Kaspersky ICS CERT

kaspersky

Ландшафт угроз для систем промышленной автоматизации в России

Ответы, которые мы знаем

20.09.2022

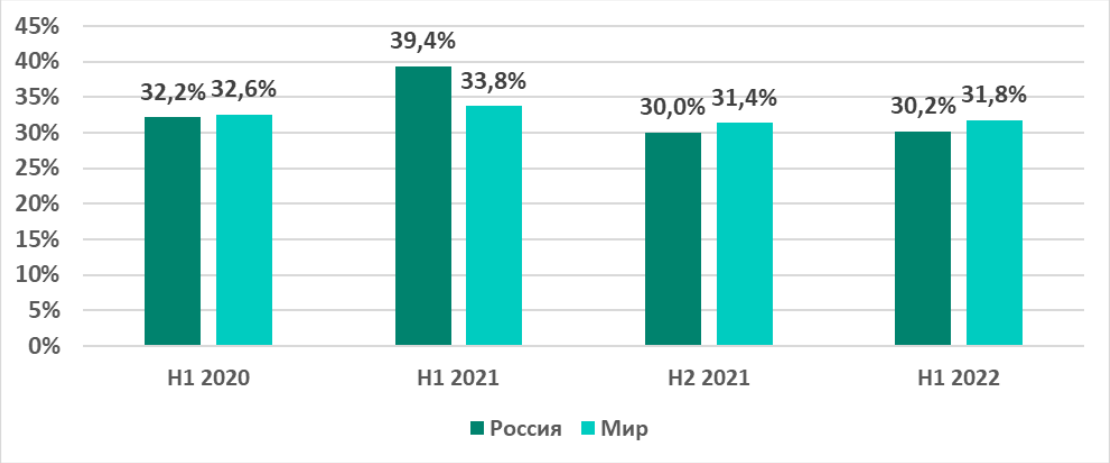
Version 1.0

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Отличается ли первое полугодие 2022 от предыдущих?

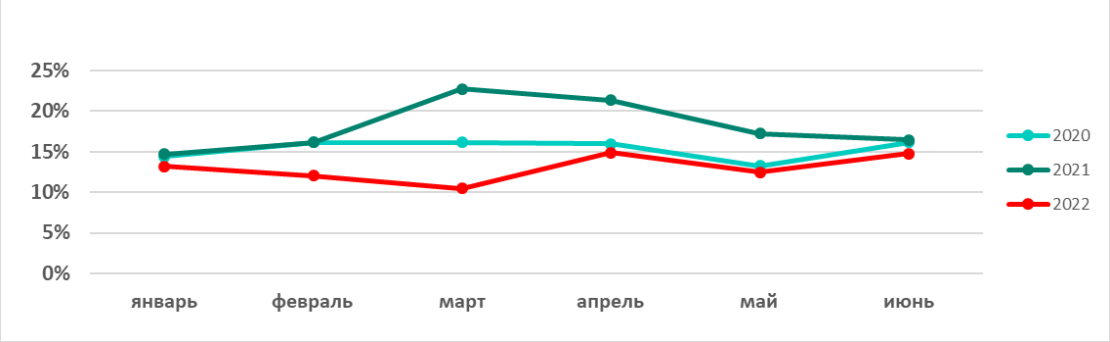
Если сравнивать процент атакованных компьютеров АСУ в России в первом полугодии 2022 с предыдущими полугодиями, то значимых изменений мы не видим. Этот процент довольно стабилен и близок к среднему по миру показателю.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



Однако в феврале и в марте отмечено не характерное для предыдущих лет снижение процента атакованных компьютеров АСУ, что, возможно, связано с началом спецоперации в Украине — подобную картину мы наблюдали и при анализе угроз для IT-сектора. По всей видимости, некоторая часть злоумышленников вынуждена была временно приостановить или уменьшить свою активность. К апрелю, впрочем, показатель вернулся к своим прошлогодним значениям.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам первого полугодия 2020, 2021 и 2022 годов

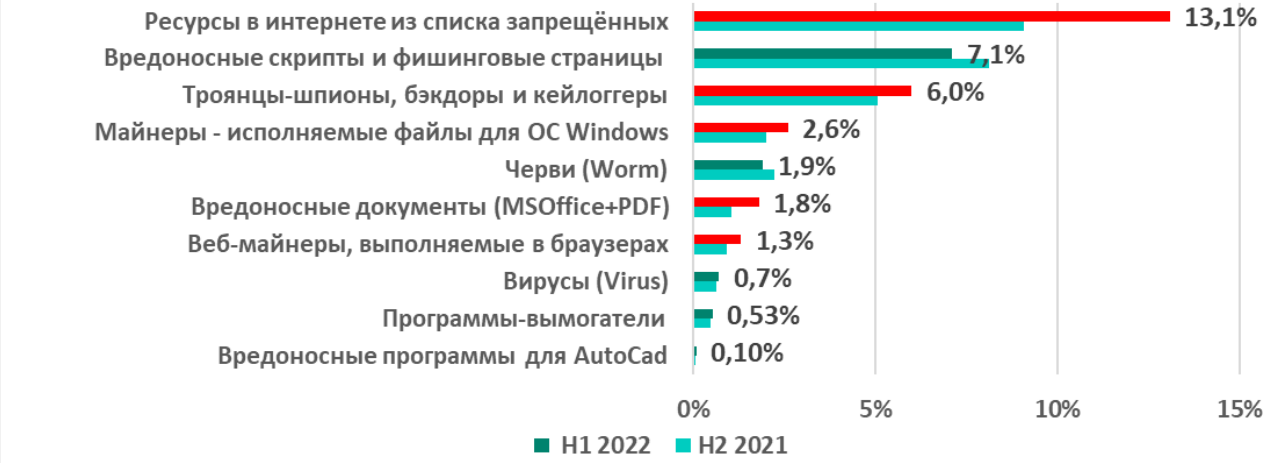


© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

От каких угроз мы защищаем компьютеры АСУ?

Во втором полугодии 2021 года защитными решениями «Лаборатории Касперского» на компьютерах АСУ в России было заблокировано более 4,6 тысяч модификаций вредоносного ПО из 2419 различных семейств.

Вредоносные объекты, которые продукты «Лаборатории Касперского» блокируют на компьютерах АСУ, относятся ко многим категориям.



