

Ландшафт угроз для систем промышленной автоматизации

Первое полугодие 2019

Kaspersky ICS CERT

Оглавление

_Тос19388766

Основные события полугодия	2
Кибератака на компанию HOYA привела к частичной остановке производства в Таиланде.....	2
Кибератака на объект электроэнергетики в США вызвала множественные сбои в работе межсетевых экранов	2
Атаки шифровальщиков.....	3
Атака на горно-металлургический комбинат Nyrstar.....	3
Атаки шифровальщика LockerGoga.....	3
Атака на компанию «Одинцовский Водоканал»	5
Атака на производителя авиационных компонентов ASCO Industries	6
Статистика актуальных угроз.....	7
Методика подготовки статистики	7
Важные находки.....	8
И снова вымогатели	8
Черви, распространяющиеся на съемных носителях, как вектор распространения вредоносного ПО	9
ТОР 3 Киберугроз для энергетики.....	11
Объект исследования	11
Краткие итоги	11
Шпион AgentTesla.....	12
Бэкдор Meterpreter	12
Червь-wiper Syswin.....	13
Общая статистика по миру.....	14
Процент компьютеров, на которых были заблокированы вредоносные объекты	14
Разнообразие обнаруженного вредоносного ПО	15
Категории вредоносных объектов.....	15
Результаты автоматического категорирования вредоносных объектов.....	15
Результаты детальной классификации заблокированных вредоносных объектов	16
География.....	18
Факторы, влияющие на процент атакованных компьютеров в стране	20
Какого цвета «фон»?	21
Источники угроз	24
Основные источники угроз: география	25
Интернет.....	26
Съемные носители.....	27
Почтовые клиенты.....	28

Основные события полугодия

Кибератака на компанию HOYA привела к частичной остановке производства в Таиланде

В конце февраля 2019 года [японский производитель оптического оборудования HOYA стал жертвой кибератаки](#), которая привела к частичной остановке производственных линий на три дня на ключевом заводе в Таиланде.

Около ста компьютеров предприятия были заражены вредоносным ПО, предназначенным для хищения учетных данных и последующего внедрения майнера криптовалюты.

Атака была обнаружена 1 марта после того, как специалисты компании заметили существенное замедление в работе сервера, управляющего заказами и производством, из-за чего работники предприятия не могли использовать программное обеспечение для управления заказами и производством. Несмотря на то, что внедрение криптомайнера удалось предотвратить, производительность затронутых промышленных объектов упала примерно до 40% от нормального уровня.

Инцидент также затронул компьютеры, подключенные к сети штаб-квартиры HOYA в Японии, в результате чего сотрудники компании не могли выписывать счета-фактуры.

Кибератака на объект электроэнергетики в США вызвала множественные сбои в работе межсетевых экранов

[По данным Национальной лаборатории энергетических технологий США](#), 5 марта 2019 на неназванном объекте электроэнергетики на западе США произошел киберинцидент, который вызвал перебои в работе оборудования предприятия. Соответствующая информация была приведена в [отчете о сбоях в работе энергосистем США за 2019 год](#).

March	03/05/2019	9:12 AM	03/05/2019	6:57 PM	California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County;	WECC	Cyber event that causes interruptions of electrical system operations.	System Operations
-------	------------	---------	------------	---------	--	------	--	-------------------

Согласно [отчёту](#), опубликованному Североамериканской корпорацией по надежности энергоснабжения (North American Electric Reliability Corporation, NERC), в течение примерно десяти часов межсетевые экраны, расположенные на границе сетевого периметра предприятия, подвергались атакам со стороны неустановленных злоумышленников, использовавших уязвимость данной модели устройств.

В результате атак устройства перезагружались, что вызывало их кратковременную недоступность (около 5 минут при каждой перезагрузке). Это приводило к кратковременной потере связи между центром управления и устройствами, расположенными на объектах предприятия. Однако перебои в связи не повлияли на выработку электроэнергии и не привели к отключению электричества у потребителей.

Уязвимость, использованная в атаке, была известна ранее, и производитель устройств выпустил обновление прошивки. Однако на момент атаки это обновление не было установлено на межсетевые экраны, используемые на предприятии.

После выяснения причин инцидента специалисты предприятия приняли решение провести установку обновления в три этапа: сначала обновить прошивку на межсетевых экранах в центре управления, работа которых не оказывает критического влияния на

технологический процесс организации; после этого, если не будет выявлено неблагоприятных последствий, установить обновления на уязвимые устройства одного из объектов генерации электроэнергии, а затем, в случае если предыдущие этапы пройдут успешно, установить обновление на все устройства, подверженные данной уязвимости.

Данный случай в очередной раз показал важность своевременной установки обновлений ПО и прошивки устройств, используемых в сетях промышленных предприятий.

Атаки шифровальщиков

В первом полугодии 2019 года эксперты отмечали [всплеск атак шифровальщиков](#) по всему миру. О заражении шифровальщиками сообщили, в том числе, промышленные компании. В нескольких случаях последствия атак были значительными.

Атака на горно-металлургический комбинат Nyrstar

В январе текущего года, [от атаки вымогателя пострадал бельгийский горно-металлургический комбинат Nyrstar](#). Кибератака затронула некоторые ИТ-системы, включая систему электронной почты, в штаб-квартире компании в Цюрихе, а также на производственных объектах по всему миру. К счастью, технологические операции по переработке и добыче металлов не пострадали.

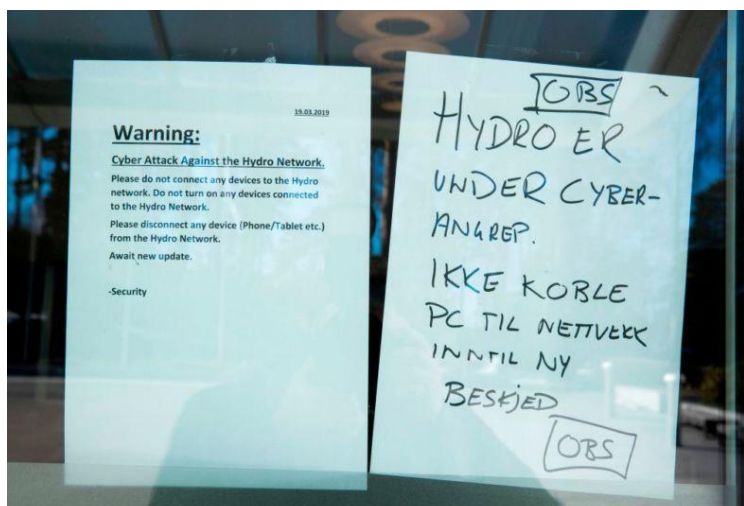
Атаки шифровальщика LockerGoga

LickerGoga стал, пожалуй, самым «шумным» шифровальщиком в первом полугодии 2019 года. На его счету сразу несколько пострадавших компаний.

Атака на металлургическую компанию Norsk Hydro

В марте текущего года один из крупнейших мировых производителей алюминия, норвежская металлургическая компания Norsk Hydro, [стала жертвой атаки программы-вымогателя LockerGoga](#), которая началась 18 марта и привела к сбою в работе производственных объектов в различных странах, включая Норвегию, Катар и Бразилию.

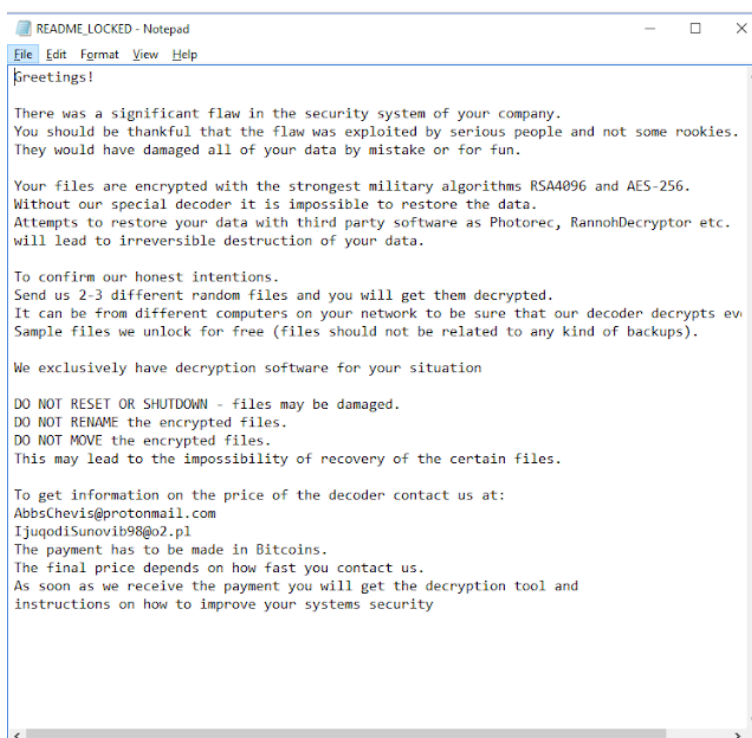
Объявления,
вывешенные в
окне офиса
компании
Источник:
[arstechnica](#)



Несмотря на усилия представителей службы безопасности Norsk Hydro по [предотвращению распространения вредоносного ПО](#), зловард успел заразить ИТ-системы во всей распределенной сети Norsk Hydro. В общей сложности было выведено из строя [22000 компьютеров на 170 различных объектах в 40 странах](#).

[В результате атаки](#) пострадали как офисные, так и технологический процессы. Так, заражению подверглись промышленные сети нескольких прокатных и экструзионных производств, из-за чего часть производственных систем была заблокирована. Это [вызвало сбои в производстве и временную остановку технологического процесса](#).

Сообщение на зараженном компьютере



По заявлению представителей Norsk Hydro, инцидент не затронул работу электростанций, ИТ-системы которых являются изолированными.

[К 21 марта все установки были изолированы](#), распространение зловреда в сети компании остановлено. Однако часть технологических операций еще продолжительное время осуществлялась в ручном режиме. Восстановление операций и продаж продолжалось в течение квартала после инцидента. Для восстановления штатного функционирования сети предприятия специалисты Norsk Hydro использовали имеющиеся резервные копии ИТ-систем.

В процессе расследования инцидента стало понятно, что [компания Norsk Hydro стала жертвой шифровальщика LockerGoga](#). Это недавно появившееся семейство шифровальщиков. Троянец написан на C++ с использованием библиотек Boost и CryptoPP. Для шифрования файлов используется гибридная схема AES + RSA-1024, зашифрованные файлы получают дополнительное расширение .locked.

Для заражения сети Norsk Hydro предположительно [могла быть использована скомпрометированная привилегированная учетная запись](#). Столь масштабное заражение вероятно объясняется отсутствием должным образом организованного сегментирования сети.

