Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2019

Kaspersky ICS CERT

24.04.2020 Version 1.0

Оглавление

2019 год: главное

- В 2019 году Kaspersky ICS CERT было выявлено 103 уязвимости в промышленных системах, системах IIoT/IoT и других типах решений.
  - 33 из обнаруженных уязвимостей до сих пор не исправлены производителями соответствующих продуктов, хотя они получили для этого всю необходимую информацию.
  - Эксплуатация 30,1% выявленных уязвимостей может привести к удаленному выполнению произвольного кода, 14,6% – к DoS. Эксплуатация 13,6% уязвимостей позволяет повышать привилегии или же перехватывать сессии.
  - Абсолютное большинство обнаруженных Kaspersky ICS CERT уязвимостей, для которых в 2019 году были опубликованы CVE, по шкале CVSS v.3 имеют вес не менее 7.0 и относятся к группе наиболее критичных.
  - Уязвимости возникают из-за ошибок, допущенных при разработке программного обеспечения. Самой популярной в 2019 году стала ошибка под номером CWE-787 “Out-of-bounds Write” (по классификации ошибок Common Weakness Enumeration).
- В 2019 году вредоносные объекты были заблокированы на 46,6% компьютеров АСУ. Во втором полугодии 2019 года этот показатель составил 39,2% – на 2 п.п. меньше, чем в предыдущем полугодии.
  - Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, различен в разных индустриях, например, автоматизация зданий (38%), автомобилестроение (37,6%), энергетика (36,6%), нефть и газ (36,3%) и инжиниринг и интеграторы АСУ (32,7%).
  - Состав первой пятерки стран в рейтинге по проценту компьютеров АСУ, на которых была предотвращена вредоносная активность, остается неизменным вот уже полтора года. Во втором полугодии 2019 в TOP 5 вошли Вьетнам (65,5%), Алжир (64,6%), Тунис (58,8%), Марокко (56,6%), и Египет (55,3%).
  - В число наиболее благополучных стран во втором полугодии 2019 вошли Ирландия (7,3%), Швеция (10,3%), Дания (11,6%), Нидерланды (12%) и Гонконг (13%).
  - Наиболее значительное увеличение процента компьютеров АСУ, на которых была предотвращена вредоносная активность, было отмечено в Сингапуре (на 9,2 п.п.), Белоруссии (на 7,6 п.п.) и в ЮАР (на 6,2 п.п.). Отметим, что в течение трех предыдущих полугодий в Сингапуре этот показатель снижался.
  - В России в течение второго полугодия 2019 года хотя бы один раз вредоносные объекты были заблокированы на 43,1% компьютеров АСУ, что на 1,7 п.п. меньше, чем в первом полугодии 2019 года (44,8%).
  - Во всех регионах мира основным источником угроз по-прежнему является интернет. Однако в Северной Европе (6,8%), Западной Европе (10%) и в Северной Америке (12,6%) процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, значительно ниже, чем в Восточной Европе (17,2%), на Ближнем Востоке (21,2%), в Латинской Америке (24,2%), Центральной Азии (30,8%), Африке (34,6%) и Юго-Восточной Азии (35,8%).

- В 2019 году мы наблюдали такую же сезонную динамику, как и в предыдущие годы: наибольшие показатели были отмечены весной и осенью. Поскольку абсолютное большинство вредоносных операций характеризуется высокой степенью автоматизации, мы полагаем, что такая динамика отражает сезонные изменения в присутствии сотрудников на рабочих местах и, таким образом, демонстрирует влияние человеческого фактора на кибербезопасность промышленных компаний.

- Многие типы вредоносного ПО, не будучи заблокированными на компьютерах АСУ, представляли бы серьёзную опасность для работы предприятия. Среди всех этих угроз воздействие вредоносных программ-вымогателей может быть наиболее пагубным. В 2019 году программы-вымогатели были заблокированы на 1,0% компьютеров АСУ. Во втором полугодии 2019 этот показатель составил 0,61%, в первом полугодии по уточненным данным – 0,76%.
  - Наибольший процент компьютеров АСУ, на которых были заблокированы программы-вымогатели в 2019 году, был отмечен в Юго-Восточной Азии (2,09%), самый низкий показатель по итогам года – в Северной Европе (0,19%).
  - На первом месте в рейтинге стран – жертв вредоносных программ-вымогателей в 2019 году была Бангладеш (3,13%). За ней следуют Алжир, Вьетнам, Индонезия, Египет, Китай, Чили, Белоруссия, Индия, Казахстан, Украина, Малайзия, Тунис, Италия и Тайланд.
  - Печально известная программа-вымогатель WannaCry всё ещё жива. Среди всех пользователей продуктов «Лаборатории Касперского», подвергшихся атакам троянских программ-вымогателей в 2019 году, более 23% были атакованы именно WannaCry. При этом процент атакованных этой программой компьютеров АСУ ещё выше – более 35%.
  - В некоторых случаях атаки вредносных программ-вымогателей могут стать ещё опаснее. Создатели вредоносного ПО GandCrab распространяли его через платфортму RaaS (Ransomware-as-a-Service). Однако летом 2019 года вредоносный «сервис» был закрыт. Это сделало шифровальщик ещё более опасным, поскольку зашифрованные последней версией GandCrab данные стало невозможно расшифровать – ни заплатив злоумышленникам, ни каким-либо иным способом (в последней версии GandCrab применены криптостойкие алгоритмы шифрования). В конце 2019 года мы всё ещё обнаруживали – и предотвращали – атаки вредоносного ПО GandCrab на компьютеры систем промышленной автоматизации.

Уязвимости, обнаруженные в 2019 году

Уязвимости в различных компонентах АСУ ТП

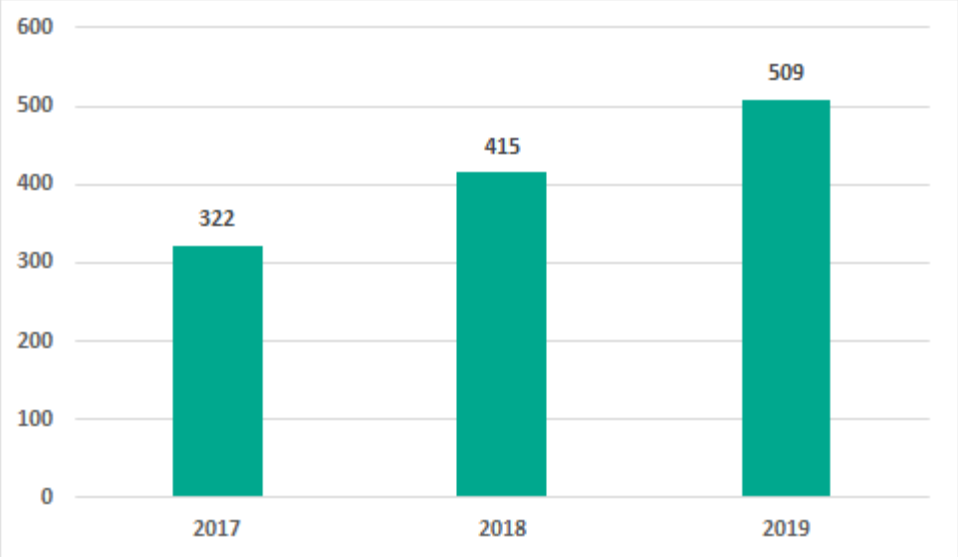
Анализ уязвимостей проводился на основе уведомлений производителей, общедоступной информации из открытых баз уязвимостей (US ICS-CERT, CVE, Siemens Product CERT), а также результатов собственных исследований Kaspersky ICS CERT.

В качестве данных для статистики использовалась информация об уязвимостях, опубликованная на сайте US ICS-CERT в 2019 году.

Количество обнаруженных уязвимостей

В 2019 году на сайте US ICS-CERT было опубликовано 509 уязвимостей, выявленных в различных компонентах АСУ ТП. Это число превышает аналогичный показатель за 2017 и 2018 год, что, на наш взгляд, связано с повышением внимания к безопасности решений промышленной автоматизации со стороны исследователей безопасности и не говорит о снижении качества разработки этих продуктов.

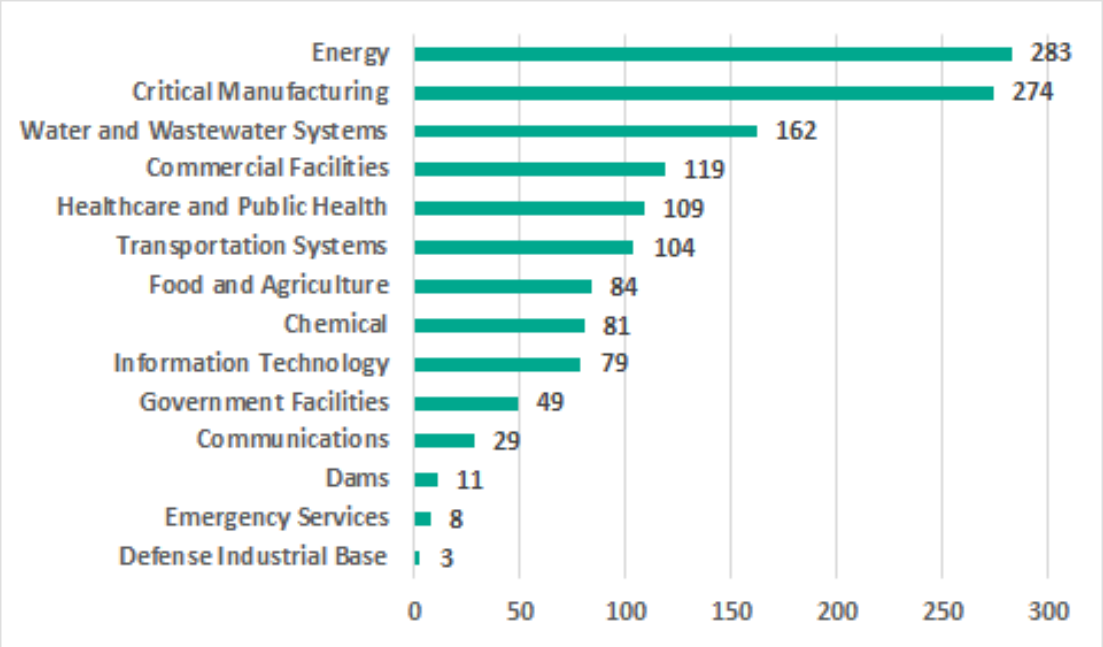
Количество уязвимостей в разных компонентах АСУ ТП, опубликованных на сайте US ICS-CERT



Анализ по отраслям

Большая часть уязвимостей затрагивает автоматизированные системы управления в энергетике (283), технологическими процессами различных производственных предприятий, относимых в США к критической инфраструктуре (274) и водоснабжением и канализацией (162).

Количество уязвимых продуктов, используемых в различных отраслях (по классификации US ICS-CERT). Уязвимости, опубликованные в 2019 году



Степень риска выявленных уязвимостей

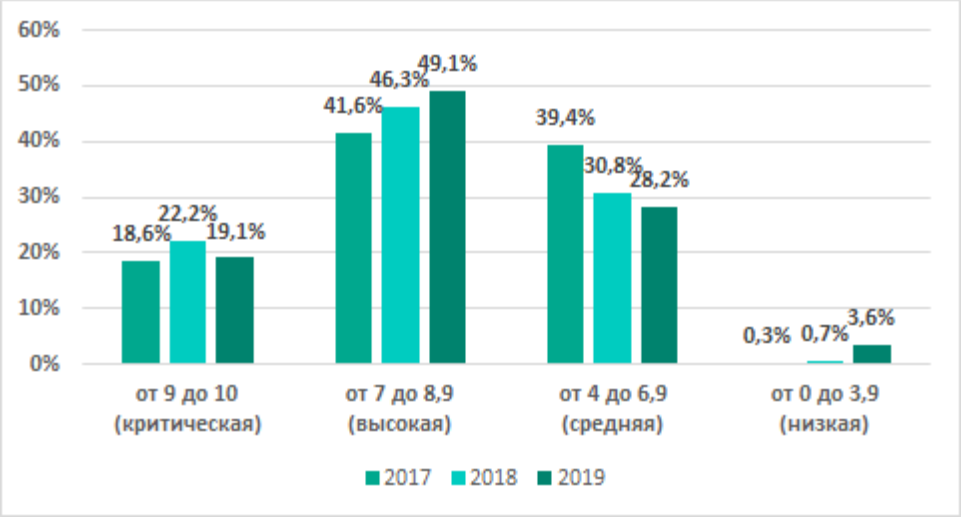
Больше половины выявленных в системах АСУ ТП уязвимостей (358, в прошлом году — 284) получили оценку более 7 баллов по шкале CVSS версии 3.0, что соответствует высокой и критической степени риска. Две уязвимости были исключены из оценки степени риска, так как им соответствует множество CVE, и они не имеют отдельного CWE ID.

Таблица 1. Распределение опубликованных уязвимостей по 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	97	249	143	18

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), 2019 год в сравнении с 2018 и 2017 годами



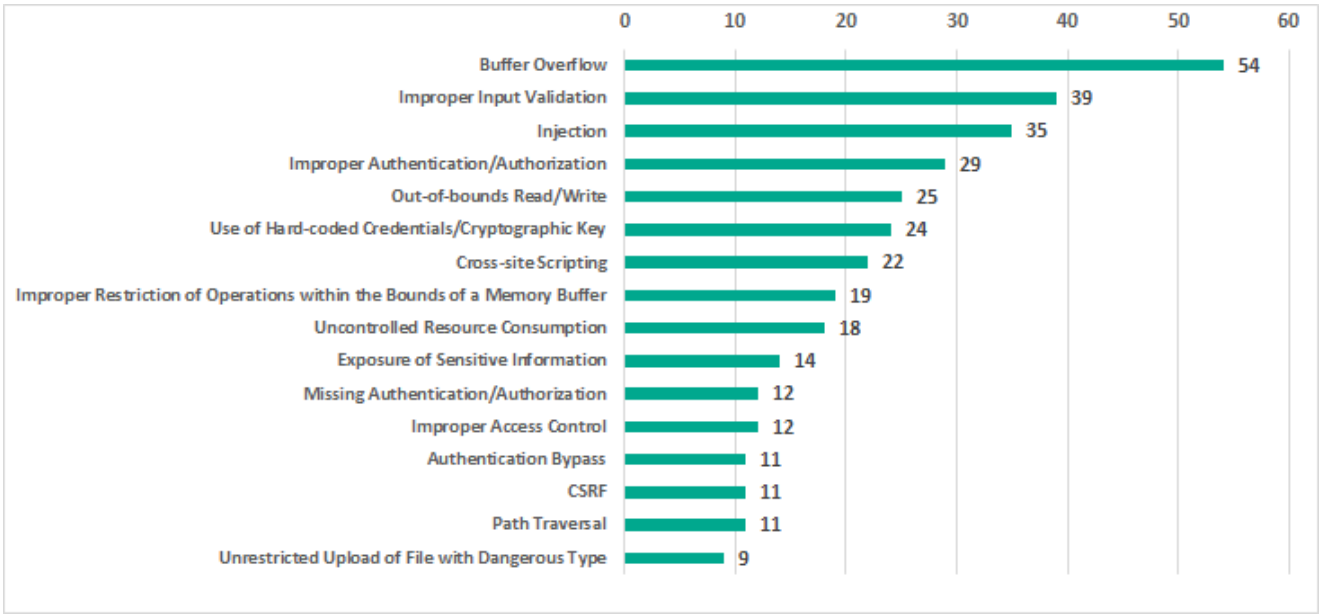
Наивысшая оценка в 10 баллов была присвоена уязвимостям, обнаруженным в следующих продуктах:

- Alaris Gateway Workstation
- Proton/Enterprise Building Management System
- Spectrum Power 4.7
- CODESYS V3 web server
- Relion 670 Series
- FlexAir
- RSLinx Classic
- WibuKey Digital Rights Management (DRM)
- PR100088 Modbus gateway

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

Как и в 2018 году, среди наиболее распространенных типов уязвимостей – переполнение буфера (Stack-based Buffer Overflow, Heap-based Buffer Overflow, Classic Buffer Overflow), некорректная проверка входных данных (Improper Input Validation) и инъекции (SQL Injection, Code Injection, Command Injection).

