

Microsoft рассказала о тактике злоумышленников, которые начинают охоту в преддверии праздников.

Microsoft – это американская многопрофильная компания, занимающаяся разработкой программного обеспечения и производством компьютерной техники. Она была основана в 1975 году Биллом Гейтсом и Полом Алленом и на сегодняшний день является одной из самых крупных и известных IT-компаний в мире.

Среди продуктов Microsoft наиболее известными являются операционные системы Windows, пакеты офисных приложений Office, браузер Internet Explorer и поисковая система Bing. Кроме того, компания занимается разработкой программного обеспечения для серверов, баз данных, игровых консолей Xbox и многих других устройств.

Microsoft также предоставляет услуги облачных вычислений и хранения данных через свою платформу Azure, а также занимается разработкой искусственного интеллекта и других инновационных технологий. Компания имеет филиалы по всему миру и сотрудничает с многими крупными корпорациями и организациями." data-html="true" data-original-title="Microsoft" >Microsoft опубликовала новый отчёт Cyber Signals, в котором поделилась свежими данными о деятельности хакерской группы Storm-0539 и резком увеличении краж подарочных карт в преддверии Дня памяти (Memorial Day) в США.

В новом отчёте Cyber Signals Microsoft подтверждает, что злоумышленники нацелены на организации, выпускающие подарочные карты, а не на конечных пользователей. Также в отчёте указывается на масштабное злоупотребление облачными сервисами для удешевления операций.

Microsoft отмечает, что злоумышленники активизируются перед крупными праздниками: во время Рождества в прошлом году активность Storm-0539 увеличилась на 60%, а с марта по май 2024 года наблюдался заметный рост на 30%.

Методы работы Storm-0539

Получив доступ к целевой среде с использованием украденных учётных данных, хакеры регистрируют свои устройства в MFA (многофакторная аутентификация) – это метод защиты аккаунта, который требует предоставления нескольких способов аутентификации для получения доступа к учетной записи. Вместо использования только логина и пароля, пользователь должен предоставить дополнительные подтверждения, такие как код, отправленный на телефон или использование биометрических данных, таких как отпечаток пальца или сканирование лица. Это делает процесс взлома аккаунта сложнее и повышает уровень безопасности.

/> 2FA (двуухфакторная аутентификация) также относится к MFA. Только термин MFA не ставит ограничений на количестве вспомогательных методов аутентификации, а в 2FA таких методов ровно два." data-html="true" data-original-title="MFA" >MFA-сервисах компаний для сохранения доступа. Затем они перемещаются по сети, компрометируя виртуальные машины, VPN, SharePoint, OneDrive, Salesforce и Citrix.

В конечном итоге Storm-0539 получает доступ к учетным данным, позволяющим им создавать новые подарочные карты для последующей продажи в даркнете, в магазинах или обналичивания через с помощью денежных молов.

Обычно компании устанавливают лимит суммы одной подарочной карты. Например, если лимит составляет \$100 000, злоумышленники создают карту на \$99 000, отправляют себе код карты и обналичивают его. Основная мотивация хакеров — похищать подарочные карты и продавать их дешевле. В некоторых случаях злоумышленники похищали до \$100 000 в день у некоторых компаний, как объясняет Microsoft.

Для создания новой инфраструктуры киберпреступники создают сайты, имитирующие благотворительные организации, чтобы зарегистрироваться у поставщиков облачных сервисов. Аккаунты используют тарифные планы «оплата по мере использования» или бесплатные пробные версии, злоупотребляя такими тарифами для масштабных операций с минимальными затратами.

Цепочка атаки Storm-0539

Рекомендации по защите

Microsoft советует операторам порталов выдачи подарочных карт постоянно мониторить аномалии и внедрять политики условного доступа, которые предотвратили бы возможность создания необычно большого количества карт одним учётным записью.

Кроме того, организациям рекомендуется внедрять меры защиты от повторного использования токенов, соблюдать принцип наименьших привилегий и использовать ключи безопасности FIDO2 для защиты учетных записей с высоким риском. Продавцы также могут сыграть важную роль в разрушении цепочки прибыли Storm-0539 и аналогичных злоумышленников, распознавая и отклоняя заказы с подозрительными признаками.

Хотя атаки не затрагивают покупателей, пользователям интернета, готовящимся к праздникам, следует проявлять повышенную осторожность в отношении мошенничества, поддельных магазинов и вредоносной рекламы.

Storm-0539 – это финансово мотивированная хакерская группа из Марокко, активная с 2021 года и специализирующаяся на мошенничестве с подарочными и платежными картами. Киберпреступники известны своей разведывательной деятельностью и специально созданными фишинговыми сообщениями по электронной почте и SMS, нацеленными на сотрудников организаций, выпускающих подарочные карты.