ОБНАРУЖЕНИЕ АТАК За шесть месяцев 2019 года количество кибератак, устроенных с целью очистки данных и отключения критических инфраструктурных систем, выросло в три раза, следует из отчета IBM X-Force Incident Responseand Intelligence Services (IRIS). Половина всех атак пришлась на производственный, нефтегазовый и образовательный секторы.

Аналогичные данные приводят и другие эксперты. По данным заместителя руководителя Управления ФСТЭК РФ по УрФО Валерия Мельникова, за прошлый год 48% компьютеров на предприятиях были подвержены атакам: 38% атак из этого числа произошло через интернет, причиной 15–20% атак стало использование съемных носителей, и 2% — фишинг.

Согласно статистике Kaspersky ICS CERT, по итогам 2018 года процент компьютеров АСУ, на которых были задетектированы вредоносные объекты, вырос по сравнению с предыдущим годом на 3,2 п.п. и составил 47,2%. В России в течение второго полугодия 2018 года хотя бы один раз вредоносные объекты были задетектированы на 45,3% компьютеров АСУ, что соответствует уровню, который мы наблюдали в первом полугодии (44,7%).

В Group-IB отмечают: количество атак на промышленные IT-системы ежегодно растет на 20%. «Атаки правительственных кибермилий происходят уже не с целью сбора разведданных, а для установления контроля над ресурсами политических оппонентов. Целью кампаний все чаще является не только шпионаж, но и получение доступа к критическим системам. На протяжении 2018 года прогосударственные хакерские группы активно атаковали объекты критической инфраструктуры — предприятия ТЭК, ядерного, коммерческого, водного, авиационного и других секторов — с целью саботажа и шпионажа»,— сообщили в пресс-службе компании. По оценкам Group-IB, в топ-3 стран самых активных проправительственных хакерских групп входят Китай, Северная Корея и Иран.

ПРИВЛЕКАТЕЛЬНАЯ ИНДУСТРИЯ Энергетический сектор — одна из индустрий, которая подвергается атакам наиболее часто, отмечает руководитель Kaspersky Industrial Cyber Security Алексей Петухов. «Скорее всего, это обусловлено большой сетевой связностью энергообъектов и тем фактом, что к их системам управления в среднем имеет доступ больше людей, чем на предприятиях других отраслей»,— уверен он.

В «Ростелеком-Solar» фиксируют более чем двукратный рост атак в отраслях ТЭК и энергетики. Причем, речь идет как о массовых, «широковещательных» методах атак, так и о специализированных именно на эти отрасли, уточнил директор центра мониторинга и реагирования на кибератаки «Ростелеком-Solar» Владимир Дрюков. В Group-IB атаки делят на две большие группы: «Вымогатели, цель которых получить доступ к инфраструктуре, парализовать ее, а потом требовать выкуп за восстановление работоспособности; и проправительственные хакерские группы, цель которых — шпионаж, supplychain атаки»,— поясняют в компании. Господин Дрюков уточняет: инфраструктура ТЭК разнородна и может быть скомпрометирована злоумышленниками с самыми разными целями. «Особенно высокие риски несут атаки, в результате которых злоумышленники могут получить доступ к автоматизированным системам управления технологическими процессами (АСУ ТП). В этом случае, если злоумышленники настроены радикально, атака может привести к техногенной аварии и выйти за пределы деятельности компании». Целевые атаки встречаются редко, однако они могут быть сопряжены с экономическими потерями, повреждением оборудования, человеческими жертвами, экологическими последствиями, добавил Алексей Петухов.

В компании PositiveTechnologies поясняют, что атаки с целью легкой монетизации совершают, как правило, «хулиганы». Руководитель отдела аналитики информационной безопасности компании Евгений Гнедин пояснил, что это — «типичный злоумышленник-одиночка, который, как правило, использует готовые инструменты для атак. «Его целью может быть легкий заработок с помощью распространения майнеров или шифровальщиков, а также тщеславие»,— рассуждает он.

Более серьезный риск несут атаки APT-группировок. «Это группа высококвалифицированных хакеров, обладающих знаниями о специфике работы систем и процессов в атакуемых компаниях, обладающих значительным начальным капиталом для атаки,— рассказывает господин Гнедин.— Группировка может спонсироваться заказчиком атаки, что дает возможность выбирать наиболее эффективные методы. Они, как правило, используют собственное ПО в атаках, но готовы купить уязвимости нулевого дня — неустраненные уязвимости — за крупную сумму, если это необходимо». Именно их целью становится получение контроля над технологическими сетями и оборудованием или политический мотив, добавляет эксперт.

Такие группировки, отмечает Евгений Гнедин, могут не наносить никакого ущерба, пока не получат команду от заказчика атаки. «Тогда атака может привести к непоправимым последствиям: авариям на подстанциях, человеческим жертвам среди сотрудников или населения, каскадным отключениям оборудования, разрушению оборудования и так далее. Это может сказаться не только на бизнесе и репутации самой компании, но и на экономике региона или всей страны»,— опасается он.

Алексей Петухов напомнил, что недавно Минэнерго выпустил рекомендации для обеспечения безопасности объектов ТЭК и критической информационной инфраструктуры. Они включают базовые меры защиты — специализированные промышленные антивирусы, «белые» списки запускаемых программ, контроль подключаемых устройств, антишифрование и межсетевое экранирование, обучение сотрудников (существуют тренинговые программы для различных специалистов, например, ИТ, административный персонал, менеджмент), выстраивание процессов информационной безопасности.

Однако ТЭК очень широкая сфера, куда входят предприятия разного размера и разных отраслей, поэтому меры защиты очень индивидуальны, признается эксперт. По его словам, крупные предприятия со сложными технологическими сетями тратят на информационную безопасность минимум сотни миллионов рублей, но часто этого недостаточно. «В холдингах находятся сотни объектов защиты, требуется проанализировать угрозы для них, сформировать решения, внедрить их и эксплуатировать, а часто компании пытаются решить вопросы кибербезопасности "заплатками"»,— полагает господин Петухов. А чтобы система была действительно эффективной, уверен он, нужно обеспечивать автоматизацию процессов информационной безопасности, внедряя сложные системы верхнего уровня, расширяя штат сотрудников и минимальный набор используемых базовых средств защиты. «Это колоссальные затраты, но потенциальный ущерб на крупных предприятиях превышает их в десятки раз»,— отмечает эксперт.

ЦЕНА ВИРУСОВ Атаки вредоносного ПО в среднем могут стоить организациям $239 млн, полагают аналитики IBM,— в 61 раз выше среднего размера ущерба от утечки данных ($3,92 млн), и потери доступа к 12 тыс. устройств. На реагирование и устранение инцидентов с кибератаками может уйти не менее 512 часов. Вредоносные программы, используемые в этих случаях, могут привести к потере данных, отключению корпоративных устройств, повреждению функций и блокированию систем в обмен на выкуп. Среди распространенных вирусов — NotPetya, Stuxnet, Shamoon и DarkSeoul.

ОЛЕГ ХАРСЕЕВ

ПОЯВЛЕНИЮ КИБЕРРИСКОВ СПОСОБСТВУЕТ ПОВСЕМЕСТНАЯ ЦИФРОВИЗАЦИЯ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