Уязвимости в программном обеспечении Microsoft стали лазейкой для новой версии трояна.

Вредоносная программа DarkGate, распространяемая по модели Malware-as-a-Service (MaaS) – вредоносное ПО как услуга – аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS (Malware-as-a-Service), изменила метод доставки финальных этапов, перейдя от скриптов AutoIt к механизму AutoHotkey. Эта смена подчёркивает стремление киберпреступников постоянно опережать системы обнаружения угроз.

Наблюдения показали, что обновления появились в DarkGate версии 6, выпущенной в марте 2024 года разработчиком по имени RastaFarEye. Программа активно продаётся по подписке и используется примерно 30 клиентами.

Вредонос DarkGate известен с 2018 года и является полнофункциональным трояном удалённого доступа (Существует две расшифровки аббревиатуры RAT:

 • Remote Administration Tool — инструмент удалённого администрирования;
 • Remote Access Trojan — троян удалённого доступа.

 В обоих случаях подразумевается инструмент, который позволяет производить удалённое подключение к целевой системе и последующее выполнение определённых действий. В зависимости от того, кто использует RAT, законный системный администратор или киберпреступник, меняется как расшифровка аббревиатуры, так и спектр выполняемых действий.

 Забавно, что само слово «RAT» можно дословно перевести с английского как «крыса»." data-html="true" data-original-title="RAT" >RAT), оснащённым Инфраструктура управления и контроля, также известная как C2, или C&C (сокр. от англ. «command-and-control»), представляет собой набор инструментов и методов, которые злоумышленники используют для обмена данными со скомпрометированными устройствами после первоначального вторжения (постэксплуатации). Конкретные механизмы атак сильно отличаются друг от друга, но обычно C2 включает один или несколько скрытых каналов связи между устройствами в атакуемой организации и контролируемой злоумышленником платформой. Эти каналы связи используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику." data-html="true" data-original-title="C2" >C2 и Руткит (rootkit) – это вид вредоносного программного обеспечения, предназначенного для скрытия присутствия злоумышленника в скомпрометированной системе. Руткиты внедряются в

ядро операционной системы или другие низкоуровневые компоненты и маскируют процессы, файлы, сетевые соединения, ключи реестра, связанные с вредоносной активностью. Они позволяют сохранять постоянный привилегированный доступ к системе, скрывать следы присутствия и действия злоумышленника, что затрудняет их обнаружение антивирусами и средствами защиты. Руткиты считаются одной из самых опасных угроз, поскольку способны глубоко внедриться в систему и оставаться незамеченными." data-html="true" data-original-title="Руткит" >руткит возможностями. Программа включает модули для кражи учётных данных, кейлоггинга, захвата экрана и удалённого рабочего стола.

«Кампании DarkGate быстро адаптируются, модифицируя различные компоненты, чтобы избегать обнаружения системами безопасности», — отметил исследователь безопасности Trellix – это компания, специализирующаяся в области кибербезопасности. Trellix предлагает широкий спектр решений и услуг, направленных на защиту информации и данных клиентов от киберугроз.

 Основными продуктами Trellix являются системы мониторинга и обнаружения вторжений, управление уязвимостями, защита от вредоносного программного обеспечения, а также услуги по анализу и предотвращению кибератак.

 Компания работает как с корпоративными клиентами, так и с государственными учреждениями, помогая им повысить уровень безопасности своих информационных систем." data-html="true" data-original-title="Trellix" >Trellix в своём анализе. «Это первый случай, когда мы обнаружили использование AutoHotkey для запуска DarkGate».

Переход на AutoHotkey впервые задокументирован McAfee Labs в конце апреля 2024 года. Атаки используют уязвимости, такие как CVE-2023-36025 и CVE-2024-21412, чтобы обойти защиту Microsoft Defender SmartScreen, применяя Microsoft Excel или HTML-вложения в фишинговых письмах.

Альтернативные методы используют Excel-файлы со встроенными макросами для выполнения Visual Basic Script, который вызывает PowerShell-команды, в конечном итоге запускающие скрипт AutoHotkey. Этот скрипт загружает и декодирует полезную нагрузку DarkGate из текстового файла.

Новая версия DarkGate включает значительные улучшения конфигурации, техник уклонения и доступных команд. Теперь она поддерживает функции записи звука, управления мышью и клавиатурой.

«Версия 6 не только добавила новые команды, но и убрала некоторые из предыдущих версий, такие как повышение привилегий, криптомайнинг и скрытое виртуальное

сетевое управление (hVNC)», — добавили в Trellix, предположив, что это может быть сделано для сокращения функций, способных вызвать обнаружение.

Также стоит отметить, что DarkGate продаётся ограниченному числу клиентов, что и могло повлиять на решение RastaFarEye об удалении некоторых функций.

Таким образом, недавнее изменение функционала DarkGate демонстрирует стремление авторов вредоноса к инновациям и повышению эффективности своих атак, подчёркивая необходимость постоянного мониторинга и быстрого реагирования со стороны отрасли кибербезопасности для защиты от новых изощренных угроз.