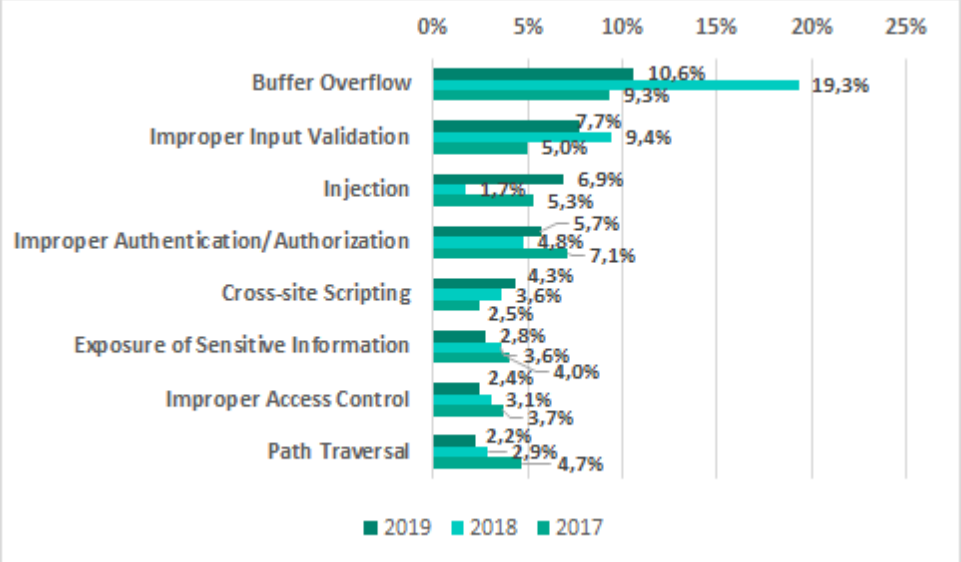


Наиболее распространенные типы уязвимостей. Уязвимости, опубликованные в 2019 году

17,3% всех опубликованных уязвимостей связанны 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).

15,5% опубликованных уязвимостей являются веб-уязвимостями (Injection, Path traversal, Cross-site request forgery (CSRF), Cross-site scripting). По сравнению с 2018 годом их доля выросла на 5,5 п.п.

Процент уязвимостей различных типов от общего числа уязвимостей, 2019 год в сравнении с 2018 и 2017 годами



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:

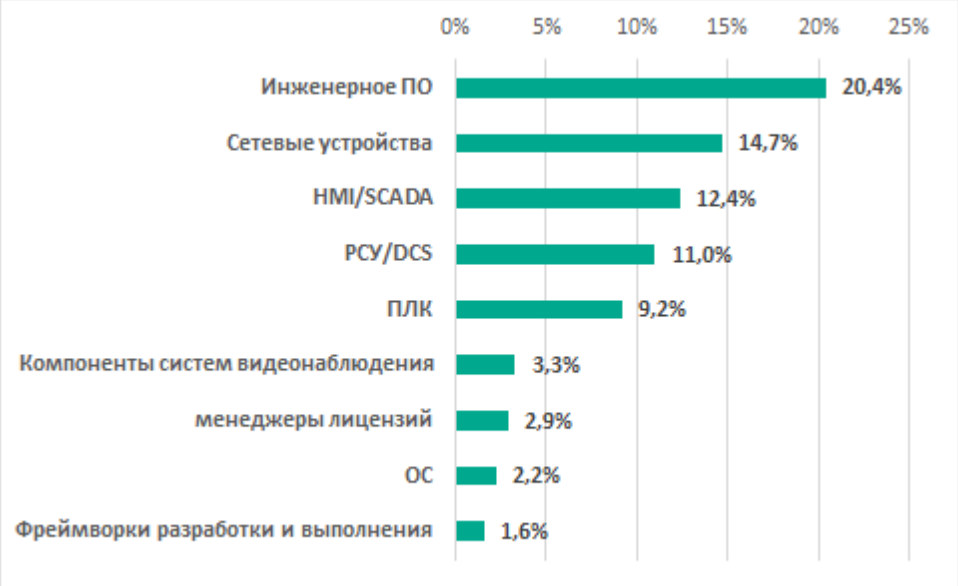
- Большинство уязвимостей (420) могут эксплуатироваться удаленно без аутентификации,
- Эксплуатация большинства уязвимостей (480) не требует от злоумышленника специальных знаний и высокого уровня навыков.
- Для 23 уязвимостей опубликованы эксплойты, что повышает риск их злонамеренного использования.

Уязвимые компоненты АСУ ТП

Наибольшее количество уязвимостей было выявлено в:

- инженерном ПО (103, 20%),
- сетевых устройствах промышленного назначения (78, 15%),
- SCADA/HMI-компонентах (63, 12%),
- РСУ (56, 11%)
- ПЛК (47, 9%).

Процент уязвимостей в различных компонентах АСУ ТП от общего числа уязвимостей. Уязвимости, опубликованные в 2019 году



Проблемы безопасности систем промышленной автоматизации зачастую связаны с уязвимостями в общих программных компонентах, которые используются вендорами в составе множества их решений. Среди таких компонентов – операционные системы (ОС), менеджеры лицензий, модули, реализующие различные механизмы защиты, а также фреймворки для разработки и выполнения программ автоматизированного управления технологическим процессом.

Уязвимости в операционных системах

Одним из основных компонентов любой системы автоматизации является ОС. Так как одна и та же ОС может использоваться производителями в составе различных продуктов, обнаружение уязвимостей в ОС чаще всего затрагивает целые линейки решений.

Так, в связи с проблемами безопасности в ОС RUGGEDCOM ROX II в 2019 году оказались уязвимыми все промышленные устройства Siemens RUGGEDCOM под управлением этой ОС.

Кроме того, множественные уязвимости, обнаруженные в ОС реального времени VxWorks, затронули решения вендоров Rockwell Automation, Schneider Electric, Xerox, Dräger.

Еще одним примером масштабного влияния уязвимостей ОС на безопасность решений является обнаружение уязвимости TCP SACK Panic в ядре Linux. Эта уязвимость затронула множество продуктов компании Siemens.

Уязвимости в менеджерах лицензий

В 2019 году исследователи безопасности сообщили об уязвимостях сразу в нескольких менеджерах лицензий:

- Yokogawa License Manager Service
- Schneider Electric Floating License Manager
- RC-LicenseManager
- SafeNet Sentinel LDK License Manager
- FlexNet Publisher

За счет использования таких компонентов в составе различных решений уязвимости в них могут затрагивать сразу несколько промышленных продуктов. Так, распределенная система управления CENTUM VP и система автоматической противоаварийной защиты ProSafe-RS производства компании Yokogawa оказались подвержены уязвимостям, найденным в Yokogawa License Manager Service.

Аналогично уязвимости в Floating License Manager затронули сразу несколько решений Schneider Electric, включая инженерное ПО EcoStruxure Control Expert, распределенную систему управления EcoStruxure Hybrid Distributed Control System (также известную как Plant Struxure PES), Power SCADA Expert и другие. Также уязвимости в этом менеджере лицензий затронули продукты Vijeo Citect и Citect SCADA производства AVEVA, являющейся дочерней компанией Schneider Electric. Отдельно стоит отметить, что уязвимости в Floating License Manager в свою очередь связаны со множественными уязвимостями в стороннем ПО Flexera FlexNet Publisher.

Кроме того, продукты сразу нескольких промышленных вендоров, включая Siemens, Phoenix Contact, Sprecher Automation и COPA-DATA, оказались подвержены уязвимостям в техническом средстве защиты авторских прав WibuKey Digital Rights Management (DRM).

Уязвимости в фреймворках разработки и выполнения программ

Отдельное внимание стоит уделить безопасности фреймворков, используемых вендорами для разработки и выполнения программ автоматизированного управления технологическим процессом. В 2019 году уязвимости были обнаружены сразу в нескольких компонентах программного комплекса промышленной автоматизации CoDeSyS, включая веб-сервер, коммуникационный сервер и OPC UA сервер.

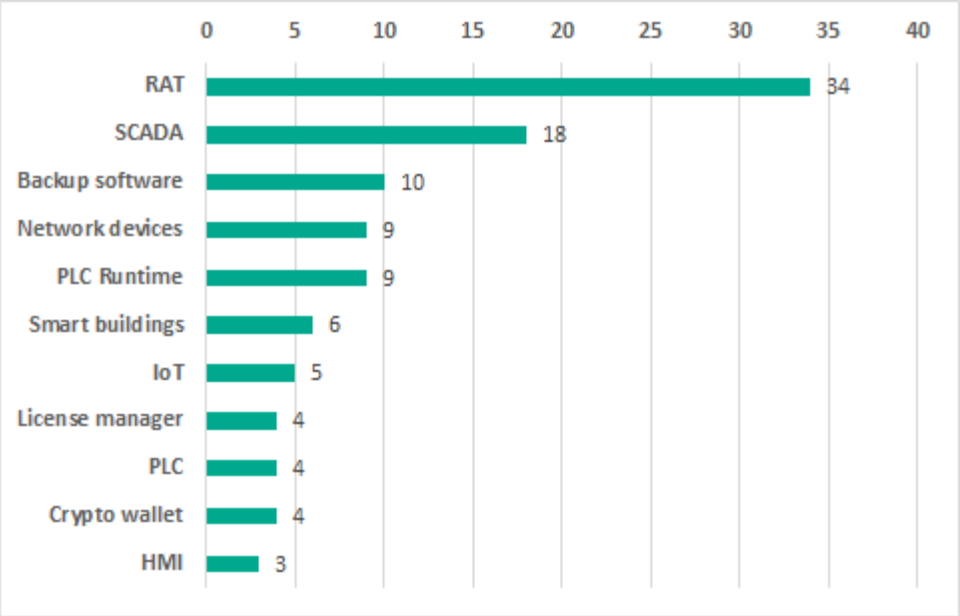
Уязвимости, обнаруженные Kaspersky ICS CERT

В 2019 году эксперты Kaspersky ICS CERT продолжили исследования проблем безопасности сторонних программных и программно-аппаратных решений, широко применяемых в системах промышленной автоматизации, решениях класса “интернет вещей” и “промышленный интернет вещей” и так далее. Особе внимание было уделено кроссплатформенным решениям и продуктам с открытым исходным кодом. Такие решения или их компоненты широко распространены как отдельные или как заимствования в составе коммерческих решений.

Количество найденных уязвимостей

В 2019 году Kaspersky ICS CERT было выявлено 103 уязвимости в промышленных системах, системах IIoT/IoT и других типах решений.

Распределение уязвимостей, найденных Kaspersky ICS CERT в 2019 году, по типам исследованных компонентов



Обо всех обнаруженных уязвимостях мы незамедлительно проинформировали производителей соответствующих продуктов.

Возможные последствия эксплуатации найденных уязвимостей

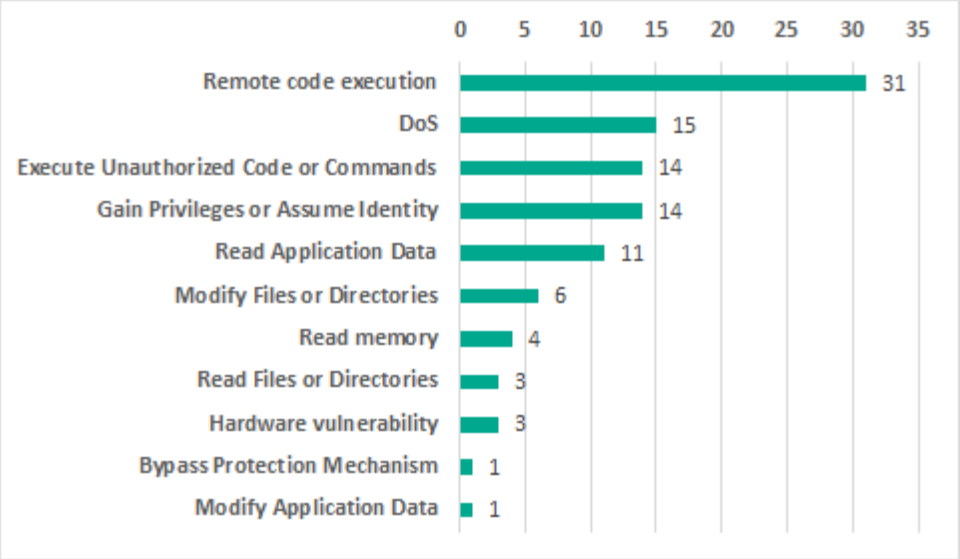
В этом году мы разделили уязвимости, которые позволяют выполнить код, на два типа:

1. Execute Unauthorized Code or Commands – выполнение кода в контексте приложения/среды выполнения. Пример: XSS, SQLi, XXE, ReadObject.
2. Remote code execution (RCE) – выполнение произвольного машинного кода. Пример: выполнение системных команд/команд операционной системы и машинного кода.

Также следует отметить, что RCE может приводить к различным последствиям – произвольному чтению и модификации папок, файлов, отказам в обслуживании и так далее.

В статистике ниже RCE и Execute Unauthorized Code or Commands разделены на две разные категории.

Распределение уязвимостей, найденных Kaspersky ICS CERT в 2019 году, по возможным последствиям эксплуатации



Эксплуатация 30,1% выявленных уязвимостей может привести к удаленному выполнению произвольного кода, 14,6% – к DoS. Эксплуатация 13,6% уязвимостей позволяет повышать привилегии или же перехватывать сессии. Также в статистике фигурируют три уязвимости, относящиеся к аппаратному обеспечению. Эксплуатация таких уязвимостей позволяет получить доступ к данным из-за недостаточной защиты аппаратной платформы или элементной базы исследуемого решения.

Результаты, которые мы считаем наиболее важными

ПО / решение	Количество обнаруженных уязвимостей	Возможные последствия эксплуатации	Результат
RAT на основе VNC протокола	34	Уязвимости различного уровня критичности, некоторые позволяют выполнить произвольный код как на серверной, так и на клиентской части	Уязвимости устранены производителем. Опубликована статья
Менеджеры лицензий	4	Уязвимости различного уровня критичности, позволяют потенциальному злоумышленнику развивать атаку на внутреннюю инфраструктуру	Уязвимости устранены производителями
Популярная среда выполнения в ПЛК	9	Выявленные уязвимости являются наиболее деструктивными для технологического процесса, ввиду того, что эксплуатация таких уязвимостей сложно детектируется. Уязвимости позволяют злоумышленнику скрытно вносить изменения в технологический процесс, как следствие, атака может иметь высокую персистентность и тяжёлые последствия с возможным физическим эффектом	Информация об уязвимостях направлена производителю

Не промышленные решения			
Устройства из инфраструктуры умных городов	6	Выявленные уязвимости позволяют: 1. подменять передаваемые данные; 2. получать доступ к защищаемой информации; 3. эксплуатировать ошибки работы с памятью.	Уязвимости устранены производителем
Аппаратный кошелек для хранения криптовалюты	4 (в программном и аппаратном обеспечении)	Выявленные уязвимости позволяют атакующему получить полный контроль над кошельком и проводить любые операции с ним	Уязвимости устранены производителем

Оценка опасности обнаруженных уязвимостей

Для оценки опасности обнаруженных уязвимостей использовалась система градации уязвимостей, основанная на метрике 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 ICS CERT уязвимостей, для которых в 2019 году были опубликованы CVE, по шкале CVSS v.3 имеют вес не менее 7.0 и относятся к группе наиболее критичных. При этом 10 уязвимостей получили по шкале CVSS v.3 максимальную оценку критичности в 10 баллов. В их числе – уязвимости в программных компонентах, общих для многих продуктов – кроссплатформенных решениях, которые работают по протоколу VNC.

Причина возникновения уязвимостей

Все существующие уязвимости возникают из-за ошибок, допущенных при разработке программного обеспечения, включая архитектуру решения. Существует классификация таких ошибок – Common Weakness Enumeration. По результатам исследований Kaspersky ICS CERT в 2019 году самой популярной стала ошибка под номером CWE-787 “Out-of-bounds Write”, которая была обнаружена при исследовании RAT решений. Такой тип ошибки является необходимым, но не достаточным условием для эксплуатации уязвимости типа Remote Code Execution (удаленное выполнение произвольного кода).

Количество опубликованных CVE

В 2019 году на основании исследований, проведенных Kaspersky ICS CERT, было опубликовано 43 CVE.