Процент компьютеров АСУ, на которых была предотвращена активность вредоносных объектов различных категорий, первое полугодие 2022 и второе полугодие 2021

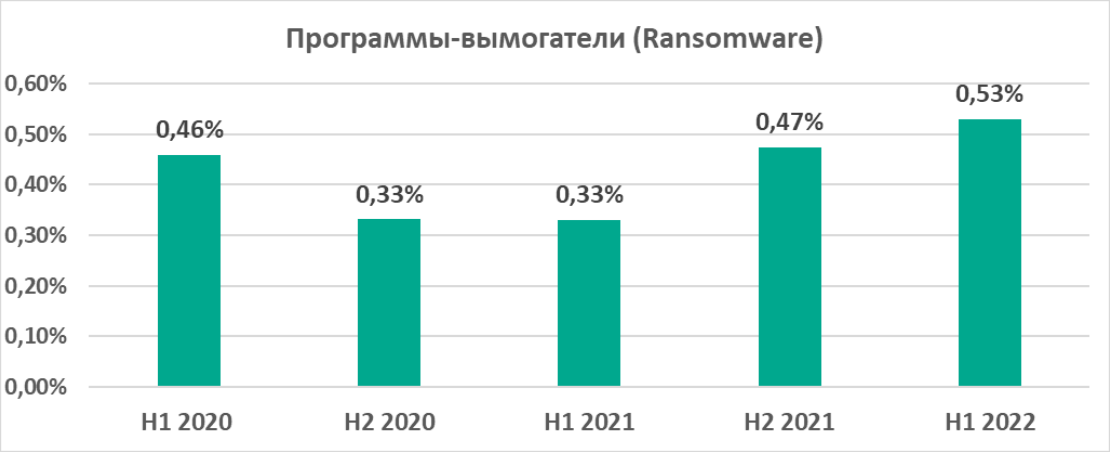
В первом полугодии 2022 года в России заметно вырос процент компьютеров АСУ, на которых были заблокированы:

- **Ресурсы в интернете из списка запрещенных** — на 4,0 п.п.;
- **Шпионское вредоносное ПО —** на 0,9 п.п.;
- **Вредоносные документы (MSOffice+PDF) —** на 0,8 п.п;
- **Майнеры** — на 0,6 п.п. майнеры — исполняемые файлы для ОС Windows и на 0,4 п.п. майнеры, выполняемые в браузерах.

Отметим также, что процент компьютеров АСУ, на которых были заблокированы **программы-вымогатели**, в первом полугодии 2022 оказался самым высоким в период первое полугодие 2020 — первое полугодие 2022. За год этот процент вырос на 0,2 п.п. Разница может показаться незначительной, но на деле это означает повышение риска серьезных финансовых потерь для сотен атакованных промышленных компаний.

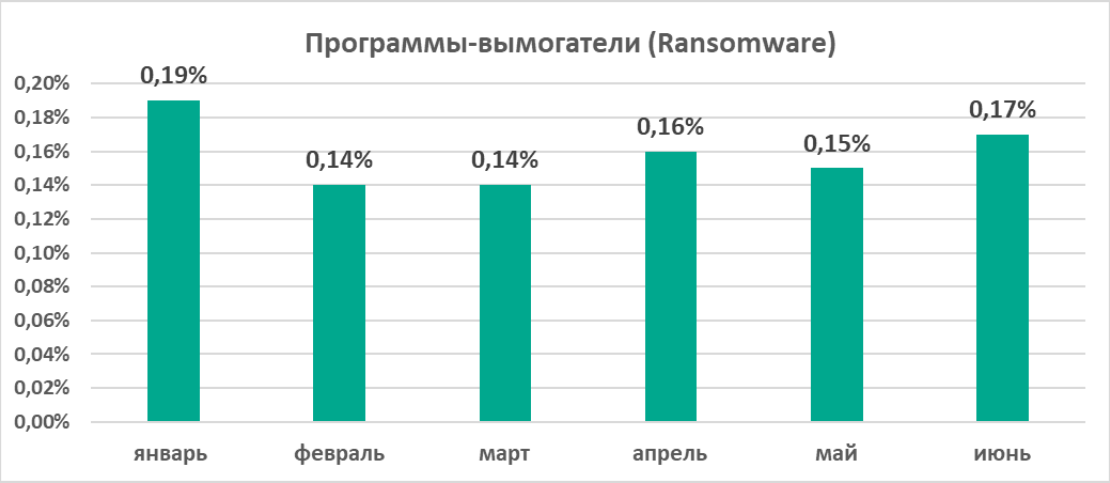
© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели



Наиболее активными вымогатели были в январе.

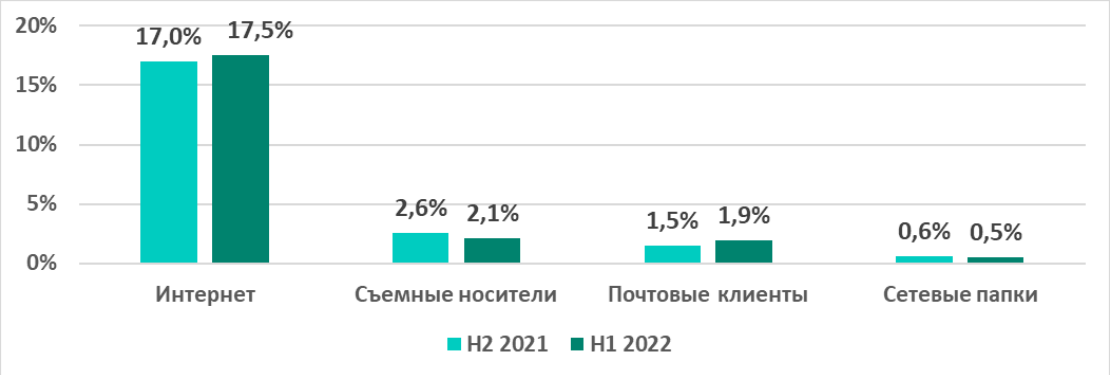
Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, январь — июнь 2022



Как вредоносное ПО попадает на компьютеры АСУ?

Основными источниками угроз для компьютеров АСУ остаются интернет, съемные носители и почтовые клиенты. За прошедшее полугодие процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из каждого источника, изменился не более, чем на 0,5 п.п.

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



© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

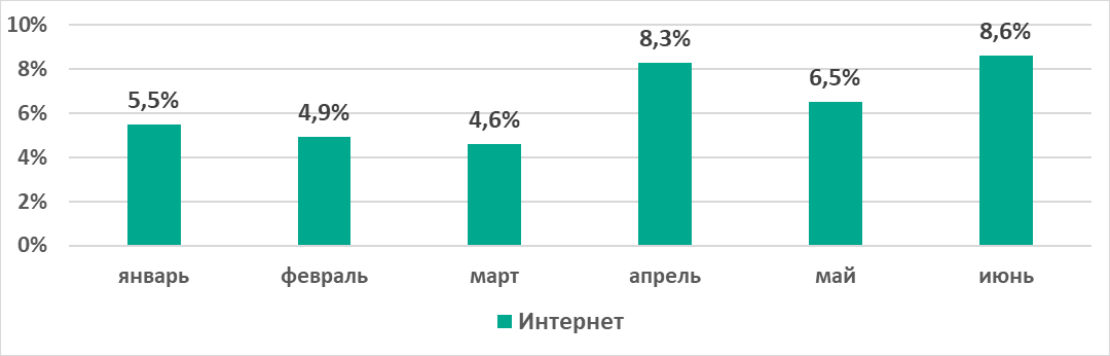
Откуда на компьютерах АСУ зловреды из интернета и почты?

