Kaspersky Lab ICS CERT

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2018

06.09.2018 Version 1.1

Оглавление

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

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 2018 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.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Основные события полугодия

Уязвимости Spectre и Meltdown в промышленных решениях

В начале 2018 года в процессорах Intel, ARM64 и AMD были обнаружены уязвимости, позволяющие получить несанкционированный доступ к содержимому виртуальной памяти. Атаки, использующие эти уязвимости, были названы Meltdown и Spectre.

Выявленная проблема связана с тремя уязвимостями:

- обход проверки границ (CVE-2017-5753/Spectre);
- манипуляция целевым кэшем адресов ветвлений (CVE-2017-5715/Spectre);
- оседание данных в кэше после отмены операции (CVE-2017-5754/Meltdown).

Атаки Spectre позволяют пользовательскому приложению получить данные другой программы, Meltdown — также содержимое памяти ядра.

Данная проблема затронула множество компьютеров, серверов и мобильных устройств под управлением операционных систем Windows, macOS, Linux, Android, iOS и Chrome OS, использующих уязвимые микропроцессоры. Промышленное оборудование – серверы SCADA, промышленные компьютеры и сетевые устройства с уязвимыми процессорами – также оказалось подвержено уязвимостям Meltdown и Spectre.

Одной из первых об уязвимостях своих продуктов заявила компания Cisco. Среди затронутых устройств — маршрутизаторы Cisco 800 Industrial Integrated Services и коммутаторы Industrial Ethernet 4000.

Затем уведомления о влиянии уязвимостей Meltdown и Spectre на свои продукты опубликовали другие промышленные вендоры.

Об уязвимости десятков своих продуктов, включая системы управления, различные промышленные компьютеры и HMI, проинформировала своих клиентов PHOENIX CONTACT.

Уязвимости Meltdown и Spectre затронули также промышленное оборудование Siemens: устройства RUGGEDCOM APE и RX1400 VPE, панели оператора SIMATIC HMI серии Comfort, промышленные компьютеры SIMATIC IPC, программируемый логический контроллер SIMATIC S7-1500 Software Controller и другие.

Помимо информации об уязвимостях Meltdown и Spectre компания Siemens сообщила о подверженности своих решений еще двум брешам из группы уязвимостей под названием Spectre Next Generation (Spectre-NG), которые были обнаружены позднее в мае 2018 года.

Информацию об использовании уязвимых процессоров в своих продуктах опубликовали также Schneider Electric, ABB, OSIsoft и другие вендоры.

Energetic Bear / Crouching Yeti: атаки на серверы

В феврале Kaspersky Lab ICS CERT опубликовал отчет об исследовании тактики первоначального заражения, используемой широко известной APT-группировкой Energetic Bear/Crouching Yeti, и результаты анализа нескольких веб-серверов, скомпрометированных группой в течение 2016 — в начале 2017 года, предоставленных нам для исследования их владельцами.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Группировка действует по крайней мере с 2010 года и атакует организации и частных лиц в разных странах мира. Первоначально исследователи CrowdStrike обнаружили фокус на энергетику и промышленность, чем, вероятно, обусловлено название «EnergeticBear». Впоследствии, когда были выявлены более широкие интересы группировки, исследователи «Лаборатории Касперского» дали ей имя Crouching Yeti. Среди мишеней атакующих преобладают компании в Европе и в США, а в последние годы значительно выросло количество атак на компании в Турции. По утверждениям US-CERT и Национального центра кибербезопасности Великобритании (UK National Cyber Security Centre), APT-группировка Energetic Bear/Crouching Yeti связана с российским правительством.

Типичная тактика первоначального заражения, используемая группой, представляет собой многоходовую комбинацию, начинающуюся с рассылку фишинговых писем с вредоносными документами и заражения различных серверов. Некоторые зараженные серверы используются группой как вспомогательные — только для размещения различного инструментария. Другие заражаются для того, чтобы использовать их в watering hole-атаках – на одних серверах размещалась SMB-ссылка, которая вела на другие серверы, осуществлявшие кражу данных аутентификации потенциальных жертв.

За редкими исключениями для проведения атак группировка Energetic Bear/Crouching Yeti использует публичный инструментарий. Все используемые злоумышленниками утилиты, которые обнаружили эксперты Kaspersky Lab ICS CERT, имеют открытый исходный код, находящийся в свободном доступе на GitHub. Такая тактика делает задачу атрибуции атак Energetic Bear/Crouching Yeti весьма сложной без дополнительных «маркеров» группы.

В большинстве наблюдаемых Kaspersky Lab ICS CERT случаев атакующие выполняли задачи по поиску уязвимостей, закреплению на различных узлах и краже данных аутентификации для обеспечения возможности дальнейшего развития атаки.

Результаты анализа скомпрометированных серверов и действий на них атакующих показали, что для Energetic Bear/Crouching Yeti практически любой уязвимый сервер в интернете может представлять интерес в качестве «плацдарма» для развития дальнейших атак на целевые объекты.

Также весьма разнообразной оказалась география первоначальных, промежуточных и последующих целей исследованной серии атак группировки. Наибольшее количество жертв и целей оказалось в России, на втором месте – Турция и Украина. Менее половины атакованных систем имело отношение к промышленности, сельскому и коммунальному хозяйству.

Криптомайнеры в промышленных сетях

В феврале 2018 года в СМИ появилось сразу несколько сообщений о заражении промышленных предприятий вредоносным программным обеспечением с функцией майнинга криптовалюты.

В одной из водоочистных станций в Европе зараженными оказались четыре сервера под управлением операционной системы Windows XP с программным обеспечением CIMPLICITY SCADA от компании GE Digital. Вредоносное ПО замедляло работу HMI и SCADA-серверов, используемых для мониторинга технологических процессов.

Также атаке подверглись облачные серверы компании Tesla с целью использования части их мощностей для добычи криптовалюты Monero. Киберпреступники атаковали

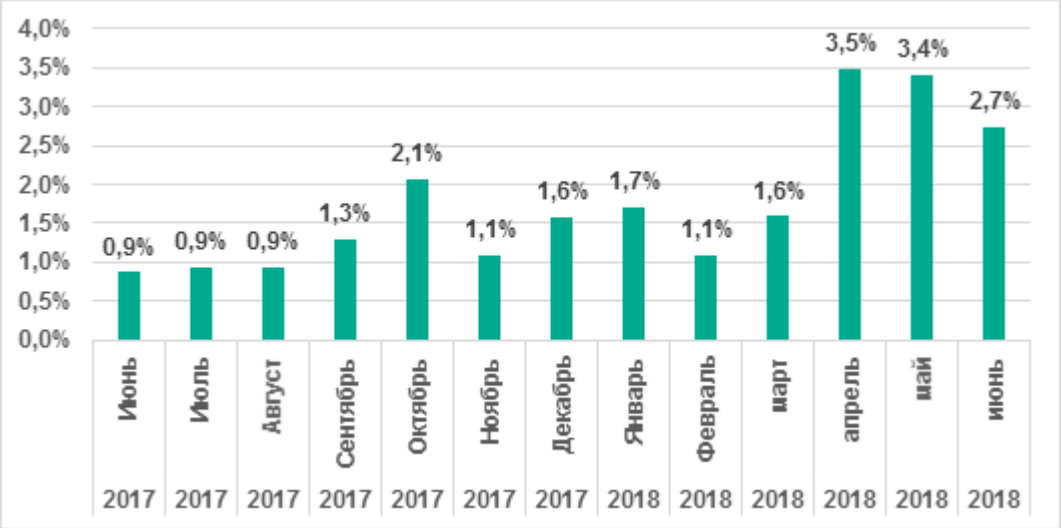
© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

фреймворк Kubernetes, который эксплуатируется в инфраструктуре ведущего производителя электромобилей, и внедрили в него вредоносное ПО для генерации криптовалюты.

По данным KL ICS CERT эти широко обсуждаемые инциденты – далеко не единичны и отражают общую неутешительную тенденцию.

С апреля 2018 года в «Лаборатории Касперского» начали использовать более точные вердикты для сбора статистики о майнерах. Как следствие, по нашей статистике процент компьютеров АСУ, атакованных вредоносными программами для майнинга криптовалют, с апреля резко вырос и по итогам первого полугодия 2018 года достиг 6% – это на 4,2 п.п. больше, чем в предыдущем полугодии.

Доля компьютеров АСУ, атакованных вредоносными программами для майнинга криптовалют



Основная проблема, связанная с работой вредоносных программ-майнеров, заключается в увеличении нагрузки на промышленные информационные системы, что может оказаться неприемлемым для систем промышленной автоматизации – угрожать стабильности их функционирования и снижать уровень контроля за технологическим процессом предприятия.

Массовые атаки на коммутаторы Cisco затронули объекты критической инфраструктуры

6 апреля по всему миру были зафиксированы массовые атаки на коммутаторы Cisco IOS. Атаки привели к сбою в работе некоторых интернет-провайдеров, дата-центров и веб-сайтов.

Злоумышленники использовали уязвимость CVE-2018-0171 в программном обеспечении Cisco Smart Install Client. По результатам исследований команды Cisco Talos, в мире насчитывается более 168 000 потенциально подверженных ей устройств.

Для атаки использовался специальный бот, который обнаруживает уязвимые устройства, перезаписывает на них образ системы Cisco IOS и меняет конфигурационный файл. В результате этого устройство становится недоступным.

В основном атакам подверглись организации России и Ирана. По данным Cisco Talos, среди компаний, подвергшихся атакам, оказались и объекты критической инфраструктуры.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Новое вредоносное ПО VPNFilter с функцией мониторинга SCADA

В мае 2018 года было обнаружено новое вредоносное ПО VPNFilter, которое заразило не менее 500 тысяч маршрутизаторов и устройств хранения данных (NAS) в 54 странах мира.

Вредоносная программа VPNFilter имеет сложную модульную архитектуру, компоненты которой реализуют различные функции, среди которых сбор сетевого трафика и данных, выполнение команд и управление устройством, перехват пакетов, а также мониторинг протоколов Modbus и взаимодействие с управляющим сервером через сеть Tor.

Для инфицирования зловред использует различные известные уязвимости, однако вектор заражения на данный момент не ясен. При заражении на устройство устанавливается устойчивый к перезагрузке устройства компонент, способный загружать дополнительные вредоносные модули.

Таким образом, VPNFilter требует пристального внимания ИБ-сообщества, так как этот зловред может быть использован для кражи учетных данных, обнаружения промышленного SCADA-оборудования, а также проведения различных атак с использованием зараженных устройств в составе ботнета.

Атака на спутниковые системы

В июне 2018 года стало известно о масштабной кибератаке с территории Китая на телекоммуникационные предприятия, операторов спутников связи, а также оборонных подрядчиков в США и странах Юго-Восточной Азии.

В ходе атаки злоумышленники инфицировали компьютеры, используемые для управления спутниками связи и сбора данных геопозиций. По мнению экспертов, целью кибератаки были шпионаж и перехват данных из гражданских и военных каналов связи. Однако потенциально атака могла привести к несанкционированному изменению позиций устройств на орбите и помехам при обмене данными.

Среди обнаруженных зловредов — троянцы Rikamanu и Syndicasec, программа для похищения данных Catchamas, кейлоггер Mycicil и бэкдор Spedear.

Для заражения вредоносным ПО злоумышленники использовали легитимные инструменты и средства администрирования PsExec, Mimikatz, WinSCP и LogMeIn. Такая тактика позволяет атакующим скрывать свою активность и оставаться незамеченными.