APT-атаки на промышленные компании в 2019 году

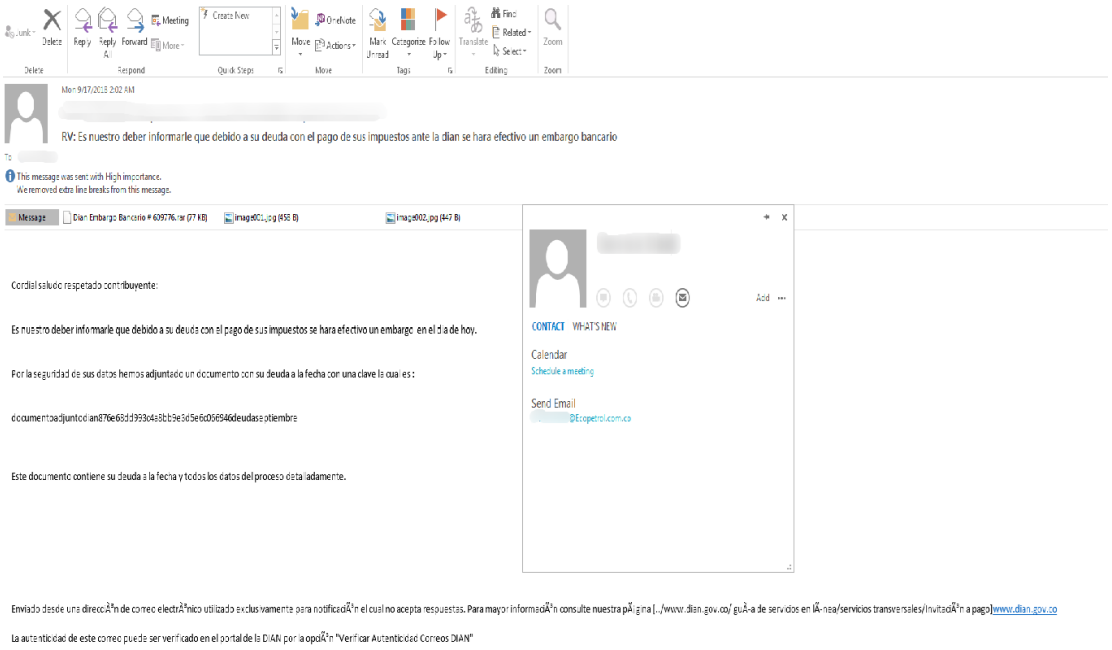
Атаки на компании в Колумбии

В феврале 2019 исследователи из 360 Threat Intelligence Center сообщили о продолжающихся целенаправленных атаках на колумбийские правительственные учреждения и крупные компании в финансовом секторе, нефтяной промышленности, обрабатывающей промышленности и других секторах. Атаки были осуществлены группировкой APT-C-36 (они же Blind Eagle). Как полагают исследователи, в нее входят злоумышленники из Южной Америки.

Атакующие нацелены на платформу Windows. Они доставляют вредоносное ПО, используя фишинговые письма, содержащие защищенное паролем вложение RAR, что может позволить избежать обнаружения на шлюзе электронной почты. Пароль для дешифровки указан в теле письма.

Внутри вложения находится документ с расширением DOC и с макросом MHTML, используемый для установки бекдора Imminent, обладающего широкими возможностями, и закрепления в целевой сети. Исследователи полагают, что злоумышленники заинтересованы в разведданных стратегического уровня, а также могут пытаться украсть бизнес-аналитику и интеллектуальную собственность.

Фишинговое письмо для Ecopetrol (Источник: 360 Threat Intelligence Center)



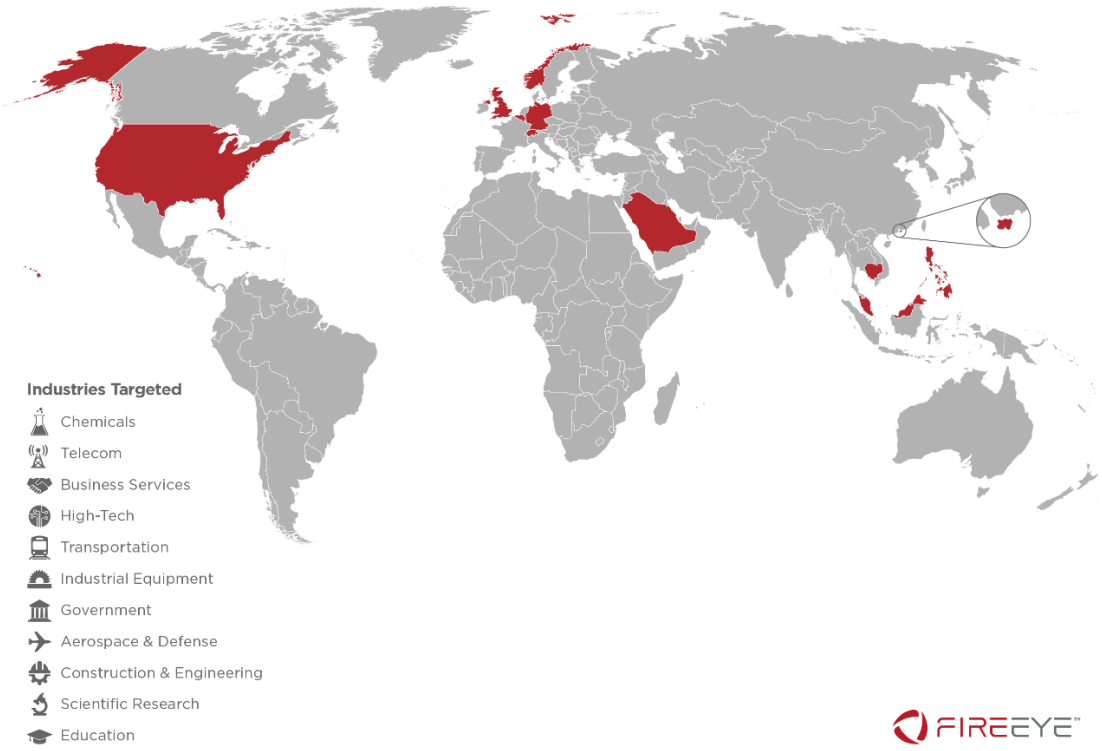
Атаки группировки APT40

В марте 2019 компания FireEye сообщила об атаках APT40, которая считается исследователями китайской группировкой, спонсируемой государством. Эта группировка проводила операции в поддержку усилий Китая по модернизации военно-морского флота, по крайней мере, с 2013 года. Эта китайская группа, осуществляющая кибершпионаж, также известна под именами TEMP.Periscope, TEMP.Jumper и Leviathan.

APT40 ориентирована на машиностроение, транспорт и оборонную промышленность, особенно там, где эти отрасли связаны с морской промышленностью. Исследователи

FireEye также наблюдали атаки на цели в странах, стратегически важных для Инициативы «Один пояс и один путь», в том числе на Камбоджу, Бельгию, Германию, Гонконг, Филиппины, Малайзию, Норвегию, Саудовскую Аравию, Швейцарию, Соединенные Штаты и Соединенное Королевство.

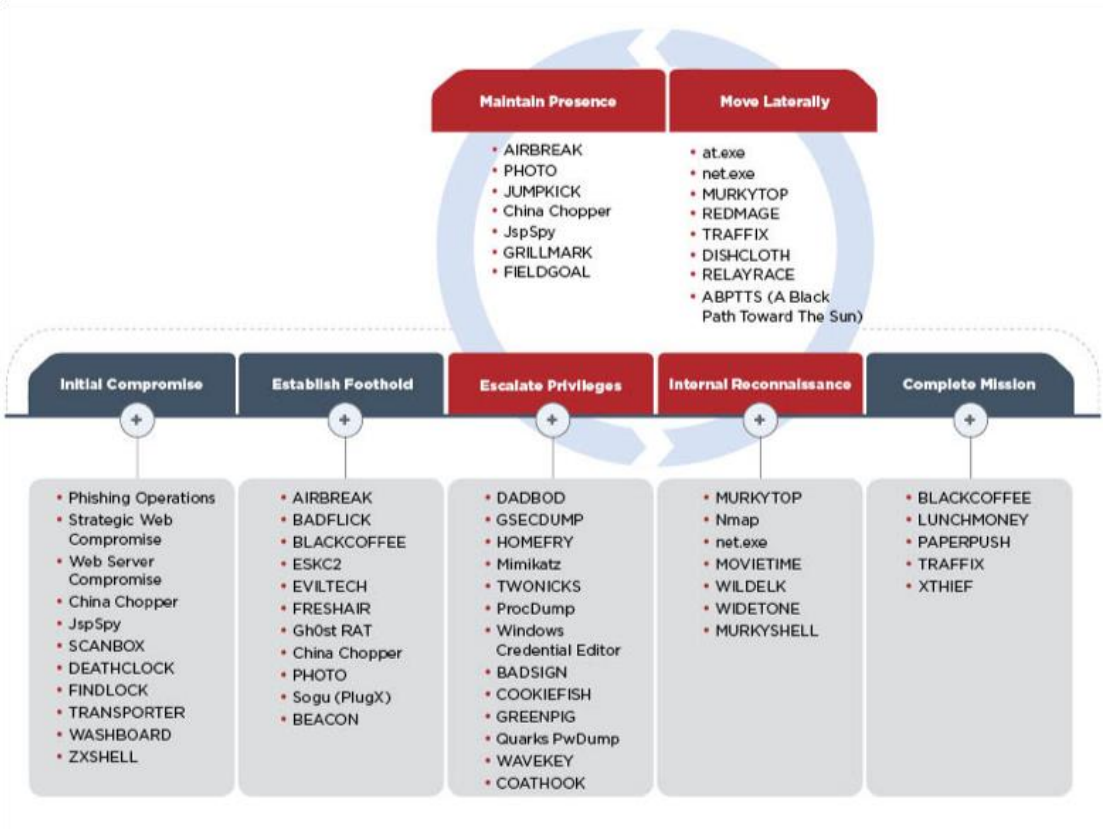
Страны и атакуемые индустрии (Источник: FireEye)



APT40 использует различные методы для первоначальной компрометации. В их числе эксплуатация веб-серверов жертв, фишинговые кампании с уязвимыми документами, устанавливающими как общедоступные, так и кастомные бэкдоры. В фишинговых письмах встречались не только вредонсоные вложения, но и ссылки на Google Drive. В некоторых случаях группировка использовала вредоносные исполняемые файлы, подписанные сертификатом, для обхода детектирования. Из арсенала группировки также стоить отметить использование веб-шеллов (вредоносные скрипты, которые позволяют управлять зараженными машинами извне сети) для первоначального закрепления в организации. Это обеспечивает атакующим более продолжительный доступ и дает возможность заново инфицировать системы.

APT40 часто нацеливается на учетные данные VPN и удаленного рабочего стола, чтобы закрепиться в организации. Эта методология очень удобна атакующим, так как после получения этих учетных данных они могут не полагаться на вредоносное ПО для продолжения атаки.

Жизненный цикл атак APT40 (Источник: FireEye)



Hexane/OilRig/APT34

1 августа 2019 года компания Dragos опубликовала обзор атак под названием «Oil and Gas Threat Perspective Summary», в котором упоминается некая новая группировка, получившая имя «Hexane». Согласно отчету, Hexane ориентирована на нефтегазовый сектор и телекоммуникации в Африке, на Ближнем Востоке и в Юго-Западной Азии. Dragos утверждает, что идентифицировала группу в мае 2019 года, связав ее с предположительно иранскими группировками OilRig и CHRYSENE. Деятельность Hexane, по-видимому, началась примерно в сентябре 2018 года, вторая волна активности – в мае 2019 года.

Хотя никаких индикаторов компрометации опубликовано не было, некоторые исследователи в ответ на сообщение Dragos о новой группировке поделились хэшами в ветке Twitter. Анализ «Лаборатории Касперского» также выявил некоторое сходство TTP новой волны атак с TTP группировки OilRig.

Во всех случаях артефакты, использованные в атаках, относительно просты. Постоянное развитие дропперов, по-видимому, указывает на период проб и ошибок, когда злоумышленники проверяли, как лучше всего избежать детектирования.

TTP, которые «Лаборатория Касперского» может связать с предшествующей появлению Hexane деятельностью OilRig, включает:

- упомянутый процесс проб и ошибок;
- применение простых документов-дропперов с использованием макросов, распространяемых посредством фишинговых писем;
- использование DNS для эксфильтрации на серверы управления.

Утечки в Telegram от Lab Dookhtegan и GreenLeakers исходного кода инструментария атакующих из Ирана позволяют предположить, как могла появиться группа Hexane. Из-за разоблачения и утечек группировка OilRig, возможно, просто изменила свой набор инструментов и продолжила работать как обычно: этим бы и объяснялась быстрая и гибкая реакция на утечки от этой группы. Или, возможно, некоторые из TTP OilRig были переняты новой группой, которая имеет схожие с OilRig интересы.

Позже в августе Secureworks выпустили отчет, в котором описали инструментарий той же группы, которой дали название Lyceum. В отчете был описан фишинговый документ, RAT первого этапа и Powershell скрипты, используемые в атаках.

IBM X-Force предполагает, что группировка APT34 (OilRig и Crambus) стоит за атакой на энергетические объекты на Ближнем Востоке с использованием вредоносной программы для уничтожения данных под названием «ZeroCleare». В отчете IBM говорится, что OilRig, а также по крайней мере еще одна группа, вероятнее всего, также из Ирана, использовали взломанные VPN аккаунты для доступа к машинам по крайней мере в одном случае.

В декабре в Бахрейнской национальной нефтяной компании Bapco произошла атака вайпера, который получил название Dustman. Национальное управление кибербезопасности Саудовской Аравии (National Cybersecurity Authority, NCA) опубликовало соответствующее предупреждение безопасности. По результатам анализа вредоносного ПО было установлено, что Dustman представляет собой обновленную и улучшенную версию вайпера ZeroCleare.

APT33

Атаки еще одной иранской группировки APT33 (NewsBeef, Charming Kitten и Elfin) нацелены на нефтяную и авиационную отрасли. Последние находки TrendMicro, свидетельствуют об использовании группировкой около дюжины серверов управления для таргетированных атак против организаций на Ближнем Востоке, в США и Азии.

Группа использует несколько уровней различных хостов для обфускации своих настоящих серверов C&C. Используемое атакующими вредоносное ПО является довольно простым и имеет ограниченные возможности, включая загрузку и запуск дополнительного вредоносного ПО.

В 2018 году эта группировка атаковала десятки тысяч компаний, пытаясь подобрать пароли к учетным записям пользователей с помощью перебора нескольких наиболее распространенных паролей (password-spraying attacks). По сообщениям Microsoft к концу 2019 года APT33 сосредоточила свою активность примерно на 2000 организациях в месяц, увеличив при этом количество учетных записей, атакованных в каждой из этих организаций, в среднем почти в десять раз. Около половины из 25 основных целей, ранжированных по количеству атакуемых учетных записей, были производителями, поставщиками или компаниями, производящими техническое обслуживание оборудования ICS.

Microsoft заявляет, что с середины октября APT33 нацелена на десятки компаний-производителей промышленного оборудования и программного обеспечения. Остается неясной мотивация хакеров и какие промышленные системы управления они фактически скомпрометировали. В Microsoft полагают, что группа стремится закрепиться в атакуемых организациях, чтобы впоследствии проводить кибератаки с физически разрушительными последствиями.

Symantec сообщила, что за последние три года эта группировка атаковала по крайней мере 50 организаций в Саудовской Аравии, в США и в других странах. Эксперты Symantec полагают, что некоторые из организаций США, возможно, стали мишенью для группы в ходе проведения атак по цепочке поставок. Так, например, в одном случае крупная американская компания подвергалась атаке в том же месяце, когда была скомпрометирована ближневосточная компания, совладельцем которой являлась американская компания.

В ходе волны атак в феврале 2019 года APT33 попыталась использовать известную уязвимость (CVE-2018-20250) в WinRAR. Эксплойт был использован против организации в химическом секторе в Саудовской Аравии. Два пользователя в организации получили файл с именем «JobDetails.rar», который скорее всего, распространялся в фишинговом письме. Также было отмечено, что APT33 использует как кастомные бэкдоры, так и множество общедоступных, таких как Remcos, DarkComet NanoCore и другие.

Forbes и WSJ рассказали об атаках иранских хакеров на государственные учреждения и критическую инфрастуктуру в Бахрейне и отметили параллель с атаками Shamoon 2012 года. Также были приведены сведения, что в июле хакеры отключили несколько систем в Управлении электроэнергетики и водоснабжения в Бахрейне. Как считают власти, это была репетиция или демонстрация уязвимости защищенных систем управления, что в случае полной компрометации может иметь очень большие последствия.

