотвращения ущерба, что может включать услуги управляемого обнаружения и реагирования (MDR).
- **Центр управления безопасностью (SOC) как услуга:** обеспечение круглосуточного мониторинга и управления угрозами для предприятий, которые не могут создать внутренний SOC.
- **Аналитика угроз:** предоставление информации о новейших тактиках взлома и возникающих угрозах.
- **Соблюдение требований и управление:** Помощь организациям в соблюдении нормативных требований и отраслевых стандартов.
- **Реагирование на инциденты:** Помощь организациям в реагировании на инциденты

безопасности и восстановлении после них, включая судебно-медицинский анализ и планы исправления.

- **Обучение кибербезопасности:** обучение сотрудников передовым методам кибербезопасности для усиления человеческого элемента безопасности.
- **Управление уязвимостями:** сканирование и анализ систем на наличие уязвимостей и предоставление решений для их устранения.
- **Защита конечных точек:** защита конечных точек, таких как ноутбуки, мобильные телефоны и планшеты.
- **Сетевая безопасность:** защита целостности и удобства использования сети и данных.
- **Облачная безопасность:** защита облачной инфраструктуры и приложений.
- **Безопасность электронной почты:** защита электронной почты от таких угроз, как фишинг, спам и вредоносное ПО.
- **Услуги управляемой безопасности:** аутсорсинг управления устройствами и системами безопасности сторонним экспертам.

IV. Публичные компании Примеры

Примеры публичных компаний, которые занимаются кибербезопасностью:

- **Palo Alto Networks (NYSE: PANW):** многонациональная компания в области кибербезопасности, известная своими передовыми межсетевыми экранами и облачными предложениями.
- **CrowdStrike Holdings, Inc. (NASDAQ: CRWD):** предоставляет облачные решения для защиты конечных точек, анализа угроз и услуг реагирования на кибератаки.
- **Check Point Software Technologies (NASDAQ: CHKP):** израильская компания, специализирующаяся на ИТ-безопасности, включая сетевую безопасность, безопасность конечных точек, облачную безопасность и мобильную безопасность.
- **CyberArk Software Ltd. (NASDAQ: CYBR):** израильско-американская компания по кибербезопасности, специализирующаяся на безопасности привилегированного доступа.
- **Cloudflare Inc. (NYSE: NET):** американская компания, предоставляющая веб-инфраструктуру и безопасность веб-сайтов, включая предотвращение DDoS-атак и сетевые услуги безопасной доставки контента.
- **Rapid7 (NASDAQ: RPD):** компания, предоставляющая решения для данных и аналитики безопасности, включая услуги по управлению уязвимостями.
- **Cisco Systems (NASDAQ: CSCO):** многонациональный технологический конгломерат, который предоставляет решения в области кибербезопасности как часть своего разнообразного портфеля продуктов.
- **Broadcom (NASDAQ: AVGO):** глобальная технологическая компания, предоставляющая широкий набор полупроводниковых и инфраструктурных программных решений, включая программное обеспечение для кибербезопасности.
- **IBM (NYSE: IBM):** многонациональная технологическая компания, предлагающая ряд решений в области кибербезопасности в рамках своих более широких предложений продуктов и услуг.
- **VMware, Inc. (NYSE: VMW):** компания, специализирующаяся на программном обеспечении и услугах облачных вычислений и виртуализации, включая услуги безопасности.

Эти компании предлагают широкий набор решений в области кибербезопасности: от безопасности сети и конечных точек до облачной безопасности и анализа угроз. Они публично торгуются, то есть их акции доступны для покупки на публичных фондовых биржах.

A. Предлагаемые услуги по компаниям

Публичные компании, занимающиеся кибербезопасностью, предлагают широкий набор услуг, предназначенных для защиты цифровых активов, данных и сетей от киберугроз и атак. Эти услуги обслуживают различные аспекты кибербезопасности, включая сетевую безопасность, облачную безопасность, безопасность конечных точек, анализ угроз и многое другое.