Если со съемными носителями как источником вредоносного ПО вопросов, как правило, не возникает (съемные носители часто используются для передачи информации в технологической сети предприятий), то наличие интернета и почтовых клиентов в статистике по источникам угроз часто вызывают недоумение. Откуда на компьютерах АСУ угрозы из интернета и почты?

Технологическая сеть помимо SCADA/OPC/Historian/HMI включает также компьютеры (в том числе ноутбуки) инженеров, разработчиков ПО и администраторов сети. Именно такие пользовательские машины часто (явно или скрытно) используют доступ к интернету, почте и прочим сервисам, одновременно имея доступ к системам АСУ и обладая повышенными привилегиями.

Стабильно высокий процент заблокированных интернет и почтовых угроз как раз является следствием сопряжения корпоративной и технологической сетей, а также подключения к интернету компьютеров из технологической сети через сети мобильных операторов (с помощью мобильных телефонов, USB модемов и/или Wi-Fi роутеров с поддержкой 3G/LTE). Что касается подрядчиков, разработчиков, интеграторов, системных/сетевых администраторов, которые подключаются к технологической сети извне (напрямую или удаленно), то они часто имеют свободный доступ к интернету. Их компьютеры входят в группу наибольшего риска и могут стать каналом проникновения вредоносного ПО в технологические сети обслуживаемых ими предприятий.

Процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, январь — июнь 2022 года

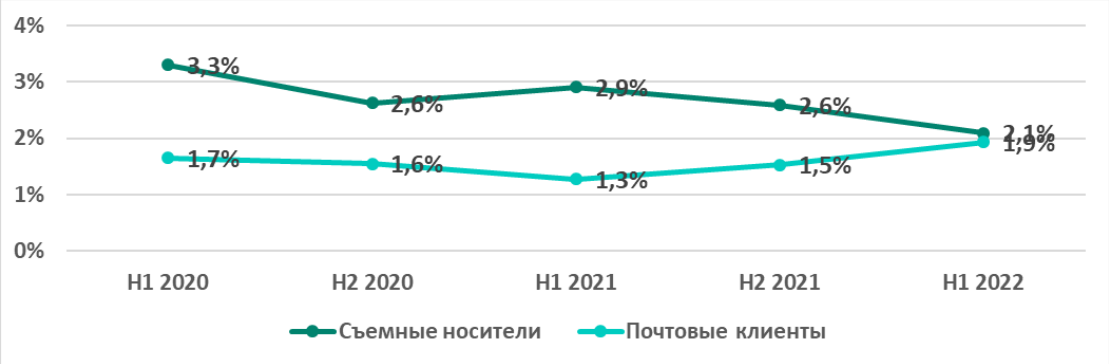


Использование корпоративной почты на компьютерах в технологической сети открывает дорогу шпионскому ПО, распространяемому через фишинговые письма, часто — от одного промышленного предприятия к другому в письмах, замаскированных под корреспонденцию организаций-жертв. Как мы уже писали в одном из наших предыдущих отчётов,

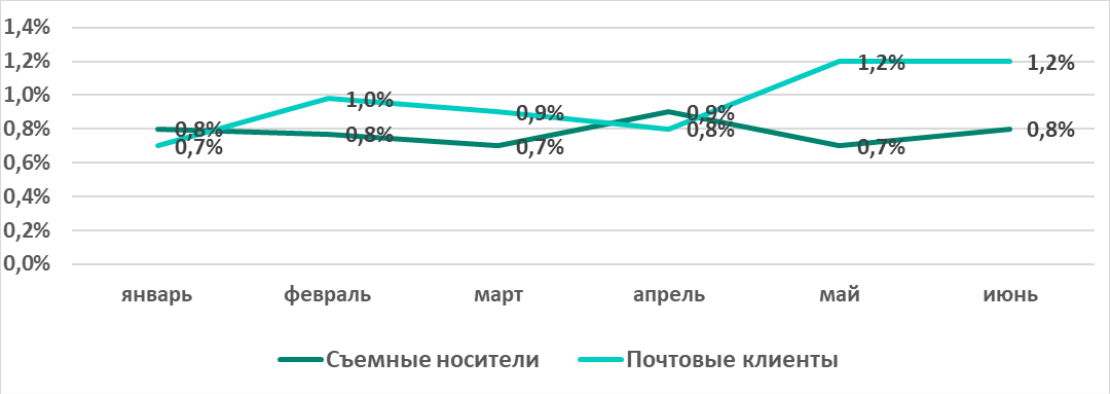
© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

злоумышленники используют корпоративную почту множества промышленных организаций для распространения вредоносного ПО по списку контактов пользователя скомпрометированной рабочей станции.

В то же время проценты компьютеров АСУ, на которых угрозы были заблокированы при подключении съемных носителей и в почте, в России меняются (больше-меньше) в «противофазе». Это актуально для изменений как по полугодиям, так и по месяцам первого полугодия 2022 года (за исключением аномального в этом году марта, когда, вероятно, падение показателей для угроз из почты было связанно с временным падением фишинговой активности).



Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки и вредоносное ПО при подключении съемных носителей



Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения и фишинговые ссылки и вредоносное ПО при подключении съемных носителей, январь — июнь 2022 года

Что касается процента компьютеров, на которых были заблокированы угрозы на съемных носителях, то схожий тренд на снижение наблюдается во многих странах, где ранее были замечены резкие всплески детектов на съемных носителях, вызванных локальными эпидемиями вирусов и червей.

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Угрозы из интернета

Ресурсы в интернете из списка запрещенных традиционно лидируют в рейтинге категорий угроз. 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 список запрещенных. Такие ресурсы связаны с распространением или управлением каким-либо вредоносным ПО.

В частности, в черные списки попадают также ресурсы, на которых распространяются **шпионские программы** и **программы-вымогатели**, замаскированные под утилиты для взлома/сброса пароля на контроллерах различных производителей, программы для взлома лицензионной защиты промышленного и инженерного программного обеспечения, используемого в технологической сети.

Значительная часть ресурсов из списка запрещенных используется для распространения **вредоносных скриптов и фишинговых страниц (HTML)**.

Вредоносные скрипты применяются злоумышленниками для выполнения большого спектра задач — от сбора информации, трекинга и перенаправления браузера пользователя на вредоносный веб-ресурс до загрузки в систему или в браузер пользователя различных вредоносных программ (например, **шпионского ПО** и/или **программ для скрытого майнинга криптовалюты**).