Операция Wocao

Исследователи Fox-IT сообщили об активности хакерской группы, которой, по их мнению, было поручено похищать информацию для шпионских целей. Эта активность получила название «Операция Wocao». Ее TTP совпадает с TTP китайской группировки, называемой в индустрии APT20. Жертвы были выявлены в десяти странах – в государственных учреждениях, среди поставщиков услуг и в самых разных отраслях, включая энергетику, транспорт, здравоохранение и высокотехнологичных производств.

В нескольких случаях начальной точкой доступа в сеть жертвы становился уязвимый веб-сервер, часто с установленным JBoss. Было замечено, что такие уязвимые серверы часто уже были скомпрометированы ранее другими группами, которые установили на серверы свои веб-шеллы.

В операции Wacao фактически используются чужие веб-шеллы для разведки и начального распространения. После этого группа загружает один из своих веб-шеллов на веб-сервер. Доступ через загруженный веб-шелл используется в качестве запасного в случае потери другого, основного, постоянного доступа – например, если украденные злоумышленникам учетные данные VPN были изменены.

В одном случае VPN-доступ к сети жертвы был защищен двухфакторной аутентификацией (2FA) с использование ПО RSA SecurID. Группа обошла реализацию 2FA с помощью техники, которую, как предполагает Fox-IT, была разработана самой группировкой.

Для генерирования пароля (токен-кода) двухфакторной аутентификации используется запатентованный RSA алгоритм. Каждому экземпляру токена соответствует начальный вектор генерации (seed). Новый токен-код генерируется раз в минуту, и его значение определяется только seed и временем генерации.

В аппаратной реализации RSA SecurID начальный вектор генерации надежно защищен и может быть получен только кражей физического токена. Но, как обнаружили Fox-IT, программный токен RSA SecurID использует уникальный ключ, сгенерированный для каждого экземпляра инсталляции ПО (и привязанный к уникальным параметрам системы), только в процессе валидации импорта токена, а в качестве начального вектора генерации используется уникальное значение, никак к системе не привязанное.

Как выяснили Fox-IT, это позволяет, пропатчив всего лишь одну инструкцию кода ПО RSA SecurID, использовать ПО для генерирования токен-кодов, валидных для любой системы, с которой злоумышленникам удалось украсть установленный программный токен.

Fox-IT полагает, что атакующие, вероятно, могли сначала украсть у жертвы программный токен, затем использовать пропатченное у себя ПО RSA SecurID для генерации действующих токенов двухфакторной аутентификации, пригодных для подключения к VPN.

APT41/Winnti

В августе 2019 компания FireEye описала активность китайской группы, работающей с 2012 года и занимающейся стратегическим шпионажем в областях, связанных с пятилетним планом экономического развития Китая. В числе атакованных организаций телекоммуникации, здравоохранение, производители полупроводников, продвинутого аппаратного обеспечения компьютеров, батарей, электромобилей и другие. Эти организации располагаются в 14 странах, включая Францию, Индию, Италию, Японию, Южную Корею, Великобританию, США.

Характерной особенностью данной группы, которая была названа APT41, является сочетание атак на различные организации с целью кибершпионажа и финансово-мотивированных атак на игровую индустрию, в которых группа манипулировала виртуальной игровой валютой, а также пыталась реализовать атаки шифровальщиков.

Группа получала доступ к Windows и Linux машинам внутри сети организаций и на нужных машинах крала исходный код и цифровые сертификаты, которые потом использовала для подписи своего вредоносного ПО.

APT41 также известна тем, что внедряла свой вредоносный код в легитимные файлы игровых компаний. В итоге получившиеся вредоносные файлы были подписаны легитимным сертификатом компании. В дальнейшем эти файлы распространялись в другие организации, то есть была реализована атака на цепочку поставок.

Из интересных особенностей TTP группы можно отметить высокую степень таргетированности атак группировки, так, перед развертыванием некоторого используемого ими next-stage вредоносного ПО могут выполняться проверки уникального системного идентификатора на конечных машинах. Также следует отметить ограниченное использование руткитов и MBR буткитов, что является очень редким для китайских APT группировок.

Анализ времени суток, в которое проводились оба типа атак – атаки кибершпионажа на компании стратегических отраслей и коммерческие атаки на игровые компании –

показал, что участники группы осуществляют второй тип атак в свободное время, вероятно, для личной выгоды. Возможно, они находятся под протекцией властей.

Согласно опубликованным ранее отчетам других компаний APT41 частично совпадает по своей активности с Barium и Winnti. Также FireEye атрибутирует к APT41 атаки CCleaner, ShadowPad и ShadowHammer.

Исследователи в ESET считают, что описанная FireEye группа APT41, стоящая за громкими атаками в цепочке поставок на игровую индустрию и на промышленные компании, – это Winnti. Они выявили, что группа Winnti продолжает обновлять свой арсенал и использует новый модульный бэкдор Windows под именем PortReuse, который, в частности, был использован для заражения серверов известного азиатского производителя мобильного оборудования и программного обеспечения. Также ESET было выявлено вредоносное ПО третьего этапа в одной атаке Winnti на игровые компании – им оказалось кастомизированная версия криптомайнера XMRig.

Несколько крупных немецких промышленных фирм, включая BASF, Siemens и Henkel, объявили в июле, что они стали жертвами спонсируемой государством хакерской группы из Китая. Также в апреле об обнаружении вторжения заявила компания Bayer. Все эти атаки, возможно, принадлежали к разным под-группам, но были объединены фактом использования бэкдора Winnti.

Атаки на аэрокосмическую отрасль

Европейский аэрокосмический гигант Airbus подвергся серии атак предположительно китайских хакеров с целью кибершпионажа. В январе 2019 был выпущен пресс-релиз, в котором сообщалось, что компания обнаружила вторжение в свои системы, связанные с бизнесом коммерческих самолетов, но инцидент не повлиял на ее коммерческую деятельность. Некоторые источники в компании также заявляли о целой серии атак в течение года.

Также сообщалось об атаках хакеров на британского производителя двигателей Rolls-Royce и французского консультанта по технологиям и поставщика Expleo, а также на двух других французских подрядчиков, работающих на Airbus. Как утверждают источники, в атаках на подрядчиков был получен доступ к VPN, который связывал компании с Airbus.

В октябре компания Crowdstrike выпустила отчет (позже он был удален с сайта компании), который разоблачал одну из самых амбициозных хакерских операций Китая. Скоординированная многолетняя хакерская кампания была направлена на то, чтобы помочь китайскому государственному авиационно-космическому производителю Comac построить собственный авиалайнер C919. Ее конечная цель, утверждает Crowdstrike, заключалась в хищении интеллектуальной собственности, необходимой для производства всех компонентов C919 внутри Китая. По информации Crowdstrike, Министерство государственной безопасности (MSS) поручило эту задачу Бюро в Цзянсу (MSS JSSD). В период с 2010 по 2015 годы эта хакерская команда успешно взломала такие компании, как Ametek, Honeywell, Safran, Capstone Turbine, GE и другие.

По данным Crowdstrike и Министерства юстиции США в группу, которую исследователи назвали Turbine Panda, вербовали местных хакеров и ИБ-исследователей, в том числе известных в андеграундных кругах. Затем им поручали найти точку входа в целевые сети, где они обычно применяли вредоносные программы таких семейств как Sakula, PlugX и Winnti, используя их для поиска конфиденциальной информации и ее хищения.

APT32/Ocean Lotus

По заверениям исследователей из FireEye вьетнамская хакерская группа APT32/OceanLotus, которая ведет свою активность по крайней мере с 2014 года и известна в основном своими атаками на журналистов и госсектор, в 2019 году стала активно проводить атаки на транснациональные автомобильные компании в явной попытке поддержать отечественный автопром. С февраля 2019 группа разослала фишинговые письма от пяти до десяти организациям автомобильного сектора. Группа также создавала фальшивые домены для Toyota Motor Corp. и Hyundai Motor Co. в попытках осуществить атаки. Неизвестно, были ли эти атаки успешными.

В марте, по словам представителя Toyota, компания обнаружила, что ее подразделения во Вьетнаме, Тайланде, а также в Японии были атакованы – в последнем случае через японскую дочернюю компанию Toyota Tokyo Sales Holdings Inc. Официальный представитель Toyota заявил, что за это несет ответственность APT32.

Основные события полугодия

Атаки программ-вымогателей

В данном разделе представлена сводка по актуальным угрозам, связанным с активностью вредоносных программ-вымогателей (Trojan-Ransom) в отношении муниципальных структур, промышленных предприятий и объектов критической инфраструктуры.

Статистика по атакам вымогателей на промышленные предприятия

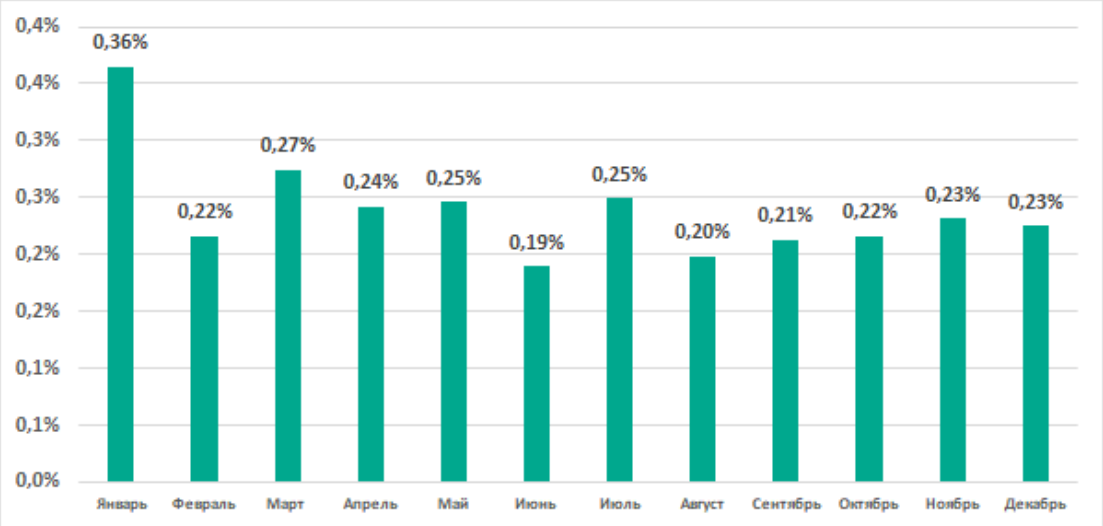
Во втором полугодии 2019 года мы провели детальный анализ данных о блокировании Trojan-Ransom и устранили ряд неточностей в классификации вредоносных объектов. Выявленные троянские программы и черви, ошибочно классифицированные как Trojan-Ransom в виду наличия схожих паттернов бинарного кода и/или поведения, были исключены из выборки, а данные представленные за прошлые периоды были пересчитаны с целью представить более точную оценку.

Всего во втором полугодии программы вымогатели были заблокированы на 0,61% компьютеров АСУ. По уточненным данным в первом полугодии этот показатель составил 0,76%.

По итогам 2019 года программы-вымогатели были заблокированы на 1,0% компьютеров АСУ.

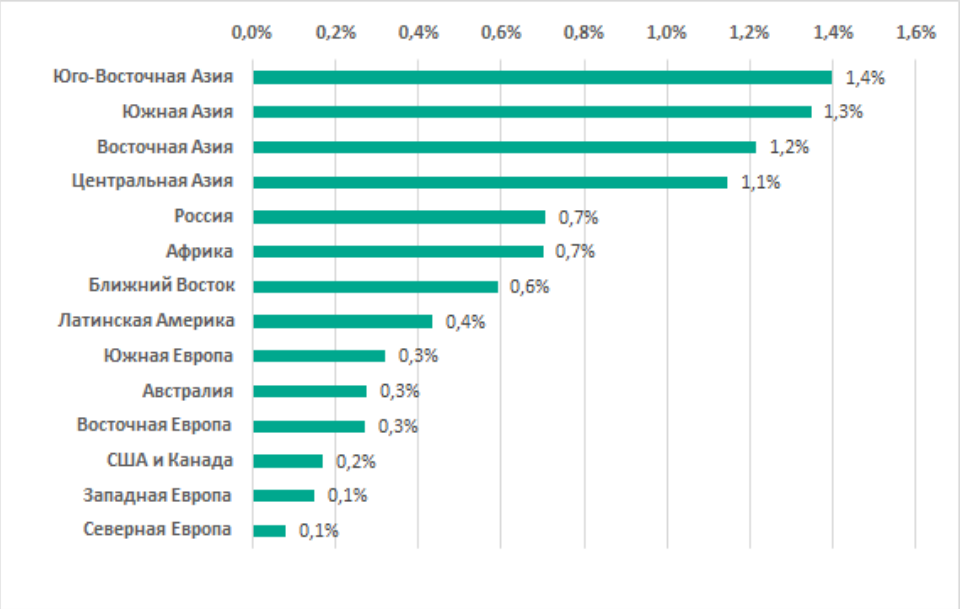
Данные за весь 2019 год по месяцам представлены ниже.

Процент компьютеров АСУ, на которых были заблокированы программы-вымогатели в 2019 году



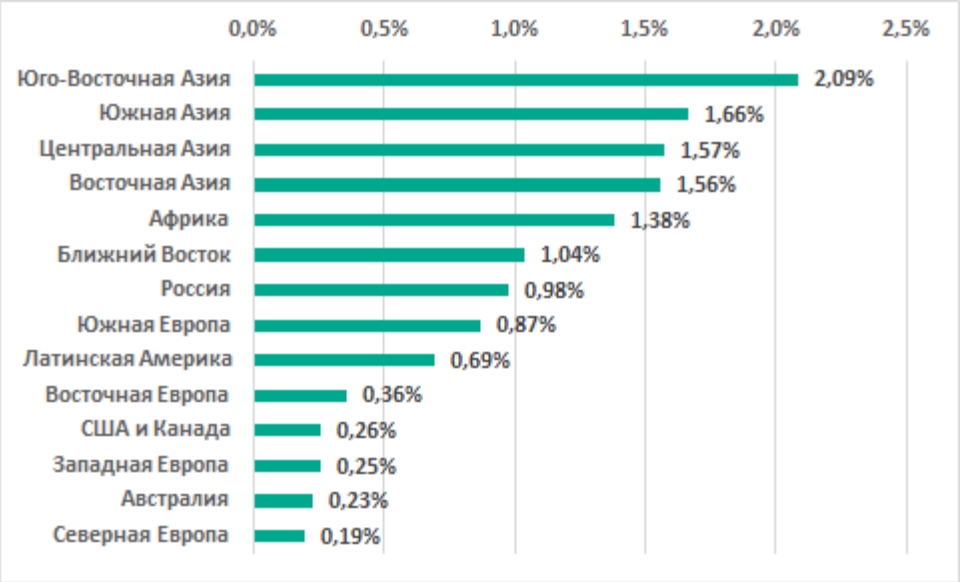
Наибольший процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, во втором полугодии 2019 приходится на Азию.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2019



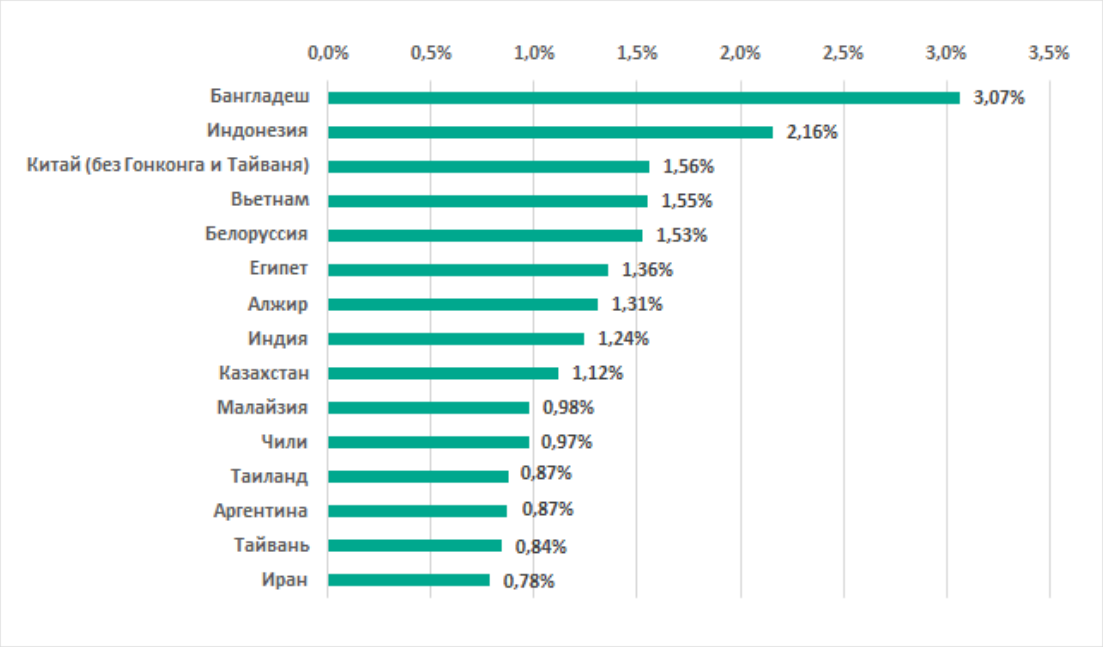
Регионы Азии заняли первые места и в рейтинге за весь 2019 год.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели в 2019 году