Palo Alto Networks (NYSE: PANW)

Palo Alto Networks предлагает комплексный набор услуг по кибербезопасности, в том числе:

- **Службы поддержки клиентов:** рекомендации по обеспечению безопасности бизнеса и техническим результатам, онлайн-поддержка сообщества самообслуживания и экспертная помощь при переходе на новые технологии безопасности.
- **Глобальная поддержка:** Быстрая экспертная поддержка для максимального увеличения времени безотказной работы, снижения рисков и оптимизации операций.
- **Обучение и сертификация:** множество вариантов обучения, сертификации и цифрового обучения для расширения знаний и навыков в области кибербезопасности.
- **Целенаправленные услуги:** расширенная поддержка с участием менеджеров по работе с клиентами и технических экспертов, знакомых со

средой клиента, индивидуальное рассмотрение обращений, анализ первопричин критических проблем, а также упреждающие оповещения и планирование обновлений.

CrowdStrike Holdings, Inc. (NASDAQ: CRWD)

CrowdStrike обеспечивает:

- Платформа CrowdStrike Falcon: унифицированная платформа для современной безопасности, предлагающая защиту от взломов в облаке с помощью унифицированной агентной и безагентной защиты, видимости в реальном времени, обнаружения и защиты от атак на основе личных данных.
- Управляемые услуги кибербезопасности и услуги по требованию: реагирование на инциденты, технические оценки, обучение и консультативные услуги для подготовки и защиты от сложных угроз.
- Полностью управляемые услуги: для обнаружения и реагирования (MDR), поиска угроз и защиты от цифровых рисков.

Check Point Software Technologies (NASDAQ: CHKP)

Check Point предлагает:

- Платформа Check Point Infinity: прогнозирует и предотвращает атаки в сетях, облаках, конечных точках и устройствах с помощью облачной безопасности на базе искусственного интеллекта.
- ThreatCloud AI: выявляет и блокирует возникающие угрозы нулевого дня, обеспечивая точное предотвращение менее чем за две секунды для сотен миллионов точек применения.
- Унифицированное решение безопасности. Защищает везде, где выполняется работа, включая электронную почту, конечные точки и мобильные устройства, с помощью мощных инструментов искусственного интеллекта для команд Центра управления безопасностью.

CyberArk Software Ltd. (NASDAQ: CYBR)

CyberArk фокусируется на безопасности личных данных, предлагая:

- Платформа безопасности личных данных: защищает каждую личность с помощью необходимого уровня контроля привилегий в любой инфраструктуре.
- Беспрепятственный и безопасный доступ: сочетает в себе безопасный единый вход, адаптивный MFA, управление жизненным циклом, службы каталогов и аналитику поведения пользователей.
- Интеллектуальное управление привилегиями: применяет средства контроля мирового класса ко всему ИТ-ресурсу, обеспечивая безопасность пользователей, сторонних поставщиков, конечных точек и идентификации компьютеров.

Дополнительные услуги

Другие компании, такие как Cloudflare Inc. (NYSE: NET), Rapid7 (NASDAQ: RPD), Cisco Systems (NASDAQ: CSCO), Broadcom (NASDAQ: AVGO), IBM (NYSE: IBM) и VMware, Inc. (NYSE: VMW).) также предлагают ряд решений по кибербезопасности. К ним относятся смягчение последствий DDoS, сетевые услуги безопасной доставки контента, решения для данных и аналитики безопасности, решения кибербезопасности как часть разнообразного портфеля продуктов, программные решения для полупроводников и инфраструктуры, а также программное обеспечение и услуги для облачных вычислений и виртуализации соответственно.