Согласно [финансовому отчету](#) норвежской компании за первый квартал 2019 года, в результате инцидента Norsk Hydro потеряла 300-350 миллионов норвежских крон (порядка \$35-41 млн). Финансовые потери во втором квартале оцениваются в 200-250 миллионов норвежских крон.

Атаки на другие компании

Первой в результате атаки вредоносной программы-шифровальщика LockerGoga в 2019 году пострадала французская консалтинговая компания [Altran Technologies](#). Атака произошла 24 января. Заражение информационных систем компании вредоносным ПО [затронуло бизнес-операции в некоторых европейских странах](#). Для защиты своих клиентов, сотрудников и партнеров компания Altran временно отключила свою сеть и все приложения. К расследованию атаки были привлечены сторонние технические эксперты.

Кроме того, из сообщений СМИ стало известно, что 12 марта, еще до атаки на Norsk Hydro, от вымогательского ПО LockerGoga [пострадали также две американские химические компании](#) – производители смол, силиконов и других материалов Hexion и Momentive. В день атаки на некоторых корпоративных компьютерах в обеих компаниях появился «синий экран смерти», а все файлы оказались зашифрованными.

Согласно письму генерального директора Momentive, которое попало в распоряжение журналистов, вредоносное ПО вызвало глобальной сбой в работе IT-систем, и компания была вынуждена закупить сотни новых компьютеров вместо зараженных.

В свою очередь, представители Hexion выпустили [пресс-релиз](#), где назвали произошедшее инцидентом сетевой безопасности, который нарушил доступ к некоторым системам и данным внутри корпоративной сети.

Атака на компанию «Одинцовский Водоканал»

15 апреля 2019 года компания «Одинцовский Водоканал» подверглась атаке программы-шифровальщика. Зловред зашифровал все данные как на самом зараженном устройстве, так и в сетевых папках. В результате под угрозой оказалась сохранность технической документации и данных абонентов организации, а также процедура выставления счетов.

Целью злоумышленников было получение выкупа, однако «Одинцовский Водоканал» отказался платить выкуп и обратился за помощью в «Лабораторию Касперского». Проанализировав образцы зашифрованных данных и самой вредоносной программы, [эксперты «Лаборатории Касперского» нашли способ полностью восстановить информацию](#) и в течение нескольких часов отправили пострадавшей компании ПО для дешифровки.

Злоумышленники проникли в сеть организации через запущенный на одном из компьютеров компании штатный сервис удаленного рабочего стола (Remote Desktop Protocol), встроенный в ОС Windows. Им удалось удаленно подобрать пароль от учётной записи и авторизоваться на системе. После этого атакующие запустили зловред на скомпрометированном компьютере в ручном режиме, и он приступил к шифрованию файлов.

По данным «Лаборатории Касперского» больше всего пользователей этот шифровальщик атаковал в России.

Атака на производителя авиационных компонентов ASCO Industries

7 июня 2019 года, [компания ASCO Industries, подверглась атаке вымогательского ПО](#). ASCO – крупный производитель авиационных деталей, поставляющий комплектующие американскому авиапроизводителю Boeing и европейскому концерну Airbus. Компания также производит детали для истребителя F-35, производимого Lockheed Martin. Заражение привело к временному закрытию четырех заводов. Из-за этого компания [отправила во внеплановый отпуск](#) 1000 сотрудников.

По данным СМИ заражение произошло на бельгийском заводе в Завентеме. Однако компания приостановила производство также в Германии, Канаде и США. Связано ли это решение с распространением вредоносного ПО на другие заводы или же является мерой предосторожности, не сообщалось. Непроизводственные офисы компании во Франции и Бразилии не пострадали.

Информация о том, какое именно ПО заразило бельгийский завод компании, уплатила ли компания выкуп за восстановление доступа к своим системам, и какие меры предпринимаются для восстановления их работоспособности, не раскрывалась.

Статистика актуальных угроз

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 APT¹.

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](#).

Важные находки

В этот раздел мы включили некоторые находки, сделанные нами при анализе статистики заблокированных угроз в первом полугодии 2019 года, которые, на наш взгляд, могут оказаться важными для широкого круга наших читателей. Раздел включает описание опасных угроз, а также некоторые обоснованные, по нашему мнению, предположения относительно векторов проникновения вредоносного ПО на компьютеры АСУ.

И снова вымогатели

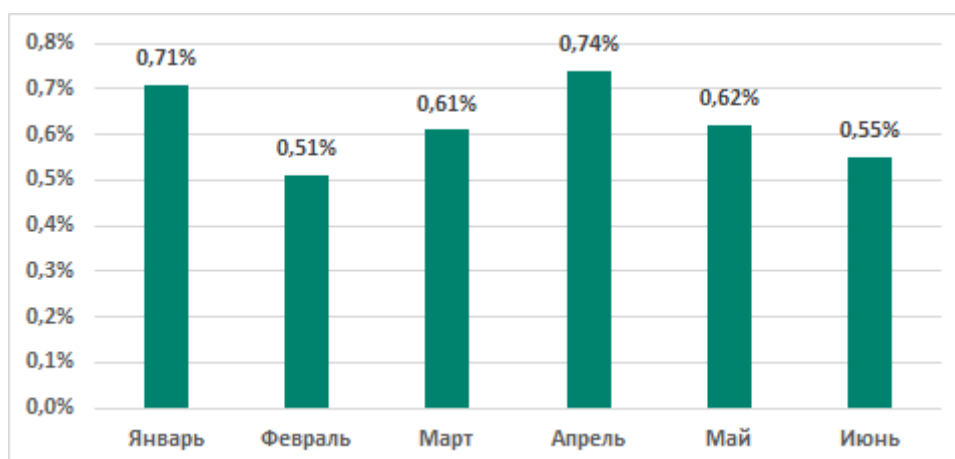
В первом полугодии 2019 года злоумышленники активно распространяли программы-вымогатели. Как следует [из сообщений СМИ](#), в результате заражений такими программами пострадали и несколько промышленных компаний. Отметим, что, вполне вероятно, не все такие случаи стали известны общественности, поскольку не все компании готовы делиться подобной информацией – особенно если предпочли заплатить злоумышленникам.

Как правило, вредоносные программы-вымогатели заражают компьютеры в офисных сетях промышленных компаний. Последствия этого могут быть весьма серьезными и приводить в том числе к сбоям в производстве, например, в случае заражения систем планирования и управления производством (MES и ERP). Но наиболее опасными эти программы могут стать в случае заражения технологической сети.

По данным Kaspersky ICS CERT, в первом полугодии 2019 года попытки заражений программами-вымогателями были предотвращены на 1,8% компьютеров АСУ. Из них на 19,6% компьютеров был заблокирован печально известный вымогатель WannaCry.

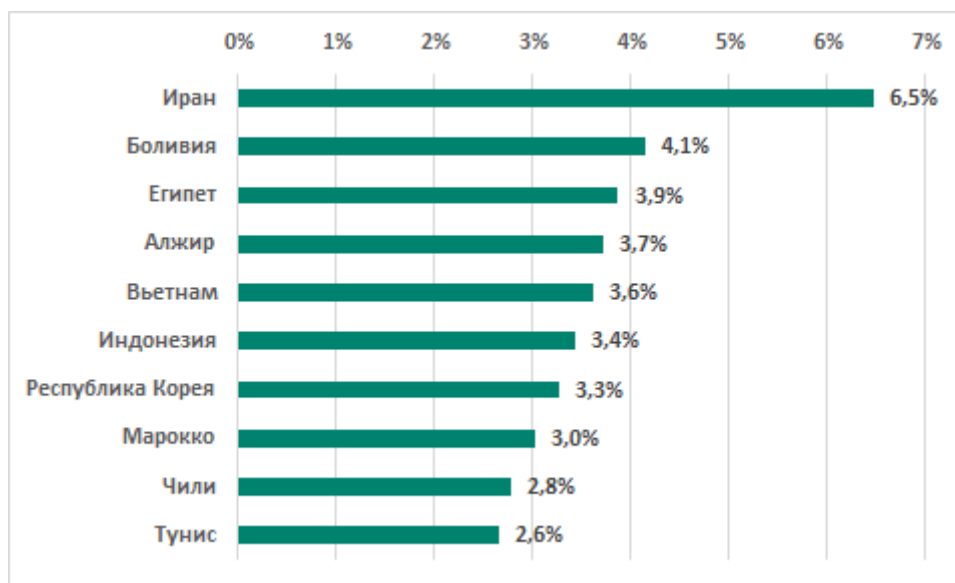
Наибольшая активность попыток заражения компьютеров АСУ программами-вымогателями наблюдалась в январе и в апреле.

Процент компьютеров АСУ, на которых были заблокированы вредоносные программы-вымогатели, первое полугодие 2019



В некоторых странах этот показатель значительно превышает средний по миру.

ТОП 10 стран в рейтинге стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные программы-вымогатели, первое полугодие 2019



По проценту атакованных программами-вымогателями компьютеров АСУ в тройку лидеров попали Иран, Боливия и Египет.

Среди стран Западной Европы по этому показателю лидирует Италия с 2,0%. В России он составил 1,1%.

Черви, распространяющиеся на съемных носителях, как вектор распространения вредоносного ПО

В некоторых странах весьма активно самораспространяющееся вредоносное ПО. В исследованных нами случаях им оказались черви (вредоносные объекты класса Worm), которые заражают съемные носители (флешки, внешние жесткие диски, мобильный телефон и т.д.). Неосведомленные об угрозах пользователи подключают зараженные устройства к компьютерам АСУ и непреднамеренно запускают замаскированные под легитимные программы файлы червей. Большинство таких файлов блокируется при сканировании съемного носителя в момент подключения или позднее при попытке запуска вредоносного файла. Но в некоторых случаях, пользователи игнорируют решение антивируса о блокировании угрозы, считая его ложным срабатыванием, или добавляют съемные носители в исключения из проверки, очевидно, не осознавая степень риска. В результате черви заражают компьютер, после чего заражают на него целевое вредоносное ПО.

