kaspersky

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2020

Kaspersky ICS CERT

15.09.2020 Version 1.0

Оглавление

Основные итоги полугодия....2
Основные события полугодия....4
Атака на металлургический концерн BlueScope....4
APT-атаки на промышленные компании....4
Целевая кампания WildPressure....4
Вредоносные кампании против правительственных и промышленных организаций Азербайджана....4
Целевые атаки на объекты водоснабжения и водоочистки Израиля....5
Атаки шифровальщиков на промышленные компании....5
Атака вымогателя остановила производство компании Picanol в Бельгии, Румынии и Китае....5
Атаки Ruyk на медицинские учреждения....6
Атака вымогателя на производителя насосных решений DESMI....6
Атака Ragnar Locker на энергетическую компанию EDP....6
Атака на промышленные объекты Stadler....6
Атаки Mailto и Nefilim на логистическую компанию Toll Group....7
Атака шифровальщика Sodinokibi на электроэнергетические компании....7
Атака на производителя напитков Lion....8
Целевые атаки на промышленные компании с использованием шифровальщика Snake....8
Влияние пандемии COVID-19....9
Общая статистика по миру....12
Методика подготовки статистики....12
Общие тенденции в ландшафте угроз для компьютеров АСУ, корпоративных и персональных компьютеров....13
Процент компьютеров, на которых были заблокированы вредоносные объекты....14
Россия....15
Некоторые индустрии....16
Разнообразие обнаруженного вредоносного ПО....17
Категории вредоносных объектов....17
Программы – вымогатели....20
Россия....21
География....22
Страны....22
Регионы....23
Источники угроз....24
Основные источники угроз: география....25
Интернет....25
Съемные носители....27
Почтовые клиенты....28

Основные итоги полугодия

Общая тенденция снижения процента атакованных компьютеров в мире

Со второй половины 2019 года в мире наблюдается снижение процента атакованных компьютеров, как среди АСУ, так и в корпоративной и персональной средах.

1. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в первом полугодии 2020 года уменьшился на 6 п.п. и составил 32,6%.
2. Среди стран наибольшие показатели – в Алжире (58,1%), наименьшие – в Швейцарии (12,7%).
3. Несмотря на общую тенденцию снижения процента атакованных компьютеров, на 1,6 п.п. выросли показали в Нефтегазовой отрасли (37,8%), на 1,9 п.п. – компьютеров, используемых в составе систем автоматизации зданий (39,9%). Показатели в этих индустриях превышают аналогичный показатель по миру в целом.

Разнообразие вредоносного ПО

Угрозы становятся более локальными, более фокусированными, и, как следствие – более разнообразными и сложными.

4. Защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 19,7 тысяч модификаций вредоносного ПО из 4119 тысяч различных семейств.
5. Стало заметно больше семейств бэкдоров, троянцев-шпионов, эксплойтов для Win32 и вредоносного ПО на платформе .NET.
6. Вредоносные программы-вымогатели были заблокированы на 0,63% компьютеров АСУ. Это незначительно отличается от итогов предыдущего полугодия (0,61%).

Основные источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и электронная почта. Показатели по этим источникам ожидаемо уменьшились.

7. Угрозы из интернета заблокированы на 16,7% компьютеров АСУ (-6,4 п.п.)
8. Угрозы при подключении съемных носителей заблокированы на 5,8% компьютеров АСУ (-1,9 п.п.).
9. Вредоносные почтовые вложения заблокированы на 3,4% компьютеров АСУ (-1,1 п.п.).

Отличия по регионам

Регионы Азии и Африка входят в число **наименее благополучных**.

10. Четыре из пяти позиций в TOP 5 по проценту атакованных компьютеров АСУ заняли регионы Азии. Второе место в этом рейтинге принадлежит Африке.
11. Самая сложная ситуация в Юго-Восточной Азии: регион лидирует сразу в нескольких рейтингах:
    - по проценту компьютеров АСУ, на которых была предотвращена вредоносная активность (49,8%),
    - по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета (14,9%)
    - по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения (5,8%).
12. Африка лидирует по проценту компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей (14,9%).

Самая благополучная ситуация в Австралии, регионах Европы, США и Канаде, которые замыкают все рейтинги, кроме рейтинга по вредоносным почтовым вложениям.

13. Самым благополучным регионом по итогам полугодия выглядит Северная Европа. У этого региона наименьшие показатели:
    - по проценту атакованных компьютеров АСУ (10,1%),
    - по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета (4,6%)
    - по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения (1,1%).
14. Наименьший процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, – в Австралии (0,8%). Показатель Северной Европы (0,9%) не сильно уступает лидеру.
15. В Австралии, Европе, США и Канаде показатели по вредоносным почтовым вложениям превышают показатели по угрозам на съемных носителях. Исключение составляет Восточная Европа (3,5% и 3,7% соответственно).

Среди регионов Европы наименее благополучны Южная и Восточная Европа.

16. Южная и Восточная Европа вошли в TOP 5 в рейтинге по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения. Южная Европа (5,2%) заняла второе место, Восточная Европа оказалась на пятом месте (3,5%).
17. Единственный регион в мире, где за полугодие увеличился (на 0,9 п.п.) показатель по проценту компьютеров, на которых были заблокированы угрозы при подключении съемных носителей, – Восточная Европа (3,7%).

Основные события полугодия

Атака на металлургический концерн BlueScope

15 мая стало известно об атаке на металлургический концерн BlueScope, которая вызвала сбои в работе некоторых предприятий.

Киберинцидент был обнаружен в одной из компаний в США. Помимо компаний в Северной Америке атака незначительно затронула предприятия в Азии и новой Зеландии. Сильнее всего от атаки пострадали производственные и торговые операции в Австралии: некоторые процессы были приостановлены, а другие, включая отправку стали, осуществлялись преимущественно без использования средств автоматизации. Другие подробности атаки пока не сообщаются.

APT-атаки на промышленные компании

Целевая кампания WildPressure

В марте 2020 года специалисты «Лаборатории Касперского» обнаружили ранее неизвестную APT-кампанию по распространению троянца, названного Milum. Согласно результатам исследования, эта вредоносная программа использовалась, по крайней мере, с начала 2019 года и исключительно для нападения на цели на Ближнем Востоке, среди которых есть организации промышленного сектора. Эта кампания получила название WildPressure.

Milum обладает возможностью удаленного управления устройствами и может загружать и выполнять команды своего оператора, собирать различную информацию с целевого устройства и отправлять ее на C&C-сервер. В инфраструктуре, созданной операторами Milum для этой кампании, использовались арендованные виртуальные выделенные серверы (virtual private servers, VPS) OVH и Netzbetrieb, а также домен, зарегистрированный через анонимизирующий сервис Domains by Proxy..

Анализ кода нового вредоносного ПО не выявил пересечений и сходств ни с одной известной ранее APT-кампанией.

Вредоносные кампании против правительственных и промышленных организаций Азербайджана

В апреле 2020 года была опубликована информация о целевых атаках с использованием ранее неизвестного троянца удаленного доступа (RAT), который получил название PoetRAT.

По мнению исследователей, атаки были направлены на государственный сектор, транспортные и промышленные компании Азербайджана, главным образом энергетические. В рамках расследования было установлено, что особенный интерес злоумышленники проявляют к SCADA-системам, связанным с ветряными турбинами.

Исследователи Cisco Talos наблюдали эти атаки с февраля 2020 года. Экспертами «Лаборатории Касперского» они были зафиксированы в декабре 2019 года, о чем сообщалось в приватном отчете. Злоумышленники использовали вредоносный документ, который содержал изображение, похожее на логотип научно-исследовательской организации Министерства обороны Индии. Две другие волны атак

прошли в апреле. В одной из них в качестве приманки использовались документы якобы правительства Азербайджана, посвященные COVID-19. В другом случае злоумышленники использовали файл без читабельного содержимого с именем «C19.docx», что возможно также является отсылкой к COVID-19.

В качестве дроперов, обеспечивающих скрытную установку троянца, использовались документы Microsoft Word. После открытия документа выполнялся макрос (Visual Basic-скрипт) или код с использование DDE (Dynamic Data Exchange), который извлекал вредоносную программу и выполнял ее.

Вредоносная программа первого этапа PoetRAT написана на Python. На компьютерах жертв было обнаружено много дополнительного инструментария, также написанного в основном на Python. Программы с использованием этого языка не первый раз используются в атаках на промышленные компании – так было, например, в истории с Triton.

В ходе расследования был обнаружен и фишинговый сайт, имитирующий веб-почту правительства Азербайджана и предназначенный для кражи учетных данных.

Целевые атаки на объекты водоснабжения и водоочистки Израиля

23 апреля Национальное киберуправление Израиля (Israel National Cyber Directorate, INCD) выпустило уведомление безопасности, в котором сообщалось о попытках атак на SCADA-системы очистных сооружений, водонасосных станций и канализационных сетей. В качестве мер по предотвращению вторжений организациям сферы водоснабжения и энергообеспечения было рекомендовано в срочном порядке сменить пароли для всех подключенных к интернету систем. Особенно подчеркивалась важность реализации этих мер для систем управления количеством добавляемого хлора. Кроме того, рекомендации включали необходимость обновить используемое программное обеспечение и прошивки оборудования.

Аналогичные предупреждения были также опубликованы Израильской группой реагирования на компьютерные инциденты и Управлением по водным ресурсам правительства Израиля.

Официальных сообщений о подтвержденном вторжении в какую-либо израильскую компанию по очистке и снабжению водой не было. Однако по информации из СМИ, атаки произошли в пятницу и субботу (24 и 25 апреля) и затронули ряд организаций в различных частях страны.

Атаки шифровальщиков на промышленные компании

Захлестнувшая в 2019 году мир волна атак шифровальщиков продолжилась и в первом полугодии 2020 года.

Атака вымогателя остановила производство компании Picanol в Бельгии, Румынии и Китае

13 января 2020 года крупный производитель высокотехнологичных ткацких станков Picanol Group стал жертвой массированной атаки вымогателей. Атака вызвала серьезные нарушения в работе заводов в Бельгии, Румынии и Китае. Какое ПО использовалось для атаки, пока не сообщается.

Атака была замечена ночью, когда сотрудники Picanol в Китае не смогли получить доступ к ИТ-системам. Аналогичные проблемы были зафиксированы в городе

Ипр (Бельгия). Деятельность компании была практически полностью остановлена. 2300 сотрудников Picanol оставались без работы более недели.

Атаки Ruyk на медицинские учреждения

В первом полугодии операторы Ryuk массово атаковали больницы и требовали выкуп за расшифровку файлов. Только в марте от атак Ryuk в США пострадали 10 больниц.

В этих атаках использовалась уже ставшая привычной для Ryuk схема заражения с использованием фишинговых писем и вредоносной программы TrickBot. Эта вредоносная программа позволяет злоумышленникам подключаться к зараженному компьютеру и исследовать сеть атакованной организации. Операторы TrickBot пытаются найти уязвимые системы, а также украсть учётные данные пользователей.

Атака вымогателя на производителя насосных решений DESMI

В ночь с 7 на 8 апреля атаке вымогателя подверглась компания DESMI, датский производитель насосных решений для судов и промышленности. Какая вредоносная программа была использована для атаки, не сообщается.

Согласно официальному заявлению, в результате атаки пострадали информационные системы коммуникаций, включая систему электронной почты, которые были временно отключены. К 14 апреля работоспособность этих систем удалось восстановить. ERP-система и финансовые системы не пострадали, поэтому производственные объекты в Китае, Индии, Америке и Дании продолжили свою работу в обычном режиме лишь с незначительными помехами.

Атака Ragnar Locker на энергетическую компанию EDP

13 апреля крупная португальская энергетическая компания Energias de Portugal (EDP) подверглась атаке вымогателя. В результате атаки с использованием вредоносной программы Ragnar Locker системы компании были зашифрованы. Помимо этого, киберпреступники утверждают, что прежде чем зашифровать данные, они украли 10 Тб конфиденциальных файлов компании и теперь угрожают опубликовать их, если не будет уплачен выкуп в размере 1580 BTC (что на данный момент составляет примерно 10,9 млн долларов).

В качестве доказательства того, что преступники действительно обладают конфиденциальной информацией EDP, операторы Ragnar Locker опубликовали часть украденных данных, в том числе имена и пароли от учетных записей сотрудников.

Согласно записке с требованием выкупа, злоумышленники смогли получить доступ к конфиденциальной информации о выставленных счетах, договорах, транзакциях, клиентах и партнерах.