Важные исследования: подробности о вредоносном ПО Triton

В конце первого полугодия 2018 стали известны подробности о вредоносном ПО TRITON, которое вызвало сбой в работе системы противоаварийной защиты предприятия, атакованного в декабре прошлого года.

Вредоносное ПО Triton создано специально для вмешательства в работу систем противоаварийной защиты Triconex Safety Instrumented System (SIS) от Schneider Electric. Известно, что для удалённого взаимодействия с Triconex при помощи среды программирования TriStation 1131 используется закрытый сетевой протокол TriStation.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Анализ вредоносного ПО показал существенное совпадение во вредоносной программе и в программном файле TriStation tr1com40.dll специфичных строк, таких как, например, мнемонические названия команд протокола TriStation. Из чего исследователи сделали вывод, что для реализации сетевого взаимодействия с Triconex разработчики Triton, по всей видимости, осуществили обратную разработку исполняемых файлов из состава TriStation 1131.

Активность IoT-ботнетов

С начала года наблюдается активный рост числа новых ботнетов из IoT-устройств, что подтверждает прогнозы экспертов о заметном увеличении числа IoT- зомби-сетей в 2018 году.

Наиболее значимыми событиями с точки зрения информационной безопасности Интернета вещей стало появление нового ботнета Hide 'N Seek (HNS), а также обнаружение новых модификаций зловреда Mirai – вредоносного ПО OMG и WICKED.

Обнаруженные ботнеты по-прежнему состоят преимущественно из незащищенных IP-камер и маршрутизаторов. Однако постепенно злоумышленники начинают использовать другие типы «умных устройств». Так, в апреле 2018 года был обнаружен ботнет, состоящий, в том числе из интернет-телевизоров. Этот ботнет использовался для осуществления DDoS-атак на организации финансового сектора.

В условиях столь бурного развития вредоносного ПО, нацеленного на устройства Интернета вещей, существенным стало известие о появлении общедоступного инструмента для автоматического поиска и взлома уязвимых IoT-устройств. Публикация таких программ в открытом доступе может значительно расширить круг злоумышленников, использующих IoT-устройства для атак на компьютерные системы и сети.

Атаки программ-вымогателей

Несмотря на глобальное уменьшение количества пользователей, атакованных программами-вымогателями, процент компьютеров АСУ, на котором были заблокированы атаки вымогателей, вырос – с 1,2% до 1,6%. Хотя этот показатель и кажется не очень значительным, опасность такого рода вредоносных программ для промышленных предприятий трудно недооценивать после WannaCry и ExPetr.

В первом полугодии вымогатели напомнили о себе опасной ситуацией, возникшей в медицинском учреждении в результате заражения вредоносным шифровальщиком. Согласно сообщениям СМИ, злоумышленники атаковали Федеральный центр нейрохирургии в городе Тюмень. В ходе атаки злоумышленникам удалось получить доступ к серверам, на которых располагались компоненты медицинской информационной системы "МЕДИАЛОГ", используемой в качестве базы данных для снимков, результатов анализов и другой информации, необходимой в процессе лечения пациентов.

В результате в тот момент, когда необходимо было начать экстренную операцию на головном мозге 13-летней пациентки, обнаружилось, что система "МЕДИАЛОГ" недоступна – как позже выяснилось, из-за того, что файлы, необходимые для работы сервисов, были зашифрованы вредоносной программой. К счастью, медикам удалось успешно провести операцию, несмотря на потерю доступа к значимой информации о результатах диагностики.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Центр нейрохирургии в Тюмени оказался не единственной жертвой данной серии атак. Установлено, что злоумышленники целенаправленно атаковали именно медицинские учреждения, при этом шифрованию подверглись исключительно файлы, находящиеся на серверах, которые обеспечивают работу сервисов, критически важных для работы организации. Это говорит о намерении причинить как можно больший ущерб рабочим процессам медицинской организации.

Эта серия атак является ярким примером того, что злоумышленники могут не просто выводить из строя компьютерные системы медицинских учреждений, но и оказывать непосредственное влияние на процесс лечения пациентов.

Атаки на промышленные предприятия с использованием RAT

Фишинговые атаки с использованием RMS и TeamViewer

Kaspersky Lab ICS CERT рассказал об очередной волне рассылок фишинговых писем с вредоносными вложениями, нацеленных преимущественно на промышленные компании в России. Вредоносная программа, используемая в атаках, устанавливает в систему легитимное ПО для удаленного администрирования TeamViewer или Remote Manipulator System/Remote Utilities (RMS), которое позволяет злоумышленникам получать удаленный контроль над атакованными системами. Используются различные техники, позволяющие скрыть присутствие и активность нелегитимно установленного ПО.

При необходимости дальнейшего продвижения внутри сети скомпрометированной организации злоумышленники могут загружать дополнительный набор вредоносного ПО с учетом особенности атаки на каждую жертву. Такой набор может содержать шпионские программы (Spyware), дополнительные утилиты удаленного администрирования, вредоносное ПО для эксплуатации уязвимостей в ОС и прикладном ПО, а также утилиту Mimikatz, позволяющую получить данные аккаунтов учетных записей Windows.

Фишинговые письма замаскированы под легитимные коммерческие предложения, их содержание соответствует деятельности атакуемой организации и учитывает специфику работы сотрудника — получателя письма. По имеющимся данным, основной целью атакующих является кража денежных средств со счетов организации. Очевидно, что, помимо финансовых потерь, данные атаки приводят к утечке конфиденциальных данных организации.

Отчет был опубликован в начале августа, однако эта серия атак длится с ноября 2017 года.

Атаки с использованием RAT в технологической сети компании

Продуктами «Лаборатории Касперского» были предотвращены множественные попытки атак, направленные на технологическую сеть автомобилестроительной/сервисной компании, в частности – на компьютеры, предназначенные для диагностики двигателей и бортовых систем грузовиков и тяжелой техники.

По меньшей мере на одном из компьютеров в технологической сети компании был установлен и периодически использовался RAT. В течение нескольких месяцев на этом компьютере было заблокировано множество попыток запуска различных вредоносных программ, запускаемых через RAT. Среди прочих были заблокированы модификации вредоносного ПО, детектируемого продуктами «Лаборатории Касперского» как Net-Worm.Win32.Agent.pm. Примечательно, что в случае запуска данный червь

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

незамедлительно начинает распространение по локальной сети, используя эксплойты для уязвимостей MS17-010 – те самые, которые были опубликованы ShadowBrokers весной 2017 года и использовались в атаках нашумевших шифровальщиков WannaCry и ExPetr.

Помимо этого было заблокировано вредоносное ПО семейства Nymaim. Представители этого семейства часто являются загрузчиками модификаций ботнет-агента семейства Necus, который, в свою очередь, часто используется для заражения компьютеров вымогателями семейства Locky.

Основываясь на периодичности попыток запуска вредоносного ПО через RAT и других данных, мы полагаем, что данные аутентификации RAT были скомпрометированы и использовались злоумышленниками для атаки на компьютеры этой организации из интернета.

Наличие программ для удаленного администрирования (RAT) на компьютерах АСУ иногда является производственной необходимостью, однако они становятся очень опасными, если используются злоумышленниками или попадают под их контроль. Мы провели специальное исследование этой проблемы, результаты которого опубликуем в ближайшее время.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

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. В силу ограничений продукта и законодательных ограничений мы не идентифицируем конкретную компанию/организацию, от которой KSN получает статистические данные.

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).

Кроме того, в статистику включены данные, полученные с компьютеров 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.

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, инженеров, разработчиков и интеграторов систем промышленной автоматизации могут иметь частые или даже перманентные подключения к интернету.

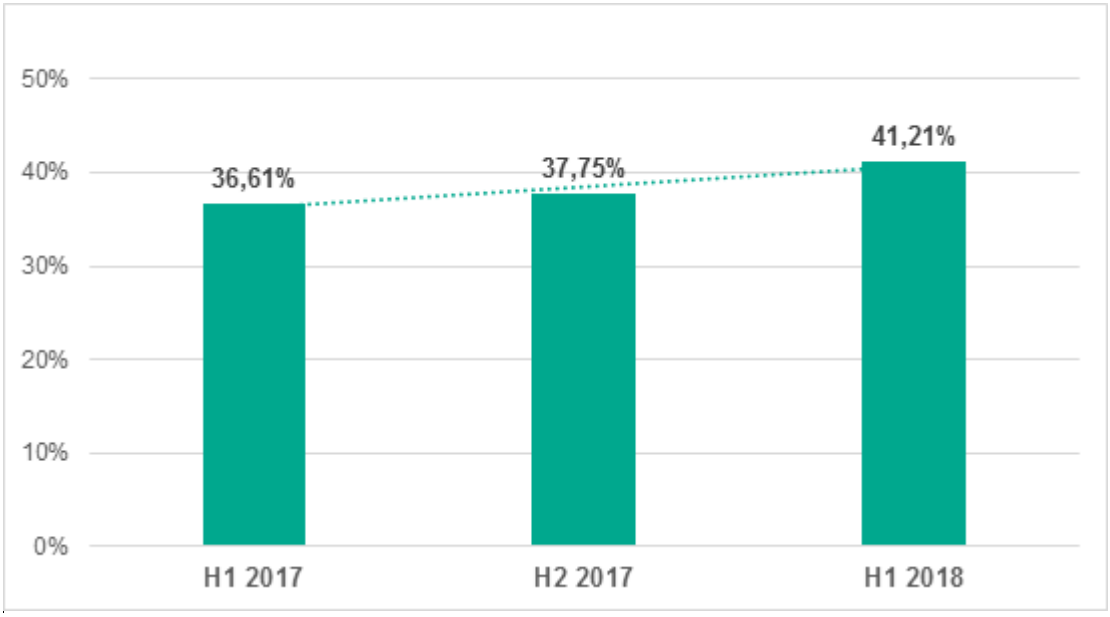
Как следствие, в нашей выборке компьютеров, которые Kaspersky Lab ICS CERT относит к технологической инфраструктуре организаций, в первом полугодии 2018 года регулярно или постоянно подключались к интернету 42% машин. Остальные – не чаще, а многие значительно реже, чем раз в месяц.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Процент атакованных компьютеров АСУ

Доля атакованных компьютеров АСУ в первом полугодии 2018 в мире выросла на 3,5 п.п. и составила **41,2%.** За год этот показатель увеличился на 4,6 п.п.