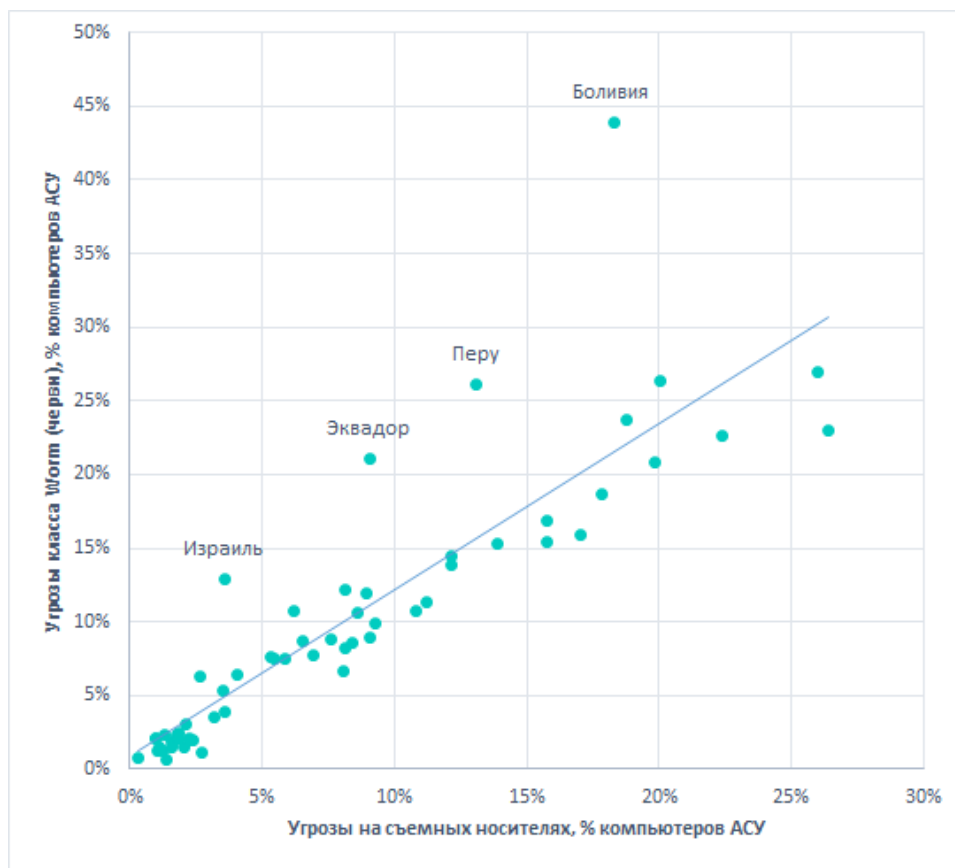
Наиболее распространенным в настоящее время методом маскировки проанализированных нами экземпляров червей, распространяющихся на съемных носителях, являются LNK-файлы. В них черви прописывают вредоносные инструкции (скрипты) в виде параметров CMD, Powershell и VisualBasicScript. В некоторых случаях такой подход позволяет вредоносному ПО обойти защитные решения, которые контролируют только запускаемые файлы, но не контролируют параметры командной строки для доверенных программ-интерпретаторов.

При наличии подключения зараженного компьютера к интернету, червь отправляет на командный центр (C&C) информацию о зараженной системе и скачивает на компьютер целевое вредоносное ПО. Чаще всего – вредоносные криптомайнеры и программы-вымогатели. Например, в Иране, где процент компьютеров АСУ, атакованных

шифровальщиками, наиболее высок (по сравнению с другими странами), такие черви используются для распространения программы-вымогателя Cerber.

По всей видимости, заражение червями через съёмные носители является наиболее частым сценарием для компьютеров АСУ. Этот факт подтверждает сильная положительная корреляция (см. график ниже): $R>.95$, $p<.001$.

Корреляция* значений процента компьютеров АСУ, на которых были заблокированы вредоносные объекты класса Worm (черви), и процента компьютеров АСУ, на которых были заблокированы вредоносные объекты на съёмных носителях



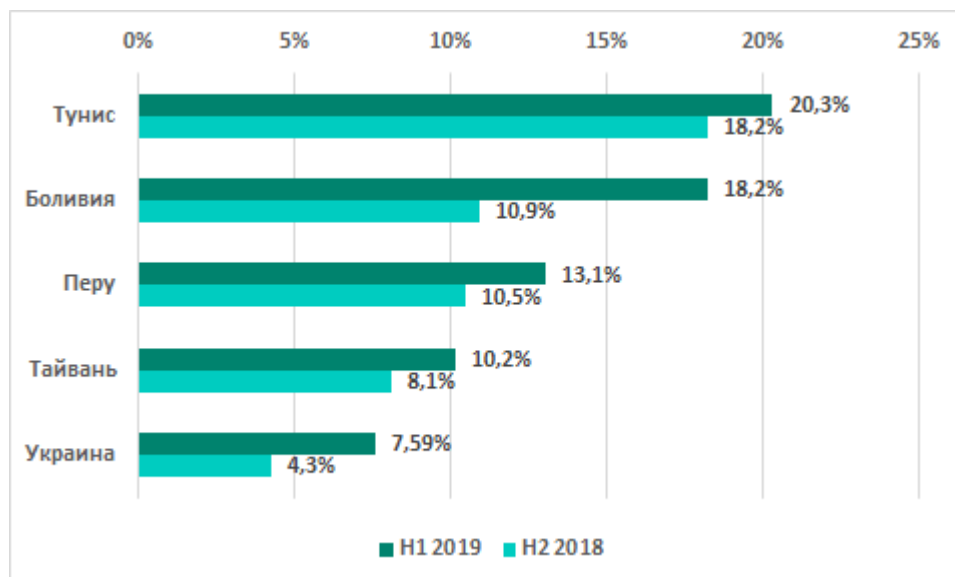
*параметры корреляции: $R>.95$, $p<.001$, без учета аномальных показателей Боливии, Перу, Эквадора и Израиля.

Отметим, что параметры корреляции получены без учета аномальных показателей Боливии, Перу, Эквадора и Израиля, где черви часто встречаются не только на съёмных носителях, но и в пользовательских и системных архивах и сетевых папках.

Так, в Боливии в первом полугодии 2019 показатель компьютеров АСУ, на которых были заблокированы черви, достиг рекордных 43,9%. В то же время при подключении съёмных носителей вредоносные объекты были заблокированы на 18,2% компьютеров АСУ – на 7,3 п.п. больше, чем в предыдущем полугодии (для сравнения: в среднем по миру этот показатель не изменился и составил 8,3%).

Частые попытки заражения червями компьютеров АСУ в странах с аномальными показателями, судя по всему, являются отражением ситуации с весьма высоким фоном активности червей. Так, например, в упомянутой выше Боливии при подключении съёмных носителей черви были обнаружены более чем на 35% **всех** компьютеров (АСУ, корпоративных и домашних).

В первом полугодии 2019 5 стран и территорий, где отмечен наибольший рост процента компьютеров АСУ, на которых вредоносные объекты были заблокированы при подключении съемных носителей, выглядят так:



Также в некоторых странах (например, в Боливии, Эквадоре, Перу и Израиле) источники распространения червей изначально чаще находятся не снаружи периметра АСУ (например, на съёмном диске, подключаемом к компьютеру АСУ), а внутри сетевого периметра АСУ. Обычно такими внутренними постоянными источниками заражения становятся компьютеры, на которых отсутствуют правильно сконфигурированные эффективные средства антивирусной защиты.

ТОР 3 Киберугроз для энергетики

В этом полугодии мы провели более детальный анализ ландшафта угроз для нескольких индустрий. Здесь представим краткие результаты исследования актуальных угроз для одной из них – энергетики.

Объект исследования

Компьютеры в технологических сетях, используемые для конфигурирования, обслуживания и управления оборудованием систем генерации, передачи и распределения электроэнергии, а также системы управления объектами энергетики, на которых стоят продукты «Лаборатории Касперского». В том числе компьютеры под управлением Windows, на которых установлены различные программные пакеты, предназначенные для энергетической промышленности.

Краткие итоги

Всего в первом полугодии 2019 года продукты «Лаборатории Касперского» сработали на 41,6% компьютеров АСУ в энергетике. Было заблокировано множество обычных (не предназначенных для АСУ ТП) вредоносных программ.

Среди них особую опасность представляют майнеры (2,9%), черви (7,1%) и различные многофункциональные шпионские программы (3,7%), заражение которыми может

оказать негативное влияние на доступность и целостность АСУ ТП и систем технологической сети.

Несмотря на то, что заблокированное на исследуемых компьютерах вредоносное ПО не является специфичным для АСУ, его опасность не следует недооценивать.

Такое ПО способно:

- похищать конфиденциальную информацию, включая информацию, которую можно потенциально использовать для дальнейшего развития атаки в нужном злоумышленникам направлении
- загружать и выполнять произвольное вредоносное ПО – по желанию злоумышленников
- предоставлять злоумышленникам возможность удаленного управления зараженным компьютером

Таким образом, побочное действие активного заражения может оказать значительное влияние на доступность и целостность АСУ ТП и систем технологической сети.

Вместе с тем, некоторые обнаруженные угрозы имеют признаки направленных атак. В настоящее время мы исследуем эти атаки.

Шпион AgentTesla

Одна из наиболее опасных угроз – [AgentTesla](#). Этот специализированный троянец-шпион написан на платформе .NET и предназначен исключительно для кражи данных, в частности – данных аутентификации, скриншотов экрана, записи веб-камеры и нажатий клавиатуры. Первые экземпляры, обнаруженные в 2017 году, отправляли собранные данные на серверы управления по HTTP. В самплах, обнаруженных в 2018 году, используемый протокол был изменен на SMTP. Во всех исследованных случаях для отправки данных злоумышленники использовали взломанные почтовые ящики различных компаний.

Чаще всего вредоносное ПО распространялось в фишинговых письмах, содержащих документ Microsoft Word со встроенным VisualBasic- загрузчиком AgentTesla.

Командные серверы/почтовые ящики вредоносной программы специфичны для конкретной атаки и используются не только для отправки украденной информации, но и для загрузки обновлений вредоносного ПО. Примечательно, что в троянце предусмотрена обработка команды “uninstall”, позволяющая вредоносной программе удалить следы заражения и самоликвидироваться.

Шпион AgentTesla представляет значительную угрозу для промышленных систем, поскольку применяется в направленных атаках, а украденные данные могут быть использованы для планирования и проведения следующих шагов атаки.

Бэкдор Meterpreter

Продукты «Лаборатории Касперского» обнаружили несколько случаев использования бэкдора Meterpreter для удаленного управления компьютерами в технологических сетях энергетических систем.

Meterpreter является частью известного фреймворка [Metasploit](#) и предназначен для ручного или полуавтоматического управления атакованным компьютером.

Meterpreter обладает значительными возможностями по организации скрытого удаленного управления благодаря использованию техники [рефлексивной загрузки](#) вредоносного кода. Эта техника позволяет злоумышленникам загружать непосредственно в исполняемую память атакованного бэкдором компьютера произвольное вредоносное ПО. Таким образом атака может долгое время оставаться незамеченной, поскольку в ней используется бестелесное вредоносное ПО, которое не записывается на жесткий диск.

Исходный вектор атак, их происхождение и назначение в настоящее время исследуются.

Атаки с использованием бэкдора Meterpreter являются направленными, скрытными и часто проводятся в ручном режиме. Возможность скрытного удаленного управления зараженным компьютером АСУ злоумышленниками представляет огромную опасность для промышленных систем.