Проанализировав различные образцы шифровальщика, эксперты «Лаборатории Касперского» пришли к выводу, что весь текст записки с требованием выкупа формируется индивидуально для каждой жертвы, а значит атаки с использованием Ragnar Locker имеют целенаправленный характер.

Атака на промышленные объекты Stadler

7 мая 2020 года о кибератаке на свои промышленные объекты сообщил швейцарский производитель поездов Stadler. Согласно заявлению компании, некоторые компьютеры

корпоративной сети были заражены вредоносным ПО, со скомпрометированных устройств были украдены данные. Злоумышленники, стоящие за атакой, связались с представителями компании и потребовали выкуп, угрожая опубликовать похищенную информацию в случае неуплаты.

Компания обратилась в соответствующие органы власти и привлекла для расследования инцидента внешних ИБ-специалистов. Для восстановления функционирования всех затронутых систем использовались резервные копии. Производственные процессы компании в результате атаки не пострадали.

Какое именно вредоносное ПО использовалось в атаке, не сообщалось. Однако требование выкупа и необходимость восстановления систем с использованием резервных копий указывает на то, что, вероятнее всего, компания Stadler стала жертвой атаки программы-вымогателя.

Атаки Mailto и Nefilim на логистическую компанию Toll Group

Австралийская логистическая компания Toll Group в первом полугодии 2020 года дважды подверглась атаке вымогательского ПО.

Первая атака произошла в конце января. В ходе этой атаки использовался вариант вымогательского ПО Mailto. Для предотвращения распространения вредоносного ПО часть информационных систем компании была отключена. Это привело к задержкам с отправкой грузов как корпоративным, так и индивидуальным клиентам. Среди клиентов Toll Group, отправка посылок которых была задержана, оказалась национальная почтовая служба Australia Post.

Во второй раз Toll Group подверглась атаке в мае. Тогда вымогательским ПО Nefilim была заражена одна из корпоративных систем компании, в которой находились данные о сотрудниках компании, а также некоторые соглашения с корпоративными клиентами. Перед шифрованием файлов злоумышленники украли около 200 Гб данных компании и потребовали выкуп за разблокировку ИТ-систем, однако руководство Toll Group отказались пойти на сделку с ними. В ответ на инцидент все ИТ-системы компании были отключены.

20 мая стало известно о том, что операторы Nefilim опубликовали часть украденных данных.

К 29 мая все информационные системы и логистические операции Toll Group были восстановлены.

Атака шифровальщика Sodinokibi на электроэнергетические компании

14 мая о заражении своих ИТ-систем вредоносным ПО сообщила крупная электроэнергетическая компания Великобритании Elexon. В результате атаки пострадали только системы внутренней IT-сети компании, включая почтовую систему, и ноутбуки. Ключевые информационные сервисы и системы электроснабжения не были затронуты кибератакой.

В июне появилась информация, что компания была атакована шифровальщиком Sodinokibi, также известного как REvil.

Еще одной жертвой Sodinokibi позднее стала Бразильская электроэнергетическая компания Light S.A. По информации из СМИ в конце июня компания подверглась атаке шифровальщика, операторы вымогателя потребовали выкуп криптовалютой Монерос

порядка 7 млн долларов США. После 19 июня размер выкупа удвоился до порядка 14 млн долларов США.

Атака не оказала негативного влияния на энергоснабжение, но нарушила бизнес-процессы компании, связанные с выставлением счетов. Несмотря на официальное подтверждение факта атаки, другие подробности инцидента не раскрывались.

Позднее исследователями был найден образец вредоносного ПО Sodinokibi, который предположительно использовался для атаки на Light S.A. Данное вредоносное ПО распространяется по модели «Вымогательское ПО как услуга» (Ransomware-as-a-Service, RaaS) и, вероятно, связано с преступной группой «Pinchy Spider», стоящей за другим вымогательским ПО GandCrab.

Атака на производителя напитков Lion

9 июня жертвой атаки вымогательского ПО стал австралийский производитель напитков Lion. В результате атаки компания была вынуждена отключить зараженные ИТ-системы, что привело к остановке некоторых технологических процессов и нарушению графика поставок продукции клиентам. В частности, была приостановлена работа пивоваренных заводов в Австралии и Новой Зеландии. Атака также повлияла на работу производственных площадок Lion Dairy & Drinks, отвечающих за производство различных молочных продуктов.

Информация о том, какое вымогательское ПО использовалось для атаки на компанию, не сообщалась.

18 июня компания Lion подверглась еще одной атаке шифровальщика. По информации из СМИ, во второй атаке использовалось вредоносное ПО Sodinokibi (REvil). Злоумышленники потребовали выкуп в размере 12234,28 XMR (порядка 800 000 долларов) и угрожали публиковать украденные у компании конфиденциальные данные. При этом атакующие угрожали увеличить сумму выкупа вдвое, если деньги не будут переведены до 19 июня.

По последней информации на официальном сайте компании, посвященной инциденту, 26 июня работа всех производственных объектов была восстановлена, однако работы по восстановлению ИТ-систем еще продолжались.

Целевые атаки на промышленные компании с использованием шифровальщика Snake

8 июня 2020 стало известно о неполадках в компьютерной сети японского мото- и автопроизводителя Honda в Европе и Японии. В частности, сообщалось о технических трудностях в работе службы поддержки клиентов Honda и финансовых служб компании.

ИБ-эксперты полагают, что, вероятнее всего, один из серверов компании был заражен вымогательским ПО Snake (EKANS): на VirusTotal был обнаружен образец вредоносной программы Snake, который проверяет доменное имя компании Honda «mds.honda.com» (вероятно, использующееся во внутренней сети компании). Если доменное имя не удается разрешить (определить IP-адрес), работа вымогателя завершается без шифрования каких-либо файлов. По мнению исследователей, это может указывать на целенаправленные действия злоумышленников.

Эксперты Kaspersky ICS CERT, используя данные собственной телеметрии, обнаружили также и другие образцы, сходные с тем, который был загружен на VirusTotal.

Результаты нашего исследования явно указывают на то, что злоумышленники проводят многоступенчатые хакерские атаки, при этом каждая атака направлена на конкретную организацию. Шифрование данных при помощи Snake – конечный этап этих атак. Сам шифровальщик Snake написан на языке Golang, который не очень распространен и на сегодняшний день встречается в основном в образцах вредоносных программ, использующихся APT-группировками.

Известно, что помимо Honda в числе жертв оказались также энергетические компании Enel Group. По данным Kaspersky ICS CERT, целью атак стали также немецкая компания – поставщик изделий для автомобилестроительных компаний и промышленного производства и немецкая компания, занимающаяся производством медицинского оборудования и расходных материалов. По всей видимости, атаке подверглись также и другие автомобилестроительные и производственные компании – схожие экземпляры Snake были обнаружены на компьютерах в Китае, Японии и в Европе.

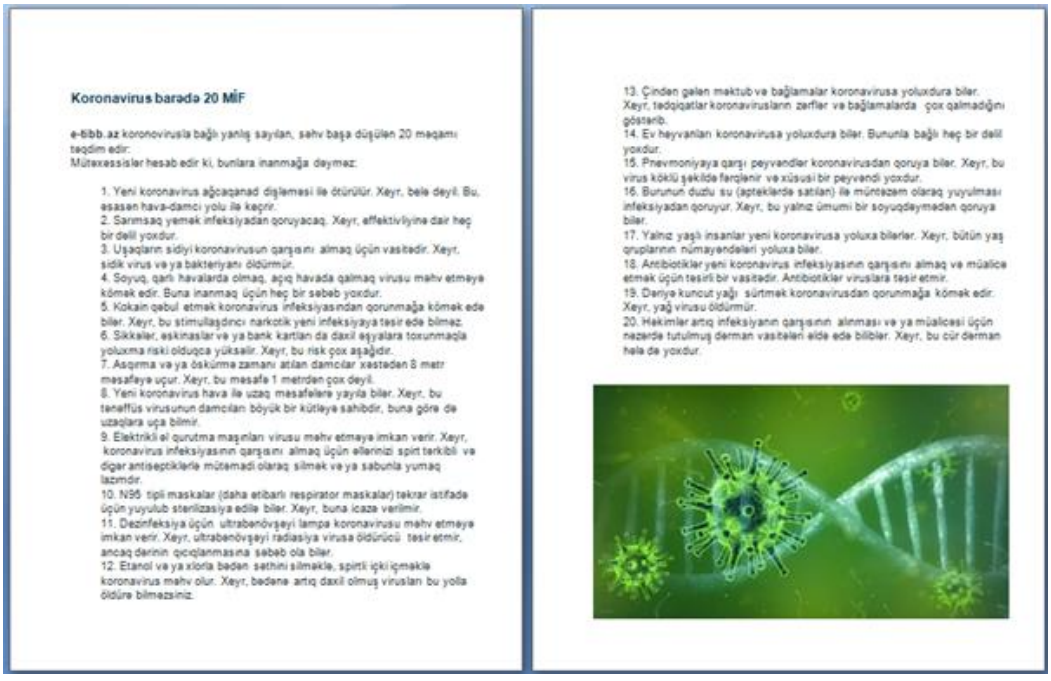
Влияние пандемии COVID-19

В ходе наших исследований мы не могли обойти вниманием широко обсуждающийся вопрос влияния пандемии COVID-19 на ландшафт угроз промышленных организаций в целом и их технологических сетей в частности.

Действительно, как и следовало ожидать, злоумышленники используют пандемию и вызванные ею глобальные изменения в обществе в своих целях. Как сообщали многократно различные источники, тема COVID-19 эксплуатируется в большом количестве фишинговых атак – как массовых, так и как целенаправленных.

В одном из наших приватных отчётов, доступных по подписке, описана APT-атака, нацеленная на предприятия и учреждения Азербайджана, в которой используются документы COVID-тематики.

Один из эксплуатирующих тему COVID-19 вредоносных документов, использованных в ходе APT-атаки



Koronavirus barədə 20 MİF

e-tibb.az koronovirusla bağlı yanlış sayılan, səhv başa düşülən 20 məqamı təqdim edir:
Mütəxəssislər hesab edir ki, bunlara inanmağa dəyməz:

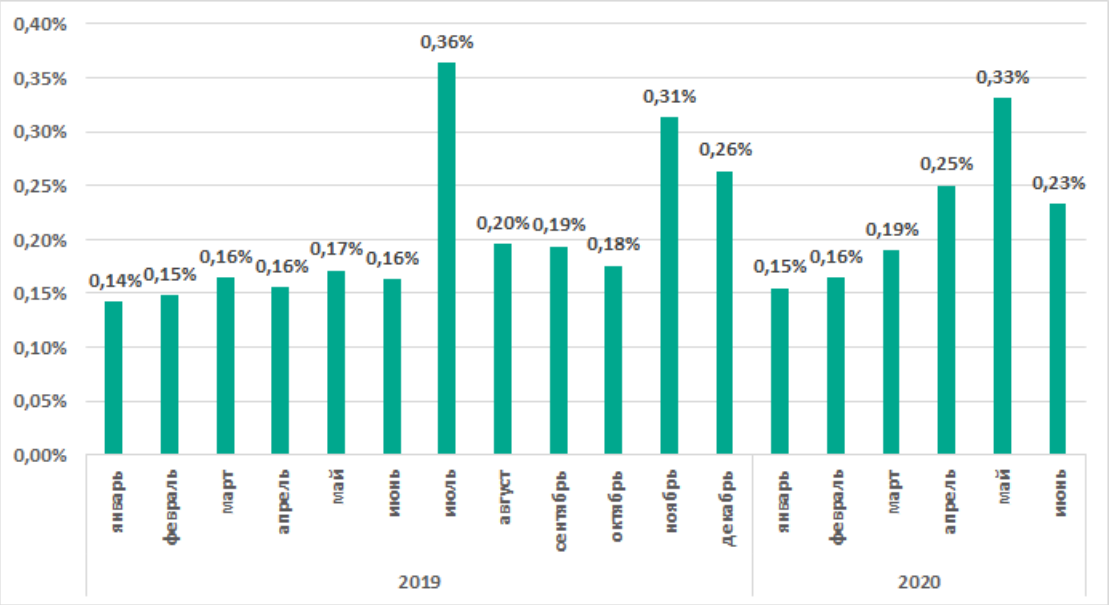
1. Yeni koronavirus ağciyərlərə düşməsi ilə ötürülür. Xeyr, belə deyil. Bu, əsasən hava-damcı yolu ilə keçir.
2. Sarımsaq yemək infeksiyadan qoruyacaq. Xeyr, effektivliyinə dair heç bir dəlil yoxdur.
3. Uşaqların sidiyi koronavirusun qarşısını almaq üçün vasitədir. Xeyr, sidik virus və ya bakteriyanı öldürmür.
4. Soyuq, qarlı havalarda olmaq, açıq havada qalmaq virusu məhv etməyə kömək edir. Buna inanmaq üçün heç bir səbəb yoxdur.
5. Kokain qəbul etmək koronavirus infeksiyasından qorunmağa kömək edə bilər. Xeyr, bu stimullaşdırıcı narkotik yeni infeksiyaya təsir edə bilməz.
6. Əlcəklər, əskinaslar və ya bank kartları da daxil əşyalara toxunmaqla yoluxma riski olduqca yüksəlir. Xeyr, bu risk çox aşağıdır.
7. Asqırma və ya öskürmə zamanı atılan damcılar xəstədən 8 metr məsafəyə uçur. Xeyr, bu məsafə 1 metrdən çox deyil.
8. Yeni koronavirus hava ilə uzaq məsafələrə yayıla bilər. Xeyr, bu tənəffüs virusunun damcıları böyük bir kütləyə sahibdir, buna görə də uzağlara uça bilmir.
9. Elektrikli əl qurutma maşınları virusu məhv etməyə imkan verir. Xeyr, koronavirus infeksiyasının qarşısını almaq üçün əllərinizi spirt tərkibli və digər antiseptiklərlə müntəmadi olaraq silmək və ya sabunla yumaq lazımdır.
10. N95 tipli maskalar (daha etibarlı respirator maskaları) təkrar istifadə üçün yuyulub sterilizasiya edilə bilər. Xeyr, buna icazə verilmir.
11. Dezinfeksiya üçün ultrabənövşəyi lampa koronavirusu məhv etməyə imkan verir. Xeyr, ultrabənövşəyi radiasiya virusa öldürücü təsir etmir, ancaq dərinin qıcıqlanmasına səbəb ola bilər.
12. Etanol və ya xlorla bədən səthini silməklə, spirtli içki içməklə koronavirus məhv olur. Xeyr, bədənə artıq daxil olmuş virusları bu yolla öldürə bilməzsiniz.
13. Çindən gələn məktub və bağlamalar koronavirusa yoluxdura bilər. Xeyr, tədqiqatlar koronavirusların zərflər və bağlamalarda çox qalmadığını göstərib.
14. Ev heyvanları koronavirusa yoluxdura bilər. Bununla bağlı heç bir dəlil yoxdur.
15. Pnevmoniyaya qarşı peyvəndlər koronavirusdan qoruya bilər. Xeyr, bu virus köklü şəkildə fərqlənir və xüsusi bir peyvəndi yoxdur.
16. Burunun duzlu su (aptekdə satılan) ilə müntəzəm olaraq yuyulması infeksiyadan qoruyur. Xeyr, bu yalnız ümumi bir soyuqdəymədən qoruya bilər.
17. Yalnız yaşlı insanlar yeni koronavirusa yoluxa bilərlər. Xeyr, bütün yaş qruplarının nümayəndələri yoluxa bilər.
18. Antibiotiklər yeni koronavirus infeksiyasının qarşısını almaq və müalicə etmək üçün təsirli bir vasitədir. Antibiotiklər viruslara təsir etmir.
19. Dəriyə kuncut yağı sürtmək koronavirusdan qorunmağa kömək edir. Xeyr, yağ virusu öldürmür.
20. Həkimlər artıq infeksiyanın qarşısının alınması və ya müalicəsi üçün nəzərdə tutulmuş dərman vasitələri əldə edə biliblər. Xeyr, bu cür dərman hələ də yoxdur.

Однако, если задаться целью количественно оценить изменение ландшафта угроз ICS, то результат оказывается неожиданным. Единственная заметная тенденция

глобального роста процента атакованных компьютеров АСУ наблюдается при анализе статистики атак на RDP (Remote Desktop Protocol), поднятых на промышленных компьютерах.

Так, в феврале – мае 2020 года чётко прослеживается постоянный помесячный рост (с последующим снижением в июне) процента компьютеров АСУ, на которых решениями «Лаборатории Касперского» фиксировались попытки подбора паролей к RDP.

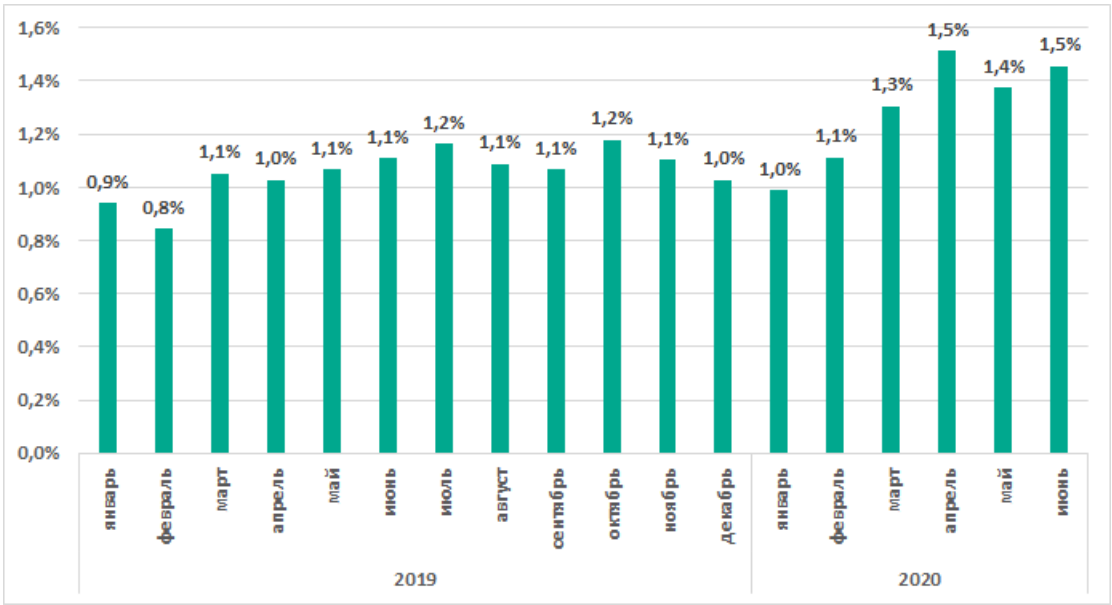
Процент компьютеров АСУ, на которых фиксировались попытки подбора паролей к RDP



Как мы видим на графике, весенний рост процента компьютеров АСУ, подвергшихся bruteforce-атакам, не превышает по амплитуде годовые колебания, хотя и оказывается более длительным по продолжительности, чем все предыдущие скачки.

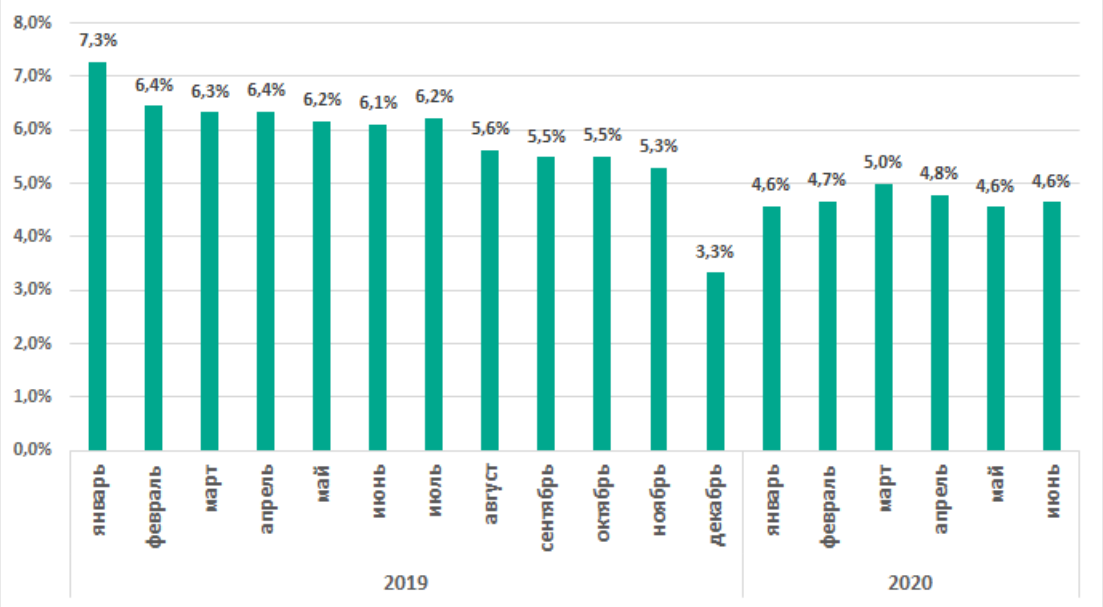
По всей видимости рост по этому параметру процента атакованных компьютеров АСУ спровоцирован увеличением частоты использования RDP в феврале – июне этого года.

Процент компьютеров АСУ, доступных по RDP, январь 2019 – июнь 2020



Примечательно, что рост процента компьютеров АСУ, на которых поднят RDP, в первом квартале 2020 года произошел на фоне довольно длительного периода борьбы с использованием RAT на промышленных предприятиях. На графике ниже хорошо видно уменьшение процента компьютеров АСУ, на которых используются программы удаленного администрирования, в течение 2019 года. Отметим, что в первом полугодии 2020 этот показатель стабилизировался (и даже немного вырос в феврале – апреле в сравнении с январём), чего не наблюдалось зимой и весной прошлого года, и что также может быть связано с последствиями пандемии.

Процент компьютеров АСУ, на которых используются RAT, январь 2019 – июнь 2020



На наш взгляд, рост процента компьютеров АСУ, на которых используется RDP, может свидетельствовать о том, что большинство из новых RDP-сессий авторизованы службами IT и ИБ АСУ ТП. Действительно, безопасное использование служб RDP при прочих равных может оказаться проще настраивать и контролировать, чем для других RAT-приложений. И, по всей видимости, разрешение новых RDP – компромисс, обусловленный объективной необходимостью выполнять производственные задачи удалённо в условиях пандемии.

Рост процента атакованных компьютеров АСУ, на которых зафиксированы (и предотвращены) попытки подбора пароля к RDP, может показаться незначительным, однако не стоит забывать, что любая такая атака, окажись она успешной, сразу дала бы злоумышленникам удалённый доступ к компьютерам инженеров и системам АСУ, и недооценивать опасность таких атак не стоит.

Как уже было сказано ранее, других аномальных всплесков вредоносной активности, которые можно было-бы объяснить последствиями пандемии, нам найти пока не удалось. Надеемся, что это действительно отражает отсутствие существенных негативных изменений ландшафта угроз ICS.

Общая статистика по миру

В разделе представлены результаты анализа статистических данных, полученных с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые добровольно подтвердили свое согласие на их анонимную передачу и обработку с целью, описанной в Соглашении KSN для установленного на их компьютере продукта «Лаборатории Касперского».

Подключение к сети KSN даёт нашим клиентам возможность улучшить скорость реакции защитных решений на неизвестные ранее угрозы и в целом повысить качество детектирования установленного продукта за счёт обращения к облачной инфраструктуре хранения данных о вредоносных объектах, которую технически невозможно передать целиком на сторону клиента из-за её объёма и потребляемых ресурсов.

Переданная пользователем телеметрия содержит только те типы и категории информации, которые описаны в соответствующем Соглашении KSN. Эти данные в значительной мере не только помогают в анализе ландшафта угроз, но и необходимы для обнаружения новых угроз, включая целенаправленные атаки и APT[1].

Методика подготовки статистики

Статистические данные, представленные в отчете, получены с защищаемых продуктами «Лаборатории Касперского» компьютеров АСУ, которые Kaspersky 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);
- компьютеры, используемые для администрирования технологических сетей;
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации.

