Эксперты выяснили самые популярные схемы доставки злоумышленниками вредоносного ПО в инфраструктуру компании.

Проведённое исследование показало, что в 2023 году вредоносное ПО стало главным методом атак на инфраструктуру компаний, занимая 60% от общего числа случаев. По данным экспертов 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, злоумышленники чаще всего используют электронную почту для доставки вредоносных программ, скрывая их в архивных файлах. Эти программы, попадая на устройства, обычно используют легитимные функции операционных систем для разведки, обхода защиты и закрепления в инфраструктуре.

Анализ вредоносных программ, распространённых в России, позволил выделить десять самых популярных техник согласно MITRE ATT&CK. Наиболее распространенной стала техника «Изучение открытых приложений», когда вредоносное ПО пытается получить список открытых окон приложений, чтобы собрать информацию об инструментах защиты и найти ценные конфиденциальные данные. В контексте второй техники — «Ослабление защиты» — ВПО модифицирует компоненты инфраструктуры жертвы, что позволяет нарушить работу средств безопасности и их механизмов. Эксперты пришли к выводу, что программы злоумышленников часто используют легитимные функции операционной системы, чтобы провести разведку на скомпрометированном устройстве, выполнить зловредные действия и ослабить защиту. Третья по популярности техника — «Обход виртуализации или песочницы», когда с помощью различных проверок ВПО умеет определять, в какой среде оно выполняется, и при обнаружении способно изменить свое поведение, чтобы скрыть свою вредоносность.

Наиболее распространённый тип вредоносного ПО — программы-шифровальщики, доля которых в 2023 году составила 57%. Чаще всего жертвами таких атак становились медицинские учреждения (18%), научные и образовательные организации (14%) и промышленные предприятия (12%). Шпионское ПО также стало популярнее: его доля в 2023 году выросла с 12% до 23%. Среди шпионских программ лидируют FormBook и Agent Tesla.

Электронная почта остаётся основным каналом доставки вредоносного ПО: 57% атак начинались с фишинговых писем. Чтобы повысить успех своих кампаний, злоумышленники маскируют послания под легитимные, опираясь на эмоции людей, например отмечают сообщения как срочные или рассылают уведомления о

недошедших письмах, которые могут вызвать любопытство. Так, эксперты Positive Technologies обнаружили у одного клиента рассылку писем под видом претензии с требованием возврата средств.

Для доставки полезной нагрузки злоумышленники обычно используют файловые вложения, прикрепленные к сообщениям: на долю таких кампаний приходится 56% инцидентов. Чаще всего киберпреступники распространяют вредоносные программы через архивы с расширением .zip, .rar, .7z и другими (37%). Этот способ позволяет замаскировать вредоносные программы под легитимные документы или изображения, скрывая их от средств защиты. Также часто используются ссылки в теле писем (43%), что позволяет загружать вредоносное ПО в фоновом режиме. Чтобы остаться незамеченными, киберпреступники могут, например, выполнить несколько последовательных переадресаций с одного ресурса на другой и приложить к письму QR-код, который позволит скрыть зловредные URL-адреса.

Для защиты инфраструктуры компании от вредоносного ПО необходимо соблюдать базовые требования кибербезопасности: не переходить по подозрительным ссылкам, использовать сложные пароли и двухфакторную аутентификацию. Важно внедрить продукты информационной безопасности для комплексной защиты, включая проверку их результативности.