KASPERSKY lab

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2017

Kaspersky Lab ICS CERT

Содержание

В течение многих лет специалисты «Лаборатории Касперского» обнаруживают и исследуют киберугрозы, направленные на различные информационные системы – коммерческих и государственных организаций, банков, телеком-операторов, промышленных предприятий и частных лиц. Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) публикует результаты исследований ландшафта угроз для систем промышленной автоматизации, полученные в течение первого полугодия 2017 года.

Основная цель публикаций – информационная поддержка глобальных и локальных команд реагирования на инциденты, специалистов по информационной безопасности предприятий и исследователей в области защищённости промышленных объектов.

Основные события полугодия

Новое кибероружие

В июне 2017 года были опубликованы результаты исследований вредоносного ПО, которое получило название CrashOverride/Industroyer. Эксперты компаний ESET, Dragos Inc. и ряд независимых специалистов пришли к выводу, что это вредоносное программное обеспечение предназначено для нарушения рабочих процессов в промышленных системах управления (ICS), в частности, на электрических подстанциях. CrashOverride/Industroyer позволяет напрямую управлять выключателями и прерывателями цепи в сети электрических подстанций.

Зловред умеет работать с четырьмя промышленными протоколами, распространенными в электроэнергетике, управлении транспортом, водоснабжении и других критических инфраструктурах: IEC 60870-5-101 (aka IEC 101), IEC 60870-5-104 (aka IEC 104), IEC 61850, OLE for Process Control Data Access (OPC DA). Создатели Crash Override/Industroyer могут перенастроить программу, чтобы атаковать любую промышленную среду, где используются целевые протоколы связи. Вероятнее всего, злоумышленники планировали использовать CrashOverride/Industroyer не в единичной атаке, а масштабировать его для атак на разные системы.

Другой особенностью CrashOverride/Industroyer, согласно отчету ESET, является дополнительная функция, позволяющая эксплуатировать уязвимости оборудования Siemens SIPROTEC, используемых в системах релейной защиты и автоматики. Отправив устройствам специально сформированную последовательность данных, можно их отключить. Для последующего включения необходима их ручная перезагрузка.

В случае использования этой функции вредоносным ПО при критической ситуации в электросети физический ущерб может не ограничиться отключением электроснабжения – атака может привести к повреждению оборудования вследствие несрабатывания релейной защиты и автоматики. При особым образом спланированных перегрузках атака в одном месте может привести к каскадным отключениям электроснабжения на нескольких подстанциях.

Эксперты ESET предполагают, что CrashOverride/Industroyer мог быть связан со сбоем энергоснабжения в Киеве в декабре 2016 года. Тогда под ударом оказалась подстанция Укрэнерго, обслуживающая север Киева. Представители Укрэнерго заявили, что сбой в работе этой подстанции был обусловлен внешним воздействием на SCADA системы подстанции.

В пользу того, что причиной этого сбоя мог быть CrashOverride/Industroyer, свидетельствует наличие в нем достаточной для реализации такой атаки функциональности, а также метка времени активации – 17 декабря 2016 года, в день отключения электроэнергии. Тем не менее, прямые доказательства использования данного вредоносного ПО в каких-либо из известных на сегодняшний день атаках на объекты электроэнергетики отсутствуют. Помимо прочего важно заметить, что эксперты ESET, в руки которых попало для анализа наибольшее число модулей вредоносного ПО CrashOverride/Industroyer, подчеркивают отсутствие каких-либо указаний на происхождение авторов.

Возможности CrashOverride/Industroyer указывают на весьма высокую квалификацию его создателей и глубокое понимание ими устройства промышленных систем управления объектов

электроэнергетики. Маловероятно, что подобное ПО было разработано без доступа к используемому на таких объектах оборудованию.

Таким образом, CrashOverride/Industroyer — это настоящее кибероружие, нацеленное на промышленные системы. Пожалуй, это самая серьезная со времен Stuxnet известная угроза для промышленных систем управления.

Атаки хакеров на системы обеспечения безопасности людей

Вывод из строя систем видеонаблюдения полиции Вашингтона

В середине января, за 8 дней до инаугурации Дональда Трампа, в Вашингтоне была выведена из строя система видеонаблюдения, которая используется окружным департаментом полиции. 123 из 187 устройств хранения данных, на которые записывается видео с установленных в общественных местах камер, были заражены вредоносной программой-шифровальщиком.

По информации Washington Post, несмотря на грядущую инаугурацию президента, которая должна была пройти в Вашингтоне, выкуп злоумышленникам власти города платить не стали. Чтобы восстановить нормальную работу устройств их пришлось отключить и переустановить на них ПО.

Систему видеонаблюдения удалось вернуть в работу до инаугурации президента. Позднее правоохранительные органы Великобритании по запросу США арестовали в Лондоне гражданина Великобритании и гражданку Швеции как возможно причастных к этому инциденту.

Взлом систем экстренного оповещения в Далласе

Последствия компьютерных атак на системы, предназначенные для обеспечения безопасности людей, в апреле этого года в полной мере ощутили жители Далласа, США. В результате взлома в городе заработали сирены системы экстренного оповещения о чрезвычайных ситуациях. В течение 90 минут 156 сирен, обычно используемых в случае опасности торнадо, включали ложную тревогу 15 раз, по 90 секунд каждый. Остановить сирены удалось только глубокой ночью, вручную отключив радиосистему и повторители.

Представители городской администрации, не раскрывая подробностей, сообщили, что атака была проведена с использованием некого радиосигнала. Специалисты компании Bastille полагают, что скорее всего кто-то провел атаку типа radio replay: во время ежемесячного тестирования системы экстренного оповещения злоумышленник записал команды управляющего центра, которые передаются на специальных радиочастотах, а затем воспроизвел их.

Работы по восстановлению системы растянулись на два дня. Случись в эти дни торнадо, горожане остались бы без предупреждения.

IoT-ботнет Persirai

В апреле 2017 года исследователь Пирри Ким (Pierre Kim) опубликовал результаты своего исследования, согласно которым более 1000 моделей IP-камер 354 разных производителей содержат опасную уязвимость во встроенном веб-сервере. Подробное описание проблемы Ким дополнил фрагментами кода и информацией о том, что через Shodan можно обнаружить более 185 000 уязвимых камер (соответствующая ссылка прилагалась). По словам исследователя, своей

публикацией он хотел привлечь внимание многочисленных производителей камер к наличию уязвимости. Но быстрее других, как это нередко бывает, на публикацию отреагировали злоумышленники.