Процент атакованных компьютеров АСУ

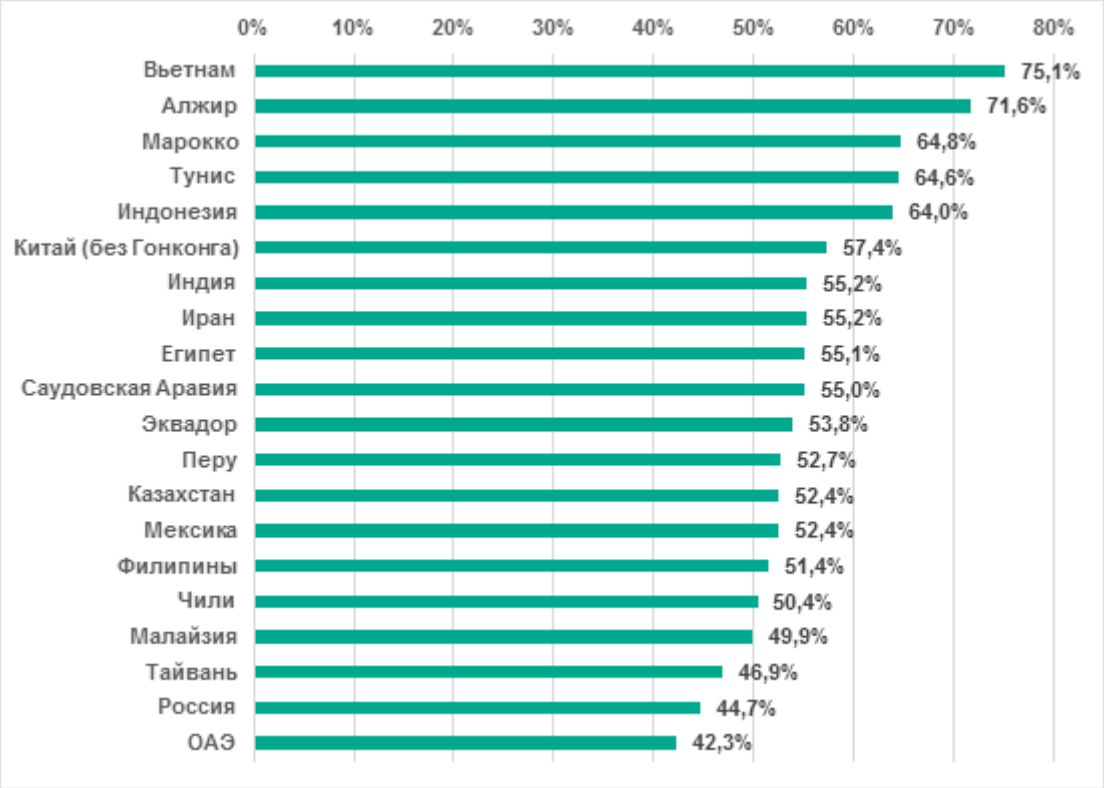


Рост процента атакованных компьютеров АСУ связан, в основном, с общим повышением вредоносной активности.

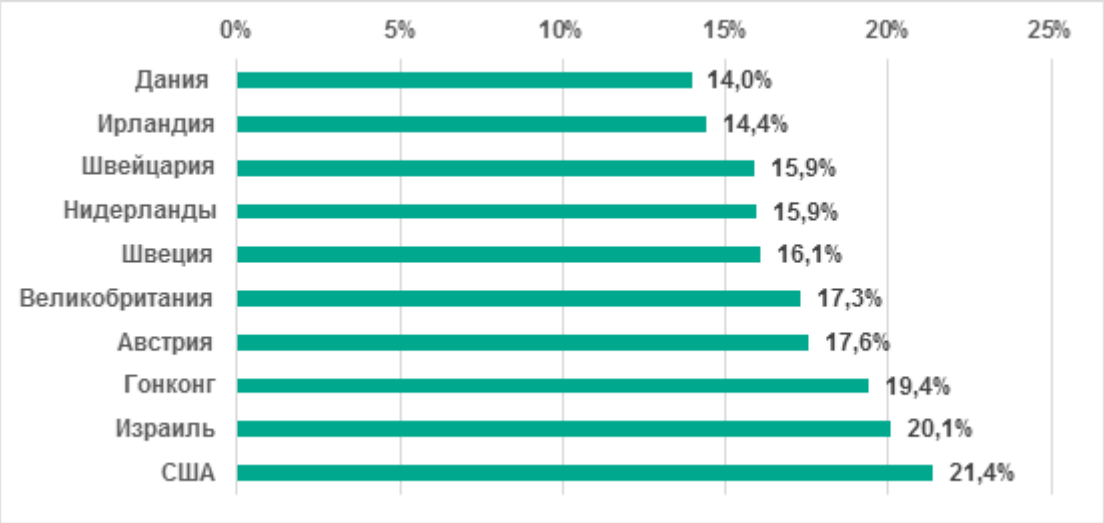
© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

География

TOP 20 стран по проценту атакованных компьютеров АСУ, первое полугодие 2018

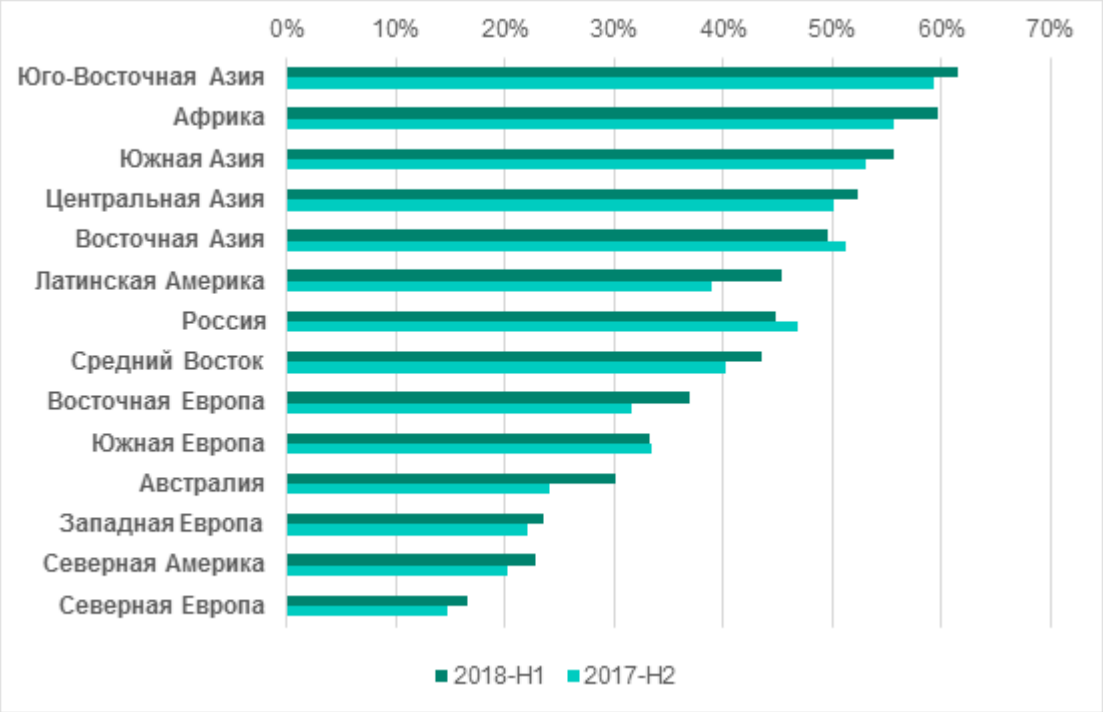


10 стран с наименьшим процентом атакованных компьютеров АСУ, первое полугодие 2018



© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Доля атакованных систем АСУ в различных регионах мира, второе полугодие 2017 и первое полугодие 2018



Сравнение показателей различных регионов мира показывает, что:

- страны Африки, Азии и Латинской Америки являются гораздо менее благополучными по проценту атакованных компьютеров АСУ, чем страны Европы, Северной Америки и Австралии;
- показатели Восточной Европы заметно выше, чем Западной;
- процент атакованных компьютеров АСУ в Южной Европе выше, чем в Северной и Западной Европе.

Можно предположить, что такая ситуация связана с объемами средств, вкладываемых организациями в решения для защиты инфраструктуры. По оценкам аналитической компании IDC, в 2017 году крупнейшими рынками ИБ с географической точки зрения являлись США и Западная Европа.

Показатели стран внутри отдельных регионов могут значительно отличаться. Так, на фоне большинства стран Африки наиболее благополучная обстановка наблюдается в ЮАР, а среди стран Среднего Востока заметно лучше дело обстоит в Израиле и Кувейте.

Факторы, влияющие на кибербезопасность компьютеров АСУ

Как мы видим, показатели разных стран мира попадают в достаточно широкий диапазон – от 14 до 75 процентов атакованных компьютеров АСУ. Мы полагаем, что столь значительные отличия могут быть связаны и с общим уровнем развитости стран, и с уровнем кибербезопасности, и с уровнем вредоносной активности в разных странах.

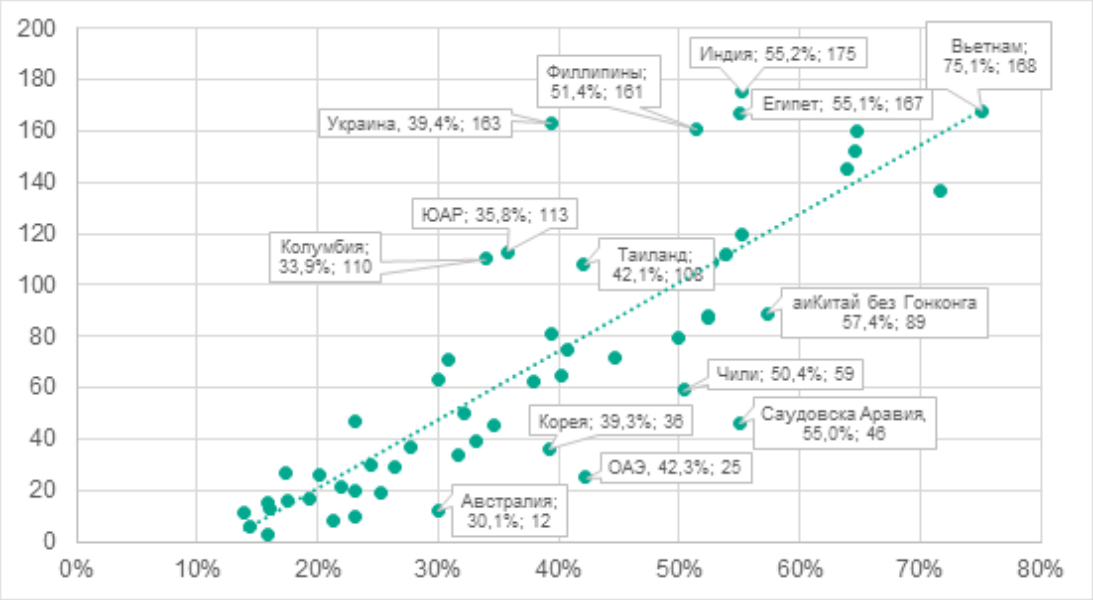
Так, все страны, имеющие, по нашим данным, минимальный процент атакованных компьютеров АСУ, классифицированы Международным валютным фондом как экономически развитые. К тому же 6 из 10 самых благополучных по проценту атакованных компьютеров АСУ стран – США, Великобритания, Нидерланды, Швеция,

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Швейцария и Израиль – в 2017 году вошли в ТОР 20 глобального индекса кибербезопасности, разработанного Международным союзом электросвязи (ITU).

Анализ соответствия процента атакованных компьютеров АСУ в каждой из стран и их позиций в рейтинге по уровню ВВП на душу населения показал, что между этими показателями существует высокая положительная корреляция (с множественным коэффициентом корреляции R = 0,84 и коэффициентом значимости P<0,001). За некоторыми исключениями, в странах с высоким уровнем ВВП на душу населения (первые места в соответствующем рейтинге) процент атакованных компьютеров АСУ меньше, чем в странах с низким уровнем ВВП.

Процент атакованных компьютеров АСУ в стране (ось X) и ее место в рейтинге стран по ВВП на душу населения (ось Y), первое полугодие 2018



7 из 10 самых неблагополучных стран по проценту атакованных компьютеров АСУ в 2017 году не попали в первую сотню стран по уровню ВВП на душу населения.

