США — главная мишень.

Согласно недавнему отчёту компании Cyfirma — это технологическая компания, специализирующаяся на кибербезопасности и разведке в интернете. Она использует искусственный интеллект и аналитику данных для обнаружения угроз и предоставления информации о потенциальных кибератаках для своих клиентов. Компания была основана в Сингапуре в 2017 году и работает с крупными корпорациями и правительственными организациями по всему миру." data-html="true" data-original-title="Cyfirma" >Cyfirma, в мае 2024 года активность программ-вымогателей значительно возросла, с заметными изменениями в деятельности ведущих групп. Наибольшее увеличение активности продемонстрировала группа LockBit, став ведущей угрозой с числом жертв 174.

Производственный сектор пострадал больше всего, с 85 инцидентами. В то время, как США стали наиболее целевой географией, с 249 зарегистрированными атаками. В числе новых киберугроз выделились группы Arcusmedia, SpiderX и FakePenny.

Активность ведущих групп программ-вымогателей в мае 2024 года изменилась по сравнению с апрелем. Так, деятельность LockBit выросла на 625%, а INC Ransom на 100%. Группа Play увеличила число атак на 10,34%, а RansomHub на 4,17%. Группировка Medusa, отсутствовавшая в апреле, вернулась с 23 инцидентами.

LockBit, появившаяся в 2019 году, продолжает развиваться, несмотря на регулярные меры правоохранительных органов. Группа быстро восстановилась после ликвидации её инфраструктуры в феврале, снова став самой активной в мае.

Активность программ-вымогателей в различных отраслях так же увеличилась в мае этого года. В сфере производства атаки выросли на 28,79%, в сфере недвижимости и строительства — на 66,67%, а в банковском деле и финансах — на 105%.

Государственные учреждения и правовые службы увеличили число инцидентов на 48%, здравоохранение — на 71,43%. В сфере электронной коммерции и телекоммуникаций рост составил 230%, в IT — 55,56%, а в сфере транспорта — 21,05%.

Образование показало рост на 250%, а гостиничный бизнес — на 17,65%. Медиа выросли на 116,67%, в то время как энергетика снизилась на 33,33%, а FMCG — на 4,26%.

США (249), Великобритания (34), Канада (23), Испания (19) и Франция (18) стали

основными целями атак в мае 2024 года.

LockBit Black в основном распространяется через ботнет Phorpiex, рассылкой фишинговых писем с заражёнными вложениями. Blackbasta использует социальную инженерию, применяя фишинговые звонки и вредоносные ссылки для получения доступа к системам.

Группа SpiderX предлагает свои услуги на подпольных форумах, демонстрируя продвинутые функции и высокую эффективность. FakePenny, использующая загрузчик и шифровальщик, требует выкупы, достигающие $6,6 миллиона в биткойнах. Arcusmedia, впервые выявленная в мае, совершила уже как минимум 17 инцидентов, нацеленных в основном на Южную Америку.

Ключевые события мая включают атаку на систему здравоохранения Singing River, затронувшую 895 204 человека, и продажу исходного кода INC Ransom на хакерских форумах за $300 000. Также были зафиксированы атаки на администраторов Windows через поддельные сайты загрузки программ.

По данным отчётов, около 31% предприятий вынуждены приостанавливать свою деятельность после атак программ-вымогателей, а 40% — сокращать штат. В 35% случаев происходят кадровые изменения на уровне топ-менеджеров. Средний финансовый ущерб компаний составляет около $200 000, а 75% малых и средних предприятий сталкиваются с угрозой закрытия.

Растущая активность программ-вымогателей подчёркивает необходимость усиления мер кибербезопасности. Инвестиции в передовые технологии защиты, обучение сотрудников, разработка планов реагирования на инциденты, страхование киберрисков и регулярные аудиты безопасности помогут снизить риски и минимизировать ущерб.