Уже в мае 2017 года специалисты Trend Micro обнаружили новый IoT-ботнет из уязвимых камер, названный ими Persirai. По данным Trend Micro, ботнет используется злоумышленниками преимущественно для проведения DDoS-атак.

Атаки типа Business Email Compromise на промышленные компании

Эксперты Kaspersky Lab ICS CERT сообщили об атаках нигерийских злоумышленников типа Business Email Compromise (BEC), нацеленных преимущественно на промышленные и крупные транспортные и логистические предприятия. В исследованных «Лабораторией Касперского» атаках среди потенциальных жертв на долю промышленных компаний приходилось свыше 80%. Всего было обнаружено более 500 атакованных компаний более чем в 50 странах мира.

На первом этапе мошенники рассылают на адреса компаний письма с вредоносными вложениями. Вредоносное ПО предназначено для кражи конфиденциальных данных и в некоторых случаях установки скрытых средств удалённого администрирования заражённых систем. Заразив корпоративный компьютер, злоумышленники снимают скриншоты переписки сотрудника компании с помощью вредоносных программ, либо ставят скрытое перенаправление сообщений почтового ящика атакованного компьютера на собственный почтовый ящик. Это дает им возможность отслеживать, какие сделки купли-продажи готовятся в компании.

Выбрав из готовящихся транзакций наиболее перспективную для себя, атакующие регистрируют домены, имена которых очень похожи на имена продающих компаний. Используя эти домены, преступники могут осуществлять атаку типа “man-in-the-middle”: они перехватывают сообщение с инвойсом от компании-продавца и пересылают с почтового ящика на фишинговом домене это же сообщение покупателю, заменив реквизиты компании-продавца на реквизиты счета, который принадлежит атакующим. Либо присылают от имени продавца в дополнение к легитимному сообщению с инвойсом запрос на срочное изменение реквизитов.

Еще один вариант: получив с помощью троянца-шпиона и/или бэкдора доступ к легитимному ящику одного из сотрудников атакованной компании, злоумышленники ведут мошенническую переписку с этого ящика. Фишеры также могут отправлять письма от имени продавца, подделав поля в заголовках письма так, чтобы они указывали в качестве отправителя на легитимный ящик продавца.

В любом случае шансы на то, что получатель не заподозрит неладное, и злодеи получат деньги, весьма велики.

Такие атаки опасны для индустриальных компаний. В случае успеха атакующих компания-покупатель не только теряет деньги, но и не получает вовремя покупаемый товар. Для промышленных компаний это может быть критичным: если этот товар, например, сырье, используемое в производстве, или необходимые для ремонта оборудования запчасти, то возможны и остановка производства, и срыв сроков выполнения регламентных и пуско-наладочных работ.

Однако это не все возможные последствия. Программы-шпионы, которые используют фишеры, пересылают на свои командные серверы различную информацию с зараженных машин, в том числе об основной деятельности и основных активах индустриальных компаний – например, информацию о контрактах и проектах. На некоторых командных серверах злоумышленников были обнаружены скриншоты, сделанные с рабочих станций операторов, инженеров, проектировщиков и архитекторов.

Пока эксперты не зафиксировали случаев продажи украденной злоумышленниками информации на черном рынке. Но очевидно, что для атакуемых компаний атака типа BEC, помимо прямой финансовой потери по какой-то конкретной сделке, таит и прочие, возможно, более значительные, угрозы.

Отметим, что атаки типа BEC на промышленные компании продолжаются и во втором полугодии 2017 года.

Опасные публикации

WikiLeaks: архив ЦРУ

Важным событием полугодия стала утечка архива спецподразделения ЦРУ США, который описывал хакерские инструменты ЦРУ: вредоносное ПО, в том числе эксплойты для уязвимостей нулевого дня, вредоносные системы удаленного доступа и связанную с этим документацию. Часть этого архива была опубликована на WikiLeaks.

Дамп, попавший в распоряжение WikiLeaks, известен как Vault 7. Начиная с марта 2017 года, в серии публикаций в открытый доступ выложено около девяти тысяч документов, свидетельствующих о возможности скрытного проникновения на различные электронные устройства, от сотовых телефонов и «умных» телевизоров до корпоративных систем. Вредоносные программы ЦРУ нацелены на ПО OS Windows, macOS, Linux, iPhone, Android, телевизоры SmartTV, маршрутизаторы.

В опубликованных документах перечислено множество уязвимостей. В частности, после публикации Vault 7 Cisco предупредила своих клиентов о наличии критической уязвимости, позволяющей исполнить произвольный код и получить полный контроль над коммутаторами и роутерами более чем 300 разных моделей, произведённых компанией (уязвимость была закрыта в мае).

По оценкам экспертов, большая часть опубликованных уязвимостей была закрыта вендорами еще до их публикации. Инструменты взлома или эксплойты WikiLeaks не раскрывали. Однако даже опубликованная часть может помочь злоумышленникам в разработке собственного вредоносного арсенала. По всей видимости, мы еще будем наблюдать как массовые атаки, так и последствия скрытых проникновений на основе информации, опубликованной в Vault 7.

Shadow Brokers: архив АНБ

В апреле хакерская группа Shadow Brokers открыла доступ к архиву с эксплойтами и инструментами для проведения атак Агентства Национальной Безопасности США (АНБ).

Архив, раздобытый Shadow Brokers, хакеры сначала пыталась продать. Позже большая его часть была опубликована. В публичном доступе оказались эксплойты для сетевого оборудования и маршрутизаторов, для банковских систем, UNIX-подобных систем и для различных версий

Windows. В числе опубликованных уязвимостей были и неизвестные ранее уязвимости нулевого дня.

Корпорация Microsoft объявила, что большинство уязвимостей из опубликованного архива уже исправлены либо не актуальны для Windows 7 и выше. Три уязвимости были закрыты Microsoft за месяц до публикации Shadow Brokers – в обновлении MS17-10.

Этим патчем закрывалась и брешь в SMBv1, на которую среди прочих были нацелены эксплойты АНБ EternalBlue и EternalRomance. Уже через полтора месяца после публикации Shadow Brokers модификации этих экспойтов использовались для распространения ставших печально знаменитыми шифровальщиков — WannaCry и ExPetr (Petya).

