Автоматизированные скрипты помогают хакерам обойти защитные системы.

Исследователи в области кибербезопасности из компании Morphisec – это компания, специализирующаяся на кибербезопасности. Она предоставляет решения для защиты от вредоносных программ и атак хакеров.
 Основной продукт Morphisec – это платформа Morphisec Endpoint Threat Prevention, которая использует уникальный метод защиты от атак, называемый "нулевым доверием". Этот метод предполагает, что любое подозрительное поведение программы или процесса должно быть автоматически остановлено, даже если этих программ нет в списках известных угроз.
 Компания работает с клиентами в различных отраслях, включая финансы, здравоохранение, производство и государственные учреждения.
 Morphisec имеет партнерские отношения с другими компаниями в области кибербезопасности, такими как Microsoft и McAfee. За свои инновационные продукты и решения компания неоднократно получала различные награды." data-html="true" data-original-title="Morphisec" >Morphisec раскрыли детали вредоносной активности группы Sticky Werewolf («Липкий оборотень»), связанной с кибератаками на предприятия в России и Беларуси.

Выявленные ранее атаки были нацелены на неназванную фармацевтическую компанию и российский исследовательский институт микробиологии и разработки вакцин. Теперь же основной удар на себя принял российский авиационный сектор.

«В предыдущих кампаниях Sticky Werewolf цепочка заражения начиналась с фишинговых писем, содержащих ссылку для скачивания вредоносного файла с таких платформ, как gofile.io», — рассказал исследователь безопасности Арнольд Осипов. «В последней кампании использовались архивные файлы с LNK-файлами, ведущими на полезную нагрузку, хранящуюся на WebDAV-серверах».

Sticky Werewolf — одна из многих групп, нацеленных на Россию и Беларусь, наряду с Cloud Werewolf, Quartz Wolf, Red Wolf и Scaly Wolf. Впервые группу задокументировали исследователи компании BI.ZONE – это российская компания, специализирующаяся в области кибербезопасности. Основанная в 2016 году, она предоставляет широкий спектр услуг и решений для защиты информации и инфраструктуры от киберугроз.

 Компания предлагает услуги в области прогнозирования и предотвращения кибератак, анализа уязвимостей, мониторинга событий и инцидентов, а также консультирования по вопросам кибербезопасности.

 BI.ZONE активно сотрудничает с организациями из различных отраслей, помогая им создавать надёжные стратегии и решения для минимизации рисков, связанных с киберугрозами." data-html="true" data-original-title="BI.ZONE" >BI.ZONE в октябре 2023 года.

Считается, что Sticky Werewolf активна как минимум с апреля 2023 года.

Новая цепочка атак, наблюдаемая Morphisec, включает использование вложений RAR-архивов, которые при извлечении содержат два LNK-файла и отвлекающий PDF-документ.

Само письмо написано от имени АО «ОКБ Кристалл» — реальной существующей российской компании, специализирующейся на разработке и производстве микроэлектронных компонентов и систем, задействованных в самых разных отраслях российской промышленности.

Получателям письма предлагалось загрузить архив и запустить LNK-файлы в нём для получения повестки дня «предстоящей видеоконференции». Открытие любого из LNK-файлов запускает исполняемый файл, размещённый на WebDAV-сервере, что приводит к выполнению обфусцированного скрипта Windows.

Этот скрипт затем запускает AutoIt (произносится "АвтоИт") – это бесплатная программа для автоматизации действий на компьютере в Windows. С ее помощью можно написать скрипты, которые могут взаимодействовать с окнами, выполнять действия с мышью и клавиатурой, запускать программы, работать с файлами и папками, а также выполнять другие задачи.

 В то же время, из-за своей способности маскировать процессы, AutoIT может быть использован злоумышленниками для создания и распространения вредоносного ПО.
" data-html="true" data-original-title="AutoIt" >AutoIt-скрипт, который в конечном итоге внедряет финальную полезную нагрузку, обходя при этом программное обеспечение безопасности и избегая попыток анализа.

«Данный исполняемый файл — это самораспаковывающийся архив NSIS, который является частью ранее известного криптора CypherIT», — отметил Осипов. «Хотя оригинальный CypherIT больше не продаётся, текущий исполняемый файл — это его вариация, распространяемая сразу на нескольких хакерских форумах».

Цель данной кампании — доставить на устройства в целевых компаниях трояны удалённого доступа (RAT) и похитители информации, например, Rhadamanthys и Ozone RAT, тем самым скомпрометировав предприятия критически важных отраслей.

Изощренные попытки «Липкого оборотня» атаковать российскую авиапромышленность — чёткий сигнал о необходимости усилить кибербезопасность критической

инфраструктуры. Хакерские группировки постоянно совершенствуют свои методы, поэтому своевременное внедрение ответных защитных мер является задачей первостепенной важности.