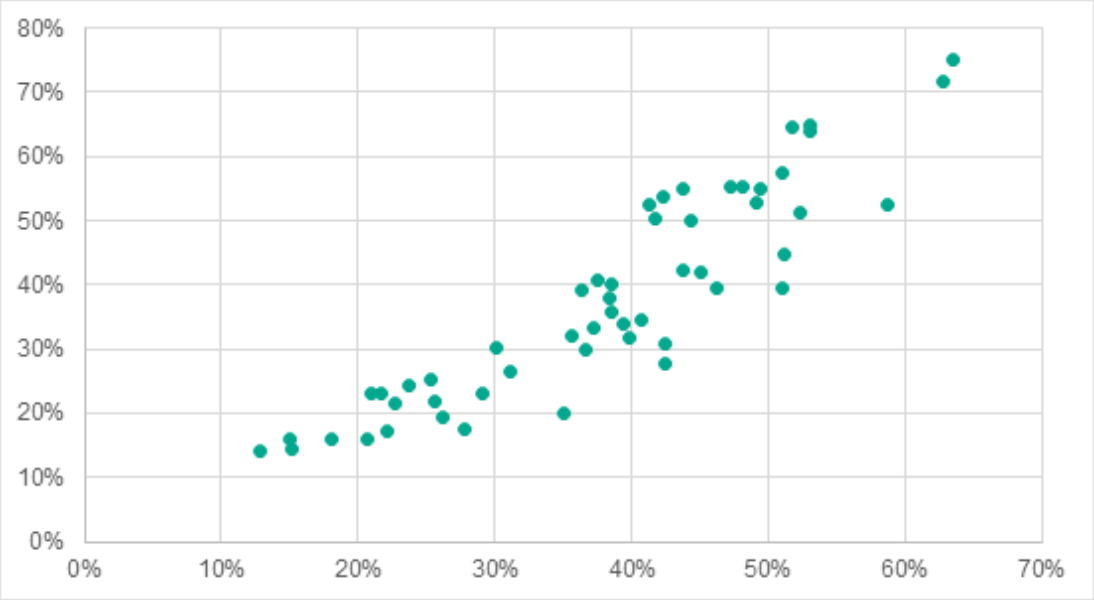
Высокий показатель процента атакованных компьютеров АСУ в развивающихся странах может быть связан с тем, что промышленность в этих странах относительно молодая. Как известно, зачастую при проектировании и введении в эксплуатацию промышленных объектов первоочередное внимание уделяется экономическим аспектам их работы и физической безопасности технологического процесса, а обеспечению информационной безопасности ставится значительно более низкий приоритет.

Вероятно, те несколько примеров, которые отмечены на диаграмме, – это некоторые страны, в которых доступные ресурсы используются для защиты промышленных активов от кибератак более (над пунктирной линией) или менее (под пунктирной линией) эффективно, чем в других странах.

Чтобы оценить уровень вредоносной активности в разных странах, мы посчитали процент всех атакованных компьютеров (домашних, корпоративных пользователей и компьютеров АСУ) в каждой из стран. И обнаружили, что существует высокая положительная корреляция (с множественным коэффициентом корреляции R = 0,89 и коэффициентом значимости P<0,001) между процентом атакованных компьютеров АСУ и показателем вредоносной активности в стране (процентом всех атакованных компьютеров).

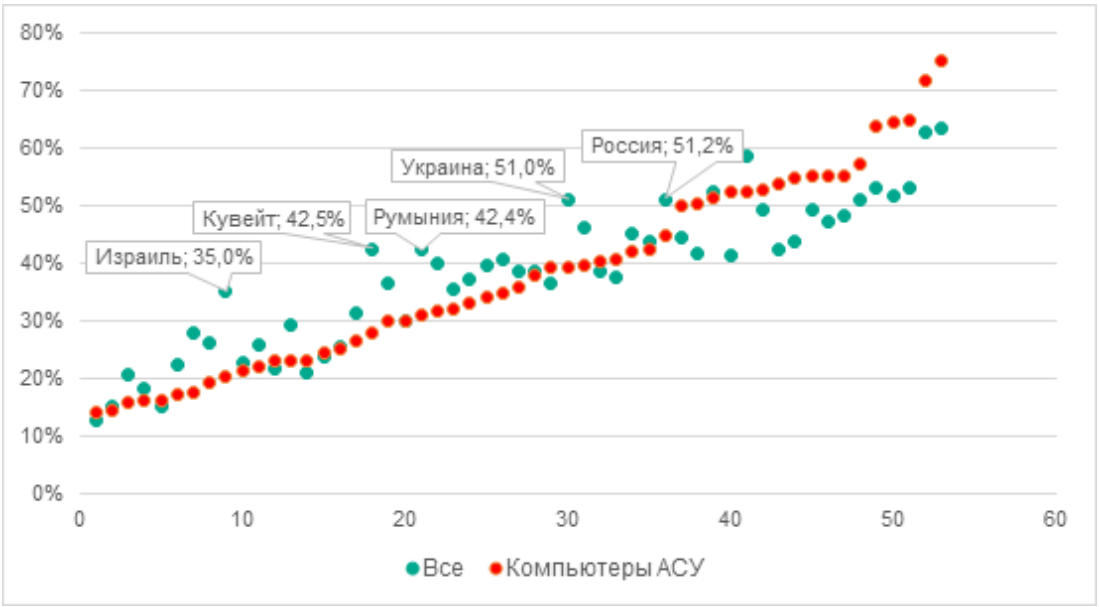
© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Процент всех атакованных компьютеров в стране (ось X) и процент атакованных компьютеров АСУ (ось Y), первое полугодие 2018



Эти данные согласуются с предположением, что компьютеры в инфраструктуре технологических сетей, сопряжённые с корпоративной сети и/или подключающиеся интернету даже эпизодически, в подавляющем большинстве случаев подвергаются атакам вредоносного ПО в той же мере, в которой им подвергаются такие традиционные для злоумышленников мишени, как офисные компьютеры организаций и частных лиц в той же стране.

Процент всех атакованных компьютеров в стране и процент атакованных компьютеров АСУ, первое полугодие 2018



Отметим, что почти во всех странах, где в течение полугодия было атаковано не менее половины всех компьютеров АСУ (TOP 20 нашего рейтинга), процент атакованных машин в инфраструктуре технологических сетей оказался выше, чем показатель по всем атакованным компьютерам в стране. Такая ситуация вызывает особую тревогу, учитывая, что по данным Всемирного банка и Организации экономического сотрудничества и развития 8 стран из этого списка – Индонезия, Китай, Индия, Иран, Саудовская Аравия, Мексика, Филиппины и Малайзия – в 2017 году по объему промышленного производства вошли в TOP 30.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Основные источники заражения

Основные источники заражения компьютеров в технологической инфраструктуре организаций – интернет, съемные носители и электронная почта.

Интернет за последние годы стал основным источником заражения компьютеров технологической инфраструктуры организаций. Более того, процент компьютеров АСУ, на которых были заблокированы попытки загрузки вредоносного ПО из интернета, доступ к известным вредоносным и фишинговым веб-ресурсам, фишинговые письма и вредоносные вложения, открываемые в почтовых веб-сервисах через браузер, растет.

Если год назад, в первом полугодии 2017, интернет стал источником угроз, заблокированных на 20,6% компьютеров АСУ, с которых мы получаем обезличенную статистику, то в первом полугодии 2018 года – уже на 27,3%.

Основные источники угроз, заблокированных на компьютерах АСУ (процент атакованных компьютеров АСУ по полугодиям)

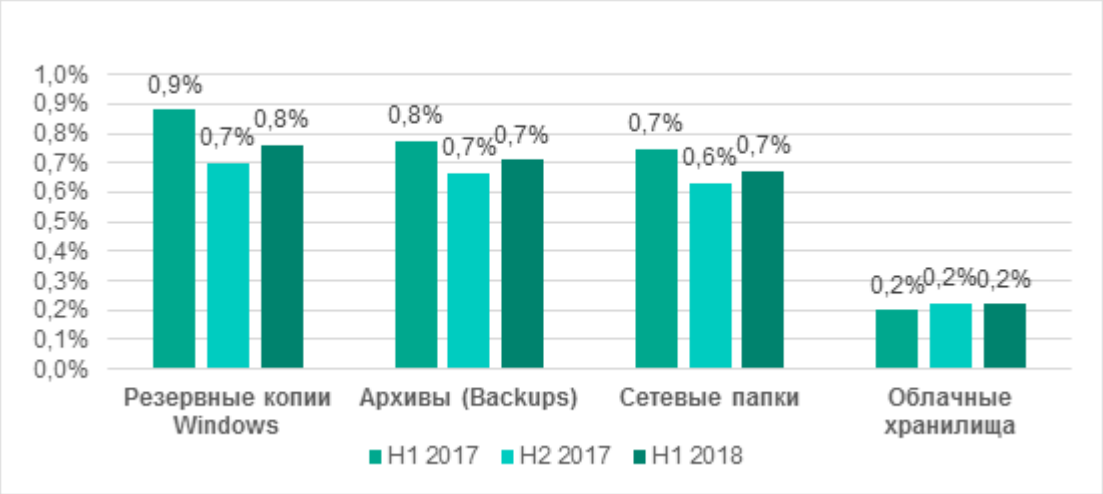
Такая динамика кажется закономерной – современные технологические сети трудно назвать изолированными от внешних систем. В настоящее время сопряжение технологической сети с корпоративной сетью необходимо как для управления производством, так и для администрирования промышленных сетей и систем. Вынужденной необходимостью может быть и доступ к интернету из технологической сети – например, для сопровождения и технической поддержки систем промышленной автоматизации сотрудниками организаций-подрядчиков. Компьютеры подрядчиков, разработчиков, интеграторов, системных/сетевых администраторов, которые подключаются к технологической сети обслуживаемого предприятия извне (напрямую или удаленно) и при этом часто имеют свободный доступ к интернету, также могут быть одним из каналов проникновения вредоносного ПО в технологические сети.

Кроме того, такой канал создают подключения 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). Второе и третье места среди наиболее распространенных источников заражения промышленных сетей заняли съемные носители информации и почтовые клиенты, соответственно. Показатели по этим источникам заражений за полугодие изменились незначительно.