Угрозы в почте

Вредоносные скрипты и фишинговые страницы распространяются не только через интернет, но и посредством фишинговых рассылок.

Фишинговые письма, замаскированные под деловую переписку, — один из основных векторов первичного заражения, который используется злоумышленниками. В таких письмах зачастую распространяются вредоносные вложения **в формате офисных документов, таких как MSOffice и PDF**, а также архивы, содержащие исполняемые файлы вредоносного ПО.

Вредоносные документы (MSOffice и PDF), как правило, содержат эксплойты, вредоносные макросы и зловредные ссылки.

Шпионские программы (троянцы-шпионы, бэкдоры и кейлоггеры), встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. В большинстве случаев конечная цель таких

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

атак — кража денег, но используются они и в целевых атаках, для кибершпионажа.

Вредоносные программы и скрипты, встраиваемые в тело электронных писем, часто используются и в целевых атаках на промышленные предприятия. В таких атаках злоумышленники используют тщательно подготовленные письма, составленные с учетом специфики атакуемого объекта.

Как видно на графике выше, шпионское ПО входит в тройку лидеров по проценту компьютеров АСУ, на которых были заблокированы зловреды определенной категории.

Угрозы на съемных носителях и в сетевых папках

Вирусы и черви распространяются в сетях АСУ через съемные носители, сетевые папки, зараженные файлы (в том числе бэкапы) и сетевые атаки на устаревшее ПО (например, Radmin2).

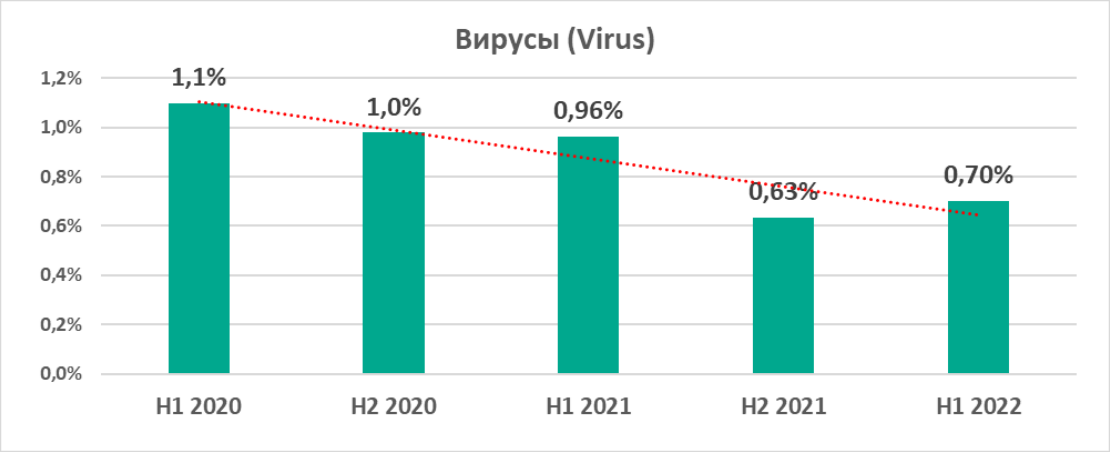
Среди распространяющихся вирусов и червей довольно много старых (например, таких как Kido/Conficker). Несмотря на то, что их командные серверы уже отключены, они не только ослабляют безопасность зараженных систем — например, открывая сетевые порты и изменяя конфигурацию, — но также могут приводить к сбоям в работе ПО и отказам в обслуживании.

Вместе с тем, в сетях АСУ встречаются и новые версии червей, используемые злоумышленниками для распространения в сети шпионского ПО, программ-вымогателей и майнеров. Чаще всего для распространения по сети эти черви используют эксплойты для исправленных производителями, но еще актуальных в технологических сетях уязвимостей сетевых сервисов (например, SMB, RDP), украденные ранее данные аутентификации или перебор паролей.

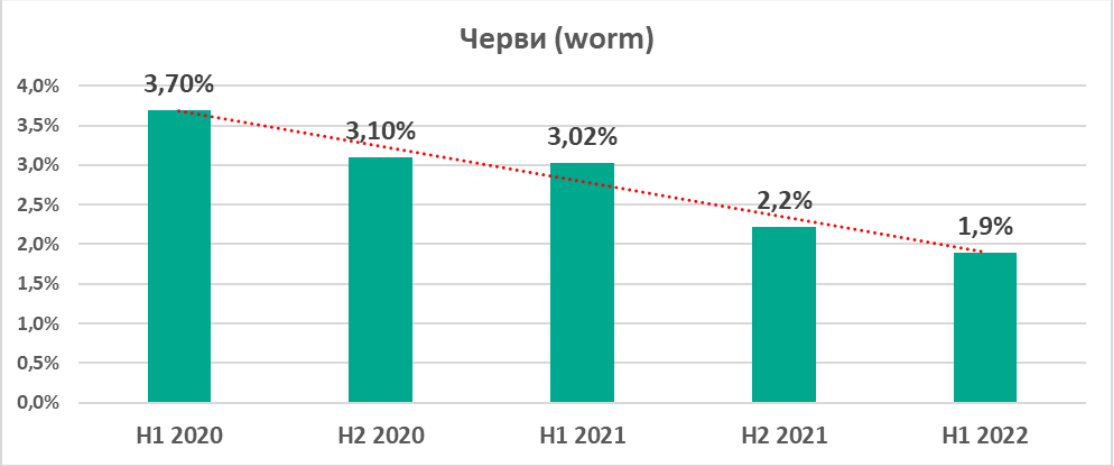
Начиная с первого полугодия 2020 года, мы наблюдаем снижение процента компьютеров АСУ, на которых были заблокированы вирусы и черви:

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Процент компьютеров АСУ, на которых были заблокированы вирусы



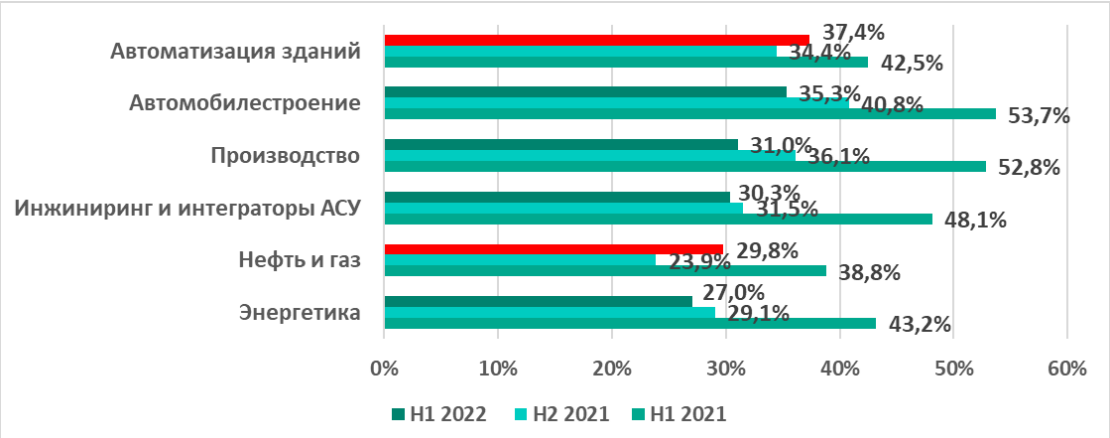
Процент компьютеров АСУ, на которых были заблокированы черви



Отличается ли ситуация в разных отраслях?