Атаки программ-шифровальщиков

Первое полугодие 2017 года запомнится атаками программ-шифровальщиков, причем не только экспертам по безопасности. Эпидемия Wannacry и атаки ExPetr привлекли к этой проблеме всеобщее внимание.

Шифровальщики стали значимой угрозой для компаний, в том числе промышленных. Для предприятий, имеющих объекты критической инфраструктуры, эти зловреды особенно опасны, поскольку активность вредоносного ПО может нанести вред производственному процессу.

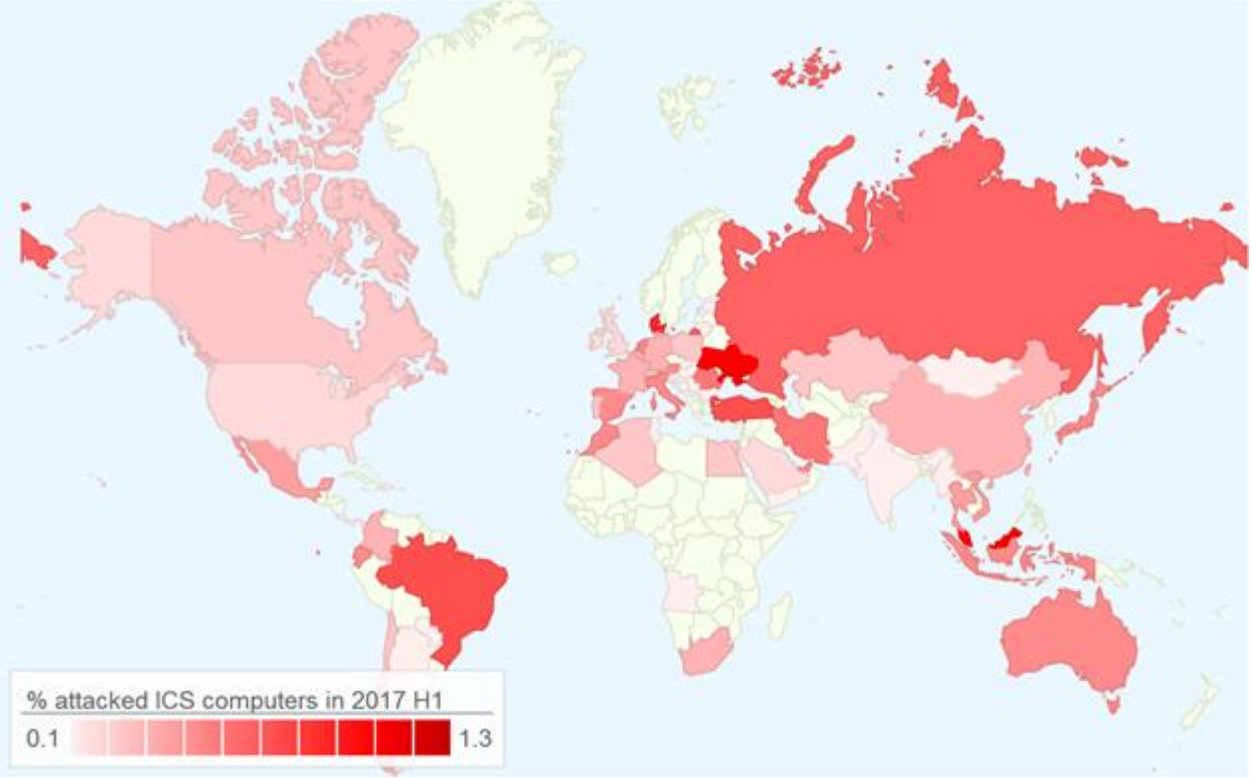
Продукты «Лаборатории Касперского» регулярно блокировали атаки программ-шифровальщиков на компьютерах АСУ в 63 странах мира. На карте ниже отражен процент атакованных шифровальщиками систем промышленной автоматизации в каждой стране по отношению к общему количеству таких систем в стране.

По нашим данным **0,5%** компьютеров технологической инфраструктуры организаций в течение первых шести месяцев 2017 года хотя бы раз были атакованы программами шифровальщиками.

Top 10 стран по проценту атакованных шифровальщиками компьютеров АСУ:

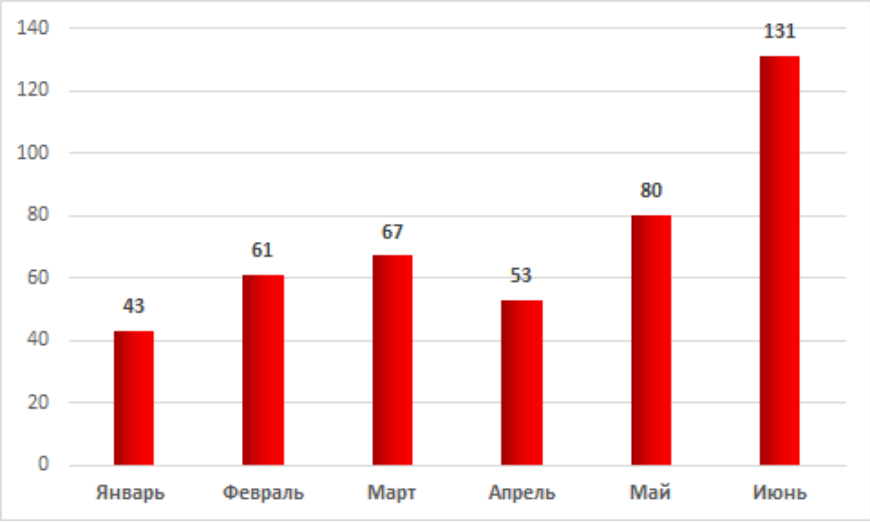
	Страна*	**% атакованных систем**
1	Украина	1,33
2	Малайзия	1,31
3	Дания	1,12
4	Республика Корея	1,06
5	Турция	0,88
6	Бразилия	0,85
7	Россия	0,80
8	Румыния	0,67
9	Иран	0,65
10	Австрия	0,65

* При составлении рейтинга мы исключили страны, в которых число наблюдаемых Kaspersky Lab ICS CERT компьютеров АСУ недостаточно для получения репрезентативных данных.



География атак троянцев-шифровальщиков на промышленные системы (процент атакованных компьютеров АСУ в стране)

Наибольшее число атакованных компьютеров АСУ в течение первых шести месяцев 2017 года мы зафиксировали в мае и июне, в ходе эпидемии WannaCry.