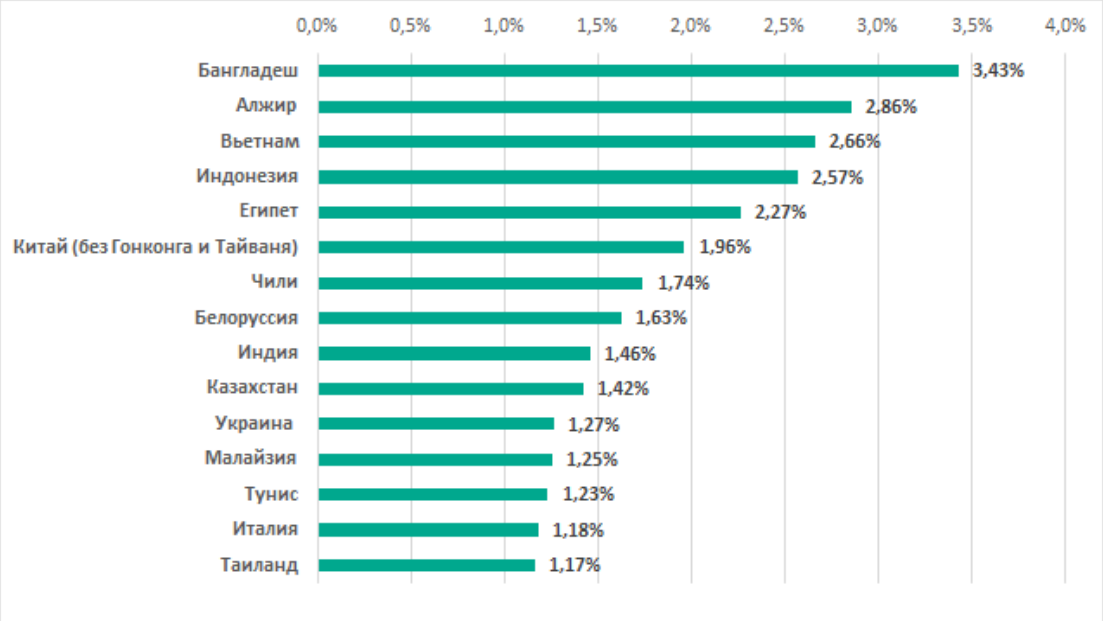
Однако в TOP 15 стран за второе полугодие 2019 вошли не только азиатские страны.

TOP 15 стран по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, второе полугодие 2019



Отметим, что по итогам всего 2019 года в TOP 15 стран попали три страны из Европы: Италия, Украина и Белоруссия.

TOP 15 стран по проценту компьютеров АСУ, на которых были заблокированы программы-вымогатели, 2019 год



В России по итогам года процент компьютеров АСУ, на которых были заблокированы программы-вымогатели, составил 1,0%.

Города и промышленные объекты под прицелом вымогателей

На протяжении 2019 года по всему миру наблюдалась волна атак шифровальщиков. Жертвами этих атак в том числе стали различные организации критической инфраструктуры и промышленные компании. Значительно возросло количество атак вредоносных программ-вымогателей на объекты муниципальных служб. Согласно общедоступной статистике и заявлениям, отслеживаемым экспертами «Лаборатории Касперского», в 2019 году целями программ-вымогателей стали по меньшей мере 174 муниципальные структуры. По сравнению с прошлым годом этот показатель вырос приблизительно на 60%.

Ryuk

За наиболее громкими атаками шифровальщиков часто стояли операторы вредоносной программы Ryuk (вердикт Trojan-Ransom.Win32.Hermez). В течение 2019 года он постоянно появлялся в отчётах об инцидентах на различных крупных предприятиях и в муниципальных службах.

В качестве примера можно привести атаку на город Лэйк (Lake city) в штате Флорида, США. В результате действий вредоносной программы Ryuk работоспособность потеряли все серверы городских служб, за исключением полицейского и пожарного департаментов, которые имели выделенный сервер. Отключены оказались даже телефоны городских служб (такое возможно в тех случаях, когда используется IP-телефония). Сообщается, что городские службы производили резервное копирование своих систем, однако воспользоваться резервными копиями не удалось т.к. они были удалены атакующими. В результате, городские службы были вынуждены заплатить злоумышленникам 460 тысяч долларов США.

Мы напоминаем, что важно не только регулярно создавать резервные копии критически важных систем, но и выполнять другие мероприятия, направленные на обеспечение сохранности резервных копий. В частности, необходимо хранить резервные копии на отдельном сервере, права на доступ к которому с других систем позволяет только создание новых и чтение уже существующих резервных копий. Также необходимо регулярно проверять целостность резервных копий и следить за состоянием оборудования, отвечающего за их хранение.

В декабре 2019 года береговая охрана США выпустила информационный бюллетень об атаке вымогательского ПО Ryuk на объект, попадающий под действие закона США «О безопасности морских перевозок». Название объекта в уведомлении не сообщалось. Известно, что атака была совершена при помощи фишингового письма, а вредоносное ПО было загружено на систему, после того как сотрудник организации перешёл по вредоносной ссылке. Вредоносное ПО проникло в системы, которые контролируют передачу грузов, и зашифровало файлы, критически важные для технологических операций. В связи с этим все операции на пострадавшем объекте были приостановлены более чем на 30 часов. Также Ryuk отметился заражениями систем видеонаблюдения и систем контроля и управления доступом.

Кроме того, вредоносное ПО Ryuk нанесло ущерб пяти нефтегазовым объектам. Атаки не привели к остановке производства, но удаленный мониторинг промышленного оборудования был парализован на срок до 72 часов, что вынудило предприятия переключиться в ручной режим.

Абсолютное большинство атак с использованием Ryuk проходят по одной и той же схеме. На первом этапе жертва злоумышленников получает фишинговое письмо,

содержащее документ с вредоносным макросом. Если жертва разрешает выполнение макроса, на машину загружается вредоносная программа TrickBot. Эта вредоносная программа позволяет злоумышленникам подключаться к зараженному компьютеру и исследовать сеть атакованной организации. Операторы TrickBot пытаются найти уязвимые системы, а также украсть учётные данные пользователей.

Злоумышленники стремятся проникнуть в системы, которые обеспечивают работу критически важных для атакованной организации сервисов. Именно на этих системах информация шифруется вредоносной программой Ryuk.

Ryuk использует криптостойкие алгоритмы шифрования и, к сожалению, расшифровка файлов без наличия закрытого ключа шифрования не представляется возможной. Однако всё же можно снизить риски потери доступа к данным, подготовившись к такой атаке, либо выявив её на начальном этапе. Наши рекомендации вы можете найти здесь.

RobinHood

Одной из наиболее громких атак шифровальщиков на муниципалитеты в 2019 году стало заражение систем города Балтимор, штат Мэрилэнд, США, вредоносной программой RobinHood (вердикт Trojan-Ransom.Win32.Robin). Несмотря на то, что IT-специалисты мэрии оперативно приняли меры (в том числе отключили все компьютеры и серверы, чтобы остановить распространение шифровальщика), зловред успел вывести из строя около 10 000 устройств, пострадали в том числе базы данных, относящиеся к муниципальным службам. В результате атаки часть городских служб была полностью парализована. Вскоре на сайте города появилось сообщение о том, что связаться с властями можно только по телефону.

По информации The New York Times, злоумышленники воспользовались эксплойтом EternalBlue уязвимости CVE-2017-0144 в сервисе SMB v1 ОС Microsoft Windows различных версий. Широкую известность EternalBlue получил благодаря другому шифровальщику – WannaCry, который вызвал серьезную эпидемию и заразил миллионы компьютеров в 2017 году.

Инцидент в Балтиморе иллюстрирует другую серьёзную проблему, которую мы видим как в муниципальных предприятиях, так и в системах промышленной инфраструктуры. Речь идёт об использовании устаревших версий операционных систем и другого программного обеспечения, содержащих критические уязвимости. В абсолютном большинстве случаев при атаках шифровальщиков злоумышленники используют известные уязвимости, для которых давно выпущено обновление безопасности. Например, обновление MS17-010, исправляющее уязвимость, которая эксплуатируется EternalBlue, было выпущено компанией Microsoft 14 марта 2017 года.

На промышленных предприятиях зачастую такая ситуация связана с тем, что системы имеют устаревшую аппаратную базу, что не позволяет выполнить обновление ПО. В свою очередь, замена таких систем требует значительных финансовых вложений. В таких случаях мы рекомендуем создавать надёжный сетевой периметр, чтобы затруднить злоумышленникам проникновение на уязвимые системы. Подробнее о техниках использования подобных уязвимостей злоумышленниками, а также о методах защиты от таких атак вы можете прочитать в нашей статье.

Sodinokibi (REvil)

В августе 2019 года системы сразу 22 городов штата Техас в США подверглись атакам с использованием шифровальщика Sodinokibi, также известного как REvil (вердикт Trojan.Win32.DelShad). Такая массовая атака стала возможной благодаря взлому сети

провайдера удаленного управления услугами (Managed services providers, MSP). Согласно имеющимся данным, этим провайдером может являться компания CyrusOne. Скомпрометировав системы MSP, злоумышленники получили возможность удаленного доступа к системам муниципалитетов, которые являлись клиентами данного провайдера. В результате их файлы были зашифрованы, а часть социальных сервисов оказалась парализована. Согласно публичным заявлениям все города-жертвы атаки отказались платить деньги злоумышленникам за расшифровку файлов, однако сам процесс восстановления после инцидента занял несколько недель и потребовал значительных ресурсов, как человеческих, так и финансовых.

К сожалению, атаки с использованием систем подрядных организаций, а также поставщиков стороннего ПО перестают быть редкостью. При этом возможны совершенно разные сценарии. Злоумышленники могут атаковать делового партнёра потенциальной жертвы, чтобы похитить содержимое деловой переписки. Эта информация потом может быть использована, например, для создания фишинговых писем. В других случаях, например, как в описанном выше инциденте, могут быть использованы средства удаленного доступа, применяемые подрядчиком для обслуживания атакуемой организации. Наконец, могут быть скомпрометированы сами поставщики стороннего ПО, как было в случае с атаками шифровальщика ExPetr, который устанавливался на компьютер жертвы вместе с обновлением бухгалтерского ПО M.E.Doc.

Для снижения рисков возникновения подобных инцидентов необходимо контролировать подключения между сетью организации и сетями других предприятий (поставщиков, подрядчиков и т.д.). Особое внимание необходимо уделять контролю применения средств удаленного администрирования. Как правило, инциденты с атаками шифровальщиков на крупные предприятия развиваются продолжительное время, за которое злоумышленники производят обследование сети предприятия и выбирают системы для шифрования. Это означает, что команда по реагированию на инциденты информационной безопасности имеет все шансы пресечь деятельность преступников на ранней стадии. Выявлению таких инцидентов поможет практика предварительного согласования всех сеансов удаленных подключений со стороны подрядных организаций. Также рекомендуется тестировать все обновления прикладного ПО перед их установкой на критически важные системы.

Новые шифровальщики нацелены на нарушение работы промышленного ПО

Почему работа промышленного ПО под угрозой

Среди шифровальщиков, замеченных в атаках 2019 года, были обнаружены новые вредоносные программы MegaCortex и Snake, которые привлекли особое внимание экспертов из-за списков процессов, которые завершаются перед началом шифрования. Эти списки, помимо процессов антивирусных решений, серверов баз данных, браузеров, содержат также процессы, связанные с программным обеспечением систем промышленной автоматизации.

Первой подобной вредоносной программой стала MegaCortex, которая была обнаружена в середине 2019 года в атаках на корпоративных сектор. В течение года она активно развивалась, появлялись новые версии, обладающие дополнительной функциональностью. Используемый MegaCortex список процессов, завершаемых перед началом шифрования, содержит более 1000 наименований.

В середине декабря был обнаружен еще один шифровальщик, названный Snake (или EKANS). Snake также содержит список процессов, которые завершаются перед началом

шифрования, при этом большая часть этого списка совпадает со списком из MegaCortex, включая специфичные для промышленных систем процессы.

Речь идёт о процессах, связанных с программным обеспечением систем промышленной автоматизации:

- General Electric Proficy data historian (клиентская и серверная части);
- General Electric Fanuc licensing server;
- Honeywell's HMIWeb application;
- FLEXNet licensing server;
- Sentinel HASP license managers;
- ThingWorx Industrial Connectivity Suite;
- Различные процессы баз данных, используемые в различных Historian серверах.

Важно отметить, что никаких иных действий по отношению к процессам, кроме их завершения, обе вредоносные программы не совершали. То есть они не имеют возможности вводить команды или каким-либо образом манипулировать промышленными процессами. Однако сам факт завершения процессов, связанных со специфичным для промышленных систем программным обеспечением, может вызывать негативные киберфизические последствия. Наиболее вероятно, что завершение процессов приложений необходимы злоумышленникам для успешного шифрования баз данных, файлы которых могут использоваться и быть заблокированными для записи.

Появление сразу двух шифровальщиков, функциональность которых направлена в том числе на нарушение работы систем промышленной автоматизации, в очередной раз говорит о заинтересованности злоумышленников в проведении атак на промышленные предприятия. В случае аварийной остановки технологического процесса, возникшей из-за отказа системы, файлы которой были зашифрованы, организация может понести серьезные убытки, что с большой вероятностью заставит жертву такой атаки заплатить крупную сумму денег за расшифровку файлов.

Подробности атак

Мы полагаем, что атаки MegaCortex и Snake носят целевой характер, и наши предположения совпадают с мнениями других экспертов. Исходя из этого, можно предположить, что, как и в других подобных случаях, заражения производятся преимущественно вручную. Как правило, в качестве начального вектора атаки используется подбор аутентификационных данных к учетным записям сотрудников, имеющих удаленный доступ посредством RDP.

Получив удаленное управление первой системой, злоумышленники обычно используют утилиту Mimikatz или её аналоги, что позволяет преступникам украсть данные учетных записей, при помощи которых выполнялся вход на зараженную систему. Собирая всё больше учетных данных, злоумышленники получают возможность проникнуть на большее количество систем, пока не добираются до компьютера, на котором использовалась учетная запись, имеющая права доменного администратора.

Выводы о таком характере распространения описываемых вредоносных программ косвенно подтверждаются тем фактом, что в атаках MegaCortex злоумышленникам удалось скомпрометировать контроллер домена атакованной организации, предположительно, воспользовавшись ранее украденными аутентификационными данными.

Сам процесс шифрования файлов в MegaCortex и Snake является стандартным и не имеет принципиальных отличий от других вредоносных программ этого класса.

Примечательно, что в атаках MegaCortex, исполняемые файлы вредоносной программы имели действительные цифровые подписи. Первая подпись была выдана на имя компании Mursa Pty Ltd., а вторая принадлежала компании ABADAN PIZZA Ltd. Наиболее вероятно, что преступная группировка, стоящая за MegaCortex, либо самостоятельно выкрала цифровые подписи у этих организаций, либо приобрела их на чёрном рынке у других злоумышленников.

В последних версиях MegaCortex злоумышленники не только требуют выкуп за расшифровку файлов, но и угрожают опубликовать конфиденциальные данные жертвы в случае отказа от уплаты выкупа.

Интересной особенностью Snake является возможность злоумышленника настроить вредоносную программу таким образом, чтобы шифрование файлов началось в определённый момент времени, например, в нерабочие часы организации, когда на месте может не быть специалистов по информационной безопасности или IT администраторов. Это может замедлить и усложнить реакцию на инцидент со стороны организации-жертвы.