Червь-wiper Syswin

Еще одна серьезная угроза, которую продукты «Лаборатории Касперского» заблокировали на компьютерах энергетической промышленности, – [Syswin](#), новый червь-wiper, написанный на Python и упакованный в формат исполняемых файлов Windows.

Червь распространяется через сетевые папки и съемные носители, которые подключаются к зараженной системе.

При запуске червь заражает систему, прописывая себя в автозагрузку компьютера. После этого выставляет флаг “для удаления” для каждого исполняемого файла на жестких дисках. В результате после перезагрузки компьютера все отмеченные флагом файлы будут удалены операционной системой, что приведет к неработоспособности компьютера.

При заражении съемных носителей червь изменяет размер всех файлов на 0, то есть уничтожает информацию в этих файлах.

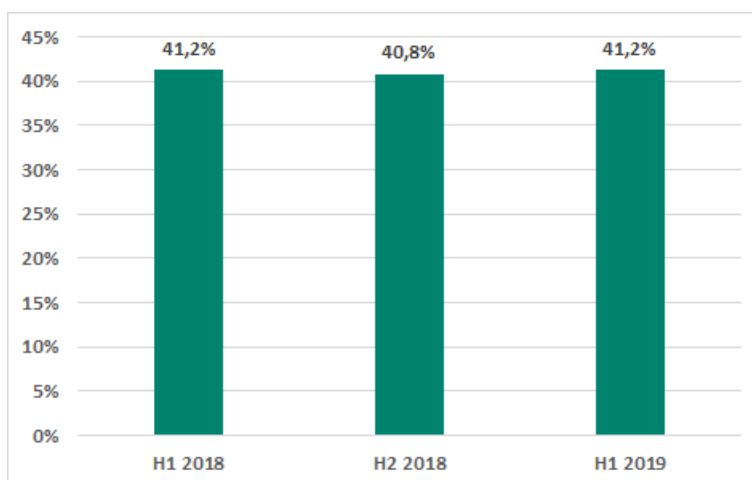
Угроза может оказать на компьютеры АСУ значительное влияние, обусловленное способностью вредоносного ПО к самораспространению и уничтожению данных.

Общая статистика по миру

Процент компьютеров, на которых были заблокированы вредоносные объекты

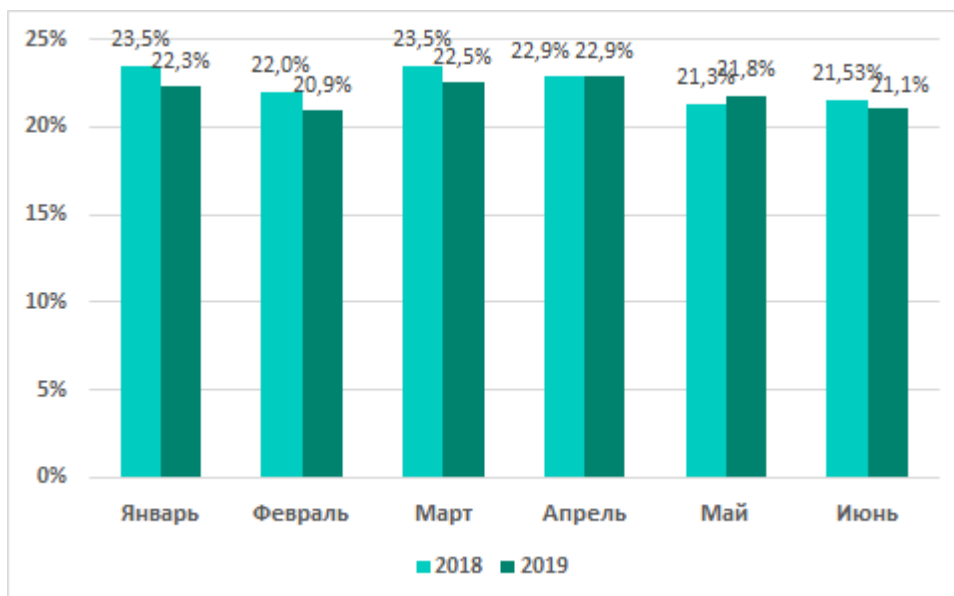
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в первом полугодии 2019 года составил 41,21%. Этот показатель совпадает с показателем за аналогичный период прошлого года. По сравнению с предыдущим полугодием мы наблюдаем незначительный рост на 0,37 п.п.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

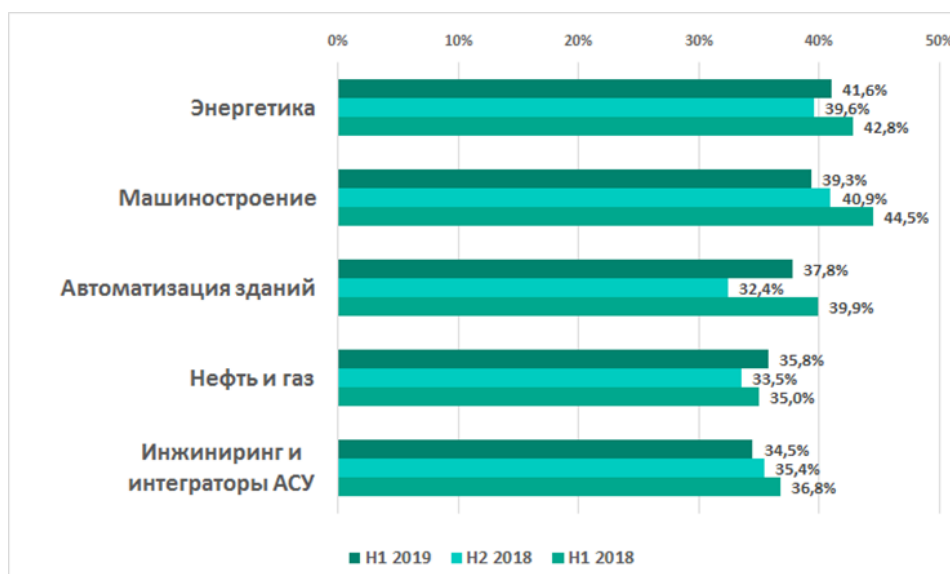


Наибольший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в январе и марте 2019 года.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам, первые полугодия 2018 и 2019 годов



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



Разнообразие обнаруженного вредоносного ПО

В первом полугодии 2019 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 20,8 тысяч модификаций вредоносного ПО из 3,3 тысяч различных семейств. Это на 1,7 тысяч больше, чем в предыдущем полугодии, когда было заблокировано более 19,1 тысяч модификаций вредоносного ПО из 2,7 тысяч различных семейств.

Категории вредоносных объектов

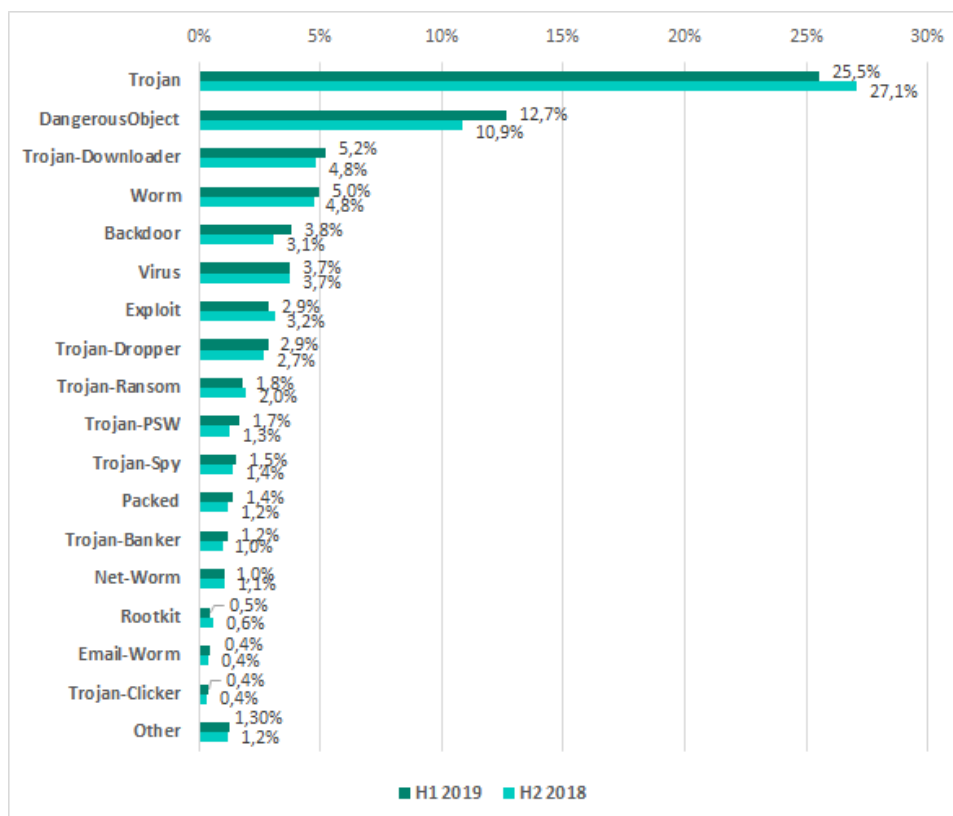
Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям. Ниже перечислены основные из них и приведен процент компьютеров АСУ, на которых была предотвращена вредоносная активность объектов этих категорий.

Результаты автоматического категорирования вредоносных объектов

Приведем результат классификации заблокированных вредоносных объектов на основе вердиктов, вынесенных защитными технологиями в продуктах «Лаборатории Касперского». Именно так их видят пользователи наших продуктов.

Отметим, что приведенный ниже анализ классов и семейств вредоносного ПО отражает только результаты сигнатурного и эвристического обнаружения, тогда как значительная часть вредоносных объектов детектируется продуктами «Лаборатории Касперского» методами анализа поведения неизвестного ПО с выдачей общих Genegis-вердиктов, которые не позволяют автоматически различать реальные типы вредоносного ПО. Поэтому процент атакованных компьютеров АСУ для некоторых категорий вредоносного ПО на самом деле выше.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных классов



Актуальными угрозами для компьютеров АСУ остаются вредоносные программы класса Trojan. Хотя на протяжении последних лет мы наблюдаем снижение процента компьютеров АСУ, на которых были заблокированы вредоносные объекты этого класса: по сравнению с прошлым полугодием этот показатель снизился на 1,52 п.п.

По сравнению с показателями за прошлое полугодие на 0,75 п.п. вырос процент компьютеров АСУ, на которых были предотвращены попытки заражения бэкдорами (Backdoor) и на 0,41 п.п. – троянцами-шпионами (Trojan-PSW).

Результаты детальной классификации заблокированных вредоносных объектов

Для того, чтобы дать лучшее представление о типах заблокированных угроз, мы выполнили более детальную их классификацию, потребовавшую, в том числе, значительное количество ручного анализа. Заметим, что получившиеся проценты (как и цифры на графике выше) не корректно суммировать, потому что во многих случаях на одном компьютере за отчетный 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:

- 11,8% – 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.

- 8,5% – зловерные скрипты и перенаправления на веб-ресурсах (JS и Html), а также эксплойты для браузеров – 0,16%.
- 6,0% – черви (Worm), распространяющиеся, как правило, через съемные носители и сетевые папки, а также черви, распространяющиеся через почтовые сообщения (Email-Worm), сетевые уязвимости (Net-Worm) и мессенджеры (IM-Worm). Большинство червей являются устаревшими с точки зрения сетевой инфраструктуры. Но есть среди них и такие как Zombaque (0,02%) – с реализованной P2P сетевой архитектурой, позволяющей злоумышленникам активировать его в любой момент.
- 3,29% – веб-майнеры, выполняемые в браузерах, 1,31% – майнеры - исполняемые файлы для ОС Windows.
- 5,16% – вредоносные LNK-файлы.

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

В этой категории также широко представлены LNK-файлы с уязвимостью CVE-2010-2568 (0,62%), 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 зловерный файл.

В редких случаях запускаемый вредоносный powershell скрипт скачивает и внедряет в память бинарный код, являющийся специфичной модификацией пассивного TCP бэкдора из набора metasploit.

- 2,82% – вредоносные документы (MSOffice+PDF), содержащие эксплойты, зловерные макросы и зловерные ссылки.
- 2,16% – 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 зловеров старых семейств (Palevo, Sality, Kido и др.).

- 3,76% – вредоносные программы класса Virus. Среди этих программ уже много лет детектируются такие семейства как Sality (1,18%), Nimnul (0,77%), Virut (0,54%). 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.
- 1,81% – программы-вымогатели.

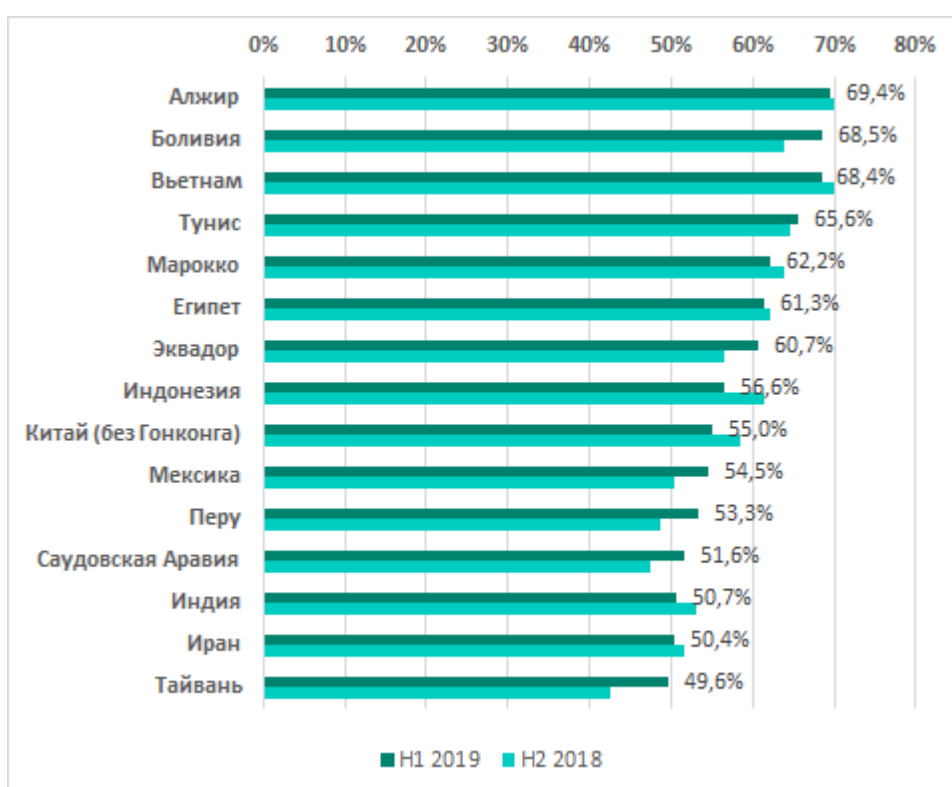
- 1,32% – банковские троянцы.
- 0,88% – вредоносные программы для AutoCad.

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.

- 0,64% – вредоносные файлы для мобильных устройств, которые блокируются при подключении устройств к компьютерам.

География

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



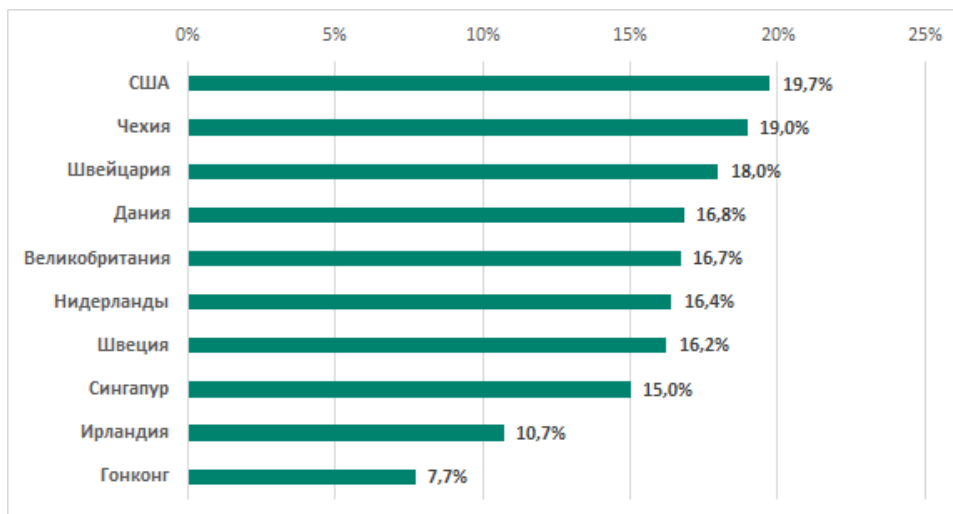
В рейтинге стран и территорий по проценту компьютеров АСУ, на которых была предотвращена вредоносная активность, первую строчку занял Алжир. В первую пятёрку стран вошла Боливия, которая заняла второе место, оттеснив Вьетнам, Тунис и Марокко на 3-е, 4-е и 5-е места, соответственно.

Заметные увеличения процента компьютеров АСУ, на которых была предотвращена вредоносная активность, наблюдаются в Израиле (на 9,8 п.п.), Аргентине (на 7,2 п.п.) и в Тайване (на 6,9 п.п.).

В России в течение первого полугодия 2019 года хотя бы один раз вредоносные объекты были заблокированы на 44,8% компьютеров АСУ, что немного ниже уровня, который мы наблюдали во втором полугодии 2018 года (45,3%). Россия занимает 19-ю строчку рейтинга.

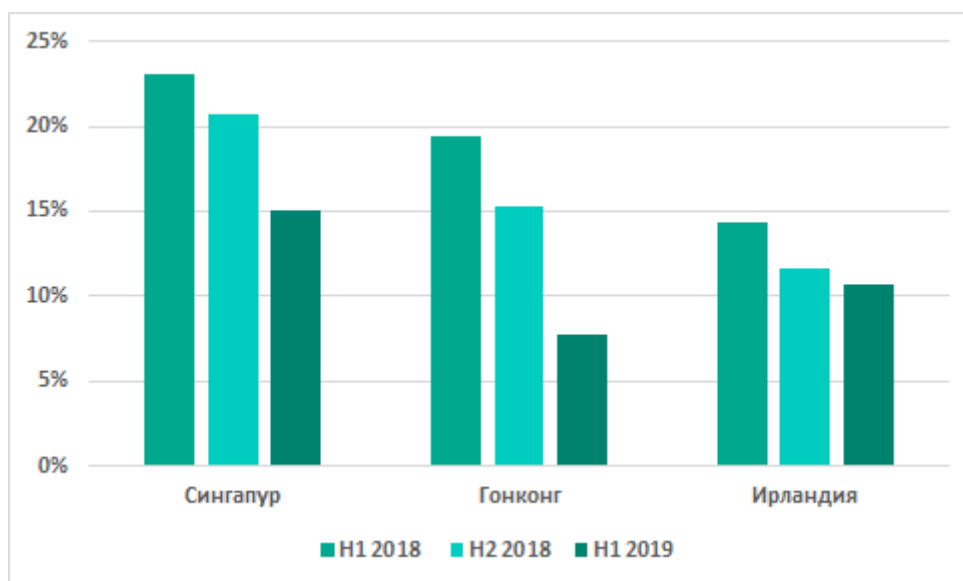
Список десяти наиболее благополучных стран и территорий в основном остается прежним уже на протяжении нескольких полугодий.

10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2019



Наиболее благополучные в этом рейтинге – Гонконг (7,7%), Ирландия (10,7%) и Сингапур (15%), где процент компьютеров АСУ, на которых была предотвращена вредоносная активность, уже не первое полугодие продолжает снижаться.

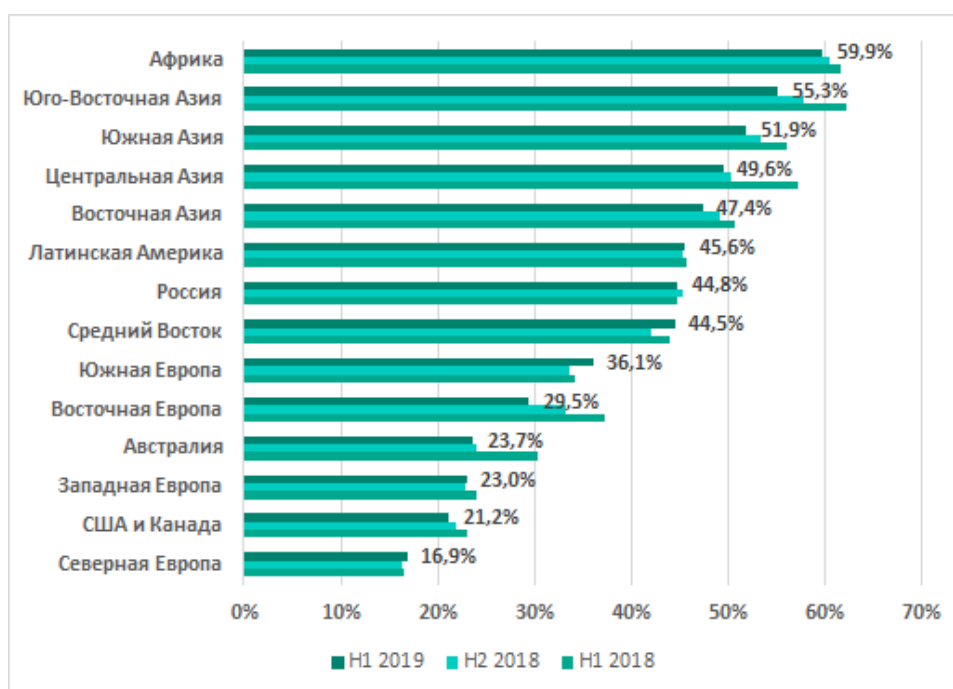
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в Сингапуре, Гонконге и в Ирландии



В то же время в Дании мы наблюдаем постепенный рост этого показателя – с первого полугодия 2018 года он вырос с 14,0% до 16,8%.