Показатели по остальным источникам заражений не превышают 1% и остались на уровне прошлого полугодия.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Минорные источники угроз, заблокированных на компьютерах АСУ, (процент от всех атакованных компьютеров АСУ по полугодиям)



Основные источники заражения компьютеров АСУ в регионах

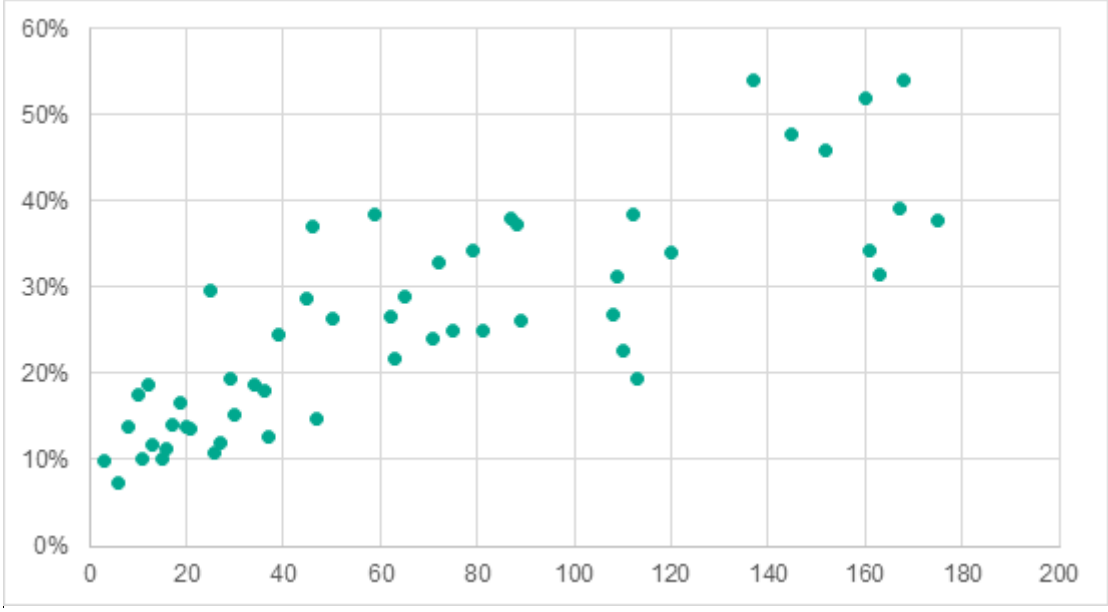
Основные источники угроз, заблокированных на компьютерах АСУ в регионах, первое полугодие 2018

Интернет

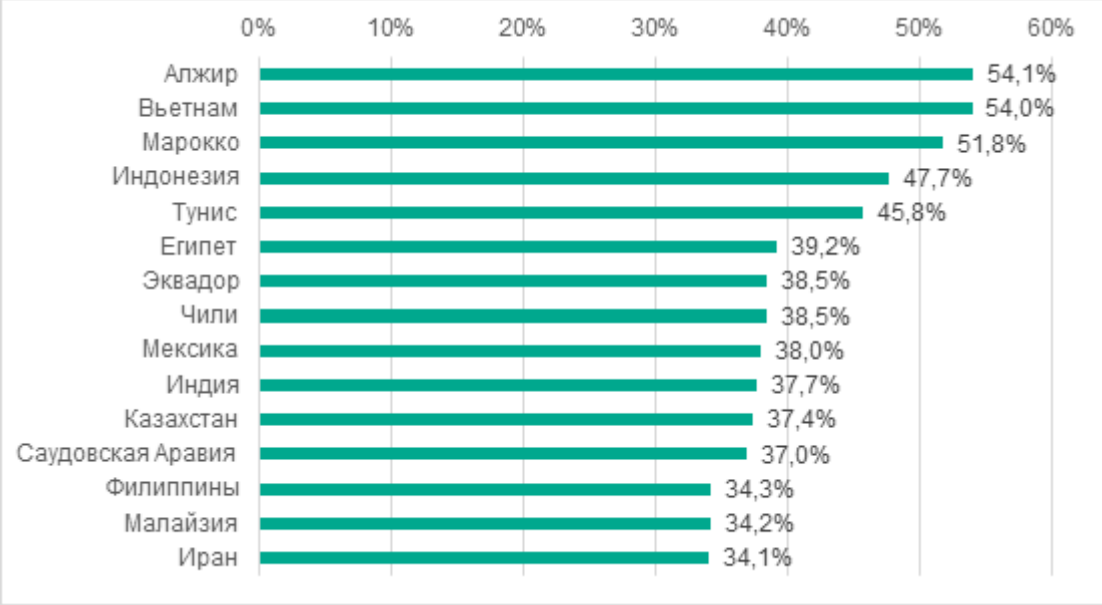
Интернет вносит основной вклад в атаки на компьютеры АСУ. Поэтому ожидаемо, что, как и в случае всех атакованных компьютеров АСУ, есть корреляция уровня ВВП на душу населения и процента компьютеров АСУ, на которых были заблокированы угрозы из интернета в разных странах (множественный коэффициент корреляции R=0,82, коэффициент значимости P<0,001).

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Место страны в рейтинге стран по ВВП на душу населения (ось X) и процент компьютеров АСУ в стране, атакованных угрозами из интернета (ось Y)



TOP 15 стран по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, первое полугодие 2018

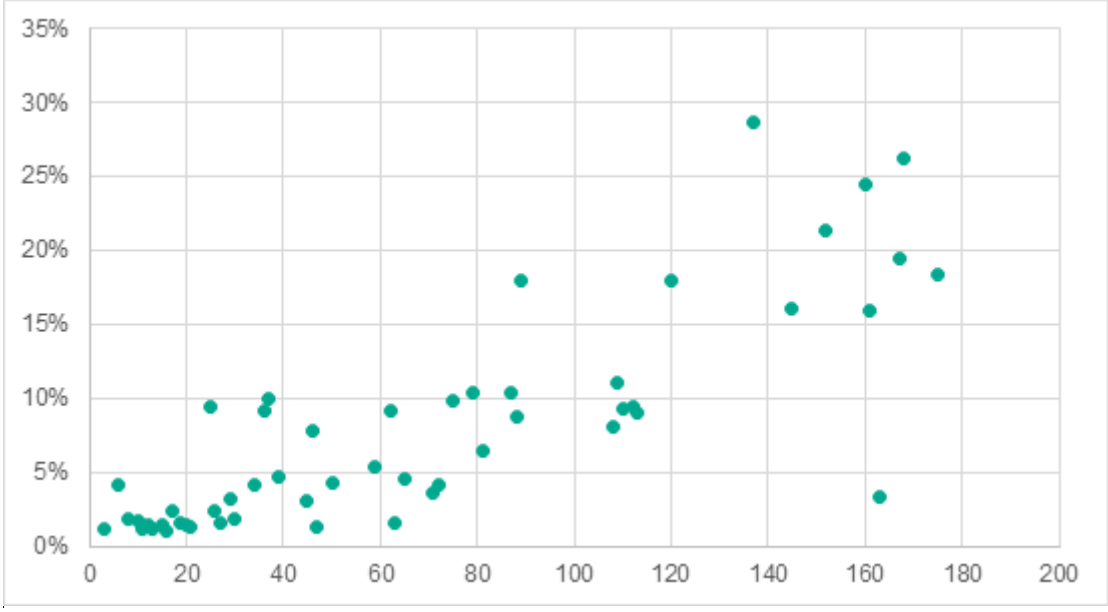


Съемные носители

В случае с угрозами со съемных носителей за некоторыми исключениями ситуация аналогичная – в странах и низким уровнем ВВП на душу населения процент компьютеров АСУ, атакованных со съемных носителей, выше (множественный коэффициентом корреляции R=0,82, коэффициент значимости P<0,001).

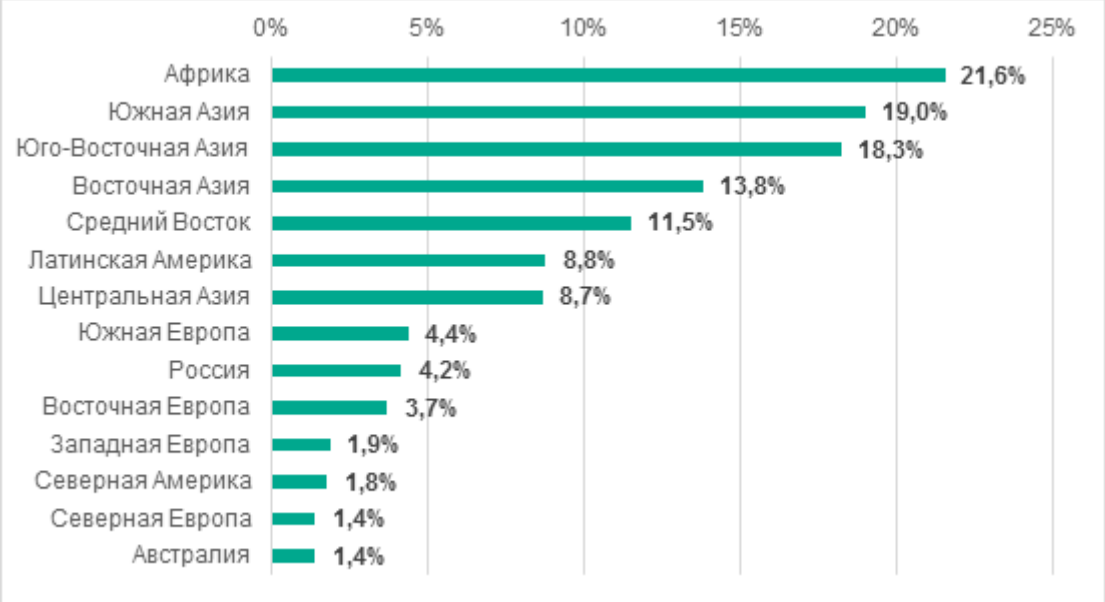
© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Место страны в рейтинге стран по ВВП на душу населения (ось X) и процент компьютеров АСУ в стране, атакованных угрозами со съемных носителей (ось Y)



Это во многом определяет рейтинг регионов по проценту компьютеров, атакованных со съемных носителей.

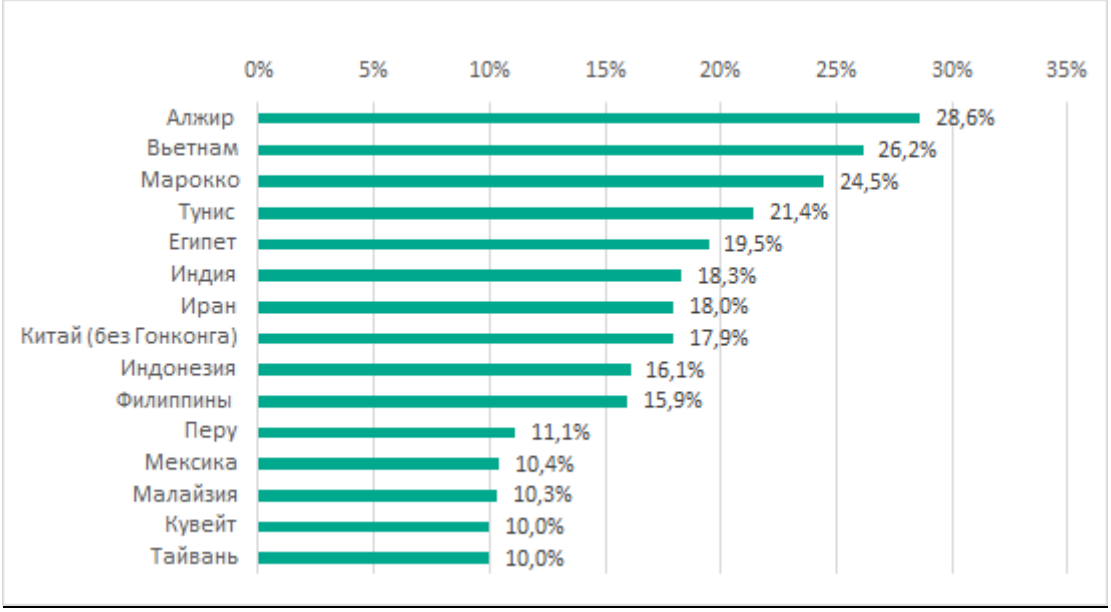
Рейтинг регионов по проценту компьютеров АСУ, атакованных через съемные носители, первое полугодие 2018



Максимальный процент атакованных через съемные носители компьютеров АСУ отмечен в Африке, на Среднем Востоке и в Юго-Восточной Азии. Такие данные могут свидетельствовать о том, что в этих регионах съемные носители широко применяются для передачи информации между компьютерами АСУ, что в совокупности с общим невысоким уровнем угроз кибербезопасности обуславливает высокий процент атакованных компьютеров АСУ. При этом в Западной Европе и Северной Америке этот показатель – минимальный. Мы предполагаем, что это связано как с более высоким уровнем защитных мер в целом, так и с менее распространенным использованием съемных носителей.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

