Новая версия TargetCompany с новыми возможностями бесследной атаки.

Специалисты Trend Micro – это международная компания в области кибербезопасности, специализирующаяся на защите от вредоносного программного обеспечения, угроз в интернете и других кибератак. Она была основана в 1988 году и с тех пор стала одной из ведущих компаний в своей отрасли.

 Основной продукт Trend Micro – это программное обеспечение, которое предлагает защиту от вирусов, троянов, шпионского и рекламного ПО, фишинга и других угроз. Кроме того, компания предлагает решения для обнаружения и предотвращения атак, контроля уязвимостей, защиты электронной почты и облачных сервисов, а также безопасности мобильных устройств.

 Trend Micro обслуживает широкий круг клиентов, включая частных пользователей, малые и средние предприятия, а также крупные корпорации. Компания также активно занимается исследованиями в области кибербезопасности и предоставляет информацию и ресурсы для обнаружения и реагирования на новые угрозы." data-html="true" data-original-title="Trend Micro" >Trend Micro обнаружили новую версию программы-вымогателя TargetCompany, ориентированную на VMware ESXi. Злоумышленники используют кастомный shell-скрипт для доставки и выполнения вредоносного ПО.

TargetCompany (Mallox, FARGO, Tohnichi) впервые появилась в июне 2021 года и специализируется на атаках на базы данных MySQL, Oracle и SQL Server, преимущественно в Тайване, Южной Корее, Таиланде и Индии. В феврале 2022 года Avast выпустила бесплатный декриптор для более ранних версий вымогателя.

Цепочка заражения TargetCompany

Согласно отчету Trend Micro, новый Linux – это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах, таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-

title="Linux" >Linux-вариант TargetCompany требует административных привилегий перед началом выполнения вредоносных действий. Для загрузки и выполнения вымогательского ПО злоумышленники используют кастомный скрипт, который также способен отправлять данные на два различных сервера, вероятно, для обеспечения отказоустойчивости.

После попадания на целевую систему скрипт проверяет окружение на наличие VMware ESXi, выполняя команду «uname» и проверяя на наличие «vmkernel». Далее создается файл TargetInfo.txt" с информацией о жертве (имя хоста, IP-адрес, данные ОС, имена вошедших пользователей и их привилегии, уникальные идентификаторы и информация о зашифрованных файлах и директориях), который отправляется 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.

Вредоносное ПО шифрует файлы с расширениями, связанными с виртуальными машинами (vmdk, vmem, vswp, vmx, vmsn, nvram), добавляя к ним расширение «.locked». После этого на систему добавляется записка с инструкциями по оплате выкупа и получению ключа для дешифровки.

Записка о выкупе TargetCompany

После завершения всех задач скрипт удаляет полезную нагрузку, поэтому все следы, которые можно использовать при расследовании инцидентов, удаляются с затронутых компьютеров.

Аналитики Trend Micro связывают атаки новой Linux-версии TargetCompany с киберпреступником под именем «vampire», упомянутым в отчете Sekoia. IP-адреса, использованные для доставки вредоносного ПО и получения файлов с информацией о жертвах, были привязаны к провайдеру из Китая, что, однако, недостаточно для точного определения происхождения атакующих.

В отчете Trend Micro содержатся рекомендации по защите, включая установку многофакторной аутентификации (MFA), создание резервных копий и обновление систем. Исследователи также предоставили список индикаторов компрометации, включая хэши для Linux-варианта вымогателя, кастомного скрипта и образцов, связанных с аффилиатом «vampire».

Ранее специалисты Trend Micro выяснили, что хакеры Mallox используют собственное вымогательское ПО в сочетании с RAT-трояном Remcos и обфускатором BatCloak, что позволяет закрепиться в системе жертвы и избежать обнаружения.

Кроме того, в мае вирус-вымогатель Mallox использовался в атаках на серверы Microsoft SQL (MS-SQL). После проникновения в систему киберпреступники устанавливали Remcos RAT для установления полного контроля заражённого хоста.