Чем ещё смогла удивить киберэкспертов новая хакерская группировка из КНДР?

Относительно новая северокорейская кибергруппировка, известная под названием Moonstone Sleet, недавно была идентифицирована как ответственная за атаки на сектор программного обеспечения, информационных технологий, образования и оборонной промышленности с использованием вымогательского софта и прочих видов вредоносного ПО.

Согласно новому анализу команды обнаружения угроз 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, Moonstone Sleet создаёт фальшивые компании и вакансии, чтобы обманывать своих жертв. Группа использует троянизированные версии легитимных инструментов, разрабатывает вредоносные игры и активно внедряет вымогательское ПО.

В атаках Moonstone Sleet применяются как традиционные методы, используемые другими северокорейскими хакерами, так и абсолютно уникальные техники.

Первоначально отслеживаемая под кодовым именем Storm-1789, группировка имела некоторые тактические сходства с Lazarus Group, но затем выделилась в отдельную группу с собственной инфраструктурой и методами.

Moonstone Sleet активно использует код уже известного вредоносного ПО, такого как, например, Comebacker, впервые замеченного в январе 2021 года. Также в своих атаках группа часто применяет программу PuTTY, разнообразные фриланс-платформы и социальную сеть LinkedIn.

Для достижения своих целей хакеры Moonstone Sleet используют целый ряд различных

стратегий, основанных на методах социальной инженерии:

Так, в апреле этого года хакерам Moonstone Sleet удалось внедрить новую вариацию вымогательского ПО FakePenny в неназванную оборонную технологическую компанию.

Эксперты Microsoft подчёркивают необходимость принятия мер безопасности для защиты от атак Moonstone Sleet и предупреждают о возможных атаках на цепочки поставок. Тем временем, северокорейские хакеры продолжают адаптировать свои методы для достижения поставленных киберцелей.