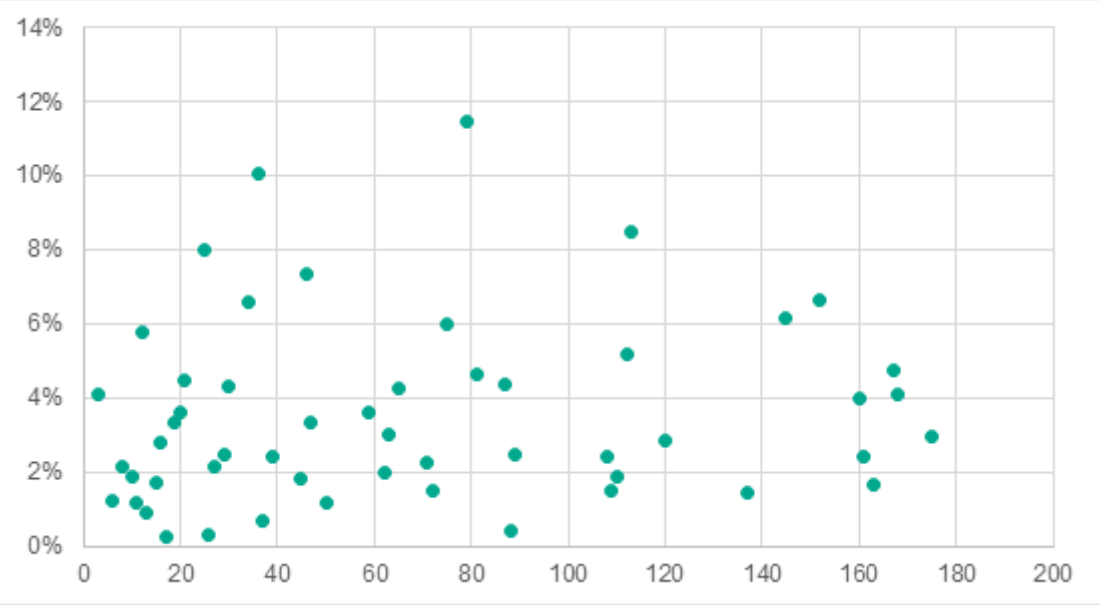
ТОР 15 стран по проценту компьютеров АСУ, атакованных через съемные носители, первое полугодие 2018



Почтовые клиенты

А вот с угрозами из почты ситуация иная – процент компьютеров АСУ, атакованных через почтовые клиенты, не коррелирует с уровнем ВВП на душу населения.

Место страны в рейтинге стран по ВВП на душу населения (ось X) и процент компьютеров АСУ в стране, атакованных через почтовые клиенты (ось Y)

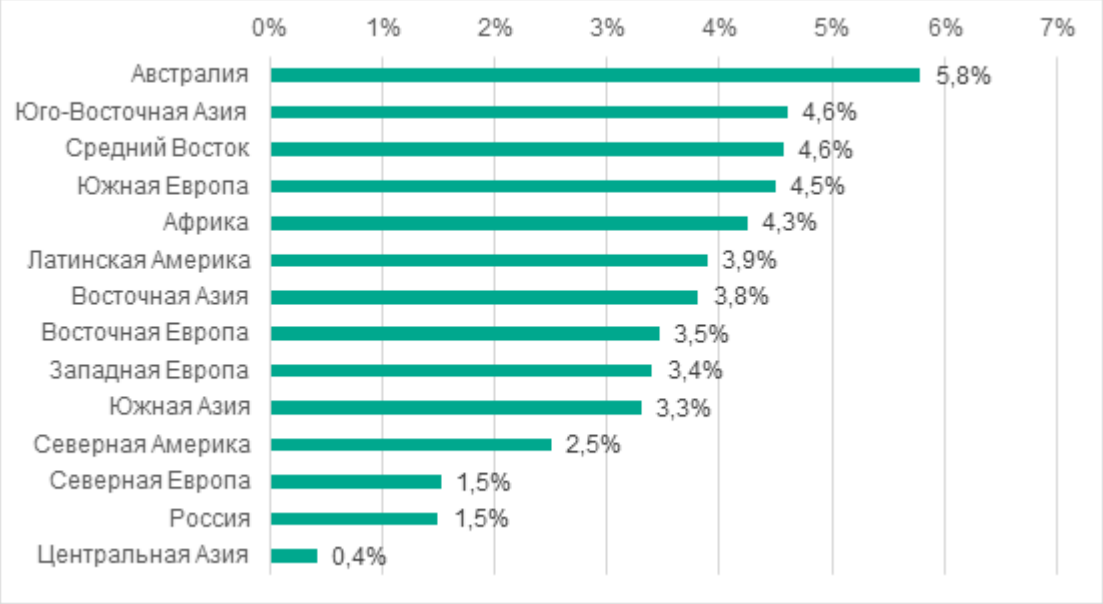


Это означает, что если справедливо предположение о том, что общий высокий уровень обеспечения информационной безопасности, характерен для стран с высоким ВВП на душу населения, это не помогает избавиться от атак из почты. То есть уровень обеспечения информационной безопасности практически не влияет на то, сколько фишинговых писем и вредоносных почтовых вложений проходит через средства защиты на периметре сети и доходит до компьютеров АСУ. Мы можем предположить, что вне зависимости от общего уровня кибербезопасности предприятия эффективные средства защиты от почтовых атак на периметре сети либо не используются, либо плохо настроены.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

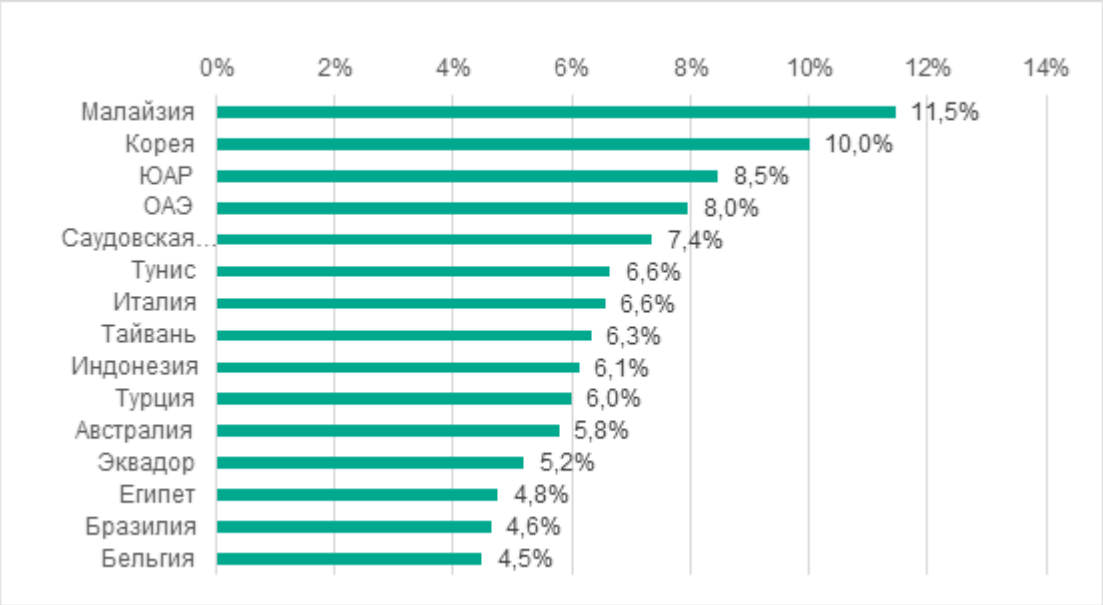
В рейтинге регионов по проценту компьютеров АСУ, атакованных через почтовые клиенты, большого разброса значений нет. Возглавляет его относительно благополучная в остальных отношениях Австралия, а показатели большинства регионов колеблются в небольшом интервале от 2,5 до 4,6 процентов.

Рейтинг регионов по проценту компьютеров АСУ, атакованных через почтовые клиенты, первое полугодие 2018



Отметим, что в рейтинге *стран* по проценту компьютеров АСУ, атакованных через почтовые клиенты, Австралия находится лишь на 11-м месте. Примечательно, что в список 15 наиболее неблагополучных с точки зрения атак через почту стран попала также благополучная по другим показателям Бельгия, относительно благополучные Италия и ЮАР.

ТОР 15 стран по проценту компьютеров АСУ, атакованных через почтовые клиенты, первое полугодие 2018



Данные наблюдения, на наш взгляд, требуют особого внимания, поскольку почта часто используется в целевых атаках на промышленные предприятия. О некоторых таких кампаниях мы писали здесь и здесь.

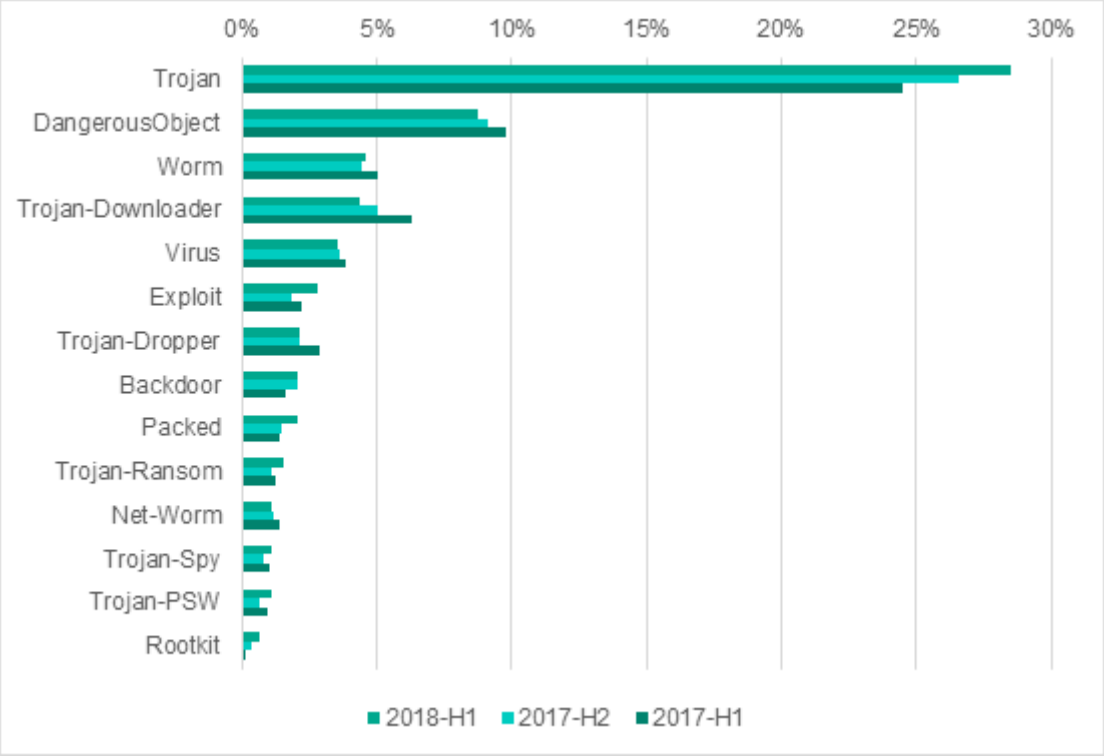
© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Вредоносное ПО на системах промышленной автоматизации

В первом полугодии 2018 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было обнаружено более 19,4 тысяч модификаций вредоносного ПО из 2,8 тысяч различных семейств.