Мы сравнили статистику в нескольких отраслях. Как видно на графике ниже, процент компьютеров АСУ, на которых было заблокировано вредоносное ПО, варьирует в исследованных отраслях от 27% (Энергетика) до 37,4% (Автоматизация зданий).

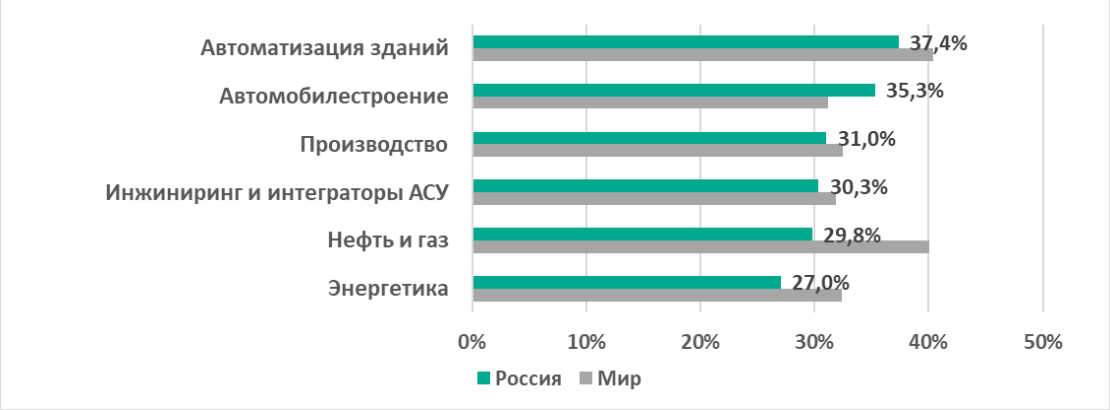
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в некоторых отраслях, первое полугодие 2022



© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

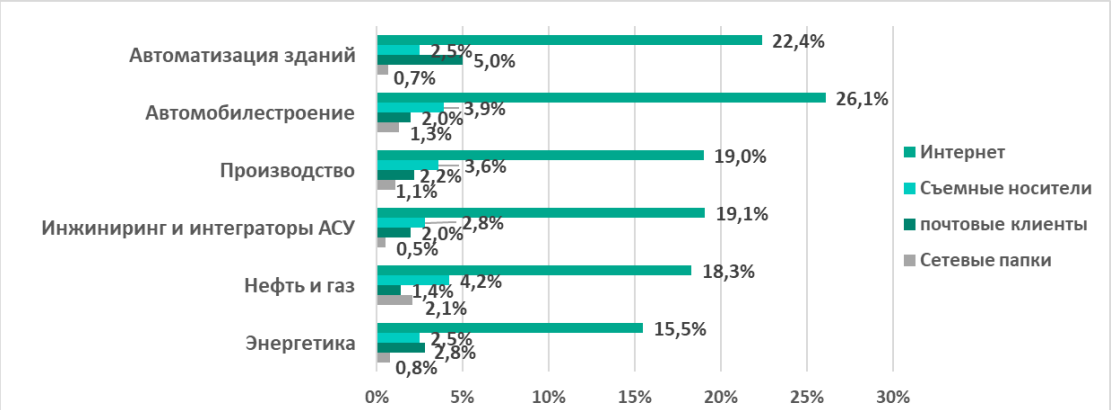
Во всех исследованных отраслях, кроме Автомобилестроения, в России этот показатель ниже, чем в среднем по миру.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты в некоторых отраслях, Россия и мир, первое полугодие 2022



Основные источники угроз в отраслях — все те же интернет, съемные носители и почтовые клиенты (отрасли на графике ниже выстроены по убыванию процента компьютеров АСУ, на которых были заблокированы угрозы из всех источников).

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников, в некоторых отраслях



В первом полугодии 2022 процент атакованных компьютеров АСУ вырос в двух из шести отраслей — Нефть и газ и Автоматизация зданий. В остальных отраслях проценты уменьшились.

Рассмотрим отрасли в порядке их позиций в рейтинге по проценту атакованных компьютеров АСУ.

1. Автоматизация зданий (37,4%)

По проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО, среди исследованных отраслей Автоматизация зданий лидирует не только в России, но и в мире в целом. По всей видимости российским организациям (и не только из числа промышленных!) стоит озаботиться данной проблемой. Мы уже наблюдали примеры целевых атак,

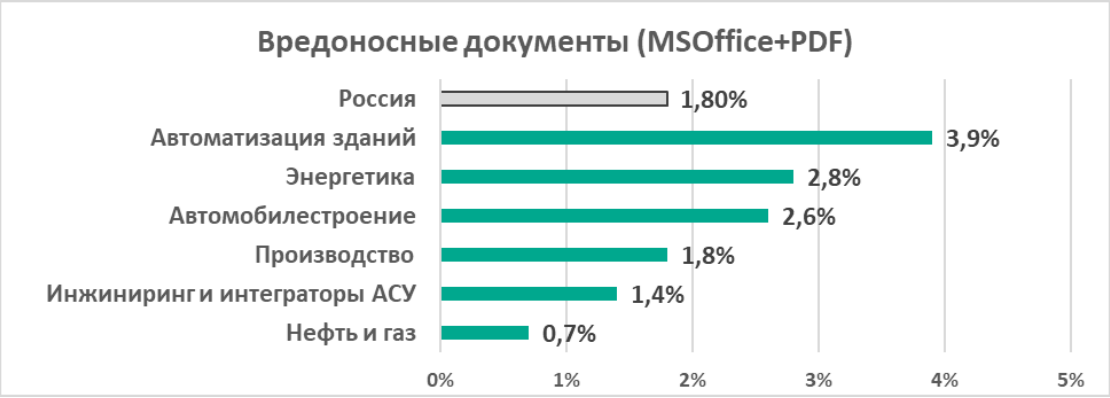
© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

в которых злоумышленники атаковали одновременно и системы автоматизации зданий, и информационные системы расположенных в этих зданиях организаций — к сожалению, далеко не всегда они достаточно надёжно изолированы друг от друга.

В российских рейтингах эта отрасль на первом месте по проценту компьютеров АСУ, на которых были заблокированы:

- Угрозы из почты — вредоносные почтовые вложения и фишинговые ссылки.