Рейтинг различных регионов мира по доле машин АСУ, на которых была предотвращена вредоносная активность, остается без изменений на протяжении нескольких лет. Традиционно по данному показателю лидируют Африка, Юго-Восточная и Южная Азия.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах мира



Факторы, влияющие на процент атакованных компьютеров в стране

Как мы уже рассказывали в [одном из наших отчётов](#), мы обнаружили положительную корреляцию между процентом атакованных компьютеров в стране и её GDP-рейтингом, который, в частности, даёт грубые представления о количестве ресурсов, доступных промышленным организациям, в том числе для защиты от компьютерных атак.

Мы предполагаем, что в каждой стране этот фактор во многом определяет уровень изоляции технологических сетей от внешних угроз. Он может зависеть от многих составляющих, таких как

- Эффективные меры и средства защиты периметра ОТ и периметра корпоративной среды;
- Нормы и практики работы с общекорпоративными ресурсами внутри сегмента ОТ, в частности, ограничения и контроля доступа к интернету и корпоративной почты из ОТ;
- Меры и средства ограничения и контроля удалённых подключений инженеров, сетевых администраторов, интеграторов и производителей систем АСУ ТП;
- Проработанность архитектуры и структуры информационной сети организации;
- Меры, средства и практики обновления ПО и контроля использования нецелевого ПО;
- Осведомлённость персонала промышленных предприятий об угрозах кибератак и случайных заражений, уровень кибергигиены сотрудников;
- Степень автоматизации предприятий, количество персонала и рабочих мест, оборудованных компьютерами;
- Общая степень IT-развития страны, наличие собственных компьютеров и доступность интернета для сотрудников предприятия за его пределами.

Мы также обнаружили (см. выше), что важным фактором может стать активность самораспространяющегося вредоносного ПО (червей) в сегменте АСУ ТП, которая в обнаруженных нами частных случаях, вероятно, обусловлена общей высокой активностью червей в стране.

Это наблюдение заставляет задаться вопросом, насколько вообще уровень вредоносной активности внутри сегмента АСУ ТП связана с общей «фоновой» вредоносной активностью в стране.

Какого цвета «фон»?

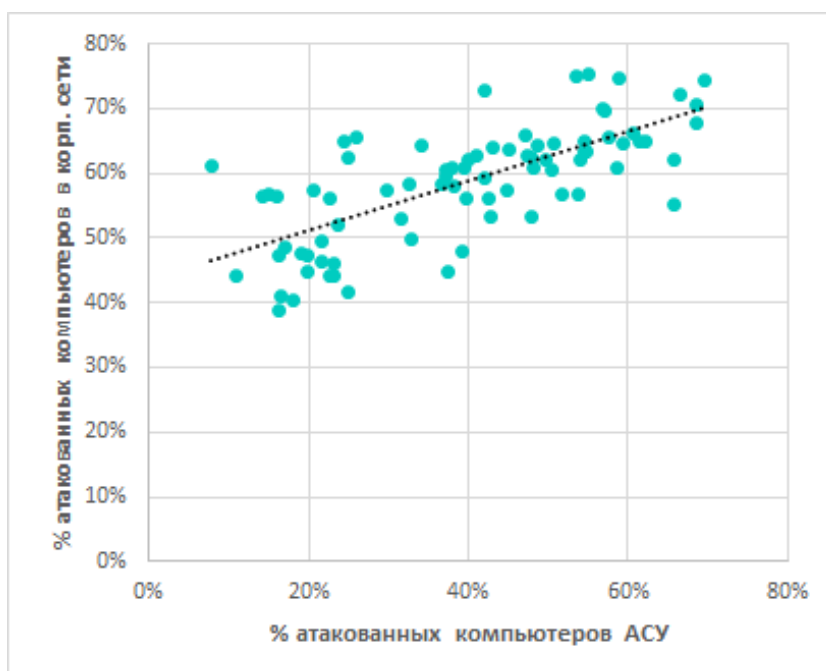
Чтобы понять, что же определяет вредоносный «фон» для компьютеров АСУ из нашей выборки, проверим, есть ли корреляция между показателем процента атакованных компьютеров АСУ и соответствующим показателем для компьютеров в корпоративной среде вообще, а также показателем для компьютеров домашних пользователей в каждой из стран.

Для того чтобы провести границу между «корпоративной средой» и «всем остальным ИТ-пространством» в стране, воспользуемся тем фактом, что условия приобретения и использования корпоративных продуктов очень редко подходят для частных лиц, и наоборот – покупка продуктов, предназначенных для частных лиц, оказывается экономически нецелесообразной для организаций.

Это позволяет построить две выборки, которые дают хорошее представление об искомых показателях. Первая демонстрирует статистику, которая получена с корпоративных продуктов «Лаборатории Касперского» в стране, вторая – с продуктов, предназначенных для частных пользователей.

Для начала приведём график, демонстрирующий обнаруженную корреляцию показателей для компьютеров АСУ и корпоративного сегмента.

Корреляция* значений процента компьютеров, на которых были заблокированы вредоносные объекты, внутри сегмента АСУ ТП и в корпоративной сети, в сравнении по странам

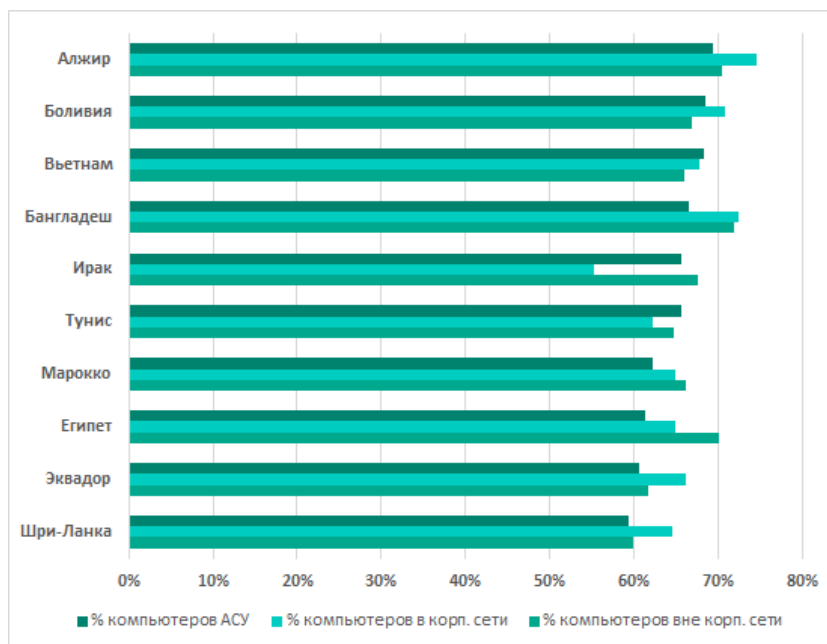


*параметры корреляции: $R > .70$, $p < .001$

Как оказалось, корреляция между показателями в корпоративной среде и в среде АСУ ТП несомненно есть, и она достаточно высока ($R > .70$).

Заметим, что все три показателя – процент компьютеров, на которых были заблокированы вредоносные объекты, в среде АСУ ТП, корпоративной среде и компьютеров за её пределами – ближе друг к другу в области высоких значений.

Сравнение максимальных показателей* процента компьютеров, на которых было заблокировано вредоносное ПО в среде АСУ ТП, и аналогичных показателей в корпоративной среде и за её пределами

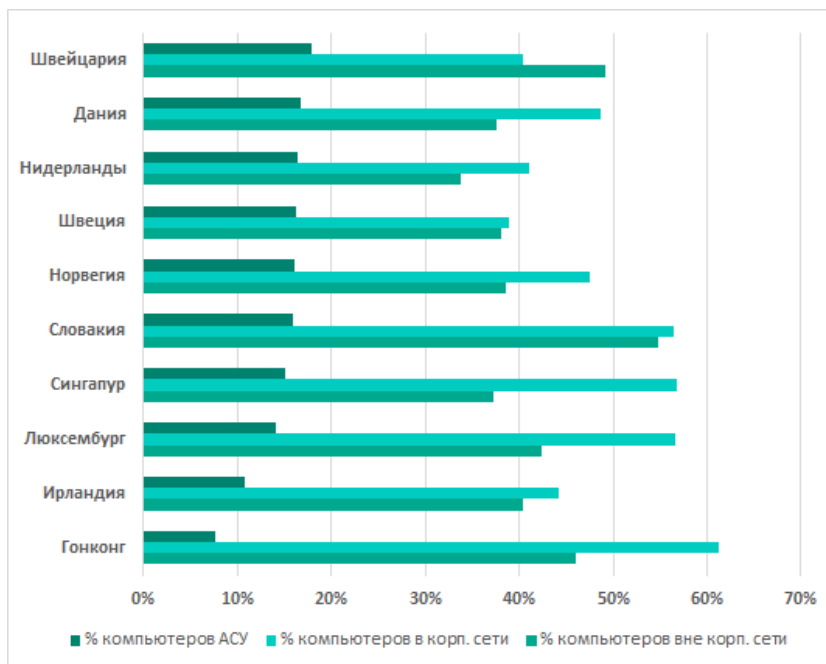


***ТОП 10 стран по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты, первое полугодие 2019**

Так, например, в странах, лидирующих в этом рейтинге, процент атакованных компьютеров АСУ близок к аналогичным показателям компьютеров в корпоративной среде. Причиной этому в большей степени является то, что в этих странах и на компьютерах АСУ, и на корпоративных компьютерах детектируется множество вредоносных программ, имеющих функциональность самостоятельного распространения (в основном посредством USB), а также блокируется вредоносная активность майнеров, распространяющихся по локальной сети с использованием уязвимостей.

Показателен также и тот факт, что в странах и на территориях с низким значением процента компьютеров АСУ, на которых было заблокировано вредоносное ПО, этот показатель значительно ниже аналогичного показателя компьютеров за пределами АСУ ТП.

