Вредоносная операция CLOUD#REVERSER эксплуатирует легитимные облачные сервисы для обхода обнаружения.

Исследователи компании Securonix – это американская компания, специализирующаяся на решениях по кибербезопасности, которые помогают защищать организации от кибератак и внутренних угроз. Securonix также предоставляет аналитические инструменты и платформу для обработки данных, которые позволяют организациям обнаруживать и предотвращать кибератаки, минимизировать утечки данных и снижать риски безопасности." data-html="true" data-original-title="Securonix" >Securonix обнаружили новую кампанию кибератак под названием CLOUD#REVERSER. В ходе этой операции злоумышленники используют легитимные облачные сервисы, такие как Google Drive и Dropbox, для размещения там вредоносных файлов.

«Скрипты на VBScript (VB – Visual Basic, Script – сценарий) – это скриптовый язык программирования, основанный на Visual Basic и разработанный компанией Microsoft Он был создан для автоматизации задач в операционных системах Windows и веб-браузерах.

 VBScript обычно используется для написания скриптов, которые выполняются на клиентской стороне веб-страницы или в контексте операционной системы Windows. Он может быть использован для создания простых программ, обработки текстовых файлов, работы с базами данных и многого другого.

 В последние годы VBScript утратил свою популярность и поддержка его функциональности в веб-браузерах сократилась. Это произошло из-за развития других технологий, таких как JavaScript, которые стали более распространенными и мощными для разработки веб-приложений." data-html="true" data-original-title="VBScript" >VBScript и Windows PowerShell – оболочка командной строки на основе задач и языков сценариев. Она специально разработана для администрирования систем. Встроенная в .NET Framework, оболочка Windows PowerShell помогает ИТ-специалистам и опытным пользователям контролировать и автоматизировать процесс администрирования операционной системы Windows и приложений, работающих в системе Windows." data-html="true" data-original-title="PowerShell" >PowerShell в рамках CLOUD#REVERSER выполняют 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

Все права защищены

связи используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику." data-html="true" data-original-title="C2" >C2-действия, используя Google Drive и Dropbox как платформы для управления загрузками и скачиванием файлов», — сообщили исследователи Ден Иузвик, Тим Пек и Олег Колесников в своём отчёте.

Атака начинается с фишингового письма, которое содержит ZIP-архив с исполняемым файлом, маскирующимся под Microsoft Excel. Мало того, что этот файл использует иконку с логотипом Excel, в имени файла также применён скрытый символ Unicode (U+202E), который переворачивает порядок следующих символов в строке, обманывая пользователя и заставляя его думать, что он открывает файл Excel.

Так, рассмотренный в рамках кампании исполняемый файл «RFQ-101432620247fl[U+202E]xslx.exe» отображался в системе жертвы под видом «RFQ-101432620247flexe.xlsx».

В ходе атаки исполняемый файл запускает восемь вредоносных нагрузок, включая поддельный Excel-файл и сильно обфусцированный скрипт на Visual Basic, который открывает файл Excel и запускает два других скрипта.

Оба скрипта создают постоянное присутствие на компьютере жертвы, используя задачу в планировщике Windows, маскируясь под обновление браузера Google Chrome. Эти задачи запускают уникальные VB-скрипты каждые 60 секунд.

Каждый из этих скриптов запускает по два PowerShell-скрипта, которые подключаются к управляемым злоумышленниками аккаунтам Dropbox и Google Drive для загрузки дополнительных скриптов.

Эти скрипты затем запускают загруженные PowerShell-скрипты и скачивают дополнительные файлы из облачных сервисов, включая исполняемые файлы в зависимости от настроек системы.

Последний PowerShell-скрипт загружает файлы с Google Drive на локальную систему в директорию ProgramData, выполняя их в зависимости от критериев, установленных злоумышленниками.

Также через «68904.tmp» загружается PowerShell-скрипт, способный выполнять сжатый бинарный файл напрямую из памяти, поддерживая подключение к серверу

Все права защищены

командного управления.

«Этот подход позволяет злоумышленникам оставаться незамеченными, встраивая вредоносные скрипты в обычные облачные платформы, обеспечивая постоянный доступ к целевым системам и используя эти платформы для эксфильтрации данных и выполнения команд», — заключили исследователи.

Исследователи Securonix сообщили, что пока не могут предоставить информацию о целях и масштабе кампании, так как расследование всё ещё продолжается.

Этот инцидент подчёркивает тенденцию злоумышленников использовать легитимные сервисы для скрытого проведения атак и демонстрирует их способности адаптироваться, применяя такие методы и техники, о которых даже опытные специалисты могут не догадываться.

Всё это требует от пользователей и компаний повышенного внимания к безопасности и необходимости регулярно обновлять свои системы и освежать технические знания для защиты от подобных киберугроз.

Все права защищены