Kaspersky Crimeware Intelligence Reporting

kaspersky BRING ON THE FUTURE

Развитие угроз

Угрозы категории crimeware постоянно меняются. Это вредоносные программы, созданные специально для совершения финансовых киберпреступлений. Программы-вымогатели, которые блокируют доступ к данным или снижают производительность устройства, – самый яркий пример. Фантазия злоумышленников безгранична: они изобретают все более изощренные способы получения доступа к системам, учетным записям и данным для извлечения финансовой выгоды.

Введение

Киберпреступники, нацеленные на получение финансовой выгоды, действуют в разных отраслях и не ограничиваются атаками на банкоматы и платежные терминалы. Программы-вымогатели могут угрожать любой компании, чем бы она ни занималась. За последние пару лет границы между различными типами угроз и профилями киберпреступников размылись. Распространились APT-атаки, направленные не на кибершпионаж, а на кражу денег для финансирования различных преступлений. Не стоит недооценивать растущую сложность crimeware-угроз.

Kaspersky Crimeware Intelligence Reporting предлагает актуальную информацию о вредоносных кампаниях, атаках на финансовые организации и инструментах, нацеленных на банки, платежные компании и их инфраструктуру. Это помогает предприятиям лучше защищать свои активы от злоумышленников.

В состав сервиса входят:

Подробные описания самых известных и распространенных вредоносных программ

Сведения об опасных широкомасштабных вредоносных кампаниях

Наблюдения экспертов и ранние оповещения, в том числе о новом и обновленном вредоносном ПО

Подробное описание возможных атак на финансовые инфраструктуры и соответствующих инструментов, которые разрабатываются киберпреступниками и продаются через теневой интернет в разных странах

Преимущества сервиса

Профили киберпреступников, использующих ПО категории crimeware. Эти данные включают предполагаемую страну происхождения, основной вид деятельности, используемые семейства вредоносных программ, отрасли и регионы, на которые нацелены атаки, а также описания всех используемых тактик и методов, сопоставленных с базой данных MITRE ATT&CK.

Ретроспективный анализ. В течение срока действия подписки сохраняется доступ ко всем ранее выпущенным закрытым отчетам.

Привилегированный доступ. В рамках привилегированного доступа предоставляются технические описания угроз, обнаруженных в ходе текущих расследований, до того как они попадают в публичный доступ.

Технические данные, в том числе расширенный список индикаторов компрометации в стандартных форматах, таких как openIOC и STIX, а также доступ к YARA-правилам.

API на основе REST. Полная интеграция и автоматизация процессов безопасности.

Инструменты для атаки на финансовые организации

Наблюдения экспертов/ ранние предупреждения

Описания вредоносных программ

Вредоносные кампании

Kaspersky Crimeware Intelligence Reporting

Пробный доступ

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru