Исследователи выделили основные тенденции хакеров за год.

Согласно новому отчету Mandiant, в 2023 году значительно возросла активность программ-вымогателей. Количество публикаций на сайтах утечек данных увеличилось на 75% по сравнению с предыдущим годом, а число расследований Mandiant возросло более чем на 20%.

Особое внимание привлек тот факт, что около 33% новых семейств вымогательского ПО в 2023 году оказались вариантами ранее известных программ. Злоумышленники продолжают использовать легитимные и коммерчески доступные инструменты для реализации своих атак, что отмечает снижение использования Cobalt Strike представляет собой законный фреймворк для проведения тестов на проникновение, позволяющий доставить на компьютер жертвы полезную нагрузку и управлять ею. Злоумышленники же могут использовать Cobalt Strike в реальных атаках на целевые системы, эффективно совмещая фреймворк с другими инструментами." data-html="true" data-original-title="Cobalt Strike" >Cobalt Strike Beacon и рост применения легитимных средств удаленного доступа.

Повторное использование кода, дублирование групп или ребрендинг группировок в 2023 году

В 33% инцидентов вымогательское ПО было развернуто в течение 48 часов с момента первого доступа киберпреступников. Более 76% всех развертываний произошли вне рабочего времени, преимущественно рано утром. Это подчеркивает, насколько важно для организаций быть наготове круглосуточно.

По мнению специалистов Mandiant – это компания, которая занимается информационной безопасностью и аналитикой инцидентов. Она специализируется на обнаружении и решении вопросов, связанных с киберпреступностью, таких как взломы, шпионаж, вредоносное ПО и кибертерроризм. Компания предлагает широкий спектр услуг, включая аналитику инцидентов, консультационные услуги, создание и тестирование систем защиты, а также обучение и поддержку.
 Компания также сотрудничает с правоохранительными органами по всему" data-html="true" data-original-title="Mandiant" >Mandiant, рост активности вымогательского ПО в 2023 году частично связан с восстановлением киберпреступной экосистемы после бурного 2022 года, когда наблюдался спад из-за политических факторов и утечки чатов Conti. В 2023 году киберпреступники вернулись к активным действиям, используя новые тактики, техники и процедуры (TTPs (Tactics, Techniques, and Procedures) – метод определения

поведения и стратегий, которые злоумышленник использует в кибератаке.

 • Тактика – способ получения доступа к сети жертвы;
 • Техника – инструменты, которые использует хакер во время атаки;
 • Процедуры – описание того, как киберпреступник использует техники." data-html="true" data-original-title="TTPs" >TTPs) для увеличения давления на жертв.

Атаки вымогателей в 2023 году затронули организации в более чем 110 странах, причем среди жертв оказались компании из всех отраслей. Особую тревогу вызывает тенденция вымогателей к нападениям на пациентов медицинских учреждений. Вымогатели угрожают обнародовать личные данные пациентов и даже совершают ложные вызовы экстренных служб, чтобы усилить давление на медицинские организации.

В 2023 году количество публикаций на сайтах утечек данных достигло рекордного уровня с более чем 1300 постами в третьем квартале. Число уникальных сайтов с хотя бы одной публикацией увеличилось на 15%, а число новых сайтов утечек данных выросло на 30% по сравнению с 2022 годом. Примерно 30% публикаций в 2023 году были на новых сайтах, связанных с различными семьями вымогательского ПО, такими как ROYALLOCKER.BLACKSUIT, RHYSIDA и REDBIKE.

По мнению специалистов Mandiant, одной из эффективных мер защиты от программ-вымогателей является использование стратегий защиты и сдерживания угроз, которые включают в себя повышение безопасности инфраструктуры, идентификационных данных и конечных точек.