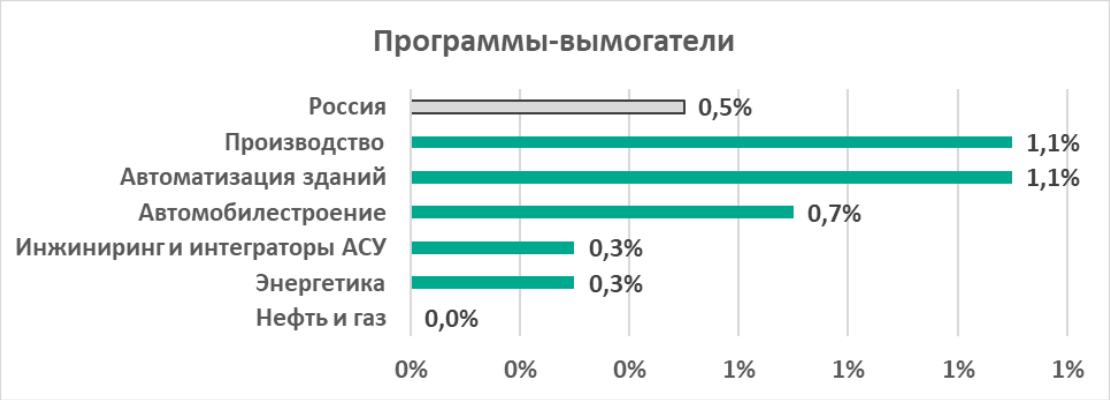
- Вредоносные документы (MSOffice + PDF).
  Как уже было сказано выше, фишинговые письма часто маскируются под деловую переписку с вложенными вредоносными документами.



© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Программы-шпионы.
  Это еще одна категория вредоносного ПО, которая активно распространяется в фишинговых письмах.

- Программы-вымогатели.
  В этом рейтинге Автоматизация зданий разделяет первое место с производственным сектором.



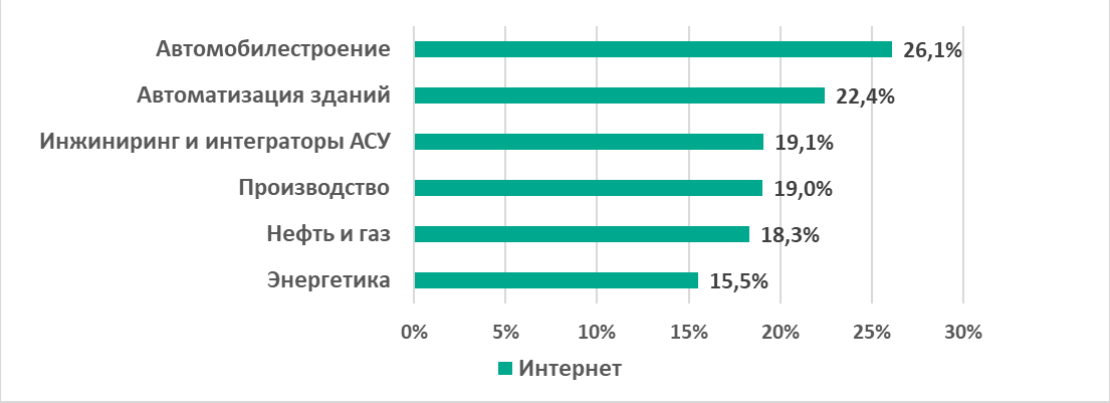
- Автоматизация зданий на втором месте в рейтингах по угрозам из интернета (22,4%) и ресурсам в интернете из списка запрещенных (14,2%).

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

2. Автомобилестроение (35,3%)

Эта отрасль лидирует по проценту компьютеров АСУ, на которых были заблокированы:

- Угрозы из интернета.



- Ресурсы в интернете из списка запрещенных.

- Автомобилестроение на втором месте по проценту компьютеров АСУ, на которых угрозы были заблокированы при присоединении съемных носителей (3,9%). Разница показателей с отраслью, которая заняла первое место в этом рейтинге, — всего 0,3 п.п. (см. график ниже в разделе «Нефть и газ»).

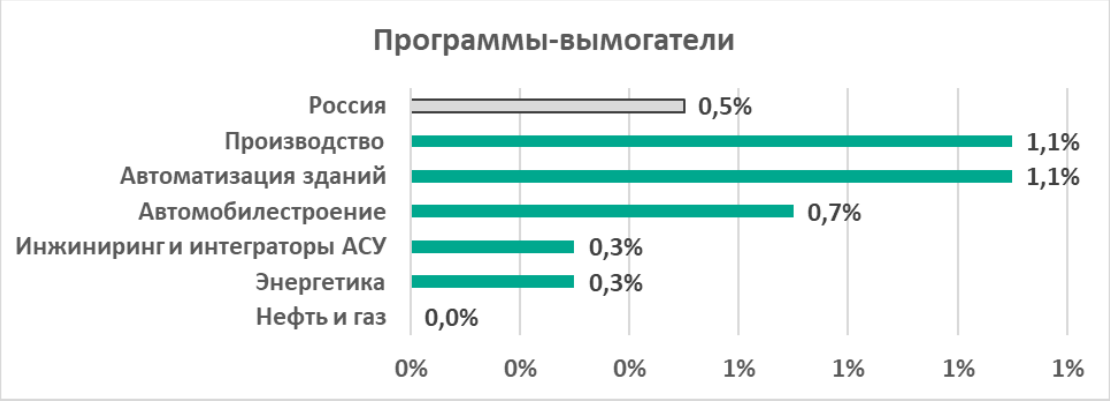
3. Производство (31,0%)

Производство лидирует по проценту компьютеров АСУ, на которых были заблокированы:

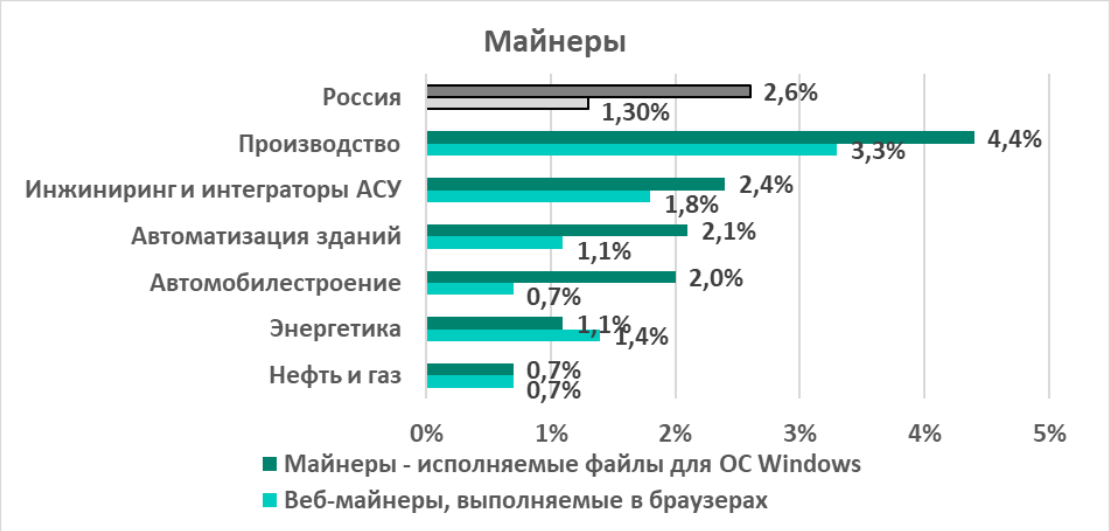
- Программы-вымогатели.
  В производственном секторе процент атакованных вымогателями

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

компьютеров АСУ вдвое выше, чем аналогичный показатель в среднем по России.