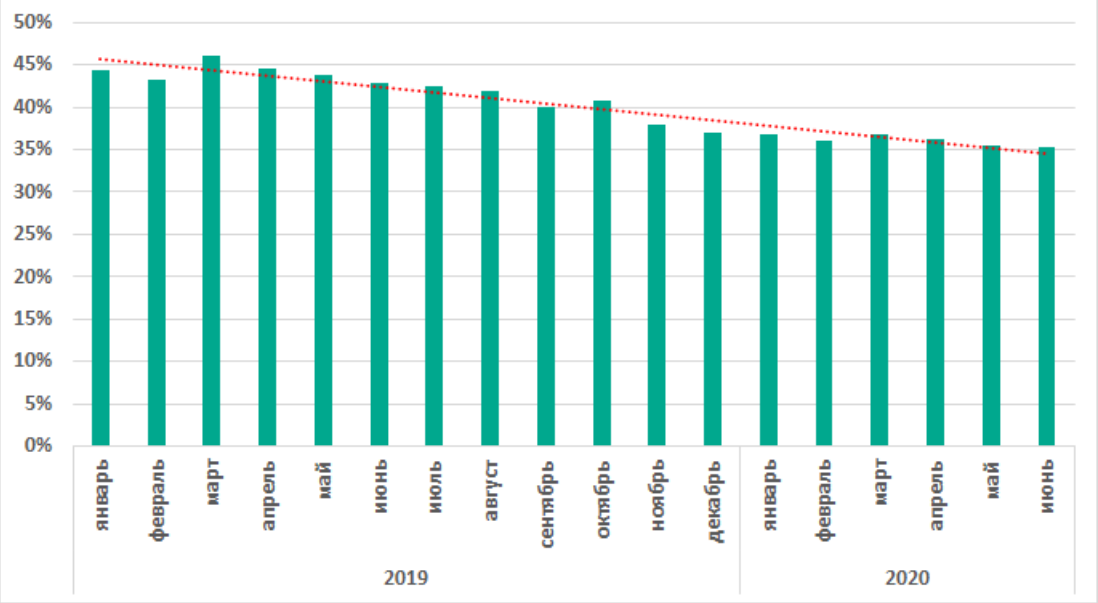
Атакованными мы считаем те компьютеры, на которых в течение отчетного периода защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете процента машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение отчетного периода, по отношению ко всем компьютерам из нашей выборки, с которых в течение отчетного периода мы получали обезличенную информацию.

[1] Организациям, в отношении любых данных которых наложены ограничения на их передачу во вне периметра организации, рекомендуем рассмотреть вариант использования сервиса Kaspersky Private Security Network.

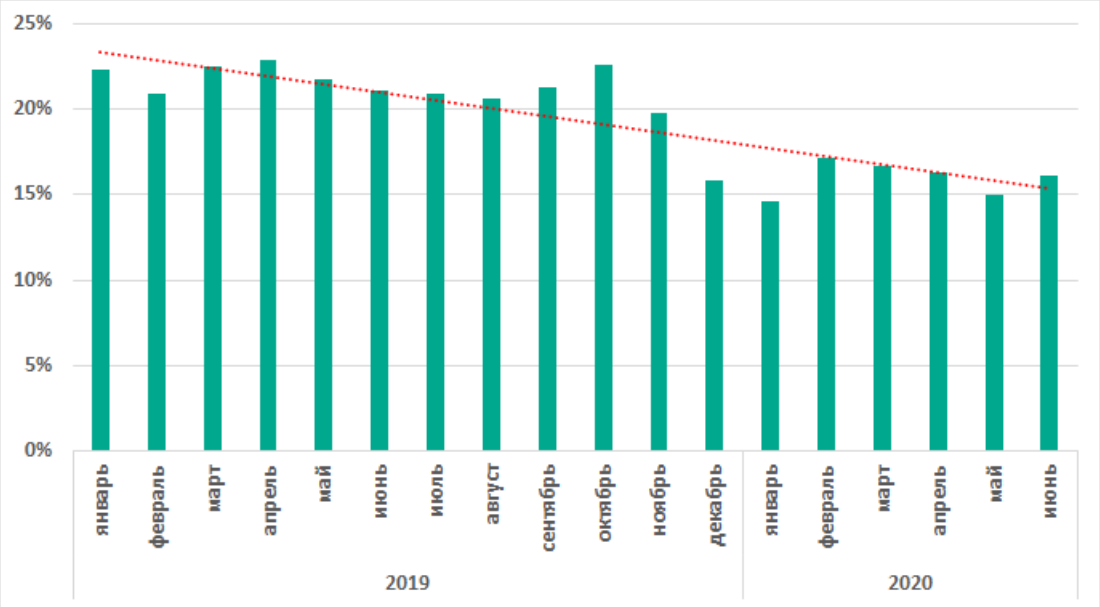
Общие тенденции в ландшафте угроз для компьютеров АСУ, корпоративных и персональных компьютеров

Со второй половины 2019 года наблюдается снижение процента атакованных компьютеров, как среди АСУ, так и в корпоративной и персональной средах.

Процент компьютеров *всех пользователей «Лаборатории Касперского»*, на которых были заблокированы вредоносные объекты, по месяцам (январь 2019 – июнь 2020)



Процент *компьютеров АСУ*, на которых были заблокированы вредоносные объекты, по месяцам (январь 2019 – июнь 2020)



Среди множества факторов, влияющих на этот показатель, можно выделить следующие:

- Уменьшение количества массовых атак, направленных на заражение компьютеров шпионским ПО и агентами различных ботнетов, криптомайнерами, агресивными загрузчиками рекламы (Adware);

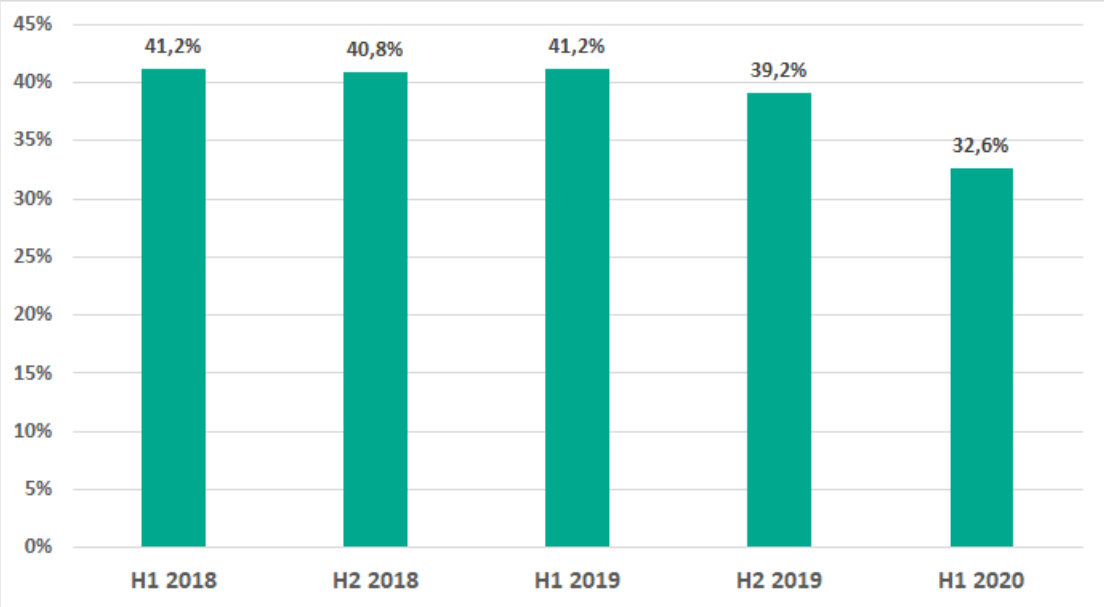
- Переход от масштабных массовых атак к более локальным, в частности:
  - уменьшение количества целей фишинговых рассылок – массовые рассылки сменяют небольшие локальные кампании;
  - уменьшение количества вредоносных и зараженных веб-ресурсов, используемых для массового распространения вредоносного ПО;
- сокращение количества компьютеров, зараженных старым самораспространяющимся ПО – червями и вирусами.

Вместе с тем, угрозы становятся более локальными, более фокусированными, и, как следствие – более сложными и менее заметными.

Процент компьютеров, на которых были заблокированы вредоносные объекты

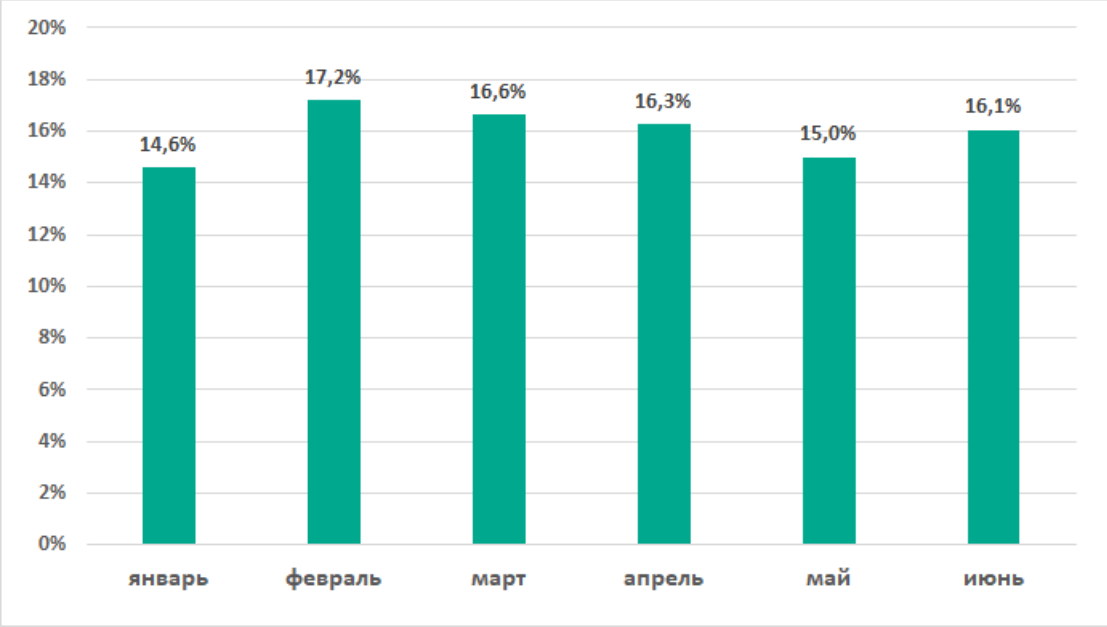
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в первом полугодии 2020 года составил 32,6%. По сравнению с предыдущим полугодием этот показатель снизился на 6,6 п.п.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



В первом полугодии 2020 года наибольший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в феврале, наименьший – в январе.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам (январь – июнь 2020)

