**Кибератаки и компании: статистика за 2017 год**

Аналитическая компания Positive Technologies подробно изучила направленность **кибер атак хакеров**, сведя это в обобщенную статистику. Как выяснилось, лакомыми кусочками для злоумышленников являлись крупные компании, вместе с их веб-ресурсами и целой инфраструктурой. Также наблюдалась тенденция роста активности на рынках по предоставлению услуг взлома и развитие троянов-шифровальщиков. Сами злоумышленники осуществляли множество кибер преступлений, направленных на криптовалютные компании и банковские учреждения.

Трояны-шифровальщики удостоились почетного места в области кибер преступлений. Принцип их работы заключается в необратимом шифровании данных, что наносит неоценимый ущерб компаниям.

Также стоит отметить и возросшие темпы производства вредоносного ПО. Очень популярной «фичей» всех современных троянов стала так называемая «ransomware as a service», когда один и тот же вирус может быть задействован несколькими лицами. Более того, порог вхождения в мир кибер преступлений стал крайне низок, а предложения на черных рынках как никогда широки. И эта тенденция будет лишь увеличиваться.

**Кибер атаки хакеров** были направлены не только на компании, но и на частных лиц. За первый квартал было зафиксировано 21 уникальных случаев взлома, а до конца 2017-го этот показатель увеличился до 100. В итоге, общий показатель атак на частных лиц составил 26%. А все благодаря той же возможности «ransomware as a service».

Согласно статистике, 70% **кибер атак хакеров** осуществлялись ради кражи денег, а 26% - компрометированные персональных данных. В частности, злоумышленники «интересовались» информацией о платёжных картах и медицинских карт. Это обусловлено и тем, что на черном рынке за многие персональные данные не предложат внушительную сумму, как это было несколько лет назад.

Ни для кого не секрет, что в 2017 году очень популярной темой стали криптовалюты, чем и воспользовались хакеры. Персональные кошельки, ложные транзакции и атаки на сервера крупных ICO-компаний – всё это сопровождало растущий рынок биткоинов и альткоинов. Очевидно, что персональные данные держателей счетов так же подвергались краже.

В 2017 году хакеры не обделили вниманием популярные ныне смарт-приборы. В их число входят не только смартфоны, наручные часы и система «умный дом», но и бытовые вещи, роутеры и камеры. Все это подвергалось множественным взломам ради использования мощностей оборудования для майнинга или наблюдения за владельцами.

Но самая масштабная часть кибер атак была направлена именно на крупные компании. Подобные массовые взломы наблюдались повсеместно, а итоговая доля от общего их количества составила 57%. Аналитики насторожены положительной тенденцией подобных атак, учитывая их растущую сложность и масштабность. Примечательно, что хакерские атаки далеко не всегда обусловлены желанием получить финансовую выгоду, имея под собой лишь деструктивный и компрометирующий характер. Самое время задуматься об оптимизации и модернизации средств сетевой защиты!

Как показала статистика, основной целью масштабных хакерских атак на компании является «Active Directory» (AD). Важно помнить, что эволюционируют не только средства защиты, но и вредоносное ПО. А значит, новые возможности для атак и неявные уязвимости появляются регулярно. Яркий пример, разработка системы защиты «golden ticket» в конце 2017 года, которая может защитить компанию от брутфорсов и метода «pass-the-hash». Но уже в начале 2018 года появилось вредоносное ПО «DCShadow», девиз которой гласит «SIEM вам не поможет». Вечная борьба добра и зла ведется не только в книгах, но и в кибер пространстве.