- Майнеры — как исполняемые файлы для ОС Windows, так и веб-майнеры, выполняемые в браузерах.



- Вредоносные скрипты и фишинговые страницы, которые распространяются в интернете и во вредоносных письмах.

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

4. Инжиниринг и интеграторы АСУ (30,3%)

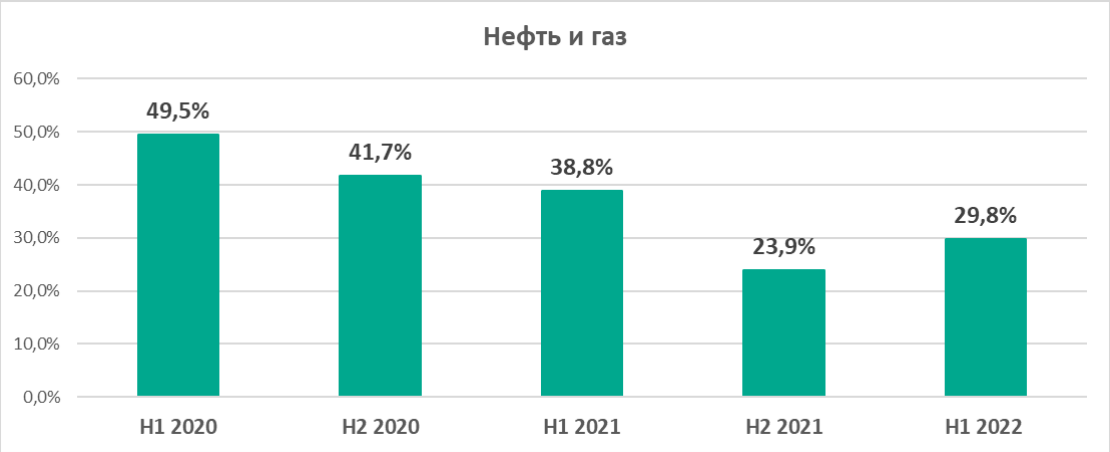
Эта отрасль ни в одном нашем рейтинге не заняла лидирующей позиции. Но она на втором месте по проценту компьютеров АСУ, на которых были заблокированы:

- вредоносные программы для майнинга криптовалюты (2,4% майнеры — исполняемые файлы для ОС Windows и 1,8% — майнеры, выполняемые в браузерах),
- вредоносные скрипты и фишинговые страницы (7,9%).

В обоих рейтингах на первом месте — производственный сектор (см. соответствующие графики выше в части про Производство).

5. Нефть и газ (29,8%)

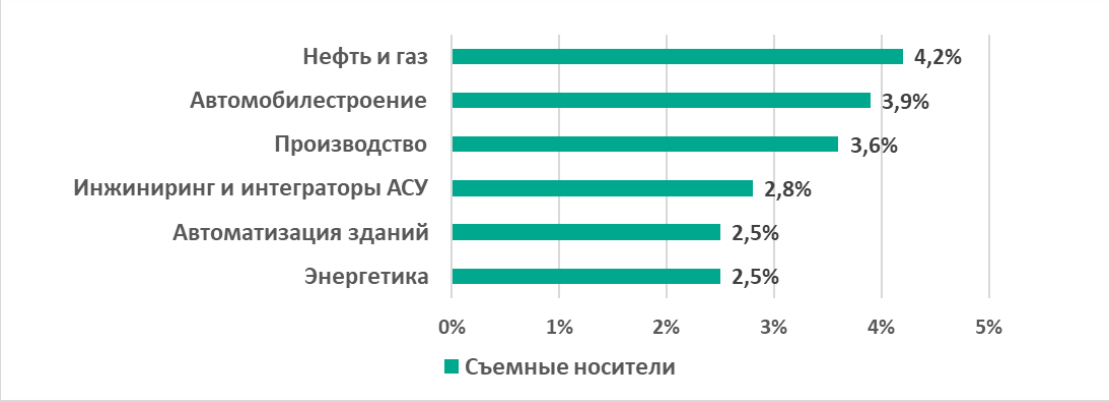
В отрасли Нефть и газ процент компьютеров АСУ, на которых было заблокировано вредоносное ПО, уменьшался с 2020 года. Однако в первом полугодии 2022 года он увеличился — и довольно заметно, на 5,9 п.п. Как уже было отмечено выше, это одна из двух отраслей, где показатель за полугодие вырос.



Нефть и газ на первом месте по проценту компьютеров АСУ, на которых были заблокированы:

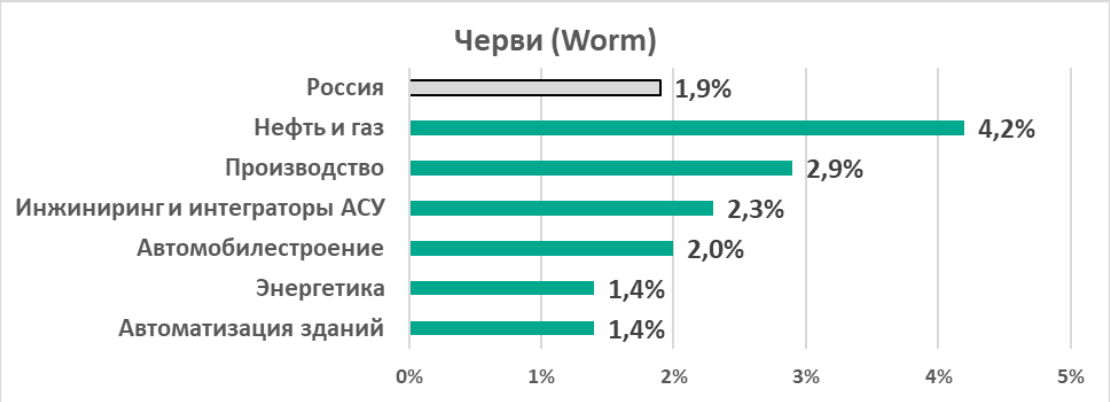
© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

- Угрозы при присоединении съемных носителей.