Связь с другими атаками

Как уже было сказано, большая часть списка процессов, используемого в Snake (включая специфичные для промышленных систем процессы), совпадает с аналогичным списком из MegaCortex, что породило теории о связи между двумя этими шифровальщиками. Мы считаем, что совпадение списков не является достаточным основанием для таких выводов, поскольку вредоносная программа MegaCortex была проанализирована до появления Snake, и у создателей Snake была возможность получить список процессов из открытых источников. При этом других технических улик, указывающих на связь между двумя вымогателями, не обнаружено.

По завершении шифрования Snake оставляет сообщение с инструкциями и требует связаться с операторами по почте, используя для этого адрес bapcocrypt@ctemplar.com. В связи с этим существует предположение, что одной из главных целей атак Snake была нефтегазовая компания BAPCO, которая незадолго до обнаружения Snake пострадала от атаки вайпера Dustman. К тому же, согласно публичной информации, компания BAPCO использует оборудование General Electric, а процессы программного обеспечения General Electric содержатся в списке завершаемых процессов MegaCortex и Snake.

Однако нет никаких технических улик, позволяющих связать Snake и Dustman, а тот факт, что предположительно было атаковано одно и то же предприятие, является недостаточным для подобных выводов. Версию о том, что эти атаки связаны, опровергает также разная направленность вредоносных программ: если Dustman является вайпером, т.е. стремится уничтожить данные жертвы, то Snake имеет техническую возможность расшифровки файлов.

Согласно имеющимся данным, вымогатель Snake не связан с деятельностью преступной группировки Snake, также известной под именем Turla – совпадение имён является случайным.

Таким образом, в настоящий момент нет достаточных доказательств, позволяющих сделать вывод о принадлежности вредоносных программ MegaCortex и Snake определённым преступным группировкам.

LockerGoga: актуальная информация

В предыдущем отчёте мы рассказывали об атаках шифровальщика LockerGoga на промышленные предприятия. В числе его жертв оказались норвежская металлургическая компания Norsk Hydro, французская консалтинговая компания Altran Technologies, а также две американские химические компании Hexion и Momentive.

Последствия атаки на Norsk Hydro были значительными: согласно официальному заявлению на сайте компании общий финансовый ущерб от атаки составил около 550–650 миллионов норвежских крон (приблизительно 60,5–71,5 миллиона долларов).

Во втором полугодии атаки шифровальщика LockerGoga продолжились. В декабре 2019 года Федеральное Бюро Расследований США выпустило предупреждение об опасности атак шифровальщиков MegaCortex и LockerGoga. Согласно этому предупреждению, для проникновения в системы злоумышленники используют фишинговые письма, SQL инъекции, украденные аутентификационные данные, а также эксплуатируют уязвимости.

В марте 2020 года история с атакой на Norsk Hydro получила неожиданное продолжение. Компания Dragos выпустила отчёт, в котором выразила сомнения, что операторы LockerGoga хотели зашифровать файлы с целью получения выкупа. Согласно отчёту, целью злоумышленников было не шифрование, а уничтожение файлов.

Об этом свидетельствует дополнительная функциональность, которую имел образец вредоносной программы LockerGoga, использованный в ходе атаки на Norsk Hydro. После шифрования вредоносная программа сменила пароли учетных записей пользователей на одно и то же зашифрованное значение, системная сетевая карта была отключена (по-видимому, для предотвращения авторизации других учетных записей через запрос к контроллеру домена), был выполнен выход из системы.

В этой ситуации пользователи были неспособны даже прочитать требование выкупа, которое вредоносная программа оставила на жестком диске и, следовательно, связаться с преступниками для обсуждения условий восстановления доступа к файлам. Все это препятствовало монетизации атаки.

По мнению экспертов Dragos, за созданием вредоносных программ LockerGoga и Ryuk стоит одна и та же преступная группировка, называемая FIN6 (согласно классификации FireEye). По их же мнению, атака на Norsk Hydro могла быть спонсирована правительством другой страны. В качестве аргумента приводится тот факт, что в это же время были атакованы и другие объекты, находящиеся в Норвегии, однако инциденты удалось своевременно выявить благодаря быстрому обмену информацией между Norsk Hydro и государственными органами.

Это не первый случай, когда вредоносные программы для уничтожения данных маскируются под вымогателей. В 2017 году эксперты «Лаборатории Касперского» обнаружили отсутствие технической возможности расшифровки систем, зараженных вредоносной программой ExPetr.

WannaCry всё ещё жив

Прошло почти три года после эпидемии вредоносной программы WannaCry, когда были заражены системы в 150 странах мира, а ущерб составил 1 млрд долларов США. Жертвами эпидемии стали в том числе компании, занимающиеся различными видами производства, нефтеперерабатывающие заводы, объекты городской инфраструктуры и распределительной энергосети.

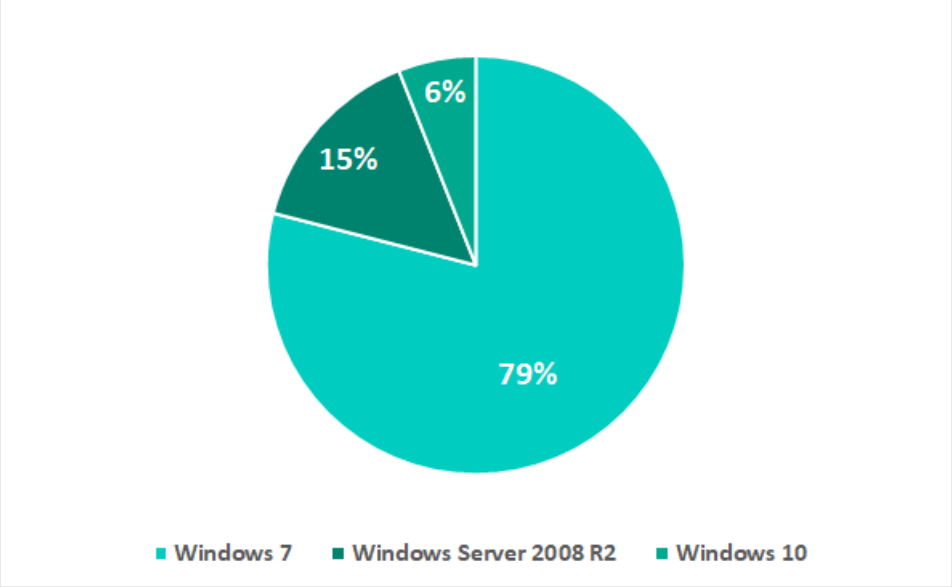
В одной из наших публикаций мы подробно рассказывали о том, как происходит заражение сетей промышленных предприятий червём WannaCry, и какие меры необходимо предпринять для защиты.

Согласно нашей статистике, среди всех пользователей продуктов «Лаборатории Касперского», подвергшихся атакам троянских программ-вымогателей в 2019 году, более 23% были атакованы именно вредоносной программой WannaCry (вердикт Trojan-Ransom.Win32.Wanna). Что касается промышленных организаций, то за 2019 год доля пользователей, атакованных WannaCry, среди всех пользователей, атакованных вымогателями, превышает 35%. Оба эти показателя говорят о том, что WannaCry продолжает распространяется по сети Интернет и по-прежнему представляет серьезную угрозу, в том числе для систем промышленной автоматизации.

Отметим, что в большинстве случаев это означает, что атакованная система не имела установленного обновления безопасности MS17-010, что позволило WannaCry успешно проэксплуатировать уязвимость в сервисе SMB v1. Однако вредоносный код не был запущен, т.к. был заблокирован продуктом Kaspersky.

Ниже приведена информация о версиях операционных систем, используемых на компьютерах АСУ, атакованных WannaCry:

Операционные системы, используемые на компьютерах АСУ, атакованных WannaCry



Как видим, подавляющее большинство составляют системы, работающие под управлением Windows 7 (79%) и Windows Server 2008 R2 (15%). Расширенная поддержка этих продуктов была прекращена в январе 2020 года. Это вызывает особое опасение, поскольку обновления для таких операционных систем выпускаются только в экстренных случаях.

GandCrab – Ransoware as a service в атаках на промышленные предприятия

GandCrab (вердикт Trojan-Ransom.Win32.GandCrypt) – известная вредоносная программа шифровальщик, создатели которой использовали бизнес-модель RaaS (Ransomware-as-a-Service). Через веб-портал различные преступные группировки приобретали доступ к вымогателю у создателей GandCrab, а затем самостоятельно распространяли шифровальщик. Сервис также обеспечивал возможность оплаты выкупа.

В 2019 году правоохранительные органы ряда стран совместно с антивирусными компаниями провели комплекс мероприятий, направленных на борьбу с GandCrab. В результате была создана полноценная утилита для расшифровки зашифрованных данных, успешно справляющаяся со всеми версиями GandCrab вплоть до 5.1. Однако последняя версия шифровальщика имеет номер 5.2. Она использует криптостойкие алгоритмы RSA и AES, что делает невозможным расшифровку файлов без наличия приватного ключа.

Летом 2019 года создатели GandCrab объявили о закрытии «сервиса». Несмотря на это атаки с применением GandCrab фиксируются по сей день. Атакам подвергаются предприятия, относящиеся к различным секторам экономики. Поскольку механизмы оплаты выкупа не работают, в случае заражения последней версией шифровальщика (5.2) невозможно даже заплатить выкуп для расшифровки, что делает этот шифровальщик, по сути, вайпером.

Подробности атак

В настоящий момент наблюдается два сценария заражения систем, в обоих случаях атака начинается с фишинговых писем, текст которых написан на языке, соответствующем стране, в которой работает атакуемая организация.

Дальше сценарий атаки различается в зависимости от типа прикреплённого вложения. В одних случаях злоумышленники используют Excel документ, содержащий обфусцированный VBA макрос, который загружает исполняемый файл GandCrab с сервера злоумышленников и запускает его.

После открытия документа пользователь видит сообщение с просьбой включить исполнение содержимого документа. Если пользователь согласится это сделать, вредоносный макрос будет выполнен.

Просьба к пользователю включить выполнение макросов

В других случаях исполняемый файл GandCrab прикреплён к письму как вложение. Чаще всего злоумышленники помещают в название файла двойное расширение, например, .doc.exe или .pdf.exe. Данная техника позволяет ввести пользователя в заблуждение, т.к. по умолчанию в ОС Windows отключено отображение расширений известных типов файлов, и на системе с настройками «По умолчанию» видимая пользователю часть имени файла будет заканчиваться на .doc или .pdf, соответственно.

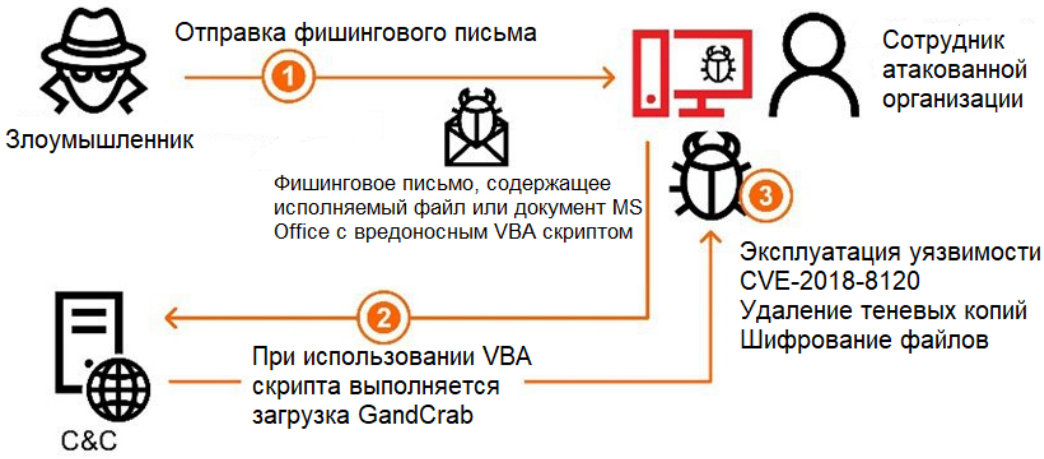
В совокупности со сменой иконки приложения это позволяет убедить пользователя в том, что перед ним документ, а не исполняемый файл.

До середины 2019 года фиксировались и заражения систем шифровальщиком GandCrab при помощи подбора аутентификационных данных к учетным записям пользователей для последующего подключения к атакуемой системе через RDP и запуска шифровальщика «вручную». Сейчас этот вектор является актуальным для других шифровальщиков.

После запуска исполняемый файл GandCrab использует уязвимость CVE-2018-8120. Данная уязвимость содержится в компоненте операционной системы Win32k и заключается в неправильной обработке объектов в памяти. Также, чтобы усложнить восстановление доступа к информации, вредоносная программа удаляет все теневые копии Windows.

Ниже представлена общая схема проведения атак с использованием шифровальщика GandCrab:

Схема проведения атаки с использованием GandCrab



Индийская АЭС Куданкулам подверглась заражению вредоносным ПО

В сентябре 2019 года появилась информация о том, что на Индийской АЭС Куданкулам обнаружено вредоносное ПО. Позднее, 30 октября, Ядерная энергетическая корпорация Индии (Nuclear Power Corporation of India Ltd, NPCIL) подтвердила, что 4 сентября компьютер в административной сети АЭС Куданкулам подвергся заражению. Вредоносное ПО было обнаружено лишь на одном компьютере, промышленные системы АЭС не пострадали.

По данным проведенного расследования наиболее вероятным способом заражения была фишинговая атака через зараженный веб-сайт или фишинговое письмо.

Некоторые исследователи считают, что компьютер в административной сети АЭС Куданкулам подвергся заражению вредоносной программы Dtrack, которая позволяет злоумышленникам собирать и отправлять злоумышленникам информацию с компьютера жертвы.

Один из найденных образцов этой вредоносной программы содержал в себе учетные данные и IP-адреса внутренней сети АЭС Куданкулам. Исходя из этого, было высказано предположение, что Индийская АЭС подверглась целенаправленной атаке.

Атака на промышленный концерн Rheinmetall

24 сентября 2019 года ИТ-инфраструктура заводов Rheinmetall Automotive, принадлежащих крупному немецкому концерну Rheinmetall Group, пострадала от атак вредоносного ПО в Бразилии, Мексике и США.

Атаки вызвали значительные сбои в производственных процессах этих заводов. Инфраструктура других подразделений и компаний группы Rheinmetall не пострадала.

По оценкам компании, устранение последствий заражения и восстановление нормального функционирования систем должно было занять примерно 2-4 недели, ожидаемые убытки составляли €3 млн — €4 млн в неделю.

Атака на ветряные и солнечные электростанции sPower

В сентябре 2019 года стало известно о кибератаке на электроэнергетический объект на западе США, которая вызвала временные перебои в работе электрических систем.

Позднее появилась информация о том, что жертвами этой атаки стали ветряные и солнечные электростанции компании Sustainable Power Group (sPower) в Вайоминге и Калифорнии, а также круглосуточный центр управления и штаб-квартира компании в Юте.

По данным Национальной лаборатории энергетических технологий США, на нескольких площадках производства электроэнергии, принадлежащих sPower, периодически возникали сбои в работе брандмауэра в течение примерно 10 часов с 9:12 до 18:57 5 марта 2019 года. Эти брандмауэры контролировали связь между центром управления и несколькими удаленными солнечными и ветряными электростанциями.

Расследование инцидента показало, что межсетевые экраны Cisco периодически перезагружались и становились недоступными в течение примерно 5 минут при каждой перезагрузке. Это, в свою очередь, нарушило связь между центром управления и устройствами, расположенными на удаленных объектах генерации. В результате операторы электросетей временно потеряли данные об устройствах на объектах генерации. Однако эти разорванные соединения не повлияли на выработку электроэнергии и не привели к отключениям электричества у потребителей.

Согласно отчету Североамериканской корпорации по надежности электроэнергии (NERC), перезагрузка брандмауэров произошла в результате атаки с использованием известной на момент атаки уязвимости в веб-интерфейсе брандмауэра. Некоторые исследователи считают, что речь идет об уязвимости отказа в обслуживании веб-служб Cisco Adaptive Security Appliance (ASA) (CVE-2018-0296).

Атаки новых вайперов на промышленные компании

29 декабря 2019 года Бахрейнская национальная нефтяная компания Bapco стала жертвой атаки вредоносного ПО Dustman. По данным Национального управления кибербезопасности Саудовской Аравии (National Cybersecurity Authority, NCA) атака

не привела к серьезным последствиям. От заражения вредоносного ПО пострадала только часть компьютеров в сети Bapco, и компания смогла продолжить свою работу.

