Хакеры скомпрометировали цепочку поставок всемирно известной программы.

Программу для видеозаписи судебных процессов Justice AV Solutions (JAVS (Justice AV Solutions) — это американская компания, специализирующаяся на разработке и предоставлении аудио-визуальных решений для судебных и правительственных учреждений.

 JAVS предлагает широкий спектр продуктов и услуг, направленных на запись и управление аудио и видео материалами в залах суда и других официальных учреждениях." data-html="true" data-original-title="JAVS" >JAVS) взломали, внедрив в установочный файл вредоносное ПО, которое способно захватить управление зараженными системами. JAVS широко используется в судах, юридических компаниях, исправительных учреждениях и государственных органах по всему миру. У программы на данный момент более 10 000 установок.

После обнаружения угрозы компания удалила скомпрометированную версию с официального сайта. Чтобы предотвратить повторение подобных инцидентов, компания провела полный аудит всех систем и сбросила пароли, чтобы украденные данные не могли быть использованы в будущем. В ходе постоянного мониторинга и сотрудничества с органами по кибербезопасности были выявлены попытки хакеров заменить программу JAVS Viewer 8.3.7 на зараженный файл.

JAVS подтвердила, что все доступные файлы на сайте JAVS.com являются подлинными и не содержат вредоносных программ. Компания также проверила, что исходный код JAVS, сертификаты, системы и другие программные продукты не были скомпрометированы в результате инцидента.

ИБ-компания Rapid7 – это американская компания в области кибербезопасности, основанная в 2000 году. Она предоставляет широкий спектр решений для обнаружения, анализа и реагирования на угрозы информационной безопасности.

 Основными продуктами Rapid7 являются платформа Insight, которая включает в себя средства для сканирования уязвимостей, анализа безопасности сетей, обнаружения и устранения инцидентов в реальном времени, а также продукты для управления безопасностью облачных сервисов и приложений.

 Компания также предоставляет услуги консалтинга и обучения для повышения компетенций специалистов в области кибербезопасности." data-html="true" data-original-title="Rapid7" >Rapid7 провела расследование инцидента. Уязвимость получила идентификатор CVE-2024-4978 (оценка CVSS 4.0: 8.7). Установлено, что группа анализа угроз S2W Talon первой обнаружила зараженный установочный файл в начале апреля и связала его с вредоносным ПО Rustdoor/GateDoor.

Во время анализа одного из инцидентов, связанных с CVE-2024-4978, Rapid7 выяснила, что вредоносная программа после установки отправляет информацию о системе на 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-сервер. Далее выполняются два скрытых скрипта PowerShell, которые пытаются отключить трассировку событий Windows (Event Tracing for Windows, Event Tracing for Windows (ETW) — это встроенная в операционную систему Windows технология отслеживания событий, которая обеспечивает детализированную запись событий и действий, происходящих в системе.

 ETW предоставляет интерфейс для сбора, записи и анализа событий от различных источников, таких как ядро операционной системы, приложения и службы." data-html="true" data-original-title="ETW" >ETW) и обойти интерфейс сканирования вредоносных программ (Anti-Malware Scan Interface, Antimalware Scan Interface (AMSI) — это интерфейс программирования приложений, представленный в Windows 10, который предоставляет дополнительные способы обнаружения и блокировки вредоносного ПО.

 AMSI обеспечивает общий интерфейс, который позволяет антивирусному ПО анализировать более сложные аспекты скриптов и другого динамически исполняемого кода. Это означает, что он может быть использован для проверки макросов в документах Office, PowerShell-скриптов, JavaScript и других видов скриптового и интерпретируемого кода на наличие вредоносного содержимого.

 Поскольку AMSI встроен в процесс выполнения скрипта, он может просканировать содержимое скрипта на любом этапе его выполнения, что делает его очень эффективным против вредоносных скриптов, которые изменяют свое поведение во время выполнения, чтобы избежать обнаружения.

 AMSI предназначен для использования совместно с антивирусным ПО. Фактически, AMSI дополняет антивирусные решения, предоставляя дополнительные способы обнаружения вредоносного ПО." data-html="true" data-original-title="AMSI" >AMSI).

Следующим этапом вредонос загружает дополнительные вредоносные файлы с C2-сервера, которые собирают учетные данные из браузеров. Rapid7 подтвердила, что зараженный установочный файл (JAVS.Viewer8.Setup_8.3.7.250-1.exe) был скачан с

официального сайта JAVS.

Rapid7 призвала всех клиентов JAVS переустановить системы на всех потенциально скомпрометированных устройствах, чтобы полностью прервать доступ злоумышленников. Кроме того, следует сбросить все учетные данные на устройствах и обновить ПО до версии 8.3.9 или выше.

Rapid7 пояснила, что простое удаление программы недостаточно, так как злоумышленники могли внедрить дополнительные бэкдоры или вредоносные программы. Переустановка систем позволяет начать «с чистого листа».