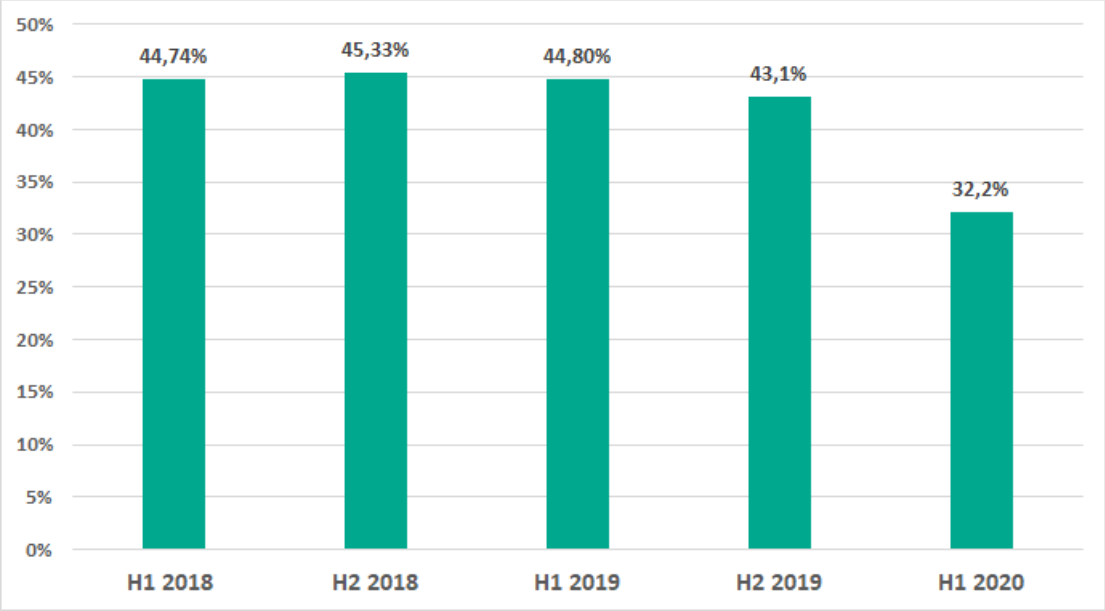


Россия

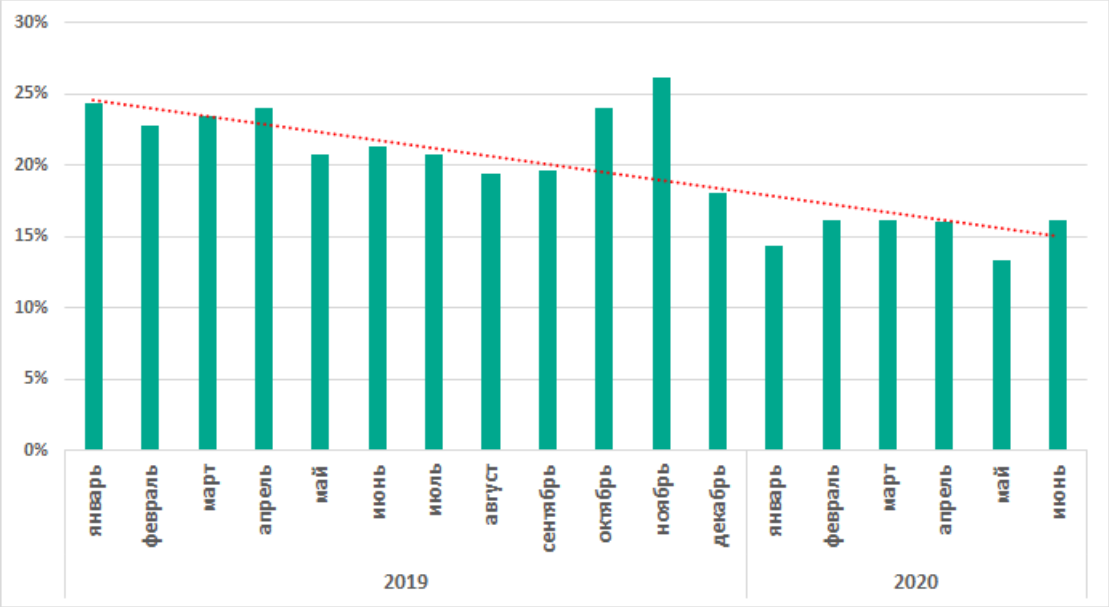
Тенденция уменьшения процента атакованных компьютеров АСУ наблюдается и в России.

В России в течение первого полугодия 2020 года хотя бы один раз вредоносные объекты были заблокированы на 32,2% компьютеров АСУ. Это на 10,9 п.п. меньше, чем во втором полугодии 2019 года.

Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

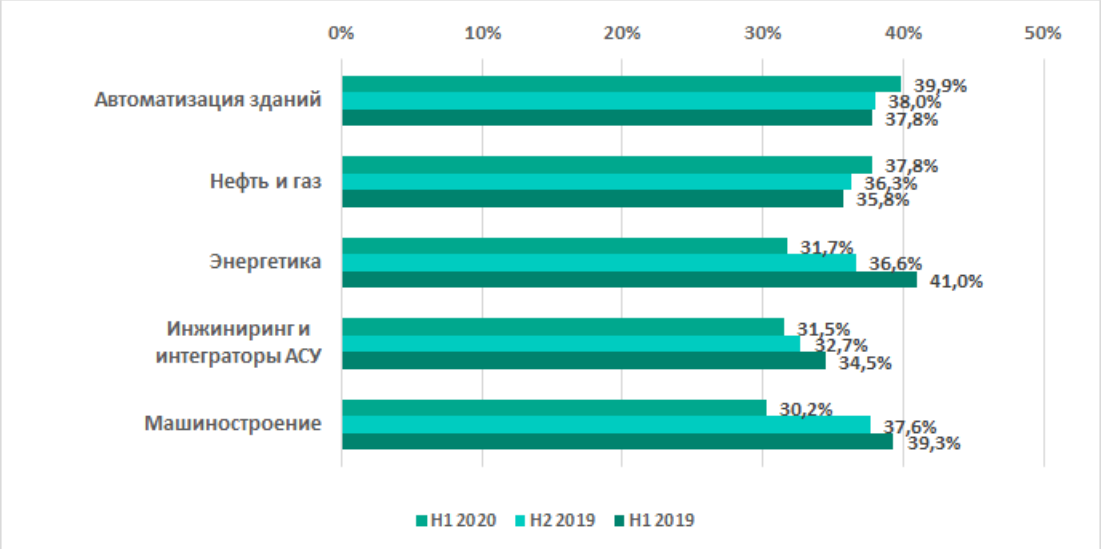


Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам (январь 2019 – июнь 2020)



Некоторые индустрии

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых индустриях



Несмотря на общую тенденцию снижения процента атакованных компьютеров, в первом полугодии 2020 немного выросли показали компьютеров из Нефтегазовой отрасли, а также компьютеров, используемых в составе систем автоматизации зданий.

Компьютеры, используемые в системах автоматизации зданий, часто подключены к корпоративной сети и имеют доступ к различным сервисам, таким как интернет, корпоративная почта, контроллер домена и пр., т.е. они имеют такую же поверхность атаки, как и обычные корпоративные системы, более широкую по сравнению с компьютерами АСУ.

В частности, как показало расследование недавних атак с использованием шифровальщика Snake, продукты «Лаборатории Касперского» блокировали вредоносное ПО не только в корпоративной сети промышленных организаций,

но и на серверах видеонаблюдения, которые были подключены к корпоративному контроллеру домена.

Нередко системы автоматизации зданий принадлежат подрядной организации и, даже имея доступ к корпоративной сети компании, не всегда находятся в ведении корпоративной службы информационной безопасности. Учитывая, что вместе с уменьшением количества массовых атак увеличивается количество и сложность направленных атак, в которых активно используются различные средства для распространения внутри атакуемой сети, системы автоматизации зданий могут оказаться даже менее защищенными, чем корпоративные системы в той же сети.

На компьютерах, используемых для проектирования, обслуживания и автоматизации промышленных систем в Нефтегазовой отрасли, в первом полугодии 2020 продукты «Лаборатории Касперского» заблокировали множество новых модификаций вредоносного ПО типа Червь (Worm), написанных на скриптовых языках программирования, в частности Python и PowerShell. Всплеск детектирования этих червей пришёлся на период с конца марта по середину июня 2020 и в большей степени затронул Китай и страны ближнего востока.

Все обнаруженные образцы червей, как на Python так и на PowerShell, способны получать данные аутентификации из памяти системных процессов атакованного компьютера с целью распространения по сети. В большинстве случаев для кражи данных аутентификации из памяти вредоносное ПО использует различные версии Mimikatz, но были обнаружены также образцы на PowerShell, которые вместо Mimikatz используют системную библиотеку comsvcs.dll (MS Windows) для сохранения на диске снимка памяти процесса, в котором далее производится поиск данных аутентификации.

Разнообразие обнаруженного вредоносного ПО

В первом полугодии 2020 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 19,7 тысяч модификаций вредоносного ПО из 4119 различных семейств. Стало заметно больше семейств бэкдоров, троянцев-шпионов, эксплойтов для Win32 и вредоносного ПО на платформе .NET.

Категории вредоносных объектов

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Для того чтобы дать лучшее представление о типах заблокированных угроз, мы выполнили их детальную классификацию. Заметим, что получившиеся проценты суммировать - некорректно, потому что во многих случаях на одном компьютере за отчётный период могли быть заблокированы угрозы двух и более типов.

Результаты нашего детального анализа дали следующие оценки процента компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий:

Процент компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий

- 11,0% – ресурсы в интернете из черного списка.

  Веб-антивирус защищает компьютер, когда установленные на нем программы (браузеры, почтовые клиенты, компоненты автообновления прикладного ПО и др.) пытаются подключиться к IP и URL адресам, занесенным в черный список. Такие ресурсы связаны с распространением или управлением каким-либо вредоносным ПО.

  В частности, в черные списки попадают также ресурсы, на которых распространяется, например, вредоносное ПО типа Trojan-Spy и Ransomware, замаскированное под утилиты для взлома/сброса пароля на контроллерах различных производителей, crack/patch для промышленного и инженерного программного обеспечения, используемого в технологической сети.
- 6,5% – зловредные скрипты и перенаправления на веб-ресурсах (JS и Html), выполняющиеся в контексте браузера, а также эксплойты для браузеров – 0,2%.
- 5,6% –троянцы-шпионы, бэкдоры и кейлоггеры, которые встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Как правило, конечная цель таких атак – кража денег.
- 5,1% – черви (Worm), распространяющиеся, как правило, через съемные носители и сетевые папки, а также черви, распространяющие через почтовые сообщения (Email-Worm), сетевые уязвимости (Net-Worm) и мессенджеры (IM-Worm). Большинство червей являются устаревшими с точки зрения сетевой инфраструктуры управления ими. Но есть среди них и такие как Zombaque (0,02%) – с реализованной P2P сетевой архитектурой, позволяющей злоумышленникам активировать его в любой момент.

- 3,2% – вредоносные программы класса Virus.

  Среди этих программ уже много лет детектируются такие семейства как Sality (0,9%), Nimnul (0,6%), Virut (0,4%). Хотя эти вредоносные семейства считаются устаревшими, поскольку их командные серверы управления давно не активны, они традиционно вносят значительный вклад в статистику в силу самораспространения и недостаточных мер по их полному обезвреживанию.
- 3,1% – вредоносные LNK-файлы.

  Такие файлы, в основном, блокируются на съемных носителях. Они являются частью механизма распространения для таких старых семейств вредоносного ПО как Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou и других.

  В этой категории также широко представлены LNK-файлы с уязвимостью CVE-2010-2568 (0,4%), которая впервые была использована для распространения червя Stuxnet, а затем стала использоваться для распространения множества семейств, таких как Sality, Nimnul/Ramnit, ZeuS, Vobfus и других.

  В настоящее время замаскированные под легитимный документ LNK-файлы могут использоваться как часть многоступенчатой атаки. Они запускают powershell-скрипт, скачивающий зловредный файл.

  В редких случаях запускаемый вредоносный powershell скрипт скачивает и внедряет в память бинарный код, являющийся специфичной модификацией пассивного TCP бэкдора из набора metasploit.
- 2,2% – вредоносные документы (MSOffice+PDF), содержащие эксплойты, зловредные макросы и зловредные ссылки.
- 1,5% – вредоносные файлы (исполняемые, скрипты, autorun.inf, .LNK и другие), которые запускаются автоматически при запуске системы или при подключении съемного носителя.

  Это файлы из множества разнообразных семейств, которые объединены фактом автозапуска. Из наиболее «безобидной» функциональности у подобных файлов – автоматический запуск браузера с предустановленной стартовой страницей. В большинстве случаев вредоносное ПО, использующее autorun.inf, является модификацией зловредов старых семейств (Palevo, Sality, Kido и др.).
- 1,3% – банковские троянцы.
- 1,2% – веб-майнеры, выполняемые в браузерах;
  0,9% – майнеры - исполняемые файлы для ОС Windows.
- 0,9% – вредоносные программы для AutoCad.

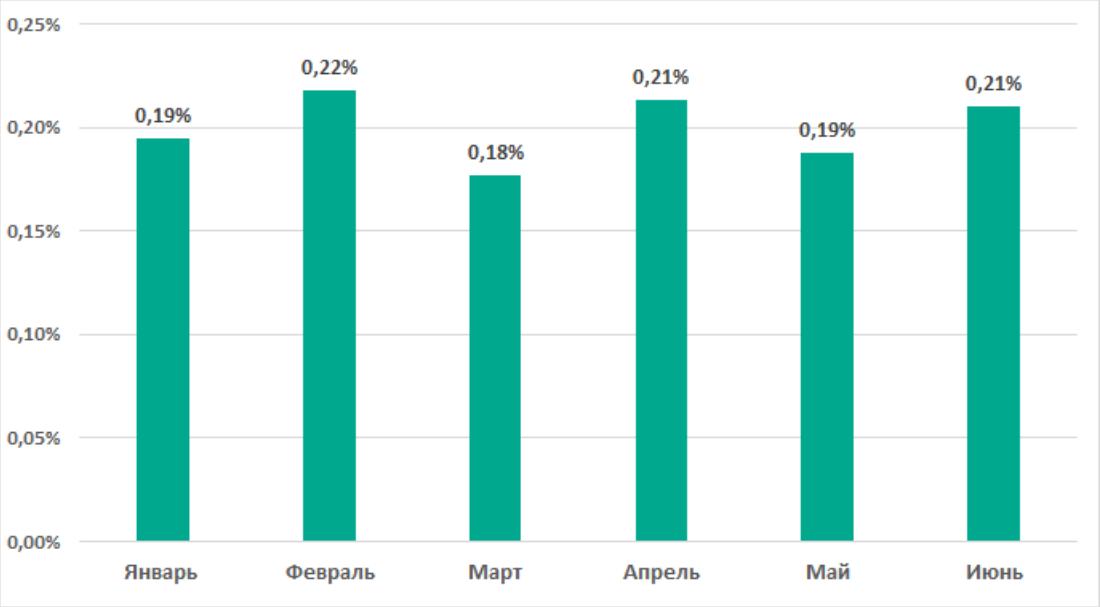
  Отметим, что вредоносное ПО для AutoCad, в частности вирусы, детектируются преимущественно в Восточной Азии – на компьютерах технологических сетей, в том числе в сетевых папках и на рабочих станциях инженеров.
- 0,6% – программы-вымогатели.
- 0,5% – вредоносные файлы для мобильных устройств, которые блокируются при подключении устройств к компьютерам.