Dustman относится к вредоносным программам типа вайпер (стиратель, уничтожающий данные на диске компьютера-жертвы) и предназначена для удаления данных на зараженных компьютерах. По результатам анализа вредоносного ПО было установлено, что Dustman представляет собой обновленную и улучшенную версию вайпера ZeroCleare, обнаруженного ранее. ZeroCleare использовался в целевых атаках на организации в сфере энергетики и промышленности на Ближнем Востоке и имеет некоторое сходство с вредоносным ПО Shamoon.

Атаки на Mitsubishi Electric

В январе 2020 года компания Mitsubishi Electric сообщила об инциденте, который произошел 28 июня 2019 года. В результате кибератаки злоумышленники получили доступ к внутренним системам и сетям около 14 подразделений компании в Японии, Китае, России и других странах.

Атака была обнаружена после того, как сотрудники Mitsubishi Electric заметили подозрительную активность на одном из серверов компании. Анализ активности показал, что информация из сети собиралась на одном компьютере и затем пересылалась во вне. По имеющимся данным, такая передача осуществлялась несколько раз.

В результате атаки были скомпрометированы как минимум 120 компьютеров и серверов в Японии и за ее пределами и украдены различные данные, включая конфиденциальную информацию. Согласно официальному пресс-релизу компании общий объем украденных данных оценивается примерно в 200 Мб.

Атаку на Mitsubishi Electric связывают с деятельностью преступной группы Tick (другие названия – The Bald Knight, BronzeButler, ShadowWali), а также группировки BlackTech (также известна как CopperTurtle, PLEAD).

Согласно информации из СМИ, несанкционированный доступ начался со взлома учетной записи одного из сотрудников филиала в Китае, и затем атака распространилась на подразделения в Японии. Несанкционированный доступ был осуществлен с использованием 0-day уязвимости в антивирусной системе, название которой не раскрывалось.

Скорее всего злоумышленники эксплуатировали уязвимость обхода каталога CVE-2019-18187 в решении Trend Micro OfficeScan (новое название Apex One). Эта уязвимость позволяет загрузку произвольных файлов и, как результат, удаленное выполнение кода (RCE). В октябре 2019 года компания Trend Micro исправила проблему и предупредила, что киберпреступники уже эксплуатируют ее в атаках.

Также существуют предположения, что атаке 2019 года предшествовала атака группировки Black Tech во второй половине 2017 года, которая также была осуществлена через филиал в Китае.

После сообщения об атаке 2019 года, также появилась информация, что за последние 10 лет на компанию Mitsubishi Electric в разное время было совершено несколько атак. Среди преступных групп, которые могут стоять за этими атаками, помимо группировок Tick и Black Tech, называются Aurora Panda (APT 17) и Stone Panda (APT10, Cloud Hopper).

Статистика: второе полугодие 2019

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

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

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

Методика подготовки статистики

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

- серверы управления и сбора данных (SCADA);
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- Human Machine Interface (HMI);
- компьютеры, используемые для администрирования технологических сетей;
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации.

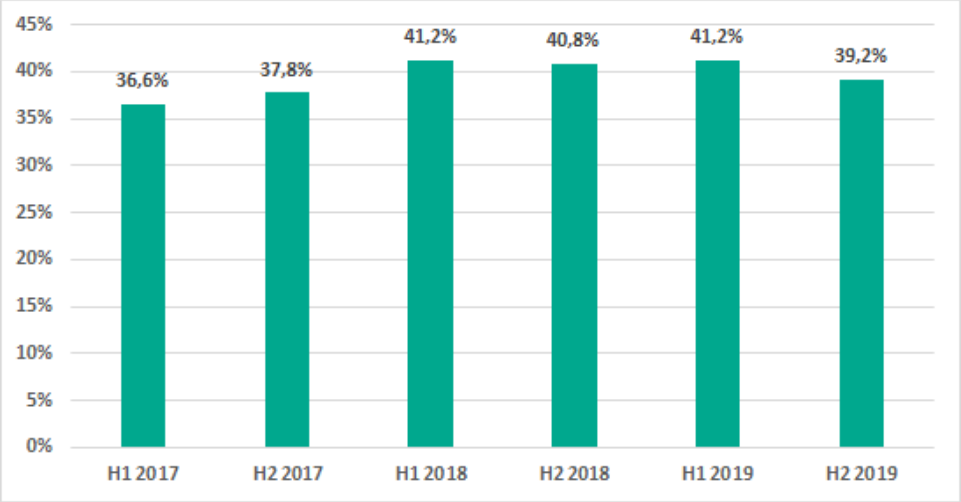
Атакованными мы считаем те компьютеры, на которых в течение отчетного периода защитные решения «Лаборатории Касперского» заблокировали одну и более угроз. При подсчете процента машин, на которых было предотвращено заражение вредоносным ПО, используется количество компьютеров, атакованных в течение отчетного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

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

Процент компьютеров, на которых были заблокированы вредоносные объекты

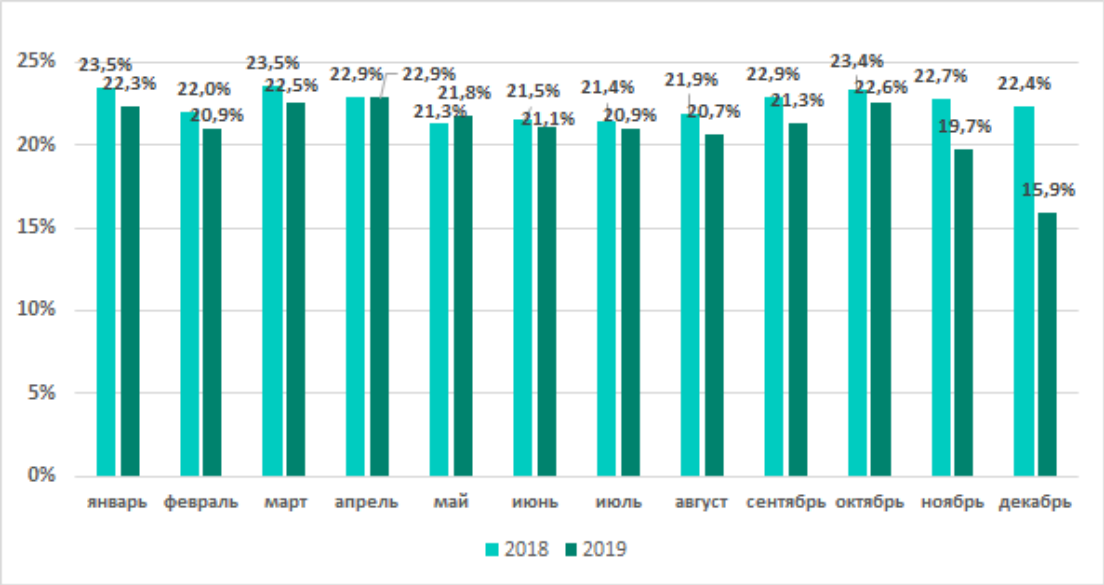
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, во втором полугодии 2019 года составил 39,2%. По сравнению с предыдущим полугодием этот показатель снизился на 2 п.п.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



Во втором полугодии 2019 года наибольший процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, наблюдался в октябре. Показатель этого месяца лишь на 0,3 п.п. уступает лидеру первого полугодия – апрелю.

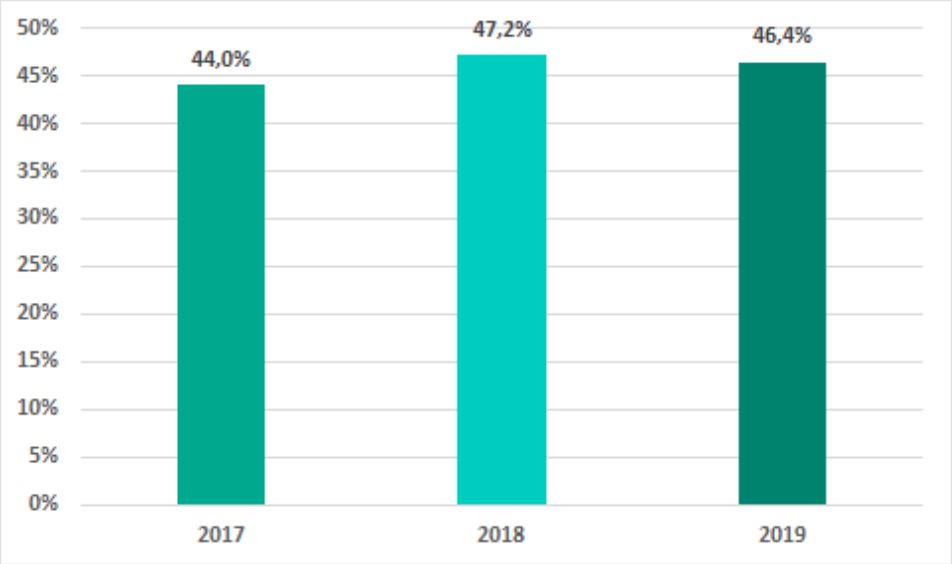
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, по месяцам, 2018 и 2019 годы



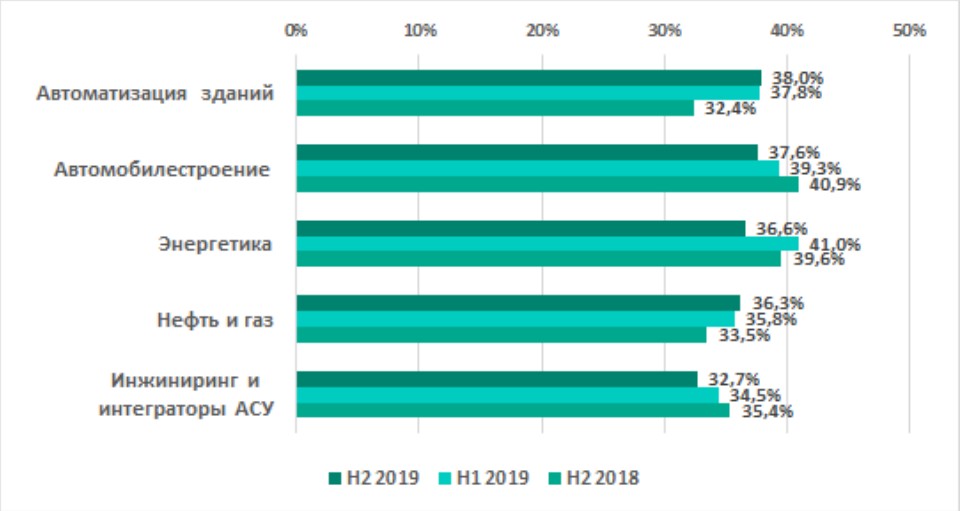
Отметим, что сезонная динамика, которую мы наблюдаем не первый год, сохранилась и в 2019: наибольшие показатели мы видим весной и осенью. Однако в 2019 году в ноябре – декабре падение показателей было более значительным, чем в 2018 году.

В целом за 2019 год процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, уменьшился на 0,8 п.п. и составил 46,6%.

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



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



Разнообразие обнаруженного вредоносного ПО

Во втором полугодии 2019 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было заблокировано более 19,5 тысяч модификаций вредоносного ПО из 2,3 тысяч различных семейств.

Категории вредоносных объектов

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

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

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

- 12,5% – ресурсы в интернете из черного списка.

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

  В частности, в черные списки попадают также ресурсы, на которых распространяется, например, вредоносное ПО типа Trojan-Spy и Ransomware, замаскированное под утилиты для взлома/сброса пароля на контроллерах различных производителей, crack/patch для промышленного и инженерного программного обеспечения, используемого в технологической сети.
- 7,8% – зловредные скрипты и перенаправления на веб-ресурсах (JS и Html), выполняющиеся в контексте браузера, а также эксплойты для браузеров – 0,14%.
- 5,8% –троянцы-шпионы, бэкдоры и кейлоггеры, которые встречаются во множестве фишинговых писем, рассылаемых промышленным организациям. Как правило, конечная цель таких атак – кража денег.
- 5,5% – черви (Worm), распространяющиеся, как правило, через съемные носители и сетевые папки, а также черви, распространяющие через почтовые сообщения (Email-Worm), сетевые уязвимости (Net-Worm) и мессенджеры (IM-Worm). Большинство червей являются устаревшими с точки зрения сетевой инфраструктуры управления ими. Но есть среди них и такие как Zombaque (0,02%) – с реализованной P2P сетевой архитектурой, позволяющей злоумышленникам активировать его в любой момент.

- 4,1% – вредоносные LNK-файлы.
  Такие файлы, в основном, блокируются на съемных носителях. Они являются частью механизма распространения для таких старых семейств вредоносного ПО как Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou и других.

  В этой категории также широко представлены LNK-файлы с уязвимостью CVE-2010-2568 (0,62%), которая впервые была использована для распространения червя Stuxnet, а затем стала использоваться для распространения множества семейств, таких как Sality, Nimnul/Ramnit, ZeuS, Vobfus и других.

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

  В редких случаях запускаемый вредоносный powershell скрипт скачивает и внедряет в память бинарный код, являющийся специфичной модификацией пассивного TCP бэкдора из набора metasploit.
- 3,6% – вредоносные программы класса Virus.

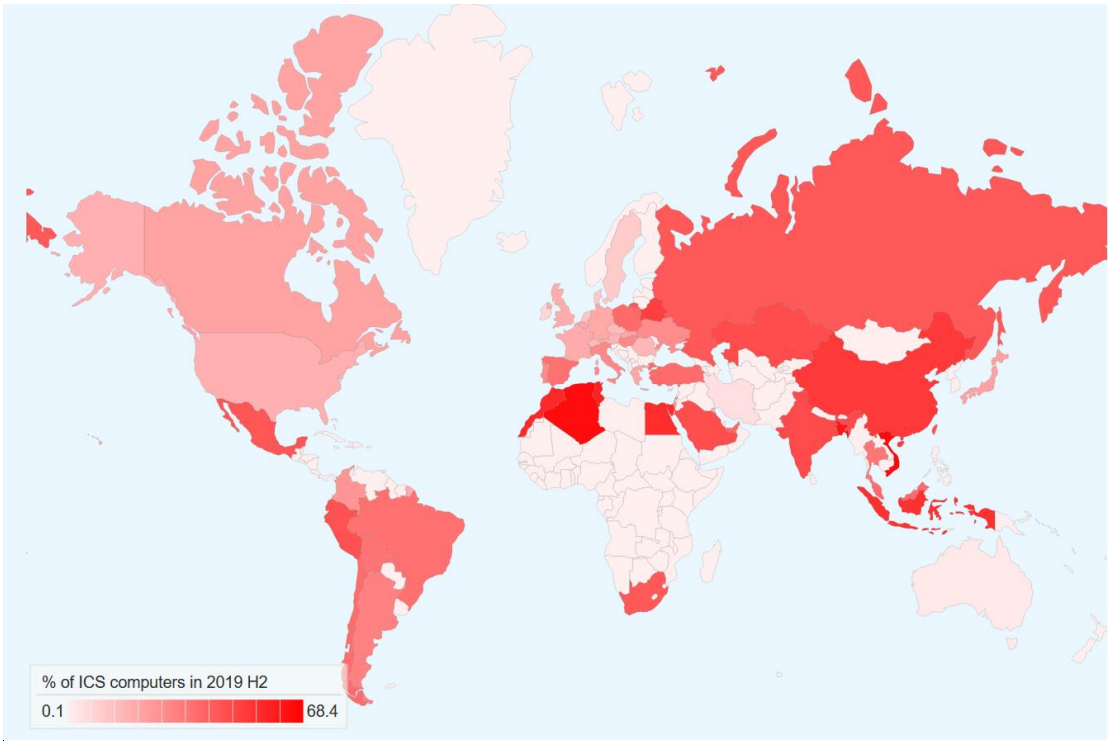
  Среди этих программ уже много лет детектируются такие семейства как Sality (1,1%), Nimnul (0,7%), Virut (0,5%). Хотя эти вредоносные семейства считаются устаревшими, поскольку их командные серверы управления давно не активны, они традиционно вносят значительный вклад в статистику в силу самораспространения и недостаточных мер по их полному обезвреживанию.
- 2,9% – вредоносные документы (MSOffice+PDF), содержащие эксплойты, зловредные макросы и зловредные ссылки.
- 2,0% – вредоносные файлы (исполняемые, скрипты, autorun.inf, .LNK и другие), которые запускаются автоматически при запуске системы или при подключении съемного носителя.