Сравнение минимальных показателей* процента компьютеров, на которых было заблокировано вредоносное ПО в среде АСУ ТП, и аналогичных показателей в корпоративной среде и за ее пределами

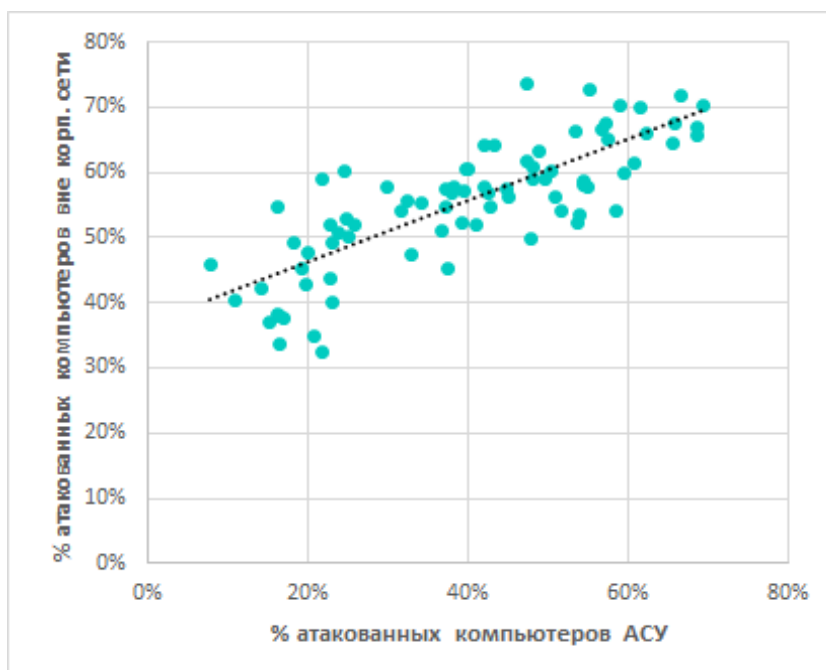


**10 стран и территорий с наименьшим процентом компьютеров АСУ, на которых были заблокированы вредоносные объекты*

Это может говорить о том, что в среднем в «благополучных» с точки зрения защиты сегментах АСУ ТП странах и территориях низкий процент атакованных компьютеров АСУ обусловлен скорее применением мер и средств защиты, чем общим низким фоном вредоносной активности.

Довольно неожиданными на первый взгляд могут показаться результаты анализа корреляции показателей для компьютеров АСУ и домашних пользователей.

Корреляция* значений процента компьютеров, на которых были заблокированы вредоносные объекты, в среде АСУ ТП и вне корпоративной сети, в сравнении по странам



**параметры корреляции: $R > .80$, $p < .001$*

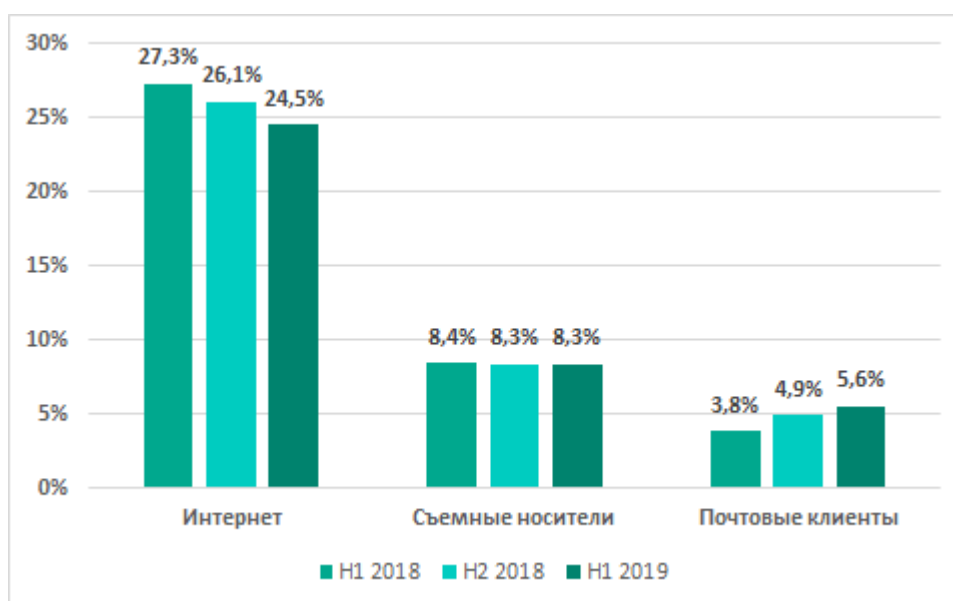
Неожиданной тут может быть обнаруженная корреляция, превышающая корреляцию с показателями для компьютеров корпоративной среды ($R > .80$ против $R > .70$, при $p < .001$).

Однако эта находка хорошо согласуется с нашими наблюдениями «в поле» — в результате оказания различных услуг по обеспечению безопасности промышленных объектов наших клиентов (проведение тренингов, аудитов, тестов на проникновение, расследования инцидентов и исследования целенаправленных атак). В свете полученного в этих проектах опыта, по нашему мнению, эта обнаруженная «на бумаге» закономерность может говорить о том, что в среднем компьютеры АСУ не находятся полностью внутри периметра безопасности, характерного для корпоративной среды, и в значительной мере защищаются от многих угроз, актуальных, в том числе, и для домашних пользователей, собственными мерами и средствами. Иными словами, задачи защиты корпоративного сегмента и сегмента АСУ ТП оказываются в какой-то мере независимыми.

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*

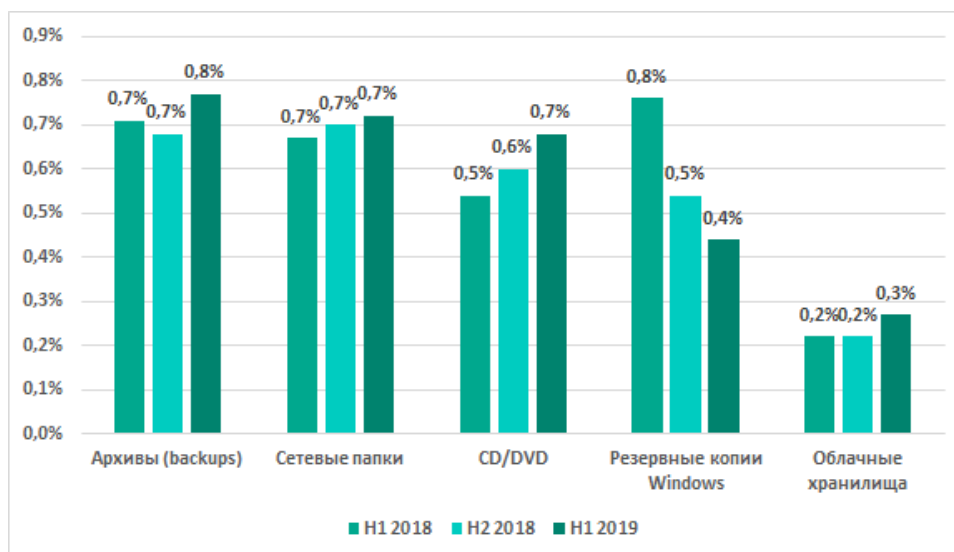


**процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

Начиная с 2018 года мы наблюдаем тенденцию снижения процента компьютеров АСУ, на которых были заблокированы вредоносные объекты из интернета. В первом полугодии 2019 года интернет стал источником угроз, заблокированных на 24,5% компьютеров АСУ. По сравнению со вторым полугодием 2018 года этот показатель уменьшился на 1,6 п.п. При этом мы наблюдаем рост (на 0,7 п.п.) процента компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения.

Другие показатели по основным источникам угроз остались на уровне прошлого полугодия.

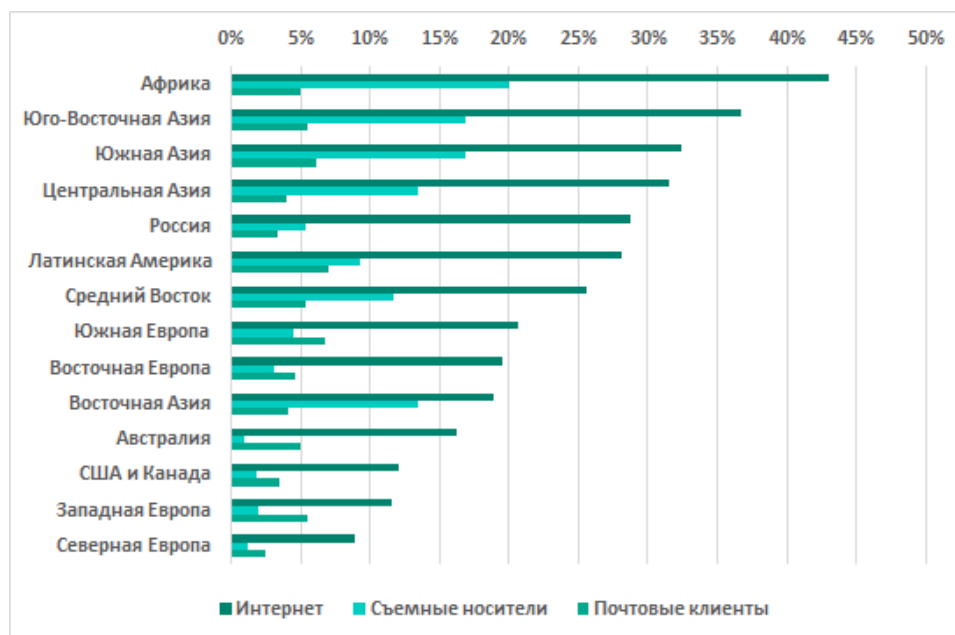
Минорные источники угроз, заблокированных на компьютерах АСУ (процент атакованных компьютеров АСУ)



