Детище хакерской группы Golden Chickens нанесло мощный удар по сегменту поиска кадров.

На прошлой неделе канадская компания eSentire – это компания, специализирующаяся на кибербезопасности и предоставляющая услуги мониторинга и защиты от киберугроз для организаций. Она предлагает инновационные решения для обнаружения и предотвращения кибератак, а также мониторит сетевую активность с целью выявления угроз и реагирования на них в реальном времени. <br /> <br /> Компания специализируется на защите от сложных киберугроз, таких как атаки с использованием вредоносных программ и угрозы со стороны злоумышленников. Её услуги помогают организациям обеспечить безопасность своих данных и сетей в современной цифровой среде." data-html="true" data-original-title="eSentire" >eSentire сообщила о неудачной фишинговой атаке, нацеленной на неназванную компанию из сферы промышленных услуг. Исследователи по кибербезопасности обнаружили, что злоумышленники использовали вредоносное ПО «More_eggs», маскируя его под резюме для поиска работы.

Атака была совершена в мае этого года и направлена на рекрутера, которого злоумышленники обманули, заставив поверить, что он имеет дело с соискателем. Мошенники привлекли его на поддельный сайт, где жертве и предлагалось загрузить вредоносный файл.

Вредонос «More_eggs», разработанный группой Golden Chickens (известной также как Venom Spider), представляет собой модульный бэкдор, способный собирать конфиденциальную информацию с заражённых устройств. Вредоносное ПО предлагается другим преступникам по модели Malware-as-a-Service (Malware-as-a-Service (MaaS) – вредоносное ПО как услуга – аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS).

В прошлом году eSentire уже раскрыла личности двух людей, управляющих этой операцией — Чака из Монреаля и Джека из Румынии. Последняя цепочка атак с применением «More_eggs» включает в себя ответы на вакансии на платформе LinkedIn – это социальная сеть для профессионалов, где они могут общаться, делиться информацией и учиться. Запрещена в РФ за неоднократное нарушение закона о персональных данных." data-html="true" data-original-title="LinkedIn" >LinkedIn, сопровождающиеся ссылкой на сайт для загрузки поддельного резюме.

Именной одностраничный сайт предполагаемого кандидата

После нажатия на кнопку «Скачать» на компьютер жертвы загружается вредоносный ярлык в формате LNK, а уже он инициирует дальнейшее заражение. Примечательно, что переход на URL из ярлыка, но уже через несколько дней после атаки, — приводит к отображению резюме в формате HTML без каких-либо признаков вредоносной активности.

В активной фазе атаки LNK-файл загружает вредоносную DLL-библиотеку, используя легитимную программу Microsoft «ie4uinit.exe», после чего библиотека выполняется через «regsvr32.exe» для установления постоянства в системе, сбора данных о заражённом устройстве и загрузки дополнительных компонентов, включая сам вредонос «More_eggs».

«Кампании «More_eggs» продолжают использовать методы социальной инженерии, выдавая себя за соискателей работы, чтобы обмануть рекрутеров и заставить их скачать вредоносное ПО», — сообщили в eSentire.

Кроме того, такие кампании, использующие MaaS, редки и избирательны по сравнению с типичными сетями распространения вредоносных писем, что также влияет на частоту их обнаружения почтовыми фильтрами.

Чтобы предотвратить такие инциденты, крайне важно повышать осведомлённость персонала, строго следовать политикам безопасности, проверять все входящие файлы на наличие угроз, а также своевременно обновлять системы защиты и ограничивать скачивание потенциально опасных файлов. Обучение сотрудников распознаванию уловок социальной инженерии также является ключевым фактором защиты.

На перекрестке науки и фантазии — наш канал