Хакеры научились внедрять вредоносные программы непосредственно в систему доменных имён (DNS). Затем злоумышленники используют искусственный интеллект для восстановления и развертывания вредоносов.

Согласно информации портала Techspot, специалисты по кибербезопасности находят новые и неожиданные способы внедрения вредоносного кода в IT-инфраструктуру. DNS, которая является основой системы именования устройств в интернете, может быть использована для скрытного распространения вредоносного ПО.

Специалисты платформы для исследования и мониторинга использования доменных имён DomainTools обнаружили, что вредоносный код был внедрён в систему доменных имён в виде записей TXT, которые были закодированы в шестнадцатеричном формате: хакер разбил вредоносный двоичный файл на сотни фрагментов, каждый из которых хранился в отдельном субдомене DNS. Причём вредонос успешно обошёл современные системы защиты.

Злоумышленник использовал искусственный интеллект для создания скрипта, который собирал фрагменты вредоносного кода воедино при развёртывании атаки.

Скрипт PowerShell, зашифрованный и подключённый к платформе Covenant, был обнаружен в записях DNS. И, как оказалось, использование зашифрованных протоколов DNS позволяет киберпреступникам обходить системы обнаружения вредоносного кода.