КИБЕРУГРОЗЫ ДЛЯ НЕФТЯНИКОВ: ЕСТЬ ЛИ МЕХАНИЗМЫ ЗАЩИТЫ?

Евгений ПИТОЛИН
управляющий директор
Kaspersky Lab в Казахстане,
Центральной Азии и Монголии

050010, Республика Казахстан,
г. Алматы, Казыбек би, 20а

За последние несколько лет мишенью кибер-преступников становились больницы, аэропорты, поезда, компьютеры банков и государственных учреждений. Затем настала эра эпидемий WannaCry, ExPetr и Bad Rabbit – они распространялись как лесной пожар, грозя множеству компаний по всему миру убытками и помехами в работе. Казахстан, напоминаю, в 2017 году занял пятое место в мире по количеству зараженных WannaCry компьютеров.

Во втором полугодии 2018 года продукты «Лаборатории Касперского» предотвратили вредоносную активность на 40,8% компьютеров АСУ.

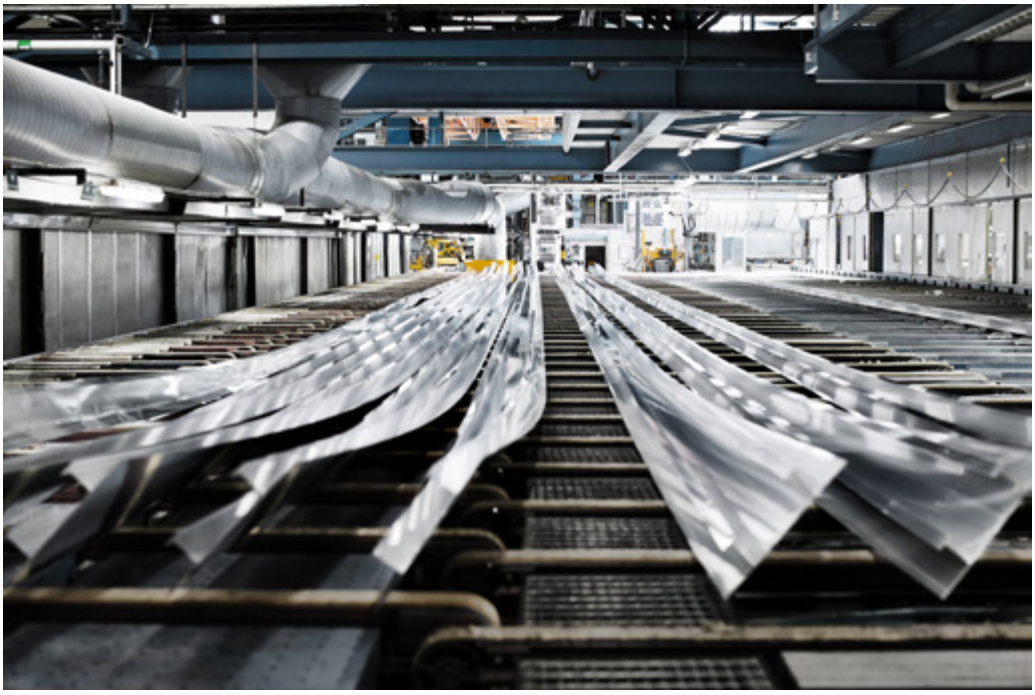
Защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было задетектировано более 19,1 тыс. модификаций вредоносного ПО из 2,7 тыс. различных семейств. По-прежнему в подавляющем большинстве случаев попытки заражения компьютеров АСУ носят случайный характер, а не происходят в ходе целевой атаки.

Актуальными угрозами для компьютеров АСУ остаются вредоносные программы класса Trojan. Такие вредоносные объекты были задетектированы на 27,1% компьютеров АСУ. На 3,2% компьютеров АСУ была предотвращена вредоносная активность эксплойтов,

на 3,1% были заблокированы бэкдоры,

на 2% – программы-вымогатели.

