Тактики группы открывают новый взгляд на её происхождение.

Недокументированный злоумышленник LilacSquid с 2021 года проводит целенаправленные атаки на различные секторы в США, Европе и Азии. Атаки направлены на кражу данных и установление долгосрочного доступа к скомпрометированным организациям.

В В компании Cisco, которая занимается разработкой и продажей сетевого оборудования, есть подразделение Talos. Оно занимается исследованиями в области угроз информационной безопасности." data-html="true" data-original-title="Cisco Talos" >Cisco Talos объяснили, что создание длительного доступа к системам жертв нужно для того, чтобы LilacSquid могла перекачивать данные на свои серверы. Цели атаки включают IT-организации, создающие ПО для исследовательского и промышленного секторов в США, энергетические компании в Европе и фармацевтические компании в Азии.

Цепочка заражения LilacSquid

LilacSquid в своих атаках используют либо известные уязвимости для взлома веб-серверов, либо скомпрометированные учетные данные Remote Desktop Protocol (протокол удалённого рабочего стола) предоставляет возможности удаленного отображения и ввода через сетевые подключения для приложений, работающих на сервере. Протокол RDP предназначен для поддержки различных типов сетевых топологий и нескольких протоколов локальной сети." data-html="true" data-original-title="RDP" >RDP для доставки вредоносного ПО и инструментов с открытым исходным кодом.

Наиболее примечательной особенностью кампании является использование MeshAgent, инструмента удаленного управления с открытым исходным кодом, который служит каналом для доставки специальной версии Quasar RAT под кодовым названием PurpleInk.

Альтернативные методы заражения с использованием скомпрометированных учетных данных RDP включают два варианта: либо развертывание MeshAgent, либо установка .NET-загрузчика InkLoader для доставки PurpleInk. Talos также обнаружила инструмент InkBox, который использовался для развертывания PurpleInk до InkLoader.

PurpleInk, поддерживаемый LilacSquid с 2021 года, отличается запутанностью и

универсальностью, что позволяет выполнять операции с файлами, получать системную информацию, запускать удаленную оболочку и подключаться к 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-серверу.

Использование MeshAgent примечательно, поскольку ранее оно применялось северокорейским злоумышленником Andariel, подразделением группы Lazarus, в атаках на южнокорейские компании. Ещё одно совпадение с Andariel заключается в использовании инструментов туннелирования для поддержания доступа: LilacSquid применяет Secure Socket Funneling (SSF) для создания канала связи со своей инфраструктурой.