Отключение макросов в Office привело к очередной лазейке для незаметного взлома.

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 выявила новый метод взлома Windows под названием GrimResource, который включает использование специально созданных файлов Файл MSC, используемый в консоли управления Microsoft (MMC), представляет собой сохранённую коллекцию настроек, которая позволяет администраторам настраивать и управлять службами и приложениями в Windows.

 Файлы MSC могут включать настройки службы безопасности, политики пользователей, мониторинг системы и другие административные инструменты.

 Файлы MSC предоставляют графический интерфейс для выполнения административных задач, что делает их важным инструментом для управления ИТ-инфраструктурой." data-html="true" data-original-title="MSC" >MSC (Microsoft Saved Console) в сочетании с неисправленной XSS (Cross Site Scripting, межсайтовый скриптинг) – один из типов уязвимостей компьютерной системы, используя которую хакер может внедрить в генерируемую скриптами на сервере HTML-страницу произвольный код. Специфика хакерских атак, с использованием XSS, заключается в том, что вместо атаки, нацеленной на сервер, мошенники используют сервер в качестве средства атаки на клиента.

 Обычно XSS-атаки направлены на хищение личных данных, таких как cookies, паролей и пр. Такая атака также может внедрять код скриптов и ссылок на web-страницы.

 Ранее программисты не уделяли должного внимания XSS-атакам, так они считались неопасными. Однако на web-странице или в HTTP-Cookie могут содержаться потенциально важные данные (к примеру, идентификатор сессии администратора). На популярный сайт при помощи XSS уязвимости можно осуществить DDoS-атаку." data-html="true" data-original-title="XSS" >XSS-уязвимостью в Windows для выполнения кода через Microsoft Management Console (MMC). Elastic поделилась видео-демонстрацией атаки GrimResource.

MSC-файлы используются в консоли MMC для управления различными аспектами операционной системы или создания пользовательских представлений часто

используемых инструментов.

6 июня 2024 года на платформе VirusTotal был обнаружен файл «sccm-updater.msc», использующий технику GrimResource, что указывает на активное использование такой методики. К сожалению, ни один антивирус не пометил файл как вредоносный.

Результаты сканирования VirusTotal

Киберпреступники используют указанную технику для первоначального доступа к сетям и выполнения различных команд. Специалисты подтвердили, что XSS-уязвимость в Windows 11 все еще не исправлена, несмотря на обнаружение ее в 2018 году.

Атака начинается с вредоносного MSC-файла, который пытается использовать XSS-уязвимость в библиотеке «apds.dll», позволяя выполнить JavaScript через URL. Тактика GrimResource позволяет объединить XSS-уязвимость с методом DotNetToJScript, чтобы выполнить произвольный .NET-код через движок JavaScript, обойдя меры безопасности.

Рассматриваемый образец использует обфускацию для уклонения от предупреждений ActiveX, а JavaScript-код активирует VBScript для загрузки .NET-компонента «PASTALOADER», который извлекает полезную нагрузку Cobalt Strike.

Системные администраторы должны обращать внимание на признаки компрометации, такие как операции с файлами «apds.dll», подозрительные выполнения через MCC и необычное создание COM-объектов .NET. Elastic Security опубликовала список индикаторов GrimResource и предложила правила YARA для помощи защитникам в обнаружении подозрительных файлов MSC.

Атака GrimResource появилась после того, как Microsoft по умолчанию отключила макросы в Office в июле 2022 года, из-за чего злоумышленники стали экспериментировать с новыми типами файлов в атаках. С тех пор возросло использование файлов ISO, RAR и LNK во вредоносных кампаниях, и сейчас к этому списку добавились MSC-файлы.