Первым средством для заражения промышленных объектов стал специализированный **к омпьютерный червь Stuxnet.**
Впервые в истории не только промышленного сектора, но и кибератак Stuxnet смог разрушить инфраструктуру промышленного объекта, существенно повысив риски техногенных катастроф. Stuxnet был только началом в разработке целого класса вирусного ПО. И если изначально вирус был направлен против определенных объектов и физических устройств, то нынешние модификации вируса существенно расширили вектор атак, нацеленных на промышленный сектор.

Исконно *автоматизированные системы управления* техническим процессом (АСУ ТП) и смежные с ними процессы были отделены от ИТ-инфраструктуры и используемых в ней проприетарных протоколов специализированного программного и аппаратного обеспечения. В последние десять лет специализированные решения стали вытесняться недорогими универсальными продуктами с поддержкой протокола IP. Такая ситуация создала дополнительные возможности для киберпреступников.

Внедрение на промышленных предприятиях централизованного управления, удаленного доступа, классических ОС и сетевых протоколов ведет к слиянию технологических сетей с обычной ИТ-инфраструктурой. Такое слияние повышает эффективность, но нарушает принцип изолированности промышленных систем, открывая новые возможности для злоумышленников и повышая уязвимость промышленных объектов.

Специфика угроз

Угрозы для АСУ ТП разнообразны: от случайных действий не информированных

сотрудников до умышленных действий террористических групп. Существующие угрозы для АСУ ТП можно разделить на несколько направлений:

1. Внешние воздействия

К внешним воздействиям следует отнести целенаправленные атаки киберпреступников. Известны случаи, когда причиной атаки были соревнования между хакерами. Если десять лет назад для проведения подобной атаки требовалась серьезная подготовка и знания специфики строения промышленных сетей, то сегодня, с появлением Stuxnet, злоумышленники имеют готовые вредоносные скрипты и программы под специализированные протоколы. В ряде случаев внешним воздействием может стать не целевое проникновение в технологическую сеть, а просто массовое заражение, например вследствие зомбирования компьютеров в бот-сеть.

Целью таких атак может стать нарушение работоспособности или шантаж компании.

2. Внутренние воздействия

Внутренние атаки опасны тем, что инсайдер внутри компании, даже не обладая специальными знаниями, пользуется обширным представлением о специфике используемых систем и работоспособности промышленной инфраструктуры. В роли инсайдера могут выступать сотрудники организации, в случае внутренних мошенничеств.

Методами социальной инженерии злоумышленник имеет возможность попадать напрямую внутрь сети, поскольку внутри компании всегда есть недовольные и обиженные, а также желающие повысить уровень своего благосостояния. Используя сотрудников компании, можно распространять целевые вирусы на съемных носителях или вводить в заблуждение сотрудников, которые имеют доступ из корпоративной сети в Интернет (через средства обмена сообщениями, форумы, социальные медиа).

Целью таких атак является злонамеренное воздействие на сеть, например с отложенным результатом нарушения работоспособности или аварии.

3. Шпионаж

Крупные и критичные промышленные объекты являются важной частью инфраструктуры государства, поэтому компании промышленного сектора могут стать целью для разведок других стран. Примечательно, что вирус Stuxnet, разработанный под промышленные объекты, по одной из самых правдоподобных версий, был создан именно при поддержке военных ведомств и разведки. Получение всей доступной информации является неотъемлемой частью работы разведывательных управлений всех стран мира.

Информация же о промышленных объектах является ключевой на случай возможных военных конфликтов различного масштаба. Реалии современного мира диктуют новые правила конкурентной борьбы, где компании ведут настоящую охоту за важной информацией.

Промышленный шпионаж с появлением средств, **аналогичных Stuxnet**, выводит вероятность кражи или подмены данных на очень высокий уровень.

Целью шпионажа может стать компрометация информации или ее кража с последующим деструктивным использованием, вплоть до полной остановки бизнеса и банкротства атакуемого.