ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ:

РУКОВОДСТВО В ОТНОШЕНИИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КОРЕЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

16 мая 2022 г.

Власти США публикуют данное **руководство** в качестве всеобъемлющего ресурса для международного сообщества, частного сектора и общественности с целью обеспечения лучшего понимания и защиты от непреднамеренного подбора, найма и оказания содействия работникам сферы информационных технологий (ИТ) Корейской Народно-Демократической Республики (КНДР), также известной как Северная Корея. Руководство содержит подробную информацию о том, как работают специалисты сферы ИТ из КНДР, и определяет индикаторы риска и меры должной осмотрительности, чтобы помочь компаниям избежать найма внештатных разработчиков из КНДР и помочь платформам фриланса и цифровых платежей выявить специалистов сферы ИТ из КНДР, неправомерно использующих их сервисы. Наем или поддержка деятельности специалистов сферы ИТ из КНДР сопряжены с многочисленными рисками, начиная от кражи интеллектуальной собственности, данных и денежных средств и заканчивая ущербом репутации и юридическими последствиями, включая санкции, предусмотренные как властями США, так и Организацией Объединенных Наций (ООН).

В нарушение санкций США и ООН КНДР направила тысячи высококвалифицированных специалистов сферы ИТ по всему миру, которые приносят КНДР доходы, способствующие реализации ее оружейных программ. Эти работники:

- неправомерно используют экосистему платформ фриланса, чтобы тайно получать контракты на разработки в сфере ИТ от компаний-клиентов по всему миру, а также платформы многих социальных сетей, чтобы общаться с клиентами, а также платежные платформы для получения гонораров за свою работу;
- разрабатывают приложения и программное обеспечение в различных отраслях, в том числе, в числе прочего, в сфере бизнеса, криптовалют, здравоохранения и фитнеса, социальных сетей, спорта, развлечений и образа жизни;
- в большинстве случаев выдают себя за работающих удаленно иностранных (не северокорейских) или американских специалистов, в том числе с помощью виртуальных частных сетей (VPN), виртуальных выделенных серверов (VPS), купленных IP-адресов третьих стран, учетных записей-посредников, а также поддельных или украденных удостоверений личности; и
- используют привилегированный доступ, полученный в качестве подрядчиков, в незаконных целях, включая создание условий для вредоносных взломов компьютерных сетей другими агентами КНДР.

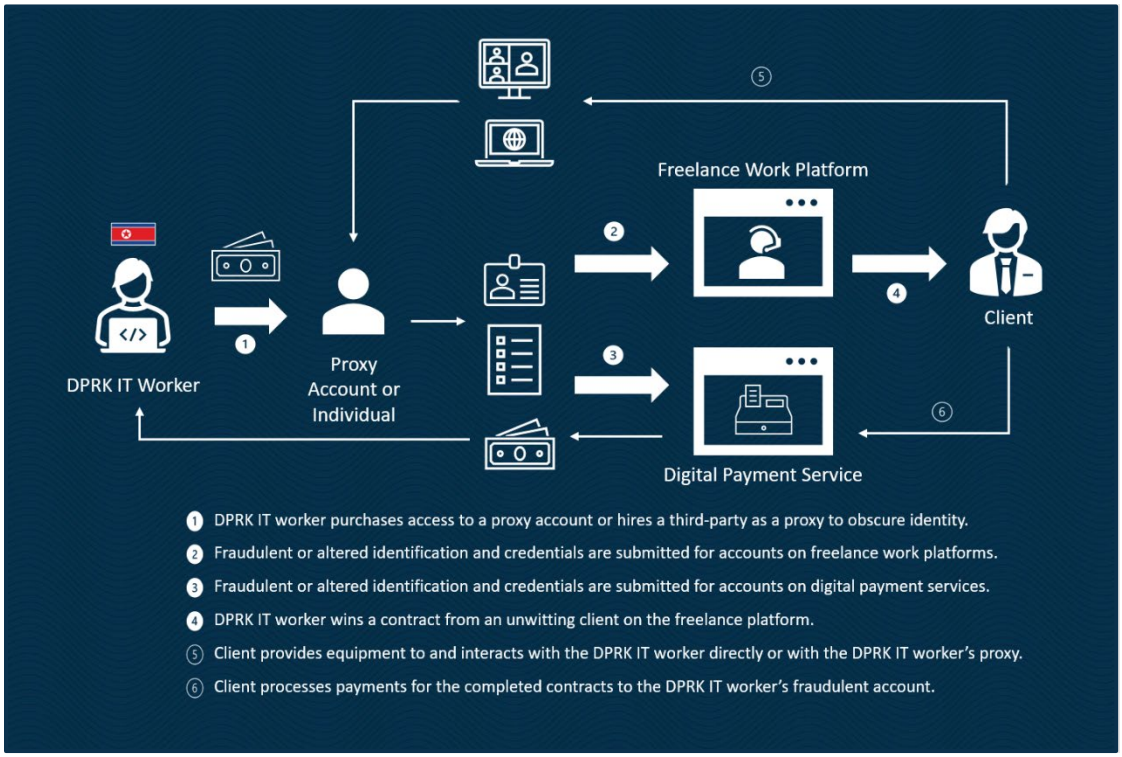
Индикаторы риска, указывающие на потенциальную деятельность специалистов в сфере ИТ из КНДР, включают:

- множественные входы в одну учетную запись с различных IP-адресов за относительно короткий период времени, особенно если IP-адреса связаны с разными странами;
- частые переводы денег через платежные платформы, особенно на банковские счета в Китайской Народной Республике (КНР), или запросы платежей в криптовалюте;
- расхождения в написании имени, сведениях о гражданстве, месте работы, контактной информации, сведениях об образовании, опыте работы и других данных в профилях разработчиков на фриланс-платформах, профилях в социальных сетях, на внешних сайтах-портфолио, в профилях платежных платформ, а также несоответствие оценочному местоположению и часовому поясу; и
- невозможность работать в требуемые рабочие часы и невозможность своевременно связаться с работником, особенно с помощью систем мгновенного обмена сообщениями.

Меры должной осмотрительности, которые компании частного сектора могут предпринять для предотвращения непреднамеренного или невольного найма специалистов в сфере ИТ из КНДР, включают следующие действия:

- проведите проверку документов, представленных в рамках рассмотрения предложений о сотрудничестве или откликов на вакансии, непосредственно в указанных заявителем компаниях и учебных заведениях (не используя контактную информацию, указанную в представленных документах);
- внимательно изучите предоставленные удостоверения личности на предмет подделки;
- проведите видеоинтервью для проверки личности потенциального внештатного работника;
- проведите проверку биографических данных перед приемом на работу и/или используйте вход в систему с помощью отпечатков пальцев/биометрических данных для подтверждения личности и заявленного местонахождения;
- избегайте платежей в криптовалюте и требуйте, чтобы данные в банковских реквизитах соответствовали данным в других идентификационных документах;
- убедитесь в отсутствии расхождений в написании имени, сведениях о гражданстве, месте работы, контактной информации, сведениях об образовании, опыте работы и других данных в профилях разработчика на фриланс-платформах, профилях в социальных сетях, на внешних сайтах-портфолио, в профилях платежных платформ, а также несоответствий оценочному местоположению и часовому поясу; и
- проявите настороженность, если разработчик не может получать отправления по адресу, указанному в его идентификационных документах.

Схема деятельности специалистов в сфере ИТ из КНДР



*Для получения дополнительной информации см. **Сообщение в отношении операций КНДР в компьютерных сетях**, посетите **Центр ресурсов Казначейства США** и/или обратитесь в **местное подразделение ФБР**. Если у вас есть информация о незаконной деятельности КНДР в киберпространстве, включая прошлые или текущие операции, вы можете получить награду в размере до 5 миллионов долларов США, предоставив такую информацию через программу **«Вознаграждение за помощь правосудию»**.*