Количество уникальных компьютеров АСУ, атакованных троянцами-шифровальщиками первое полугодие 2017

Всего в течение полугодия на компьютерах АСУ были предотвращены атаки представителей 33 семейств шифровальщиков. К счастью, среди них мы не обнаружили ни одной специфической программы, явно нацеленной на блокирование работы ПО для промышленной автоматизации.

По числу атакованных машин по итогам первого полугодия 2017 первое место занял WannaCry – на него пришлось 13,4% от всех атакованных шифровальщиками компьютеров технологической инфраструктуры организаций.

TOP 10 наиболее распространенных семейств троянцев-шифровальщиков первое полугодие 2017

Отметим, что на втором и пятом местах в нашем рейтинге оказались два семейства, которые, по оценкам экспертов Google и ученых Политехнического института Нью-Йоркского университета (NYU Tandom School of Engineering), за последние два года принесли наибольшую прибыль злоумышленникам – Locky и Cerber (соответственно 7,8 миллионов долларов и 6,9 миллионов долларов).

Большинство шифровальщиков из TOP 10 распространяются с использованием замаскированных под деловую переписку спамовых писем с прикрепленными вредоносными загрузчиками или со ссылкой на загрузчик шифровальщика.

Исключение в этом списке составляют WannaCry и ExPetr – вредоносные программы, ставшие самыми известными шифровальщиками первой половины 2017 года. Они продемонстрировали беспрецедентную для этого класса вредоносного ПО скорость распространения и эффективность заражения, чему в немалой степени поспособствовало использование ими эксплойтов Агентства национальной безопасности (АНБ) США, выложенных в открытый доступ хакерской группой The Shadow Brokers в апреле 2017 года (см. выше).

Эпидемия WannaCry

Стремительное распространение WannaCry началось 12 мая и быстро превратилось в настоящую эпидемию, в ходе которой пострадали компьютеры в 150 странах мира.

Среди атакованных WannaCry компаний оказались и компании, занимающиеся различными видами производства, нефтеперерабатывающие заводы, объекты городской инфраструктуры и распределительной энергосети. По данным Kaspersky Security Network, распределение атакованных компаний по индустриям выглядит следующим образом:

Распределение атакованных WannaCry компаний по индустриям
май – июль 2017

Известно о некоторых случаях заражений WannaCry, которые привели к остановкам работы ряда промышленных объектов и объектов социальной значимости.

Концерну Renault пришлось приостановить работу нескольких заводов; по меньшей мере в одном случае была затронута производственная линия завода Nissan; было приостановлено производство на заводе Honda в японском городе Саяма.

Испанское издание El Mundo подтвердило факты заражение WannaCry в испанских промышленных компаниях, в частности Gas Natural (поставщик природного газа) и электроэнергетической Iberdrola.

Из социально значимых объектов от атаки пострадали медицинские учреждения. В частности, в Великобритании сообщалось о затруднениях с доступом к медицинским записям в больницах, в результате чего пришлось отменить ряд операций.

Позже выяснилось, что программное обеспечение некоторых из медицинских устройств также содержит уязвимость CVE-2017-0143 (MS17-010), которую эксплуатировал EternalBlue. В середине мая компания Siemens выпустила Бюллетень по безопасности с рекомендациями для

пользователей систем магнитно-резонансной томографии и многофункциональных диагностических рабочих станций, которые могли быть затронуты в ходе атаки WannaCry.

О многих инцидентах общественности не сообщалось.

Как уже было сказано выше, атакующие использовали один из эксплойтов Агентства национальной безопасности (АНБ) США — модифицированный EternalBlue, эксплуатирующий уязвимость CVE-2017-0143 в компонентах сервиса SMBv1 операционных систем Windows. Патч к соответствующей уязвимости был выпущен Microsoft еще в марте (бюллетень MS17-010), тем не менее, в ходе эпидемии шифровальщика, по оценке Европол, пострадало более 200 тысяч компьютеров.

Для эксплуатации данной уязвимости необходима возможность установки подключения к удалённой машине по портам TCP 139 и 445. Вредоносное ПО выявляло доступные для подключения сетевые порты TCP 445. В случае успешной эксплуатации уязвимости зловред закреплялся в системе и начинал шифровать файлы. Заразив компьютер, WannaCry распространялся по локальной сети, используя для этого тот же эксплойт EternalBlue к уязвимости в компонентах сервиса SMBv1.

Промышленные системы, находящиеся внутри периметра технологической сети, как правило, не имеют прямого подключения к интернету, либо он организован через корпоративную сеть с использованием NAT, межсетевого экрана и корпоративного прокси-сервера, что должно исключать возможность заражения таких систем из интернета. Однако, по нашим данным, по меньшей мере несколько десятков компьютеров, являющихся частью систем управления технологическими процессам промышленных предприятий, были атакованы червем-шифровальщиком WannaCry. В тех случаях, когда компьютеры не были должным образом защищены, произошло заражение, и файлы на инфицированных компьютерах были зашифрованы. Это могло стать причиной остановки или нарушения работы систем автоматизации соответствующих предприятий и нарушения их производственных циклов. Каким же образом сетевой червь мог проникнуть в технологическую сеть?

К заражениям WannaCry приводили типичные ошибки в конфигурации промышленной сети. Мы проанализировали все возможности заражения и пришли к выводу, что в большинстве случаев системы промышленной автоматизации были атакованы вредоносным ПО WannaCry из локальной корпоративной сети предприятия и при подключениях через VPN.

Атака ExPetr (Petya)

Атака ExPetr началась утром 27 июня в России и на Украине и затем перекинулась в Европу, затронула некоторые важные отрасли промышленности и сервисы.

На Украине пострадали энергетические компании, украинские банки, киевский метрополитен, киевский аэропорт Борисполь, аэропорт Харькова, станция, измеряющая уровень радиации на Чернобыльской АЭС. В России примерно в то же время начали появляться сообщения о том, что серверы корпорации «Роснефть» подверглись «мощной хакерской атаке». Позднее стало известно, что в результате атаки шифровальщика пострадали и другие промышленные компании, в частности, и металлургический гигант Евраз, АО «Группа ГМС», в которую входят «Сибнефтемаш» и «ГМС Нефтемаш», а также ПАО «Гипротюменнефтегаз».

Сообщения о заражении стали поступать и из европейских стран. В числе пострадавших оказались фармацевтический гигант Merck and Co., датский логистический гигант Maersk и десятки других жертв, в том числе SaintGobain, крупная промышленная организация во Франции.