- Угрозы в сетевых папках.

- Черви
  Учитывая два предыдущих пункта, первое место отрасли Нефть и газ в этом рейтинге кажется закономерным (как было отмечено выше, черви распространяются, в основном, на съемных носителях и через сетевые папки).



© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

6. Энергетика (27%)

Самая благополучная отрасль, которая заняла последнее место в рейтинге по проценту атакованных компьютеров АСУ.

Энергетика оказалась на втором месте в двух наших рейтингах по проценту компьютеров АСУ, на которых были заблокированы:

- Угрозы из почты (2,8%).
- Вредоносные документы (MSOffice+PDF), которые распространяются как вложения в фишинговых письмах (2,8%).

Что делать со всей этой информацией?

Какие же практические выводы мы можем сделать, опираясь на приведённые выше результаты анализа данных нашей телеметрии?

Вывод 1. Банальный

Далеко не все АСУ ТП на самом деле изолированы от интернета. Да, если ваши системы действительно изолированы надёжно (нет доступа через локальную сеть организации, реализованы необходимые меры, не позволяющие подключиться через мобильные устройства, гарантированно нет никаких прочих неучтённых каналов и маршрутов), телеметрию от наших продуктов, установленных на ваших серверах и рабочих станциях, мы, скорее всего, не получили и не проанализировали, и приведённые выше оценки не имеют, кажется, к вам прямого отношения.

Однако, как показывает практика, чтобы быть в чём-то достаточно уверенным, нужно это периодически (а ещё лучше — постоянно) проверять и контролировать. Установите на свои АСУ-компьютеры адекватные средства защиты — и проверьте, так ли на самом деле ваши системы недоступны для интернет-угроз, как вы считали до этого.

Размер анализируемой нами выборки компьютеров АСУ, присылающих нам телеметрию из разных уголков мира, измеряется семизначным числом. И совсем не факт, что реальное положение дел в ваших «изолированных от внешнего мира» АСУ сильно отличается от описанной нами картины.

Вывод 2. Чуть менее банальный

Даже для «изолированных от внешнего мира» систем угрозы, попавшие с подключённой «флэшки», — более чем актуальны, и нельзя ни игнорировать

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

их, ни гарантированно защититься от них одними лишь организационными мерами. Адекватные угрозе технические средства защиты — обязательны. Без них надеяться на сознательность своих сотрудников и подрядчиков наивно.

Вы не сможете гарантировать, что будут использованы только официально разрешённые устройства, что эти устройства никогда не покинут определённый для них периметр, что они будут всегда должным образом проверены перед подключением к незащищённому компьютеру АСУ, и что этих проверок всегда будет достаточно (находящийся на «флэшке» зловред может попросту ещё не обнаруживаться средствами защиты на момент её последней проверки — обновления баз и компонентов защитных решений нужны не для того, чтобы создавать лишний трафик и потреблять вычислительные мощности при их установке).

Помните, что на «флэшке» может оказаться не только kido, но и что-то существенно более опасное, созданное специально для проникновения в «изолированные среды» и эксфильтрации данных из них — передачей данных так же через «флэшки», пока одна из них не будет подключена к системе, имеющей доступ к интернету, или контролируемой злоумышленником инфраструктуре внутри локальной сети.

Вывод 3. О Корпоративной почте в АСУ

Помните, что корпоративная почта умеет надёжно и безопасно доставлять не только уведомления от руководства и заявления от сотрудников, но и фишинговые письма с вредоносными вложениями. Понятно, что иметь по два компьютера, подключённых к разным, не связанным друг с другом, сетям на каждом рабочем месте — дорого и не всегда реализуемо. Поэтому обучайте сотрудников безопасной работе с почтой и не забудьте надёжно защитить от вредоносного ПО компьютеры, с которыми они работают.

Вывод 4. Для тех, кто не полностью убеждён в изоляции систем АСУ

Уже сейчас всем очевидно, что надёжно защитить 100% всех компьютеров АСУ для большинства организаций в ближайшей перспективе не получится. (Хотя российские организации последние несколько лет активно пытаются защитить всё большее количество компьютеров АСУ, о чём косвенно свидетельствует тенденция на спад обнаружения самораспространяющегося вредоносного ПО — сетевых червей.)

А значит, для защиты АСУ необходимо использовать дополнительные силы и средства — чтобы хоть как-то компенсировать неполную защиту узлов.

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

Средства мониторинга и интеллектуального анализа сетевого трафика внутри технологической сети могут частично помочь решить эту задачу — вы, как минимум, сможете обнаружить активность самораспространяющегося вредоносного ПО, попытки коммуникации вредоносного ПО с командными центрам, обнаружить активность, направленную на ПЛК и прочие не подлежащие пока прямой защите интеллектуальные устройства.

Вывод 5. Для тех, кто хочет разобраться, что же там внутри наших статистических данных

Да, подавляющее число угроз, добирающихся до компьютеров, имеющих отношение к АСУ, носят случайный характер и не нацелены специально ни на АСУ, ни на вашу организацию. Как правило, встреча с ними АСУ происходит в результате неаккуратных и необдуманных действиях сотрудников организации и подрядчиков. Обучение сотрудников правилам кибер-гигиены должно во многом помочь уменьшить эту угрозу.

Однако небольшой процент угроз (по нашей грубой оценке, не более 1% от общего их числа) носит всё-таки целевой характер. Это, в первую очередь, киберкриминальная активность, нацеленная на кражу денег или конфиденциальной информации (такой, как данные аутентификации и информации о системах предприятия и их конфигурации) с последующей её перепродажей другим злоумышленникам, знающим, как её эффективно использовать.

К числу последних относятся вымогатели и APT. Защититься от целенаправленных атак только тотальным соблюдением правил кибер-гигиены уже не получится. Для защиты от таких угроз придётся использовать продвинутые средства (EDR/XDR), привлекать продвинутых экспертов (MDR), растить экспертизу внутри организации (экспертные тренинги по обнаружению и предотвращению атак) и стараться быть в курсе самых последних изменений ландшафта угроз (сервисы Threat Intelligence).
И, пожалуй, самое важное — необходимо осознать, что никакие меры и средства защиты вас на 100% не защитят, и готовиться эффективно реагировать на возможные инциденты: обучать ответственный персонал (тренинги по Incident Response и Digital Forensics), разрабатывать планы реагирования и детальные инструкции для персонала (Incident Response Handbook).

За консультацией по вопросам угроз, актуальных для АСУ, и по любым вопросам, которые возникли у вас в связи с чтением этого материала, пишите нам на ics-cert@kaspersky.com — всегда будем рады ответить и помочь.

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

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

© 2022 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»