- **Cloudflare (NET):** предлагает услуги кибербезопасности через свою платформу облачной безопасности, выступая в качестве посредника между серверами и посетителями клиентских сайтов. Услуги Cloudflare предназначены для различных отраслей, включая образование, электронную коммерцию, финансы, государственный сектор и игры. Его глобальная сеть охватывает более 300 городов в более чем 100 странах.
- **Secureworks (SCWX):** Имея более чем 20-летний опыт сбора информации об угрозах и изучения кибератак, Secureworks предлагает облачную платформу безопасности SaaS. Ее платформа Taegis может обрабатывать более 470 миллиардов событий каждый день, предоставляя комплексный обзор сети компании.
- **Cyren (CYRN):** создает службы интернет-безопасности для облака, помогающие защититься от атак, связанных с электронной почтой, таких как фишинг. Технология Cyren выявляет необычные закономерности для предотвращения кибератак без ущерба для конфиденциальности данных клиентов.
- **Splunk:** специализируется на программном обеспечении кибербезопасности, которое выявляет цифровые уязвимости и предотвращает атаки вредоносных программ. Платформа Splunk использует искусственный интеллект и машинное обучение для автоматического и точного обнаружения угроз, позволяя предприятиям сосредоточиться на реальных киберугрозах.
- **Сети A10 (ATEN):** обеспечивает безопасность присутствия в облаке и беспроводной сети 5G за счет использования машинного обучения и автоматизации для распознавания и предотвращения киберугроз. A10 также предлагает встроенный анализ данных для выявления попыток взлома.
- **Fortinet (FTNT):** предоставляет программное обеспечение безопасности, используемое в различных отраслях, предлагая такие инструменты, как защита брандмауэра, VPN, защита конечных точек и облачная безопасность. Fortinet

придерживается политики нулевого доверия, чтобы обеспечить доступ к приложениям и конфиденциальной информации только одобренному персоналу.

B. Список предлагаемых услуг

Компании, занимающиеся кибербезопасностью, как публичные, так и частные, предлагают широкий набор услуг для защиты организаций от киберугроз. Эти услуги обычно включают в себя:

- **Оценка рисков:** выявление потенциальных уязвимостей сети, данных и коммуникаций, а также рекомендации по их устранению и улучшению безопасности.
- **Услуги защиты:** внедрение таких средств защиты, как межсетевые экраны, системы обнаружения вторжений (IDS) и антивирусное программное обеспечение для защиты от несанкционированного доступа и кибератак.
- **Обнаружение угроз и реагирование на них:** мониторинг киберугроз, их обнаружение и быстрое реагирование, чтобы остановить их и предотвратить ущерб. Сюда могут входить услуги управляемого обнаружения и реагирования (MDR).
- **Центр управления безопасностью (SOC) как услуга: обеспечение** круглосуточного мониторинга и устранения угроз через SOC, что ценно для предприятий, которые не могут создать внутренний SOC из-за ограничений бюджета или кадров.
- **Разведка угроз:** идти в ногу с новейшими тактиками взлома и предоставлять информацию о возникающих угрозах для защиты от них.
- **Соответствие и управление:** обеспечение соответствия организаций нормативным требованиям и отраслевым стандартам, таким как HIPAA для здравоохранения или GDPR для защиты данных.
- **Реагирование на инциденты:** предложение услуг, помогающих организациям реагировать на инциденты безопасности и восстанавливаться после них, включая судебно-медицинский анализ и планы исправления.
- **Обучение кибербезопасности:** обучение сотрудников передовым методам кибербезопасности и потенциальным последствиям их действий по усилению человеческого элемента безопасности.
- **Управление уязвимостями:** сканирование и анализ систем на наличие уязвимостей и предоставление решений для их устранения.
- **Защита конечных точек:** защита конечных точек, таких как ноутбуки, мобильные телефоны и планшеты, от использования киберпреступниками.
- **Сетевая безопасность:** защита целостности и удобства использования сети и данных с помощью различных мер, включая сегментацию сети и контроль доступа.
- **Облачная безопасность:** предложение решений для защиты облачной инфраструктуры и приложений.
- **Безопасность электронной почты:** защита электронной почты от таких угроз, как фишинг, спам и вредоносное ПО.
- **Услуги управляемой безопасности:** аутсорсинг управления устройствами и системами безопасности сторонним экспертам.