Вышла из строя система управления грузопотоком крупнейшего в Индии контейнерного порта имени Джавахарлала Неру, оператором которого является A.P. Moller-Maersk – система перестала распознавать принадлежность грузов.

Мы проанализировали распределение мишеней атак ExPetr (Petya) по индустриям. Согласно данным системы Kaspersky Security Network, на 28 июня по меньшей мере 50% атакованных компаний составляли компании, занятые в производстве и нефтегазовой промышленности.

Распределение мишеней атак ExPetr по индустриям

Для заражения и запуска вредоносной программы на компьютере пользователя злоумышленники использовали механизм обновления сторонней украинской программы для электронного документооборота M.E.Doc. Кроме того, известно о заражении по крайней мере одного веб-сайта, который использовался для перенаправления на вредоносный файл (так называемый watering hole). Это позволяет предположить, что начальный вектор атаки был довольно узким, но механизм распространения по локальной сети позволил шифровальщику «выйти в мир». Для распространения по локальной сети ExPetr использовал эксплойты АНБ США – EternalBlue и EternalRomance. Такой механизм в частности приводил к заражению компьютеров, подключившихся к инфицированной локальной сети по VPN.

Кроме того, вредоносная программа запускала саму себя на удаленных компьютерах локальной сети с помощью инструментария PsExec и WMI, используя учетные данные текущего пользователя, полученные специальной программой наподобие Mimikatz, которая была записана в ресурсы вредоносной программы.

Помимо шифрования данных, ExPetr перезаписывал MBR зараженной машины.

Вымогатели или диверсанты?

Оба шифровальщика, WannaCry и ExPetr, относятся к классу программ-вымогателей (Ransomware). За каждым из них стоят две совершенно разные группы атакующих. Обе группы, по-видимому, были способны получить огромные суммы денег в результате успешных атак программ-вымогателей. Но по разным причинам не получили.

ExPetr, строго говоря, вымогателем не является. Исследователи довольно быстро выяснили, что из-за ошибок в коде возможности расшифровать файлы не имеют даже сами атакующие. Таким образом, этот троянец относится к вредоносному ПО, уничтожающему информацию, т.е. к классу Wiper. Вероятно, истинной целью атак ExPetr было вовсе не получение выкупа, запрос выкупа мог быть всего лишь эффективным прикрытием для актов саботажа.

Что касается WannaCry, то некоторые эксперты предполагают, что и в этом случае для атакующих деньги были не главным результатом атаки. Учитывая огромное количество зараженных компьютеров, барыши атакующих были скудными. И по сравнению с другими участниками киберкриминального бизнеса с использованием вымогателей хозяева WannaCry не проявили особой заинтересованности в том, чтобы исправить ситуацию.

Специалисты «Лаборатории Касперского» считают, что активное распространение вредоносных программ-шифровальщиков продолжится. Все больше авторов таких троянцев распространяют свои продукты, используя модель SaaS (software as a service). Это дает возможность промышлять кибервымогательством тем злоумышленникам, у которых не хватает навыков, ресурсов или желания разрабатывать свои собственные зловреды. Количество разнокалиберных игроков на этом поле растет.

Промышленные компании становятся мишенями атак шифровальщиков наряду с остальными организациями. Случаи целевых атак с использованием программ-вымогателей на промышленные компании с целью получения выкупа достоверно неизвестны – пока что мишенями таких атак становятся в основном финансовые организации. Нам не встречались «в дикой природе» шифровальщики, явно нацеленные на блокирование работы ПО для промышленной автоматизации. Таким образом, зафиксированные нами случаи попыток заражения шифровальщиками компьютеров инфраструктуры промышленных сетей относятся к категории не целевых, а случайных заражений.

Беда в том, что даже случайное заражение вредоносной программой-шифровальщиком компьютеров в промышленной сети может привести к остановке или нарушению работы систем автоматизации атакованных предприятий и нарушению их производственных циклов.

Статистика угроз

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их анонимную передачу.

Методология

Данные получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky Lab ICS CERT относит к технологической инфраструктуре организаций. В эту группу входят компьютеры, работающие на операционных системах Windows и выполняющие одну или несколько функций:

- серверы управления и сбора данных (SCADA),
- серверы хранения данных (Historian),
- шлюзы данных (OPC),
- стационарные рабочие станции инженеров и операторов,
- мобильные рабочие станции инженеров и операторов,
- Human Machine Interface (HMI).

А также компьютеры сотрудников подрядных организаций, компьютеры администраторов технологических сетей и разработчиков ПО для систем промышленной автоматизации.

Атакованными мы считаем те компьютеры, на которых в течение отчетного периода хотя бы один раз сработали наши защитные решения. При подсчете процента атакованных машин используется количество *уникальных* атакованных компьютеров по отношению ко всем компьютерам из нашей выборки, с которых в течение отчетного периода мы получали обезличенную информацию.

Отметим, что ограничения доступа в интернет у компьютеров в технологической сети и компьютеров, составляющих инфраструктуру технологической сети, могут значительно отличаться.

Серверы АСУ ТП и стационарные компьютеры инженеров и операторов часто не имеют постоянного прямого выхода в интернет из-за ограничений технологической сети. Доступ в интернет им может быть открыт, например, на время технологического обслуживания.

Компьютеры системных/сетевых администраторов, разработчиков и интеграторов систем промышленной автоматизации, а также компьютеры подрядчиков, которые подключаются к технологической сети (например, с целью мониторинга состояния и оказания технической поддержки), могут иметь частые или даже перманентные подключения к интернету.

Как следствие, в нашей выборке компьютеров, которые Kaspersky Lab ICS CERT относит к технологической инфраструктуре организаций, регулярно или постоянно подключаются к интернету около 40% машин. Остальные подключаются к интернету не чаще, а многие реже, чем раз в месяц.