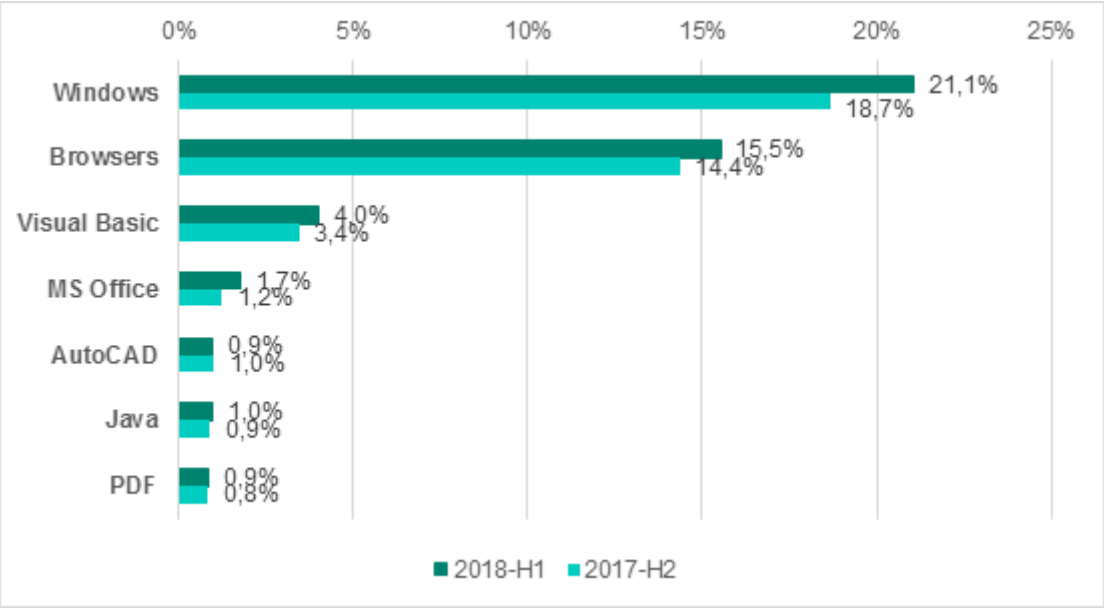
По-прежнему в подавляющем большинстве случаев попытки заражения компьютеров АСУ носят случайный характер, а не происходят в ходе целевой атаки.

Классы вредоносного ПО, процент атакованных компьютеров АСУ, первое полугодие 2018



Платформы, используемые вредоносным ПО

Основные платформы, используемые вредоносным ПО, второе полугодие 2017 и первое полугодие 2018, процент атакованных компьютеров АСУ



© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

На графике выше

- в платформе Windows учтены все угрозы для x86 и x64;
- в платформе Browsers учтены все угрозы, атакующие браузеры, а также вредоносные HTML страницы;
- в платформе Microsoft Office учтены все угрозы, направленные на соответствующее ПО (Word, Excel, PowerPoint, Visio, и т.п.).

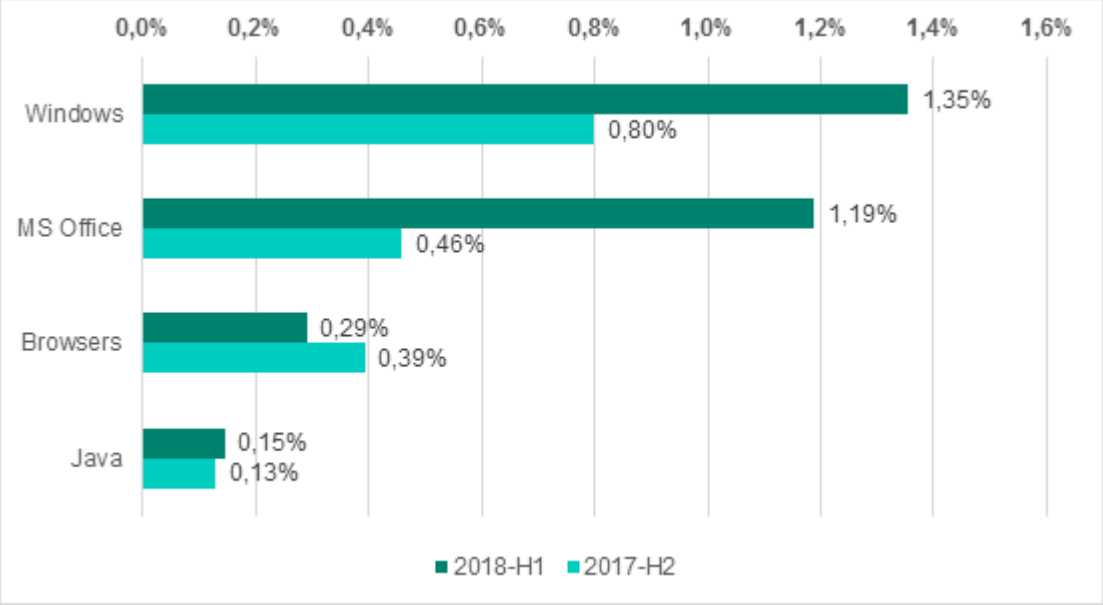
В первом полугодии 2018 злоумышленники продолжили атаковать легитимные сайты, очевидно, содержащие уязвимости в веб-приложениях, для размещения на них компонентов вредоносного ПО. В частности, увеличение процента компьютеров АСУ, атакованных через браузеры, во первой половине 2018 года обусловлено увеличением количества атак с использованием Javascript-майнеров.

Вместе с тем, увеличение процента компьютеров АСУ, атакованных с использованием документов Microsoft Office (Word, Excel, RTF, PowerPoint, Visio и др.) связано с волнами фишинговых рассылок. В таких рассылках в большинстве случаев прикрепленные к письмам вредоносные документы Microsoft Office содержат эксплойты, предназначенные для заражения компьютеров различным шпионским ПО. Часто не подозревающие об угрозе пользователи пересылают зараженные офисные документы коллегам, передают их через съемные носители и сетевые папки, и таким образом способствуют распространению вредоносного ПО. Именно поэтому для предотвращения заражений крайне желательно ограничить использование офисного ПО (Micsofot Office, PDF и др.) на компьютерах АСУ.

Эксплойты

Процент компьютеров АСУ, на которых были заблокированы попытки срабатывания эксплойтов, вырос на 1 п.п. и составил 2,8%.

Типы приложений, атакуемых эксплойтами, процент атакованных компьютеров АСУ



Важно отметить, что злоумышленники часто используют скрипты-загрузчики, написанные на Visual Basic Script, в качестве «полезной нагрузки» эксплойтов или непосредственно внедряя их в офисные документы. Необходимым условием для выполнения таких скриптов является наличие интерпретатора Windows Script Host

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

(WSH), который обычно устанавливается по умолчанию вместе с ОС Windows. Таким образом, для защиты от вредоносного ПО на Visual Basic Script рекомендуется отключить WHS в реестре Windows, если WHS не является необходимым для работы АСУ. То же самое касается и вредоносного ПО, написанного на Java, – в случае, если Java Runtime не требуется для работы АСУ, рекомендуется отказаться от его использования для снижения риска заражения.

Эксплойты ShadowBrokers, утекшие в марте прошлого года и использованные в атаках программ-шифровальщиков WannaCry и ExPetr, многократно использовались и в первой половине 2018 года в составе различного вредоносного ПО. Увеличение количества атак с использованием этих эксплойтов является причиной роста процента компьютеров АСУ, атакованных с использованием вредоносного ПО и эксплойтов для Windows x86 и x64.

Программы-шпионы

Процент компьютеров АСУ, атакованных вредоносными программами-шпионами (Trojan Spy и Trojan PSW), вырос на 0,4 п.п.

Шпионские вредоносные программы часто распространяются в фишинговых письмах. Один из ярких примеров – Южная Корея, которая заняла третье место в рейтинге стран по проценту компьютеров АСУ, на которых были заблокированы шпионские программы, с показателем 6%. Большинство вредоносных программ-шпионов в этой стране распространялись именно в фишинговых письмах, нацеленных на пользователей в Азиатско-Тихоокеанском регионе.

Примечательно, что большинство таких фишинговых рассылок очень схожи (по используемым заголовкам/тексту писем/именам файлов) в различных регионах мира, за исключением Азии – в этом регионе фишинговые рассылки имеют более выраженный «азиатский» контекст – в письмах используются названия исключительно Азиатских промышленных компаний.

Отметим, что Корея находится на третьем месте по атакам бэкдоров, которые были заблокированы на 6,4% компьютеров АСУ. На первом месте в этом рейтинге – Вьетнам с впечатляющими 9,8%.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Наши рекомендации

Для противодействия угрозам, описанным в данном отчёте, мы рекомендуем принять ряд мер по обеспечению информационной безопасности.

Предлагаемый список мер приведён в порядке, который по опыту наших специалистов соответствует убыванию соотношения их важности и сложности их реализации.

Список не следует считать исчерпывающим. При его составлении мы ориентировались на проблемы информационной безопасности промышленных предприятий и систем промышленной автоматизации, обнаруженные и проанализированные нами в ходе исследований, проделанных в течение отчётного периода.

Так, он не включает такие меры как конфигурация межсетевого экрана для запрета обращения извне технологической сети по протоколам, используемым для автоматизации технологического процесса, и запрет прямого обращения к узлам технологической сети из интернета – основываясь на результатах проделанных нами аудитов и тестов на проникновение технологических сетей промышленных предприятий, мы считаем, что подавляющее большинство организаций подобные меры уже применяют на практике.

Меры, не требующие организационных изменений, дополнительного персонала, корректировки бизнес- и производственных процессов, существенных изменений информационных систем

Мы считаем, что эти меры помогают сделать первый шаг на пути к защите технологических объектов предприятия. По нашему мнению, эти меры применимы для большинства организаций, вне зависимости от уровня зрелости их процессов обеспечения информационной безопасности.

1. Защитить все узлы промышленной сети от вредоносных атак при помощи средств антивирусной защиты.
   - Убедиться, что все основные компоненты защиты включены и функционируют.
   - Из области защиты не исключать каталоги ПО АСУ ТП, системные каталоги ОС, профили пользователей.
   - По возможности, не использовать исключения из проверки вообще.
   - Добиться частоты обновления антивирусных баз не реже одного раза в день. Желательно обновлять базы в соответствии с рекомендациями производителя средств защиты.
   - Убедиться, что настроена автоматическая проверка съёмных носителей при их подключении.
   - При возможности настроить оперативное получение актуальных вердиктов из антивирусного облака производителя.
2. Настроить правила сетевых экранов на границе технологической сети.
   - Запретить обращения к службам предоставления удалённого доступа к объектам файловой системы, таким как SMB/CIFS и/или NFS (актуально в случае атак на системы под управлением ОС Linux).
   - Настроить правила контроля использования средств удалённого администрирования. Создать белый список адресов, с которых возможен удалённый доступ к системам в технологической сети. Убедиться, что в этот список входят только адреса доверенных ресурсов и исключены облачные

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

инфраструктуры производителей средств администрирования, прочие недоверенные и неизвестные адреса.
- Запретить использование внешних почтовых сервисов внутри технологической сети.
- Запретить использование внешних HTTP/HTTPS-почтовых сервисов.
- Запретить использование социальных сетей.
- Запретить использование облачных файловых хранилищ.
- Запретить использование торрентов.