Программы – вымогатели

В первом полугодии 2020 года вредоносные программы-вымогатели были заблокированы на 0,63% компьютеров АСУ. Это незначительно отличается от итогов предыдущего полугодия (0,61%).

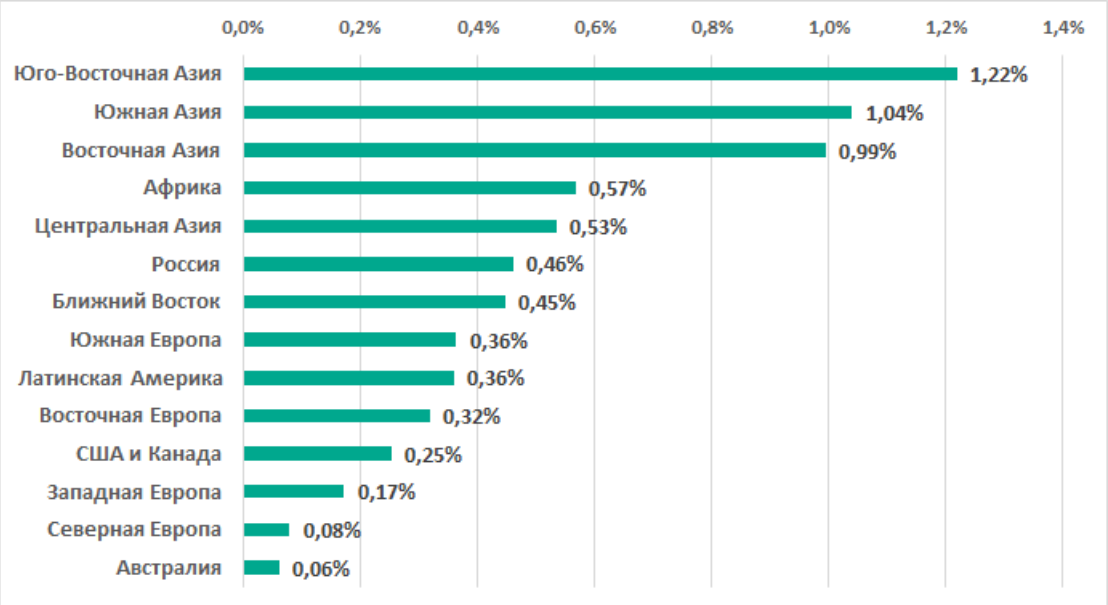
В течение первых шести месяцев 2020 года этот показатель колебался от 0,18% в марте до 0,22% в феврале.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, по месяцам (январь – июнь 2020)

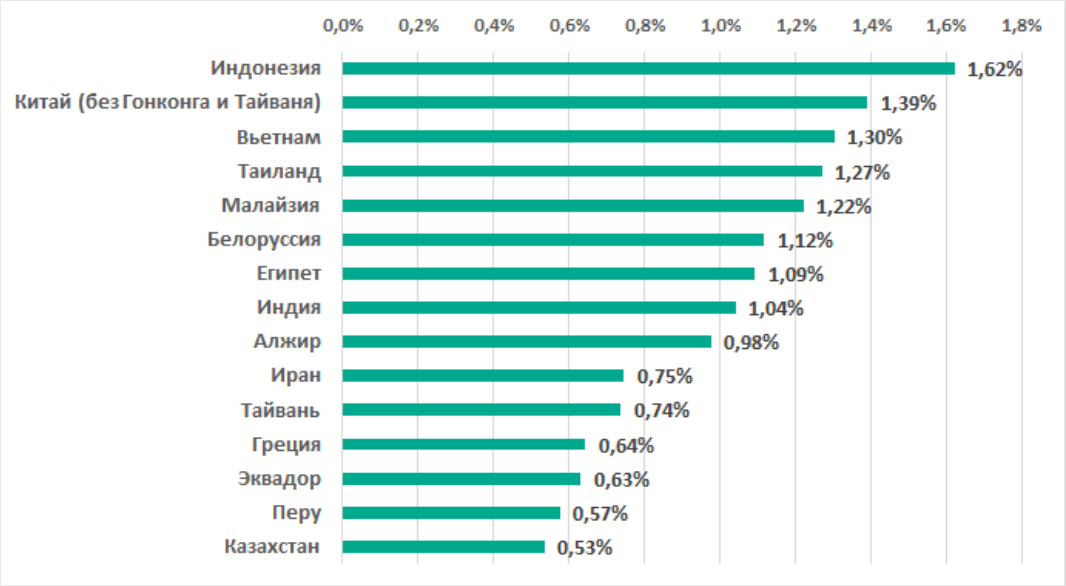


Юго-Восточная, Южная и Восточная Азия с большим отрывом от других регионов лидируют в рейтинге регионов по проценту атакованных вымогателями компьютеров АСУ.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, первое полугодие 2020



ТОР 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, первое полугодие 2020



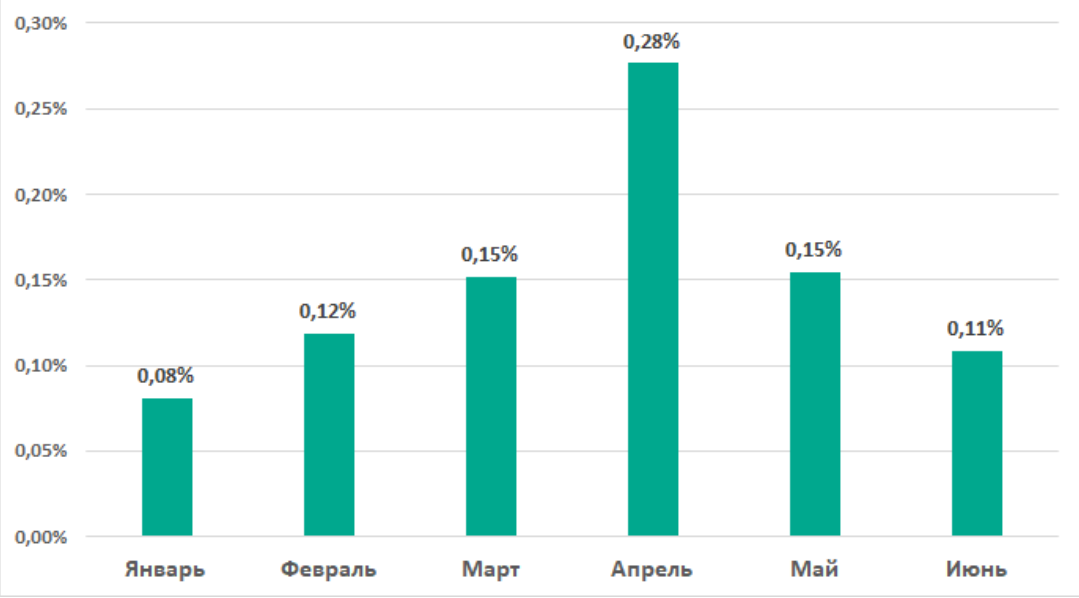
Больше половины стран в ТОР 15 – азиатские. Из европейских стран в ТОР 15 попали Белоруссия и Греция.

Россия

По проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, Россия находится в середине рейтинга с показателем 0,46%.

Как видно на графике ниже в течение первых четырех месяцев полугодия процент атакованных программами-вымогателями компьютеров в России увеличивался и достиг максимума в апреле. В мае-июне этот показатель пошел на спад.

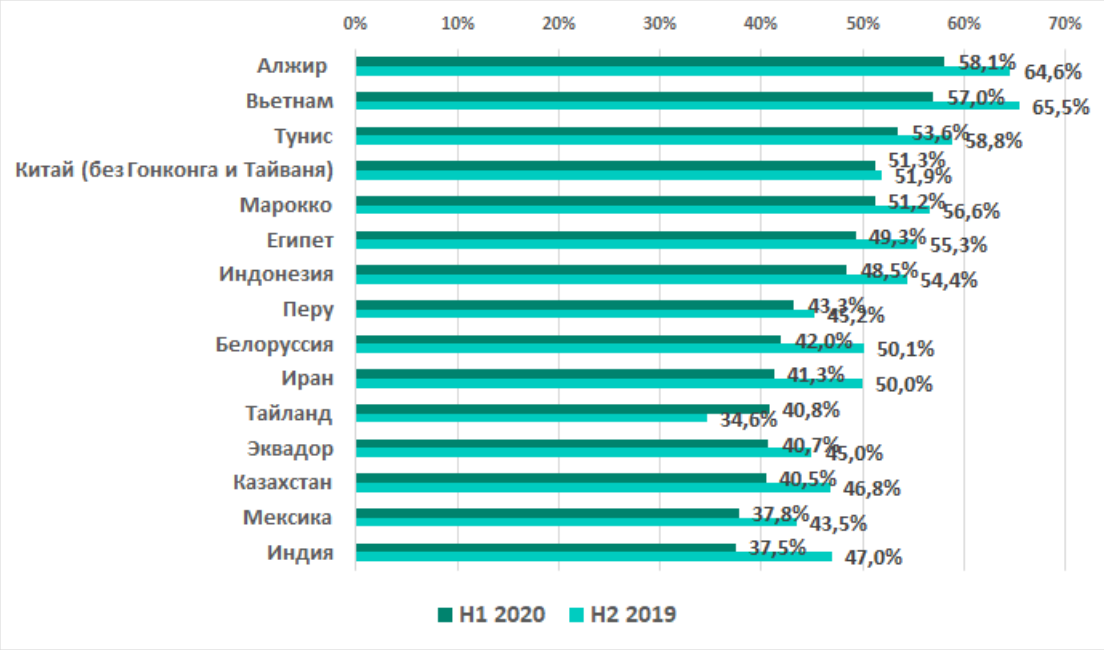
Россия. Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, по месяцам (январь – июнь 2020)



География

Страны

TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты

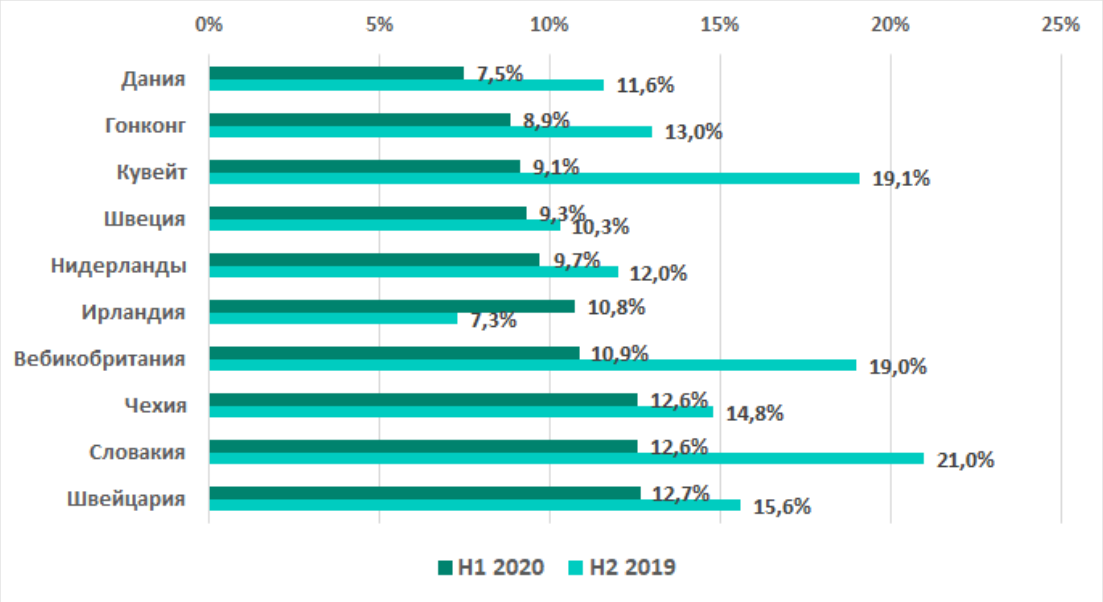


По итогам полугодия в TOP 5 впервые после 2017 года вернулся Китай.