Процент атакованных компьютеров

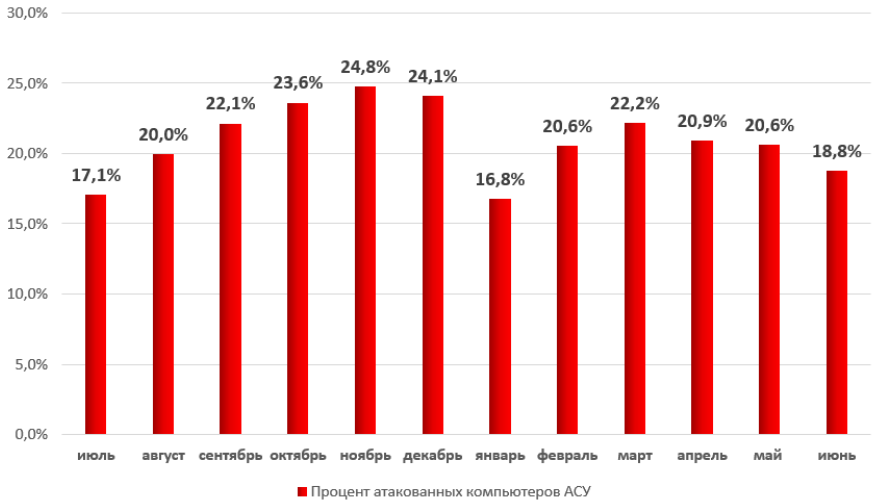
В течение первого полугодия 2017 года продуктами «Лаборатории Касперского» во всем мире были предотвращены попытки атак на **37,6%** защищаемых ими компьютеров АСУ – на 1,6 п.п. меньше, чем во втором полугодии 2016 года.

В России этот показатель составил **42,9**% – на 0,5 п.п. больше, чем в предыдущем полугодии (42,4%).

Около трети всех атак пришлось на компьютеры АСУ в компаниях, занимающихся производством различных материалов, оборудования и товаров.

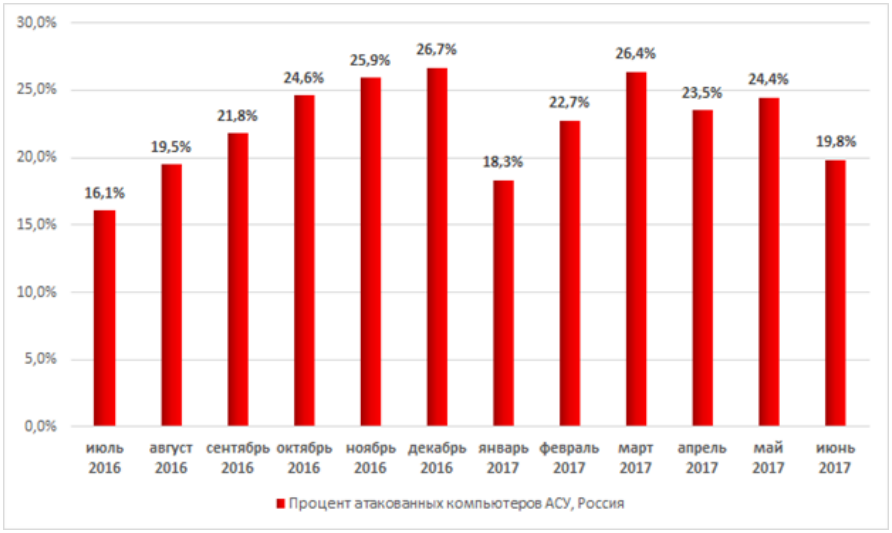
Распределение атакованных компьютеров АСУ по индустриям первое полугодие 2017

Если во втором полугодии 2016 года доля атакованных машин росла из месяца в месяц, то в первые шесть месяцев 2017 года динамика была несколько иной. Мы зафиксировали уменьшение активности злоумышленников в январе, возврат доли атакованных компьютеров на прежний уровень в феврале – марте и постепенное снижение этого показателя в апреле – июне.



Процент атакованных компьютеров АСУ по месяцам в мире
июль 2016 – июнь 2017

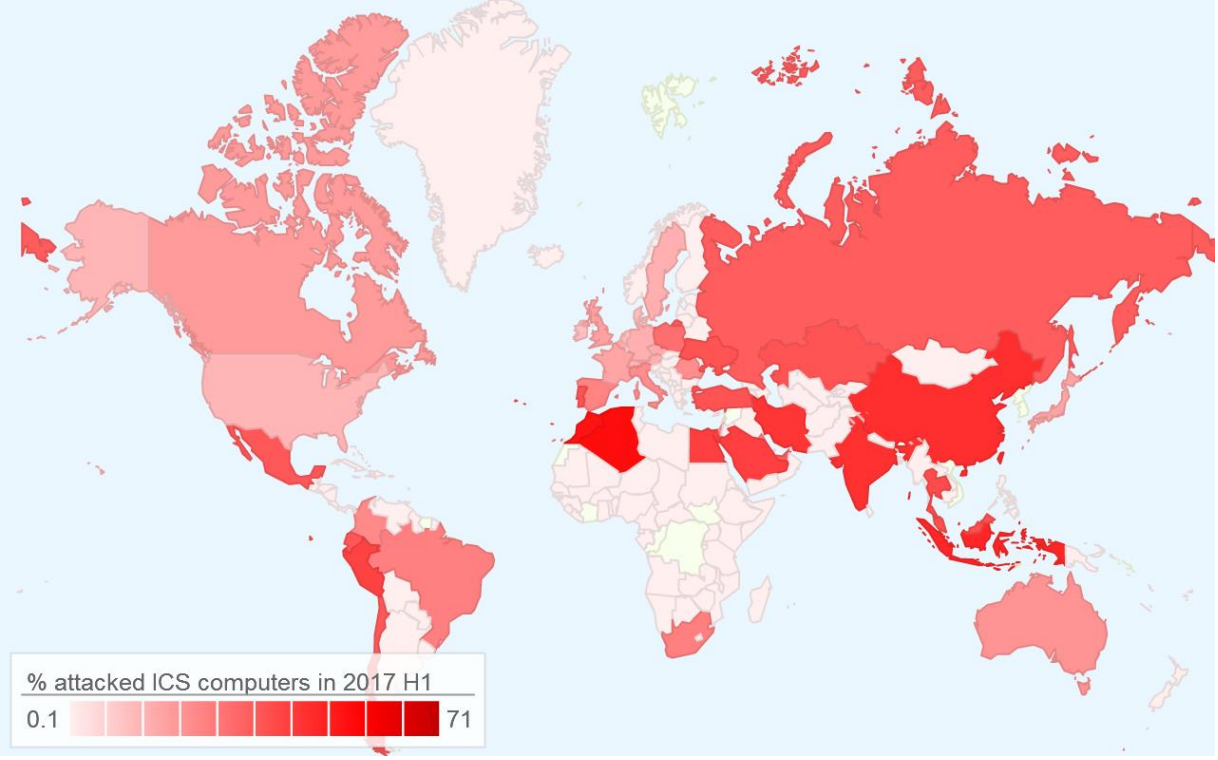
В России мы наблюдали схожую динамику:



Процент атакованных компьютеров АСУ по месяцам в России
июль 2016 – июнь 2017

География атак на системы промышленной автоматизации

На карте ниже отражен процент атакованных систем промышленной автоматизации в каждой стране по отношению к общему количеству таких систем в стране. Наименьшие показатели – в Ирландии (13,8%), Дании (14,1%), Нидерландах (15,5%), США (17,1%) и в Швейцарии (17,4%).



