Бэкдор позволяет удаленно выполнять команды и собирать данные.

Экспертный центр Positive Technologies — это российская компания, специализирующаяся на кибербезопасности. Является одним из ведущих мировых поставщиков услуг и продуктов в этой области." data-html="true" data-original-title="Positive Technologies" >Positive Technologies (PT ESC) выявил ранее неизвестный бэкдор, написанный на языке Go, который используется киберпреступной группировкой ExCobalt для атак на российские организации.

В марте 2024 года специалисты PT ESC в ходе расследования инцидента обнаружили подозрительный файл под названием scrond, сжатый с помощью упаковщика UPX (Ultimate Packer for eXecutables), на одном из Linux-узлов клиента. В данных распакованного семпла, написанного на языке Go, были найдены пути пакетов, содержащие подстроку red.team/go-red/. Это позволило предположить, что семпл является проприетарным инструментом GoRed. Во время анализа выяснилось, что различные версии GoRed ранее уже встречались при реагировании на инциденты у других клиентов.

Дальнейший анализ показал, что данный инструмент связан с группировкой ExCobalt, о деятельности которой PT ESC рассказывала в ноябре прошлого года. ExCobalt известна своими атаками на российские компании в сферах металлургии, телекоммуникаций, горной промышленности, ИТ и государственного сектора. Группировка занимается кибершпионажем и кражей данных.

Новый бэкдор, названный GoRed, обладает множеством функций, включая удаленное выполнение команд, сбор данных из скомпрометированных систем и использование различных методов коммуникации с C2-серверами (Command and Control).

Исследование Positive Technologies показало, что ExCobalt продолжает активно атаковать российские компании, постоянно улучшая свои методы и инструменты. Бэкдор GoRed расширяется для более сложных и скрытных атак и кибершпионажа. Злоумышленники демонстрируют гибкость, используя модифицированные инструменты для обхода защитных мер, что указывает на их глубокое понимание уязвимостей в инфраструктуре компаний.

Развитие ExCobalt подчеркивает необходимость постоянного совершенствования методов защиты и обнаружения атак для противодействия таким киберугрозам. Специалисты отмечают, что участники группировки демонстрируют высокую степень профессионализма и адаптивности, что делает их атаки особенно опасными.

На перекрестке науки и фантазии — наш канал