Наиболее значительное увеличение процента компьютеров АСУ, на которых была предотвращена вредоносная активность, наблюдается в Греции (на 7,8 п.п.), Таиланде (на 6,2 п.п.) и в Португалии (на 4,3 п.п.).

В подавляющем большинстве стран этот показатель уменьшился. Наиболее значительно – в ЮАР (на 19,1 п.п.), Израиле (на 12,8 п.п.), России (на 13,9 п.п.) и в Кувейте (на 10 п.п.). В результате Кувейт по итогам полугодия даже вошел в список десяти наиболее благополучных стран. Отметим, что в этом списке уже не первый раз присутствуют две страны из Восточной Европы – Чехия и Словакия.

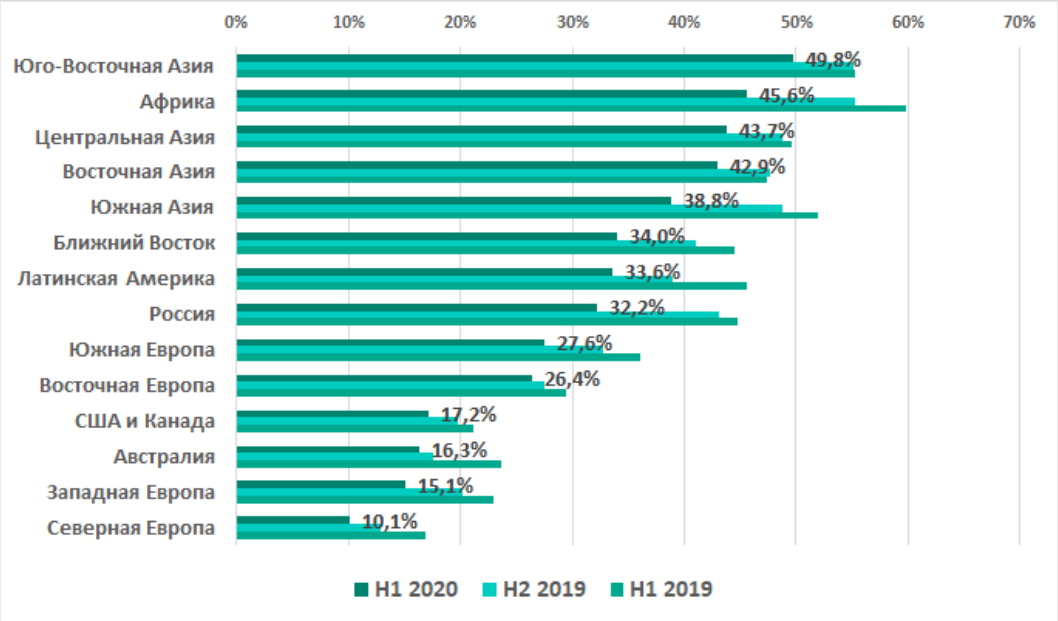
10 стран и территорий с наименьшим процентом омпьютеров АСУ, на которых были заблокированы вредоносные объекты



Регионы

В рейтинге регионов мира по доле машин АСУ, на которых была предотвращена вредоносная активность, лидируют Юго-Восточная Азия, Африка и Центральная Азия.

Рейтинг регионов мира по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты

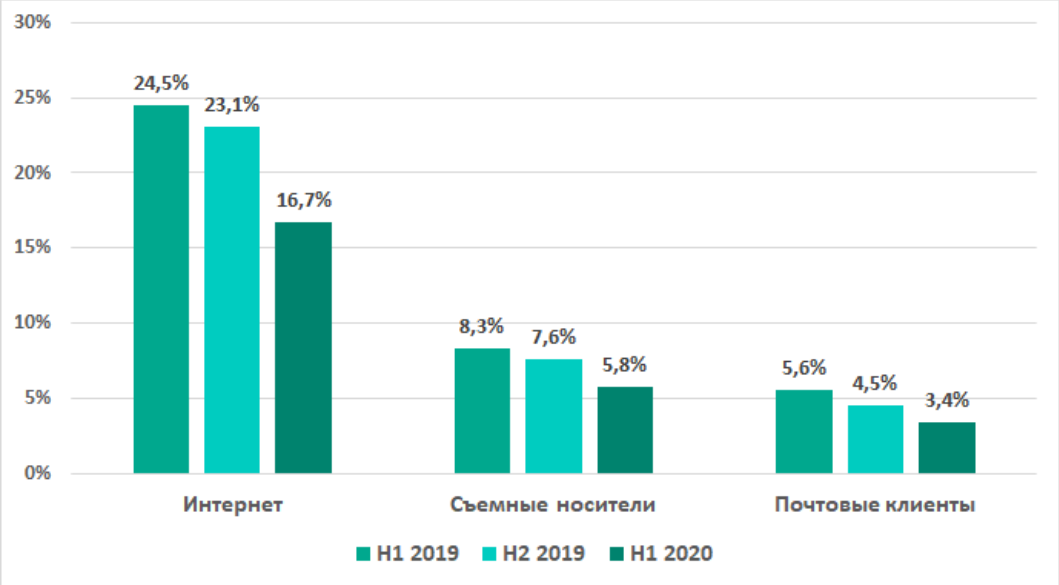


Регионы Европы, Австралия, США и Канада традиционно оказываются среди наиболее благополучных: их показатели не превышают 30%.

Источники угроз

Основными источниками угроз для компьютеров в технологической инфраструктуре организаций на протяжении последних лет являются интернет, съемные носители и электронная почта.

Основные источники угроз, заблокированных на компьютерах АСУ*

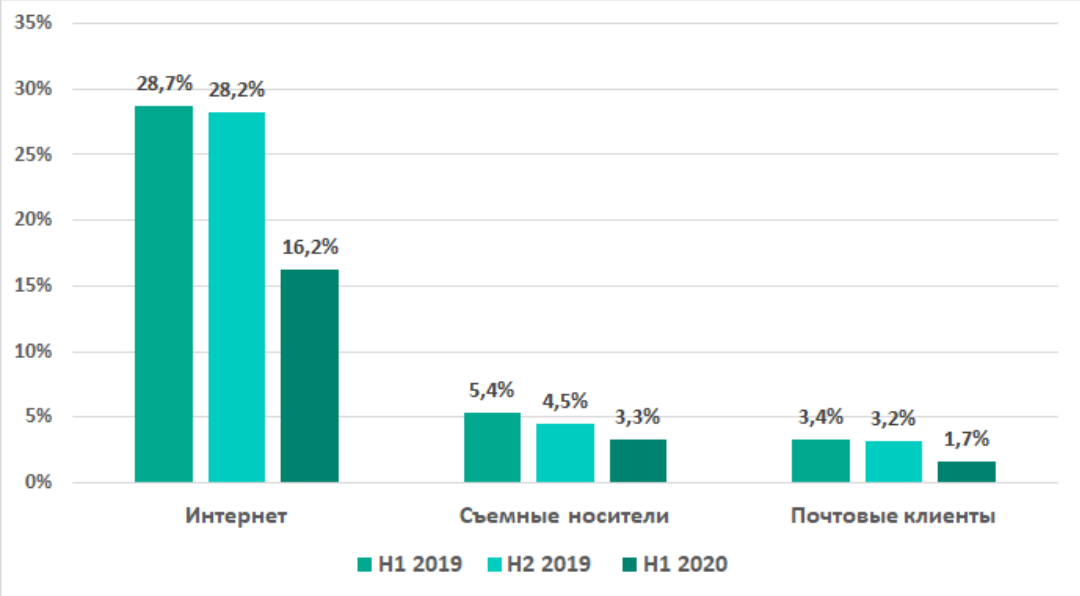


* *процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

В первом полугодии 2020 года интернет стал источником угроз, заблокированных на 16,7% компьютеров АСУ. Это на 6,4 п.п. меньше, чем в предыдущем полугодии.

В России динамика показателей по основным источникам угроз сходна с наблюдаемой в мире в целом.

Россия. Основные источники угроз, заблокированных на компьютерах АСУ*



* *процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

Основные источники угроз: география

Основные источники угроз, заблокированных на компьютерах АСУ*, в регионах, первое полугодие 2020

** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

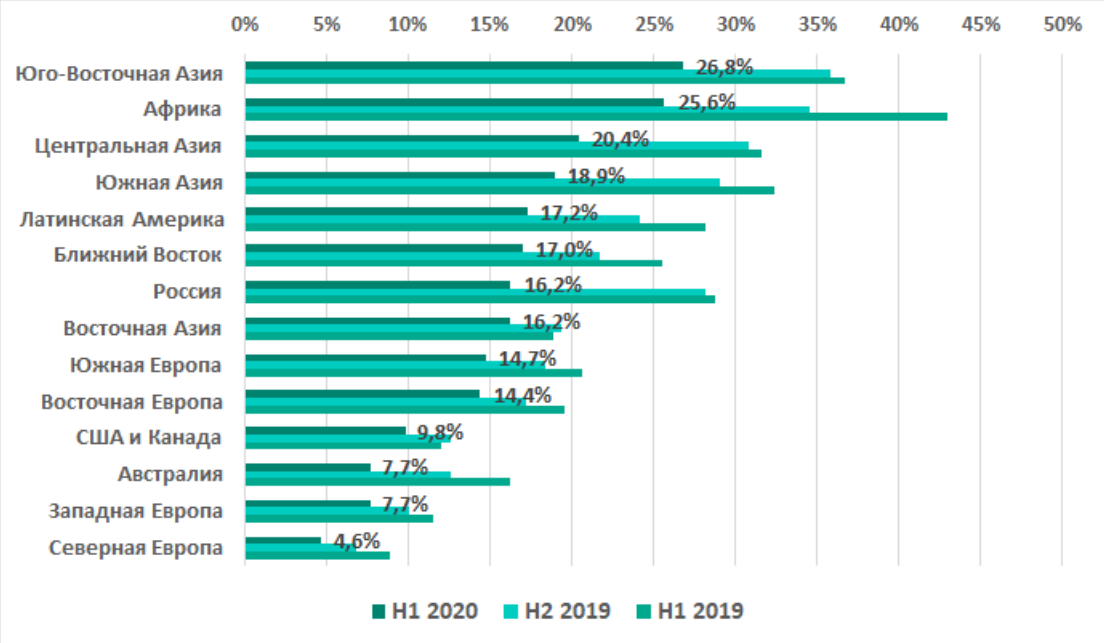
Отметим, что в тех регионах, где наименьшие проценты компьютеров АСУ, на которых были заблокированы угрозы из интернета – Европа, США и Канада, Австралия, – показатели по вредоносным почтовым вложениям превышают показатели по съемным носителям. Исключение составляет Восточная Европа, где эти величины сопоставимы.

В остальных регионах процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, заметно превышает процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения.

Интернет

Во всех регионах мира основным источником угроз является интернет.