География атак на системы промышленной автоматизации, первое полугодие 2017

ТОР 15 стран по проценту атакованных компьютеров АСУ:

	Страна*	% атакованных систем
1	Вьетнам	71,0
2	Алжир	67,1
3	Марокко	65,4
4	Индонезия	58,7
5	Китай	57,1
6	Индия	56,0
7	Иран	55,3
8	Саудовская Аравия	51,8
9	Египет	51,6
10	Перу	50,8
11	Таиланд	47,8
12	Малайзия	47,2
13	Украина	46,3
14	Португалия	46,1
15	Казахстан	45,9

* При расчетах мы исключили страны, в которых число наблюдаемых Kaspersky Lab ICS CERT систем промышленной автоматизации недостаточно для получения репрезентативных данных.

Россия в этом рейтинге занимает 21-е место.

Вредоносное ПО на системах промышленной автоматизации

По сценариям использования и по применяемым технологиям технологическая сеть все больше становится похожей на корпоративную. Закономерно, что и ландшафт угроз промышленных информационных систем становится похожим на ландшафт угроз корпоративных систем.

В первом полугодии 2017 года на системах промышленной автоматизации было обнаружено около 18 тысяч различных модификаций вредоносного ПО, относящихся более чем к 2,5 тысячам различных семейств.

В подавляющем большинстве случаев попытки заражения компьютеров АСУ носят случайный характер, а функции, заложенные во вредоносное ПО, не являются специфичными для атак на системы промышленной автоматизации.

Для компьютеров АСУ актуальны те же категории программ, которые атакуют корпоративные компьютеры. Среди них – троянцы-шпионы (Trojan-Spy и Trojan-PSW), программы-вымогатели (Trojan-Ransom), бэкдоры (Backdoor) и программы типа Wiper (KillDisk), выводящие из строя компьютер и затирающие данные на диске. Такие программы представляют особую опасность для компьютеров в промышленной сети, заражения ими могут приводить к потере контроля или к нарушению технологических процессов.

Источники заражения систем промышленной автоматизации

Основные источники угроз, заблокированных на компьютерах АСУ первое полугодие 2017

Загрузка вредоносного ПО из интернета и доступ к известным вредоносным и фишинговым веб-ресурсам в первом полугодии 2017 года были заблокированы на 20,4% компьютеров АСУ. В России этот показатель составил 25%.

Интернет остается основным источником заражения компьютеров технологической инфраструктуры организаций. Этому способствует сопряжение корпоративной и технологической сетей, наличие

ограниченного доступа к интернету из технологической сети, подключение к интернету компьютеров из технологической сети через сети мобильных операторов (с помощью мобильных телефонов, USB модемов и/или Wi-Fi роутеров с поддержкой 3G/LTE). Что касается подрядчиков, разработчиков, интеграторов, системных/сетевых администраторов, которые подключаются к технологической сети извне (напрямую или удаленно), то они часто имеют свободный доступ к интернету. Их компьютеры входят в группу наибольшего риска и могут стать каналом проникновения вредоносного ПО в технологические сети обслуживаемых ими предприятий. Напомним, что в нашей выборке регулярно подключаются к интернету около 40% всех компьютеров.

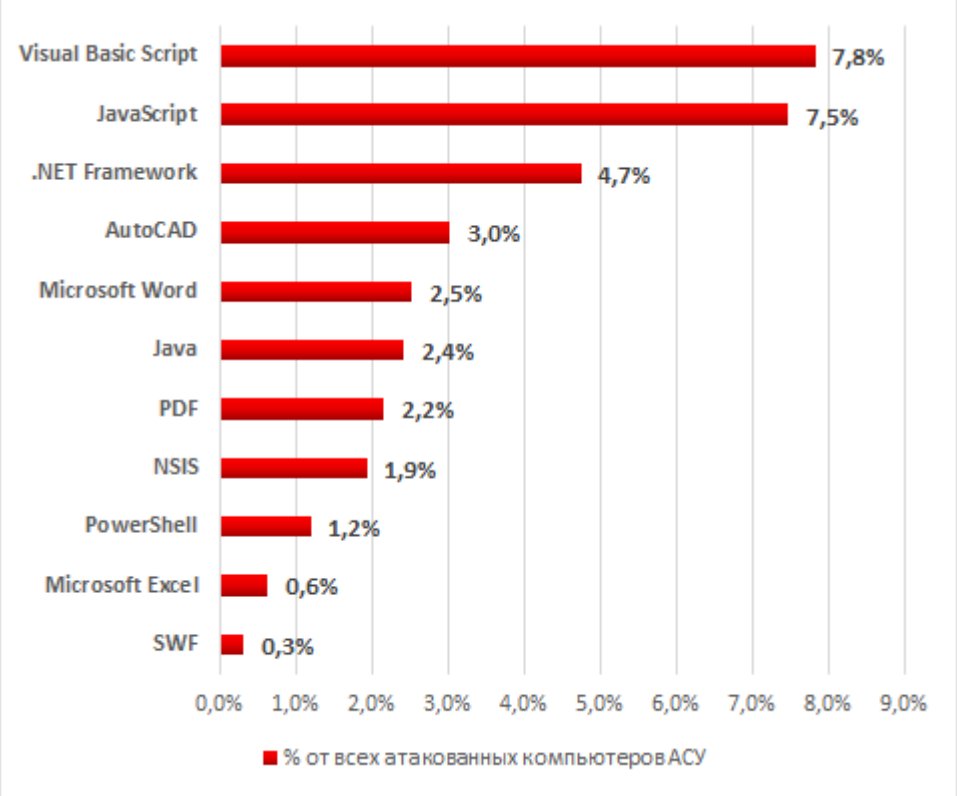
На 9,6% компьютеров АСУ вредоносное ПО было обнаружено при подключении к ним съемных носителей информации. Зловреды, которые распространяются через съемные носители и сетевые папки, часто заражают легитимные файлы или используют имена, схожие с именами легитимных файлов (так ведут себя, в частности, многие вирусы и черви). Вредоносные файлы с именами легитимных файлов могут попадать в созданные пользователем защищенные архивы данных (мы обнаружили их на 0,8% компьютеров) и в резервные копии файловой системы в процессе их создания операционной системой (также 0,8%).