*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

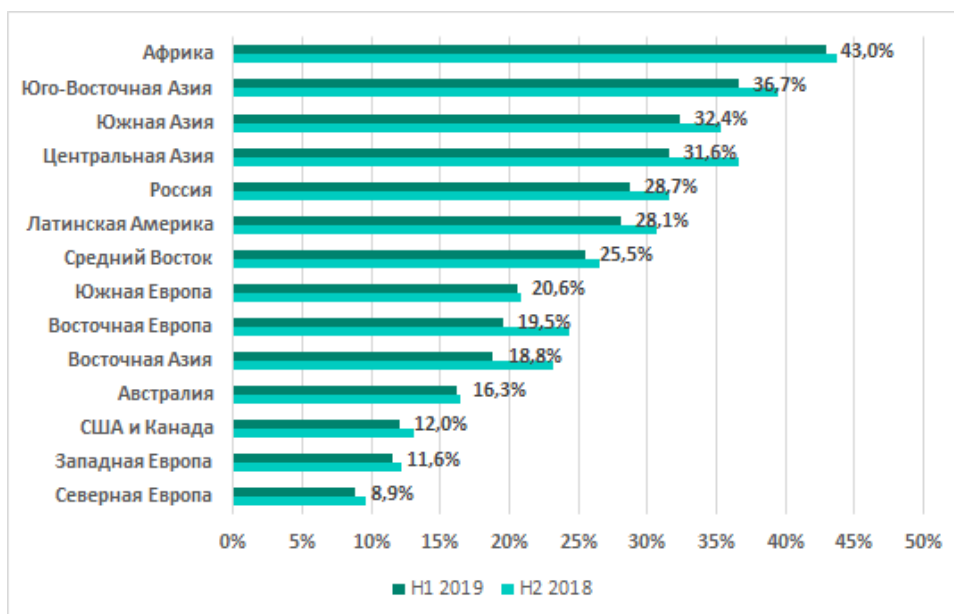


*процент атакованных компьютеров АСУ

Интернет

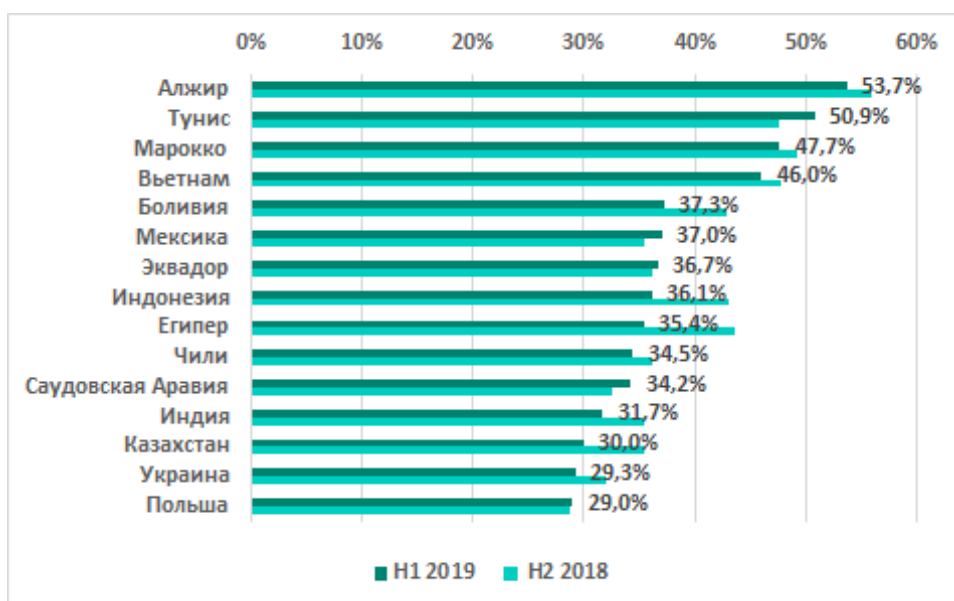
Во всех регионах мира основным источником угроз является интернет. Однако в Северной и Западной Европе и в Северной Америке процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, значительно ниже.

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



Список стран, входящих в TOP 15 по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, в основном остался без изменений. «Новичками» в этом рейтинге в первом полугодии 2019 года оказались Боливия и Польша.

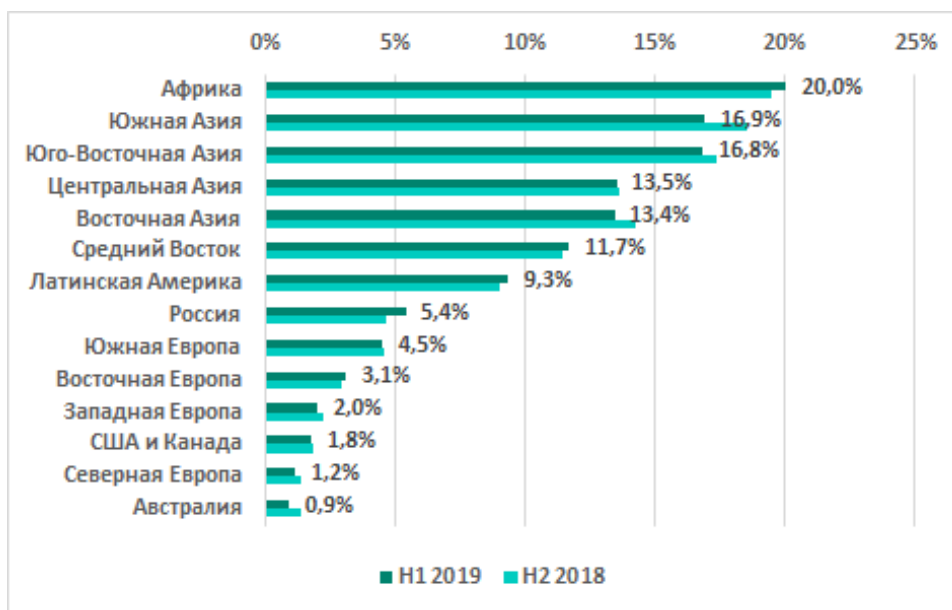
TOP 15 стран по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета



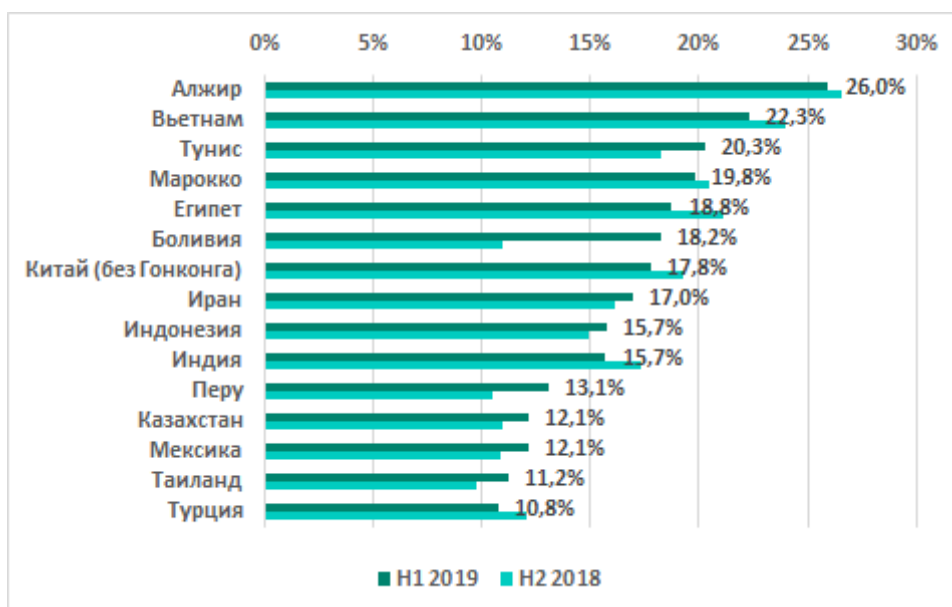
Съемные носители

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

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



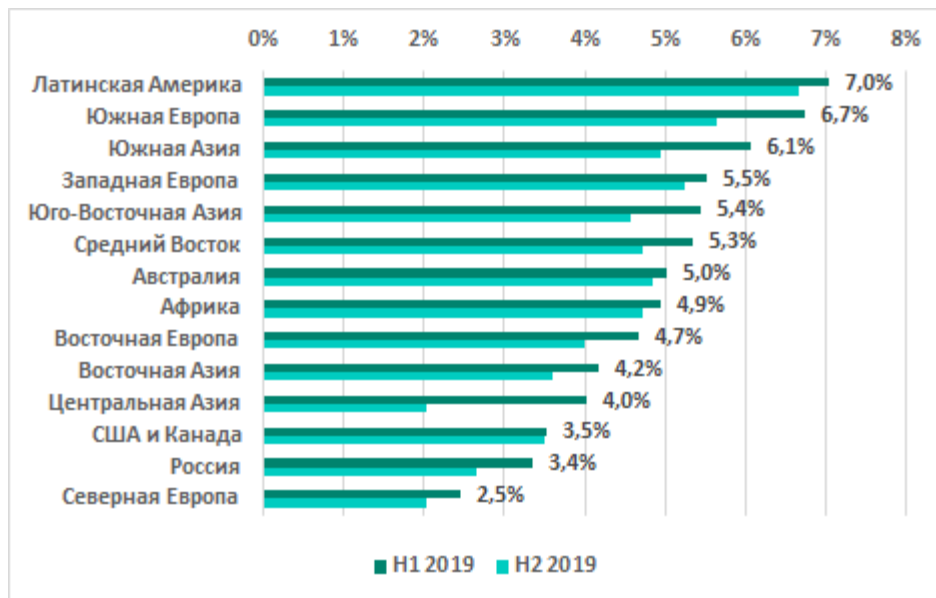
ТОП 15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей



Почтовые клиенты

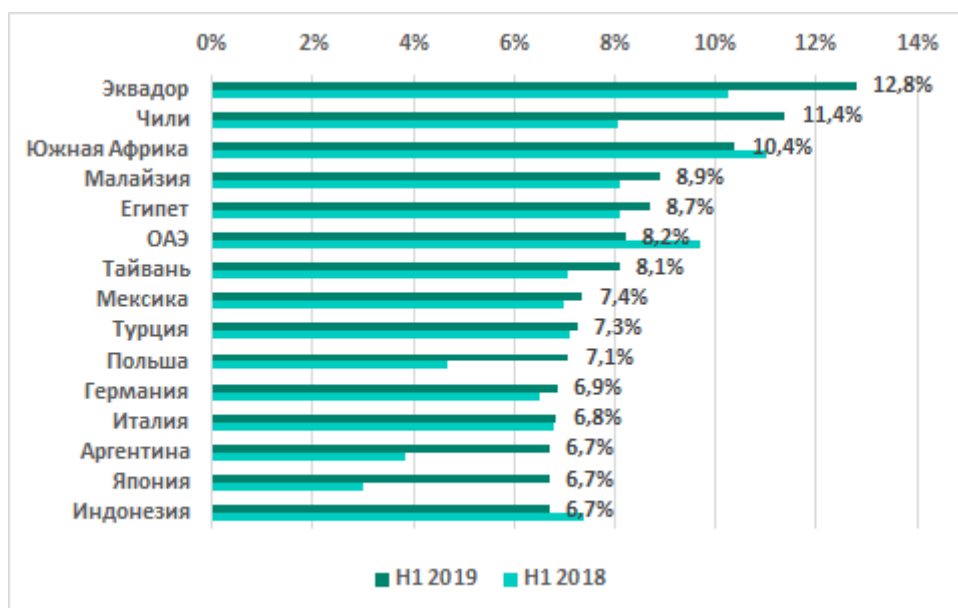
В рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, большого разброса значений нет. Возглавляет его Латинская Америка, высокие показатели мы наблюдаем также в Южной Европе и Южной Азии.

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



В первом полугодии 2019 года в список TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, вместо Кореи, Бразилии и Перу, которые фигурировали в этом рейтинге в предыдущем полугодии, вошли Япония, Аргентина и Польша.

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



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



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