В последние двенадцать месяцев крупных атак такого масштаба не наблюда-



лось, и мир расслабился. Однако 19 марта 2019 года начался новый отчет в эпохе промышленных киберугроз. Норвежский промышленный гигант Hydro, один из крупнейших производителей алюминия в мире, объявил, что попал под удар программы-вымогателя, и эта кибератака колоссально повлияла на всю компанию.

Штатные специалисты по кибербезопасности впервые заметили необычную активность на серверах компании около полуночи. Увидев, что заражение распространяется, они попытались его остановить. Сделать это получилось лишь частично: к тому времени, как были изолированы заводы, зловред уже обосновался в глобальной сети Hydro. В компании работает около 35 000 человек, и заражение затронуло немалую их часть.

Фишинговые атаки – основной вектор направленных атак на промышленные компании. Вредоносные вложения из фишинговых писем представляют угрозу не только для офисных компьютеров, но и для части машин технологической инфраструктуры промышленных компаний: как минимум на 4,3% компьютеров АСУ в мире были заблокированы троянцы-шпионы, бэкдоры и кейлоггеры, которые массово встречаются в фишинговых письмах, рассылаемых индустриальным компаниям.

Принадлежащие Hydro электростанции не пострадали, потому что были изолированы от основной сети, — и это правильный подход к критической инфраструктуре. Однако плавильные заводы изолированы не были, а степень их автоматизации за последние годы значительно выросла. В результате шифровальщик поразил ряд заводов, расположенных в Норвегии. Неспособность подключиться к основным системам вызвала проблемы на производстве и временные остановки на нескольких заводах. Вредоносные программы зашифровали данные на компьютерах с Windows,

выведя их из строя. Повезло, что под удар не попали телефоны и планшеты с другими ОС, так что сотрудники по-прежнему могли общаться между собой и оперативно выполнять первоочередные для компании задачи. Кроме того, атака, по всей видимости, не затронула дорогостоящие компоненты критической инфраструктуры, в том числе электролизные ванны для производства алюминия, каждая из которых стоит около 10 млн евро, что все их можно будет восстановить из резервных копий.

Конечно, полностью восстановить работу в штатном режиме получится нескоро. Да и расследование инцидента займет очень много времени как у самой компании, так и у норвежских правоохранительных органов. Хотя анализ происшествия все еще ведется, уже можно говорить о том, что Hydro сделала правильно, а что неправильно до инцидента и во время него.

Правильно:

- станции энергоснабжения были изолированы от основной сети;
- компания оперативно смогла отсоединить от сети плавильные заводы;
- сотрудники могли нормально взаимодействовать даже после инцидента;
- есть резервные архивы, с помощью которых можно восстановить хотя бы частично зашифрованные данные;
- есть киберстраховка, которая должна покрыть хотя бы часть ущерба от инцидента.

Неправильно:

- сеть не была должным образом сегментирована со стороны департамента АСУ;
- установленное Hydro защитное решение не сумело перехватить шифро-

вальщик, так как не взаимодействовало с промышленной сетью и было не предназначено для защиты таких сетей;
- периметр безопасности можно было дополнить специализированным продуктом по защите от вымогателей

Эксперты Kaspersky Lab ICS CERT продолжают начатые в прошлом году исследования проблем безопасности в сторонних программных и программно-аппаратных решениях, широко применяемых в системах промышленной автоматизации. Особое внимание было уделено продуктам с открытым исходным кодом, которые используются различными производителями в своих решениях.

В 2018 году Kaspersky Lab ICS CERT была выявлена 61 уязвимость в промышленных системах и системах IIoT/IoT. 29 из них было устранено вендорами в течение года.

Первые грубые экспертные оценки ущерба от атаки на Norsk Hydro – 40 млн долларов. В следующий раз, когда ИБ-специалисты принесут вам план защиты промышленной сети от кибератак, а АСУ ТП отдел начнет рассказывать, как у них все хорошо и безопасно, и независимо от мировых угроз – просто вспомните этот текст.