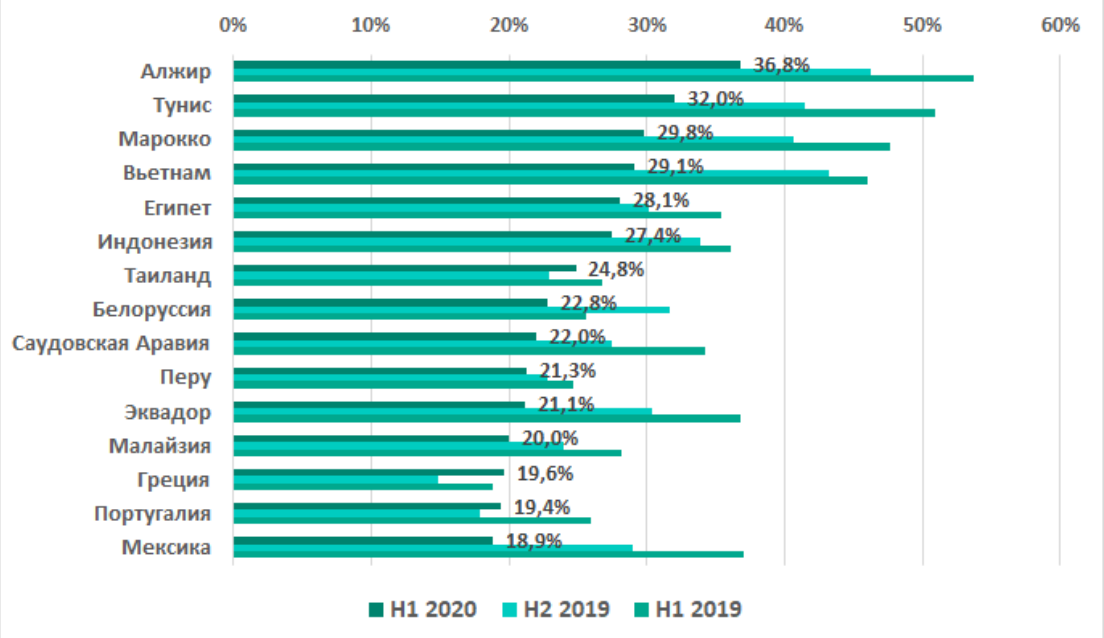
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета



В Северной и Западной Европе, Австралии и в Северной Америке процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, не превышает 10%. В то же время в Африке, Юго-Восточной и Центральной Азии этот показатель выше 20%.

В TOP 15 по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, в первом полугодии 2020 попали Греция и Португалия, которые поднялись в этом рейтинге с 29 и 33 места соответственно. Кроме этих двух стран в TOP 15 показатель вырос только у Таиланда.

TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета

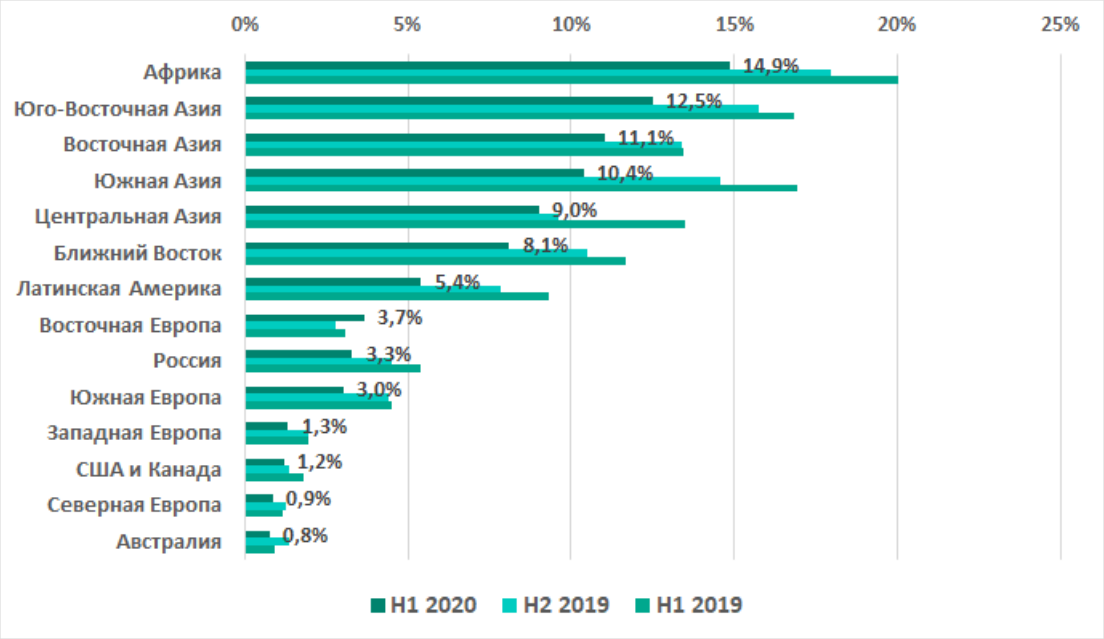


Съемные носители

Максимальный процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, отмечен в Африке, Юго-Восточной, Восточной и Южной Азии. По-прежнему в Австралии, Северной и Западной Европе и Северной Америке этот показатель – минимальный.

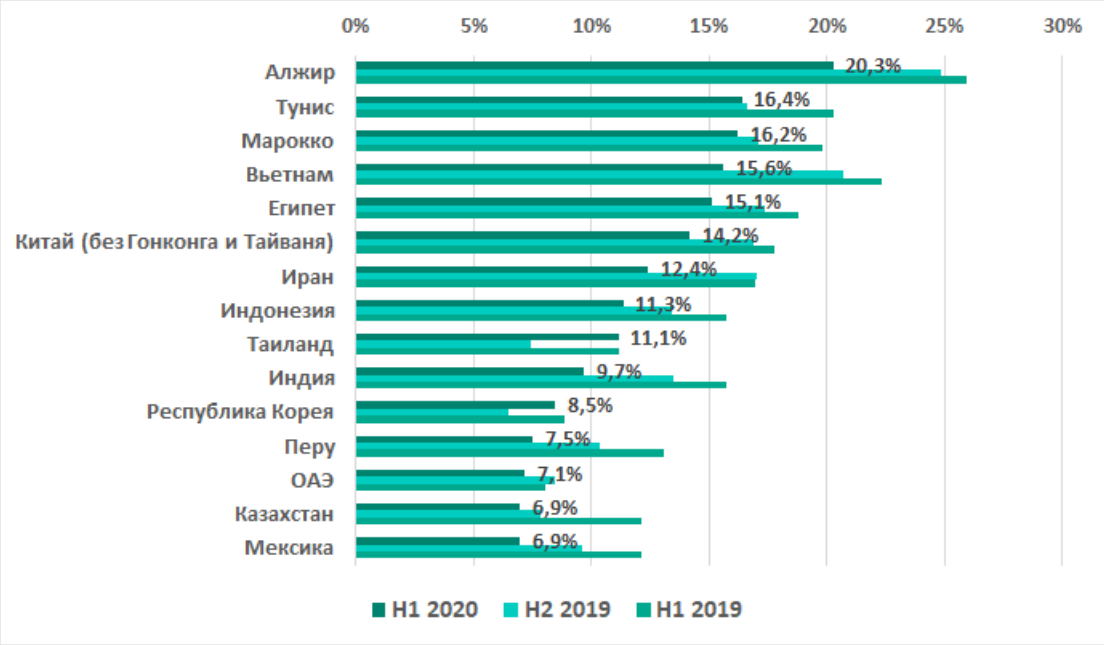
Отметим, что Восточная Европа – единственный регион, где процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, увеличился за полугодие (на 0,9 п.п.).

Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей



В первом полугодии 2020 года в TOP 15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, Тайвань, Саудовскую Аравию и Аргентину сменили Таиланд, Корея и Казахстан. Отметим, что по итогам первого полугодия 2020 в TOP 15 не попали страны Северной Америки, Европы и Австралия.

ТОР 15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей



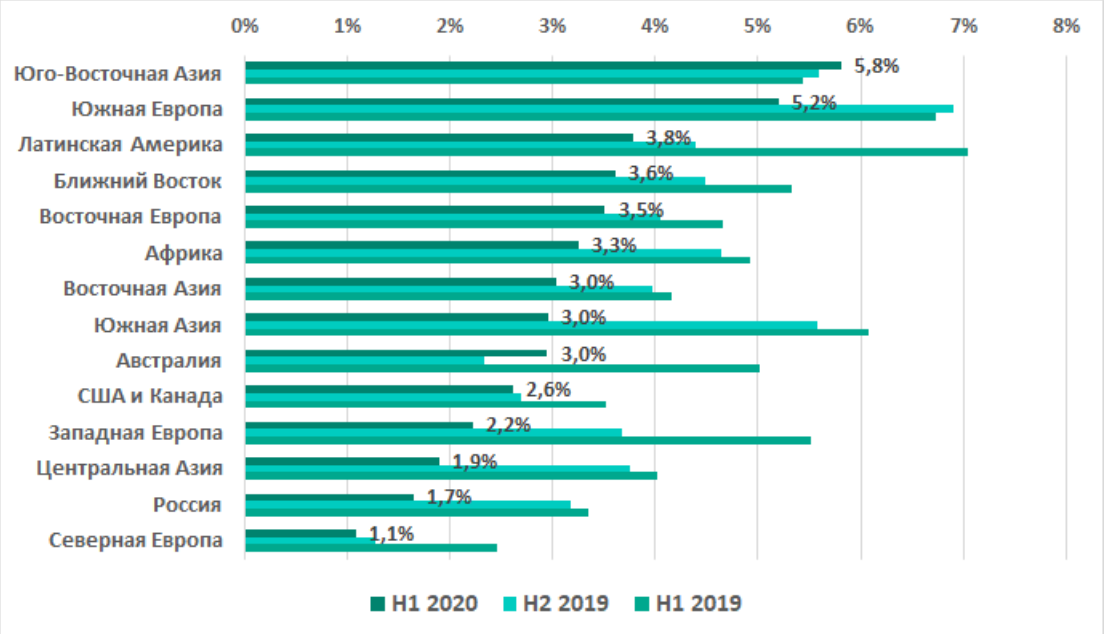
Во всех странах из этого ТОР 15, за исключением Таиланда и Кореи, показатель за полугодие уменьшился.

Почтовые клиенты

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, по итогам полугодия возглавила Юго-Восточная Азия. Кроме региона-лидера неожиданный рост показателя зафиксирован в Австралии (на 0,7 п.п.).

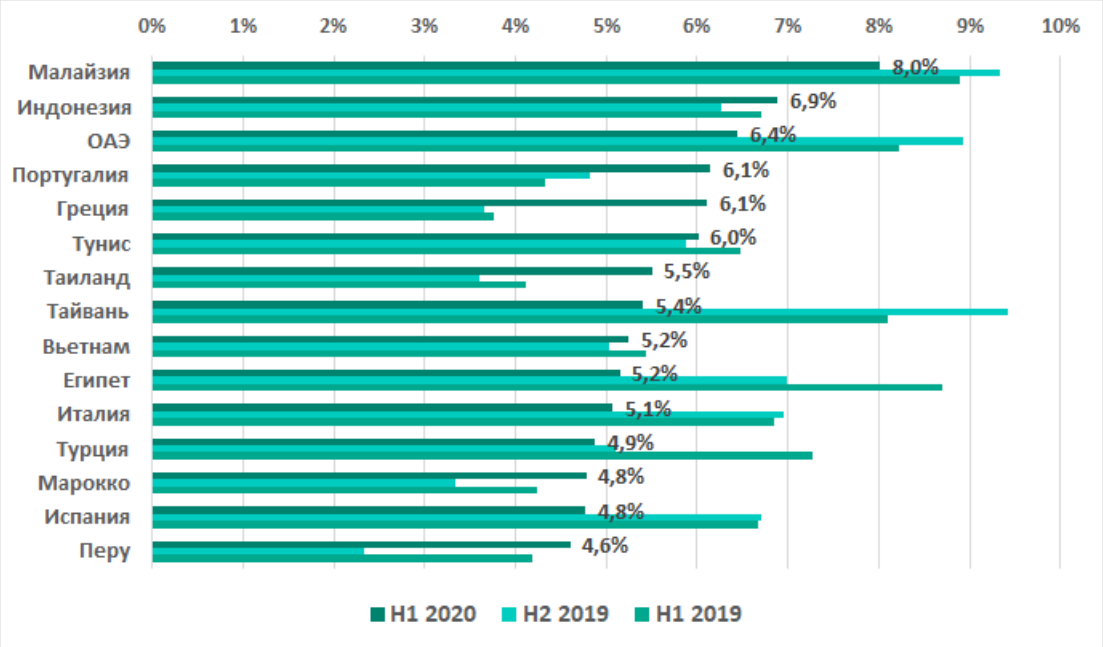
В этом рейтинге, в отличие от рейтингов по другим источникам угроз, в ТОР 5 попали два региона Европы – Южная и Восточная.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения



В семи из 15 стран, попавших в TOP по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, показатель вырос. Наиболее значительные изменения отмечены в Греции (2,5 п.п.), Перу (2,3 п.п.) и Таиланде (1,9 п.п.).

TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения



В Словакии, которая во втором полугодии 2019 года оказалась сразу на третьем месте в этом рейтинге, процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, уменьшился наиболее драматично – на 8 п.п., в Тайване и ЮАР – на 4 п.п. При этом Тайвань, в отличие от Словакии и ЮАР, остался в TOP 15 – на восьмом месте.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky 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 ICS CERT ics-cert@kaspersky.com