Вредоносные почтовые вложения и вредоносные скрипты, встраиваемые в тело электронных писем, были заблокированы на 3,9% компьютеров АСУ. В нашем рейтинге почтовые клиенты заняли третье место. В большинстве случаев злоумышленники распространяют письма с вредоносными вложениями в формате офисных документов, таких как MS Office и PDF.

На 0,1% компьютеров АСУ вредоносное ПО было обнаружено в локальных папках облачных файловых хранилищ, которые автоматически синхронизируются с облачным хранилищем при подключении компьютера к интернету. Такая синхронизация приводит к тому, что при заражении облачного хранилища (с любого имеющего к нему доступ компьютера) вредоносные файлы автоматически доставляются на все подключенные к хранилищу устройства.

Платформы, используемые вредоносным ПО

На более чем 50% всех атакованных компьютеров были заблокированы вредоносные программы, которые являются исполняемыми файлами ОС Windows (Win32/Win 64). Часто злоумышленники вместо разработки исполняемого файла реализуют вредоносный функционал на одном из скриптовых языков, который выполняется интерпретаторами, уже имеющимися на компьютере предполагаемой жертвы. Рейтинг основных платформ, которые вредоносное ПО использует помимо Windows, представлен ниже.



Платформы, используемые вредоносным ПО
первое полугодие 2017

Отметим, что злоумышленники активно используют небольшие загрузчики, написанные на JavaScript, Visual Basic Script и Powershell, которые запускают в виде параметров командной строки для соответствующих интерпретаторов.

Наши рекомендации

Для предотвращения случайных заражений и для защиты от целенаправленных атак на технологические сети мы рекомендуем принять ряд мер по обеспечению безопасности внешнего и внутреннего периметров технологической сети.

В первую очередь, для организации безопасного удаленного управления системами автоматизации и передачи данных между технологической и другими сетями необходимо максимально ограничить доступ между системами, находящимися в различных сетях или имеющими различные уровни доверия:

- Системы, имеющие постоянную или регулярную связь с внешними сетями (мобильные устройства, VPN-концентраторы, терминальные серверы и пр.) необходимо изолировать в отдельный сегмент внутри технологической сети — демилитаризованную зону (DMZ);
- Системы в демилитаризованной зоне разделить на подсети или виртуальные подсети (VLAN) и разграничить доступ между подсетями (разрешить только необходимые коммуникации);
- Весь необходимый обмен информацией между промышленной сетью и внешним миром осуществлять через DMZ;
- При необходимости в DMZ можно развернуть терминальные серверы, позволяющие использовать методы обратного подключения (из технологической сети в DMZ).
- Для доступа к технологической сети извне желательно использовать тонкие клиенты (применяя методы обратного подключения);
- По возможности не разрешать доступ из демилитаризованной зоны в технологическую сеть;
- Если бизнес-процессы предприятия допускают возможность однонаправленных коммуникаций, рекомендуем рассмотреть возможность использования дата-диодов.

Следует иметь в виду, что ландшафт угроз для систем промышленной автоматизации постоянно меняется, новые уязвимости регулярно находят как в прикладном, так и в промышленном ПО.

Для обеспечения защиты от неизвестных, в том числе целенаправленных, угроз мы рекомендуем:

1. Провести инвентаризацию запущенных сетевых служб; по возможности остановить уязвимые сетевые службы (если это не нанесёт ущерба непрерывности технологического процесса) и остальные службы, не требующиеся для непосредственного функционирования системы автоматизации; особое внимание обратить на службы предоставления удалённого доступа к объектам файловой системы, такие как SMB/CIFS и/или NFS (актуально в случае атак с использованием уязвимостей в Linux).
2. Провести аудит разграничения доступа к компонентам АСУ ТП; постараться добиться максимальной гранулярности доступа.
3. Провести аудит сетевой активности внутри промышленной сети предприятия и на её границах. Устранить не обусловленные производственной необходимостью сетевые соединения с внешними и другими смежными информационными сетями.

4. Проверить безопасность организации удалённого доступа к промышленной сети; обратить особое внимание на соответствие организации демилитаризованных зон требованиям информационной безопасности. По возможности минимизировать или вовсе избежать использования средств удалённого администрирования (таких, как RDP или TeamViewer).
5. Следить за актуальностью сигнатурных баз, эвристик, решающих алгоритмов средств защиты конечных узлов сети. Убедиться, что все основные компоненты защиты включены и функционируют, а из области защиты не исключены каталоги ПО АСУ ТП. Большую эффективность на промышленных предприятиях демонстрируют технологии контроля запуска приложений, настроенные в режиме «белых списков», и технологии анализа поведения приложений. Контроль запуска приложений не позволит запустить шифровальщик в случае его проникновения на компьютер. Технологии анализа поведения приложений полезны для обнаружения и предотвращения попыток эксплуатации уязвимостей (в том числе неизвестных) в легитимном ПО.
6. Провести аудит политики и практики использования съёмных носителей информации и портативных устройств. Не допускать подключения к узлам промышленной сети устройств, предоставляющих нелегитимный доступ к внешним сетям и интернету. По возможности отключить соответствующие порты или контролировать доступ к ним правильно настроенными специальными средствами.
7. Внедрить средства мониторинга сетевого трафика и обнаружения компьютерных атак в индустриальных сетях. В большинстве случаев применение подобных мер не требует внесения изменения в состав и конфигурацию средств АСУ ТП и может быть произведено без остановки их работы.

Конечно, полностью изолировать технологическую сеть от смежных сетей практически невозможно, поскольку передача данных между сетями необходима для выполнения множества важных функций — управления и поддержки удаленных объектов, координации работы сложного технологического процесса, части которого распределены между множеством цехов, линий, установок и систем обеспечения. Но мы надеемся, что наши рекомендации помогут максимально защитить технологические сети и системы промышленной автоматизации от современных и будущих угроз.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky Lab ICS CERT **Ics-cert@kaspersky.com**