Как новый вредонос связан с уже проявившими себя ShadowPad и Deed RAT?

«Происхождение BLOODALCHEMY и Deed RAT связано с ShadowPad, и учитывая историю использования ShadowPad в многочисленных APT-кампаниях, крайне важно уделять особое внимание тенденциям использования этого вредоносного ПО», — отметили в японской ИБ-компании ITOCHU Cyber & Intelligence.

Впервые вредонос BLOODALCHEMY был задокументирован исследователями Elastic Security Labs – это лаборатория, созданная компанией Elastic, специализирующейся на разработке программного обеспечения для анализа и обработки данных. Лаборатория Elastic Security занимается исследованием и разработкой инновационных решений в области информационной безопасности.

 Основная цель Elastic Security Labs – обеспечение безопасности данных и защита от киберугроз. Лаборатория активно изучает различные аспекты кибербезопасности, включая обнаружение и предотвращение кибератак, анализ угроз, мониторинг безопасности и реагирование на инциденты." data-html="true" data-original-title="Elastic Security Labs" >Elastic Security Labs в октябре 2023 года, когда они изучали вредоносную компанию, направленную на страны Ассоциации государств Юго-Восточной Азии (АСЕАН). Данный вредоносный инструмент, представляющий собой написанный на языке C бэкдор, внедряется в подписанный безвредный процесс «BrDifxapi.exe» с использованием техники подгрузки вредоносных библиотек DLL Sideloading.

«Хотя это не подтверждено, наличие столь малого количества встроенных команд указывает на то, что данное вредоносное ПО может быть лишь частью более крупного набора инструментов или же пока просто находится на стадии разработки. Либо оно действительно является столь узконаправленным инструментом для конкретных тактических целей», — отметили исследователи из Elastic в своём прошлогоднем отчёте.

Атаки с использованием BLOODALCHEMY включают компрометацию учетной записи на VPN-устройстве для начального доступа и загрузки «BrDifxapi.exe», который используется для подгрузки «BrLogAPI.dll». Этот загрузчик отвечает за выполнение кода BLOODALCHEMY в памяти после извлечения его из файла под названием «DIFX».

Вредоносное ПО использует специальный режим работы, позволяющий избегать анализа в песочницах, сохранять постоянство в системе, устанавливать контакт с сервером злоумышленников и контролировать зараженное устройство через удалённые команды.

Как уже было отмечено ранее, анализ ITOCHU выявил сходства кода BLOODALCHEMY с Deed RAT, многофункциональным вредоносным ПО, ранее используемым хакерской группировкой Space Pirates. Deed RAT рассматривается как следующая итерация ShadowPad, который, помимо того, сам является развитием PlugX.

«Первое заметное сходство — это уникальные структуры данных заголовка полезной нагрузки в BLOODALCHEMY и Deed RAT», — пояснили в ITOCHU. «Также были обнаружены сходства в процессе загрузки кода и файле DLL, используемом для его чтения».

Стоит отметить, что как PlugX (Korplug), так и ShadowPad (PoisonPlug) широко использовались китайскими хакерскими группировками на протяжении многих лет.

Эти данные появились на фоне расширения деятельности китайской хакерской группы Sharp Panda (также известной как Sharp Dragon), которая в рамках продолжающейся кибершпионской кампании начала атаковать государственные организации в Африке и Карибском регионе.