3. Настроить защиту от спамовых- и фишинговых рассылок на границе и внутри корпоративной сети.
   - Добиться частоты обновления антиспамовых и антифишинговых средств с частотой, рекомендованной производителем.
   - При возможности настроить подключение к облачному сервису оперативной передачи вердиктов производителя.
4. Настроить антивирусную защиту на периметре сети организации и контроль обращения к вредоносным и потенциально опасным интернет-ресурсам.
5. Провести аудит использования почты внутри технологической сети.
   - Запретить использование внешних почтовых сервисов на компьютерах технологической сети средствами антивирусной защиты.
   - По возможности, запретить использование корпоративной почты внутри технологической сети, удалить установленные почтовые клиенты либо запретить их запуск средствами контроля запуска приложений.
   - Отключить использование сервиса «mailto».
6. Провести аудит использования папок общего доступа внутри технологической сети.
   - Отключить все сетевые папки общего доступа, не обусловленные производственной необходимостью.
   - Отключить сервисы удалённого доступа к файловой системе SMB/CIFS и NFS там, где в них нет производственной необходимости.
7. Провести аудит использования сторонних средств удалённого администрирования внутри технологической сети, таких, как VNC, RDP, TeamViewer RMS/Remote Utilities. Удалить все средства удалённого администрирования, не обусловленные производственной необходимостью.
8. Отключить средства удалённого администрирования, поставляемые вместе с ПО АСУ ТП (обратитесь к документации на соответствующее ПО за детальными инструкциями), если в их использовании нет производственной необходимости.
9. Провести аудит использования прочего ПО в технологической сети, которое существенно увеличивает поверхность атаки систем АСУ. В случае если использование этого ПО не обусловлено технологической необходимостью, деинсталлировать его. Особое внимание уделить следующим типам ПО:
   - Интернет-браузеры.
   - Клиенты социальных сетей.
   - Почтовые клиенты.
   - ПО MS Office.
   - ПО Adobe.
   - Java Runtime.
   - Медиа-проигрыватели.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

- Скриптовые интерпретаторы типа Perl, Python, PHP.
- Нелицензионное «поломанное» ПО – оно часто содержит закладки и инфицировано.

10. Выключить Windows Script Host, если его запуск не требуется для работы ПО АСУ ТП и не обусловлено другой производственной необходимостью.
11. При возможности, ограничить использование привилегий SeDebugPrivilege для локальных администраторов систем промышленной сети предприятия при помощи групповых политик домена Windows (может требоваться для работы некоторого ПО, например, MS SQL Server – обратитесь к документации производителей соответствующих систем.).

Меры, рассчитанные на организации с высоким уровнем зрелости в области информационной безопасности

Применение этих мер для недостаточно зрелых организаций может потребовать существенных временных либо ресурсных затрат, организации новых процессов киберзащиты, изменений штатного расписания, быть осложнено прочими обстоятельствами.

1. Наладить процесс обучения персонала предприятия кибергигиене.
   - Организовать курсы повышения квалификации для сотрудников по теме кибербезопасности, чтобы повысить осведомлённость персонала о современных угрозах: целях, технических методах и схемах реализации атак на промышленные организации, опасностях, которые представляют атаки для бизнес- и технологических процессов, методов защиты от атак и предотвращения инцидентов.
   - Организовать периодические тренинги по теме киберугроз и способов защиты с учётом изменения ландшафта угроз и тренинги для новых сотрудников. Рассмотреть возможность использования тренинговых платформ (онлайн или развёрнутых внутри предприятия), вебинаров, записей предыдущих тренингов для повышения доступности тренингов для сотрудников предприятия.
   - Внедрить практику коротких инструктажей персонала по теме защиты от киберугроз.
   - Обеспечить сотрудников предприятия соответствующими информационными материалами – плакатами, буклетами и пр., напоминающими о необходимости защиты от киберугроз.
   - Организовать регулярные учения по кибербезопасности и проверку знаний сотрудников в этой области.
2. Организовать службу информационной безопасности и киберзащиты промышленных информационных систем.
   - Назначить ответственного за киберзащиту информационных систем технологической сети.
   - Сделать защиту технологической сети частью общего процесса обеспечения ИБ предприятия.
   - Наладить эффективную работу различных горизонтальных и вертикальных подразделений и служб организации – инженеров, операторов, IT, ИБ для защиты от кибератак.
   - Наладить эффективные коммуникации по вопросам киберзащиты с производителями средств автоматизации и производителями средств защиты.
   - Организовать процесс реагирования на инциденты ИБ в технологической сети.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

3. Ввести практику регулярных аудитов состояния информационной безопасности информационных систем технологической сети.
   - Инвентаризация запущенных сетевых служб на всех узлах технологической сети; по возможности остановить (лучше отключить / удалить) 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 SMB/CIFS, NBNS, LLMNR.
   - Аудит разграничения доступа к компонентам АСУ ТП; постараться добиться максимальной гранулярности доступа.
   - Аудит сетевой активности внутри промышленной сети предприятия и на её границах. Устранить не обусловленные производственной необходимостью сетевые соединения с внешними и смежными информационными сетями.
   - Аудит безопасности организации удалённого доступа к промышленной сети; обратить особое внимание на соответствие организации демилитаризованных зон требованиям информационной безопасности.
   - 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.
   - Аудит учетных записей и парольной политики. Пользовательские и сервисные учётные записи должны иметь только те права, которых требуют рабочие необходимости. Число учетных записей пользователей с административными правами должно быть максимально ограничено. Должны использоваться сложные пароли (не менее 9 символов, различного регистра, дополненные цифрами и специальными символами, пароли не должны состоять из словарных слов), обязательная смена пароля должна быть задана доменной политикой, например, каждые 90 дней. По возможности, следует отказаться от использования небезопасных алгоритмов аутентификации, таких как NTLM, в пользу более безопасных NTLMv2 и Kerberos.

4. Наладить процесс своевременного устранения уязвимостей безопасности систем технологической сети.
   - Получить доступ к источникам информации об уязвимостях, обнаруженных в продуктах АСУ ТП, сетевых устройствах и общих компонентах, наладить процесс обработки и анализа такой информации.
   - Внедрить процесс регулярной проверки на уязвимости систем, развёрнутых в технологической сети и на её периметре. Подумать о внедрении специализированных средств обнаружения уязвимостей систем технологической сети.
   - Регулярно устанавливать обновления операционной системы, прикладного ПО и средств защиты на системы, работающие в технологической сети предприятия.
   - Своевременно устанавливать обновлений прошивок устройств автоматизированного управления и средств противоаварийной защиты.

5. Использовать следующие специализированные технологии автоматических средств защиты. Как правило, требует тонкой настройки, тщательного тестирования и развитых процессов мониторинга и реагирования на инциденты ИБ:
   - Настроить контроль запуска программ в режиме «белых списков» (обычно входит в состав решений по антивирусной защите узлов технологической сети).

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

Там, где это невозможно, настроить контроль запуска программ в режиме мониторинга и уведомления ответственного за ИБ.
- Внедрить специализированные средства (могут входить в состав решений по антивирусной защите узлов технологической сети) обеспечения целостности компьютеров – критических областей и конфигурации ОС и прикладного ПО, в особенности ПО АСУ ТП. Там, где это невозможно, настроить контроль целостности в режиме мониторинга и уведомления ответственного за ИБ.
- Настроить контроль подключения внешних устройств (USB-носителей, мобильных телефонов и пр.).
- Включить компоненты Host-based Intrusion Prevention System (HIPS) из состава средств антивирусной защиты.
- Внедрить средства автоматической инвентаризации и контроля подключения устройств к технологической сети. Требует привлечения квалифицированных специалистов для мониторинга и реакции на обнаруженные инциденты.
- Внедрить специализированные средства мониторинга сетевого трафика и обнаружения сетевых аномалий и компьютерных атак в индустриальных сетях. В большинстве случаев применение подобных мер не требует внесения изменений в состав и конфигурацию средств АСУ ТП и может быть произведено без остановки их работы. Однако для эффективного использование таких средств, скорее всего, потребуется выделенный высококвалифицированный персонал, интеграция с прочими средствами обнаружения аномалий и развитые процессы обеспечения ИБ технологической и корпоративной сети.

6. Внедрить специализированные средства регистрации и автоматизации процедуры обработки инцидентов ИБ в технологической сети предприятия.
7. Наладить процесс получения и обработки информации об актуальных угрозах:
   - Специализированных аналитических отчётов о новых выявленных атаках и вредоносных кампаниях, нацеленных на промышленные предприятия.
   - Отчётов об исследованиях тактик, методов и средств (TTP), используемых известными группировками злоумышленников в атаках на промышленные организации.
   - Аналитических отчётов об исследовании ландшафта угроз, представляющих опасность для промышленных предприятий.
   - Индикаторов компрометации узлов технологической сети.
   - Это может помочь своевременно и правильно среагировать на новую атаку и предотвратить инцидент.

Меры, которые потребуют существенных изменений в конфигурации и топологии технологической сети и сопряжены с прочими существенными модификациями информационных систем предприятия

1. Понимая, что полностью изолировать технологическую сеть от смежных сетей чаще всего невозможно, для организации более безопасного удаленного доступа к системам автоматизации и передачи данных между технологической и другими сетями, имеющими различные уровни доверия, мы рекомендуем:
   - Системы, имеющие постоянную или регулярную связь с внешними сетями (мобильные устройства, VPN-концентраторы, терминальные серверы и пр.) изолировать в отдельный сегмент внутри технологической сети — демилитаризованную зону (DMZ).

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

- 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 (включая корпоративную офисную сеть предприятия) осуществлять только 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 использовать тонкие клиенты (применяя методы обратного подключения).
- Не разрешать доступ из демилитаризованной зоны в технологическую сеть.
- Ограничить сетевой трафик по используемым портам и протоколам на пограничных маршрутизаторах между сетью организации и сетями других компаний (если имеется передача информации из технологической сети одной компании в другую).
- Если бизнес-процессы предприятия допускают возможность однонаправленных коммуникаций, рекомендуем рассмотреть возможность использования дата-диодов.

2. Перед развёртыванием и вводом в строй новых систем и компонентов АСУ ТП рекомендуем проводить их тестирование на предмет соответствия требованиям безопасности, включая поиск известных и новых (неизвестных ранее) уязвимостей – как часть процесса аттестации новых компонентов АСУ ТП. Это позволит существенно сократить затраты на обеспечение ИБ систем после их внедрения.
3. При прочих равных рекомендуем отдавать предпочтение продуктам, производители которых ставили безопасность во главу угла при разработке архитектуры своих продуктов, например, используя подход правильного разделения доменов безопасности и реализуя принципы MILS (Multiple Independent Layers of Security).
4. Для защиты от атак типа «человек посредине» рекомендуем рассмотреть настройку криптостойкого шифрования трафика внутри и на границе технологической сети – как минимум, там, где это позволяет используемое оборудование, особенности бизнес- и технологического процесса предприятия.
5. В ряде случаев можно настроить шифрование трафика между компонентами технологической сети, даже если эта функциональность не поддерживается соответствующим оборудованием – при помощи дополнительных средств. Рекомендуем проконсультироваться с производителем ваших систем автоматизации.
6. Для доступа персонала к системам технологической сети желательно настроить использование двухфакторной аутентификации.
7. Для упрощения поддержки процедур и процессов аутентификации и шифрования рекомендуем развернуть инфраструктуру PKI.
8. Для снижения рисков атак через цепочку поставщиков и подрядчиков («supply chain») рекомендуем рассмотреть возможность внедрения политики, механизмов и процедур контроля подключения устройств (например, ноутбуков подрядчиков и инженеров) к технологической сети.

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018

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

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

© АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО», 1997 – 2018