

Из-за ошибки одного администратора может пострадать вся корпоративная сеть.

Израильская ИБ-компания Sygnia — это компания, специализирующаяся на обеспечении кибербезопасности для предприятий и организаций. Она была основана с целью помочь компаниям защитить свои сети, данные и информацию от киберугроз.

Sygnia предлагает широкий спектр решений и услуг, включая мониторинг безопасности, угрозы и инциденты, анализ рисков, пентестинг, а также консультации и обучение в области кибербезопасности." data-html="true" data-original-title="Sygnia" >Sygnia отмечает, что платформы виртуализации, такие как VMware — поставщик программного обеспечения для виртуализации и облачных вычислений, базирующийся в Пало-Альто, Калифорния. Компания VMware, основанная в 1998 году, является дочерней компанией Dell Technologies. Корпорация EMC первоначально приобрела VMware в 2004 году; Позже EMC была приобретена Dell Technologies в 2016 году. VMware основывает свои технологии виртуализации на своем гипервизоре ESX/ESXi без операционной системы с архитектурой x86." data-html="true" data-original-title="VMware" >VMware VMware ESXi (также известная как VMware vSphere Hypervisor) — это гипервизорная платформа, разработанная компанией VMware. Она позволяет виртуализировать физические серверы и создавать виртуальные машины, которые могут работать независимо друг от друга на одном физическом сервере.<br /><br /> ESXi представляет из себя «тонкий гипервизор». Платформа имеет минимальную операционную систему, которая запускается непосредственно на физическом сервере и предоставляет основные функции виртуализации. ESXi обеспечивает выделение ресурсов, управление памятью, управление процессором и ввод-выводом для виртуальных машин.<br /><br /> VMware ESXi широко используется в корпоративной среде для создания и управления виртуальными инфраструктурами. Она предлагает функциональность, такую как миграция виртуальных машин между физическими серверами, управление резервированием ресурсов, сетевую виртуализацию и многое другое. ESXi также интегрируется с другими продуктами VMware, такими как VMware vCenter Server, для централизованного управления и мониторинга виртуальных сред." data-html="true" data-original-title="ESXi" >ESXi часто страдают от неправильных настроек и уязвимостей, что делает их привлекательными целями для хакеров.

В ходе расследований, связанных с различными семействами программ-вымогателей, такими как LockBit, HelloKitty, BlackMatter и другие, Sygnia обнаружила, что атаки на среды виртуализации следуют установленному порядку действий:

Цепочка атаки

## Как защититься

Для минимизации рисков организации рекомендуется обеспечить надлежащие мониторинг и логирование, создать надежные механизмы резервного копирования, внедрить строгие меры аутентификации, укрепить инфраструктуру и ограничить сетевую активность для предотвращения перемещений внутри сети.