  Это файлы из множества разнообразных семейств, которые объединены фактом автозапуска. Из наиболее «безобидной» функциональности у подобных файлов – автоматический запуск браузера с предустановленной стартовой страницей. В большинстве случаев вредоносное ПО, использующее autorun.inf, является модификацией зловредов старых семейств (Palevo, Sality, Kido и др.).
- 1,9% – веб-майнеры, выполняемые в браузерах, 1, 1% – майнеры - исполняемые файлы для ОС Windows.
- 1,6% – программы-вымогатели.
- 1,5% – банковские троянцы.
- 0,7% – вредоносные программы для AutoCad.

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

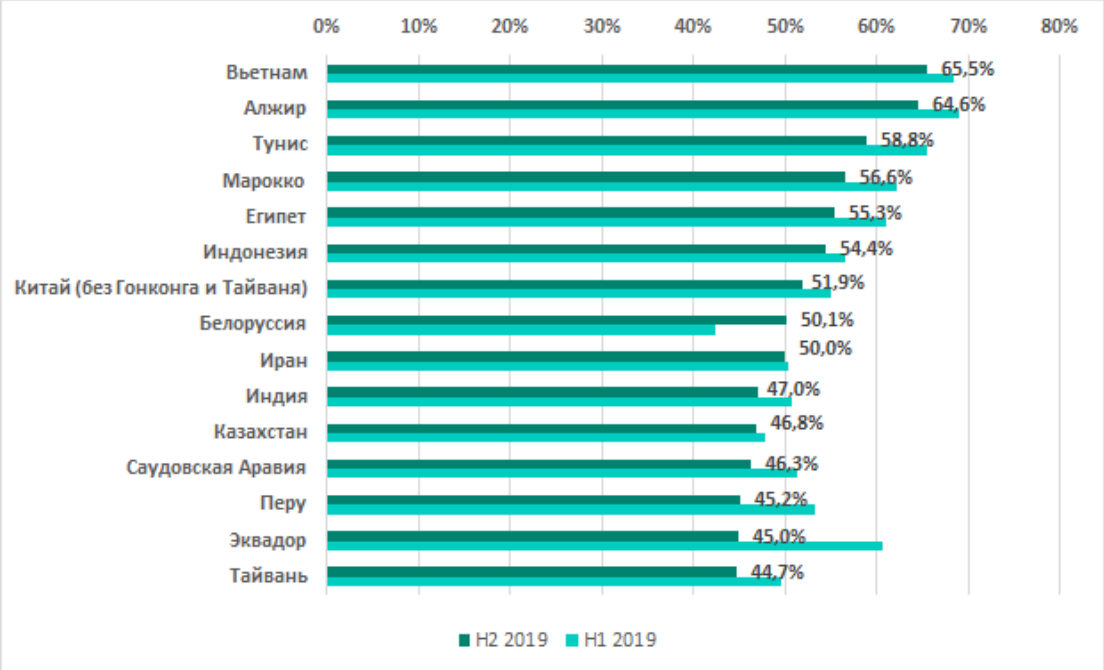
География

На карте ниже для каждой страны отражен процент систем промышленной автоматизации, на которых были заблокированы вредоносные объекты, по отношению к общему количеству таких систем в стране.



География атак* на системы промышленной автоматизации, первое полугодие 2019
**** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты***

ТОР 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты, второе полугодие 2019



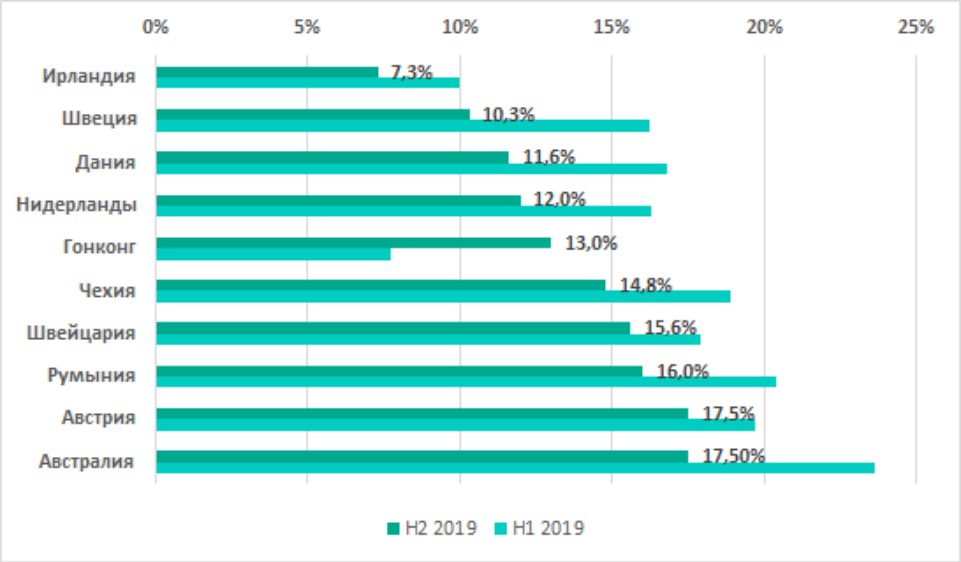
Состав первой пятерки стран в рейтинге по проценту компьютеров АСУ, на которых была предотвращена вредоносная активность, остается неизменным вот уже полтора года. Единственное исключение – прошлое полугодие, когда Боливия неожиданно заняла второе место и вытеснила из TOP 5 Египет.

Наиболее значительное увеличение процента компьютеров АСУ, на которых была предотвращена вредоносная активность, наблюдается в Сингапуре (на 9,2 п.п.), Белоруссии (на 7,6 п.п.) и в ЮАР (на 6,2 п.п.). Отметим, что в течение трех предыдущих полугодий в Сингапуре этот показатель снижался.

В России в течение второго полугодия 2019 года хотя бы один раз вредоносные объекты были заблокированы на 43,1% компьютеров АСУ, что на 1,7 п.п. меньше, чем в первом полугодии 2019 года (44,8%).

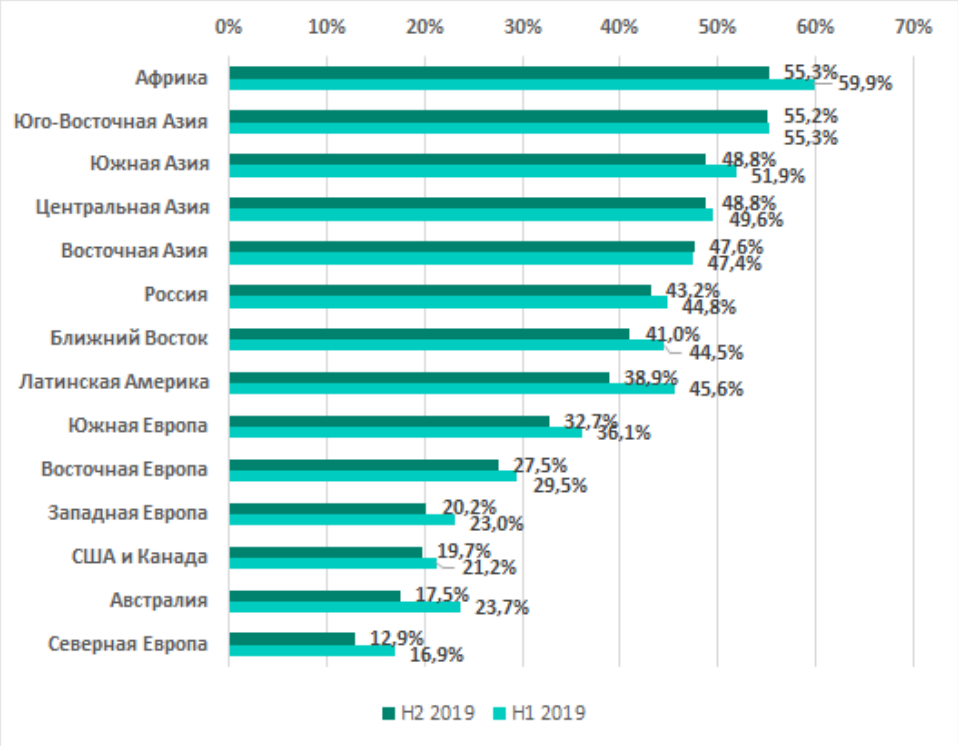
Список десяти наиболее благополучных стран во втором полугодии 2019 покинули США (18,3%), Великобритания (19,0%) и Сингапур (24,2%). Их вытеснили Румыния, Австрия и Австралия.

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



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

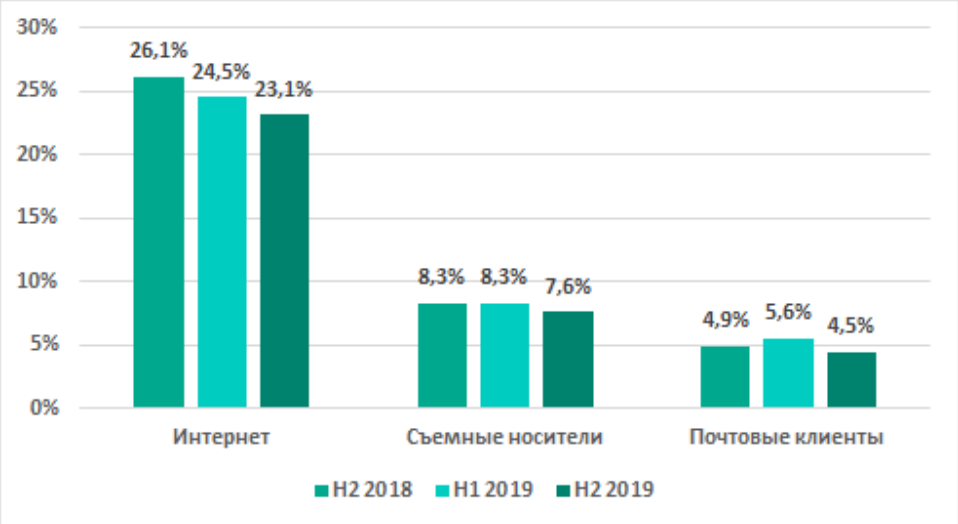
Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в регионах мира



Источники угроз

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

Основные источники угроз, заблокированных на компьютерах АСУ*

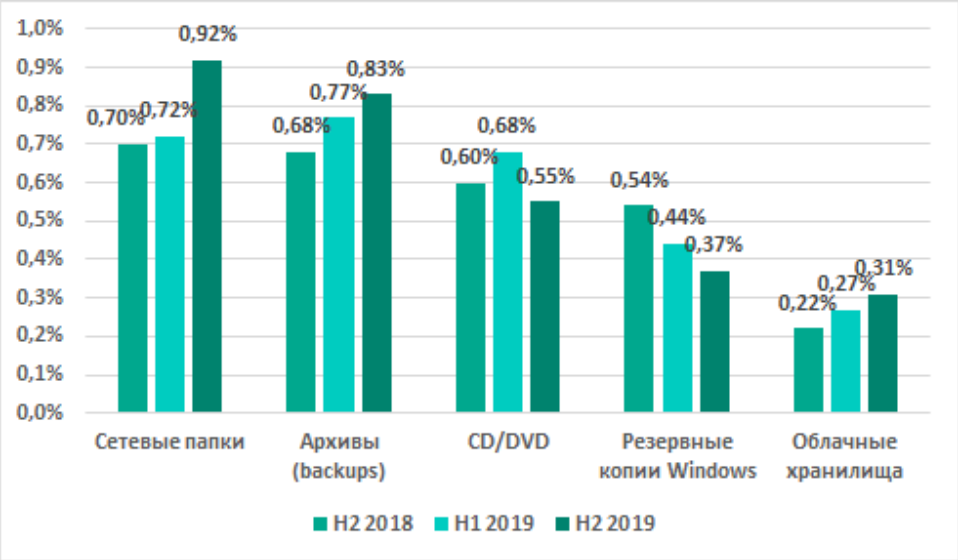


** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из интернета, продолжает снижаться. Во втором полугодии 2019 года этот показатель уменьшился еще на 1,4 п.п.: интернет стал источником угроз, заблокированных на 23,1% компьютеров АСУ.

Значительная часть интернет-угроз связана с веб-страницами различных сайтов, зараженных веб-майнерами, троянцами-загрузчиками и скриптами для кражи cookie. Снижение процента компьютеров АСУ, столкнувшихся с этими угрозами, связано в том числе с уменьшением числа переходов на такие сайты и с устранением заражений на стороне веб-ресурсов.

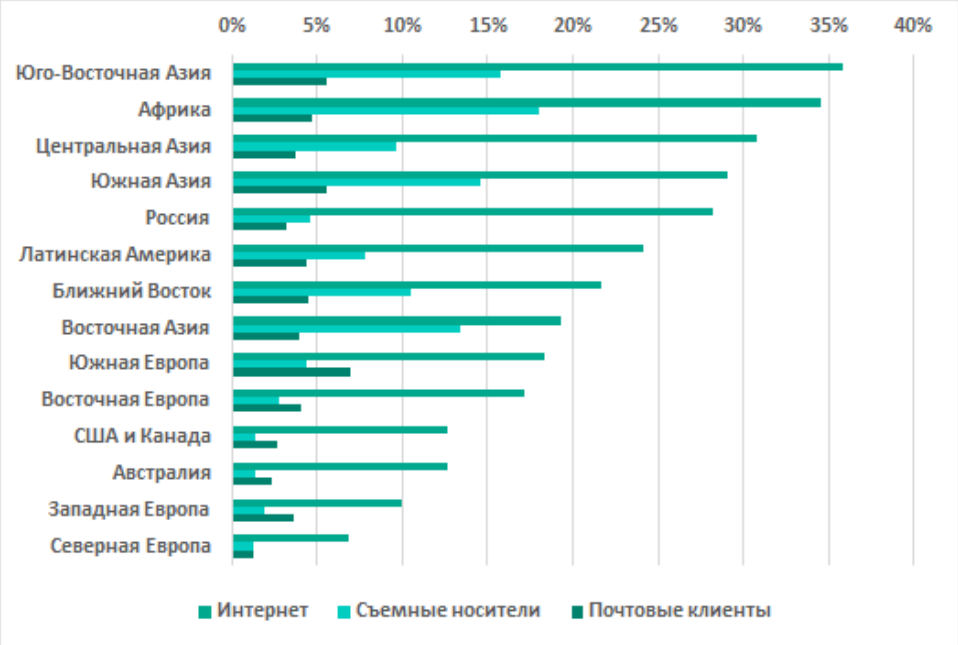
Минорные источники угроз, заблокированных на компьютерах АСУ*



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

Основные источники угроз: география

Основные источники угроз, заблокированных на компьютерах АСУ*, в регионах, второе полугодие 2019

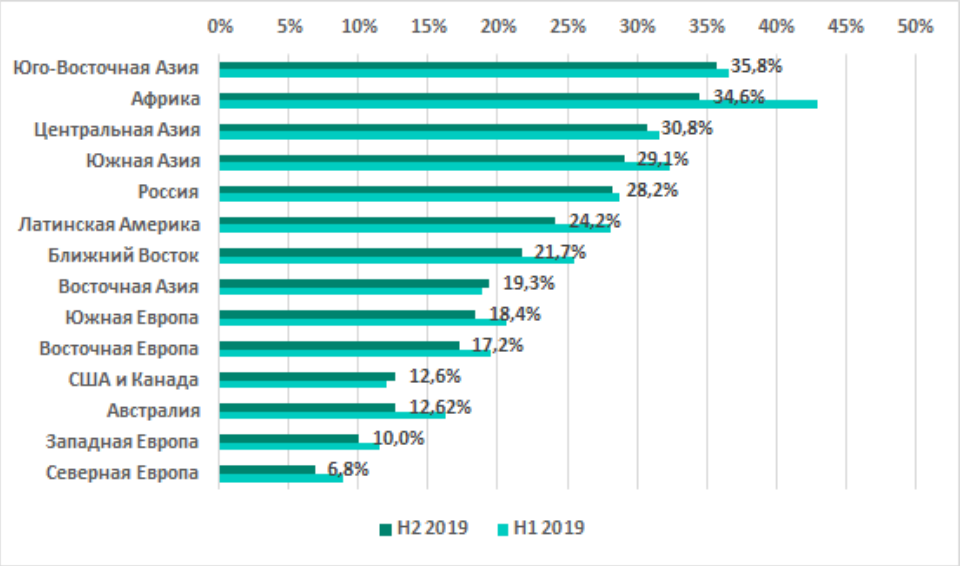


** процент компьютеров АСУ, на которых были заблокированы вредоносные объекты из различных источников*

Интернет

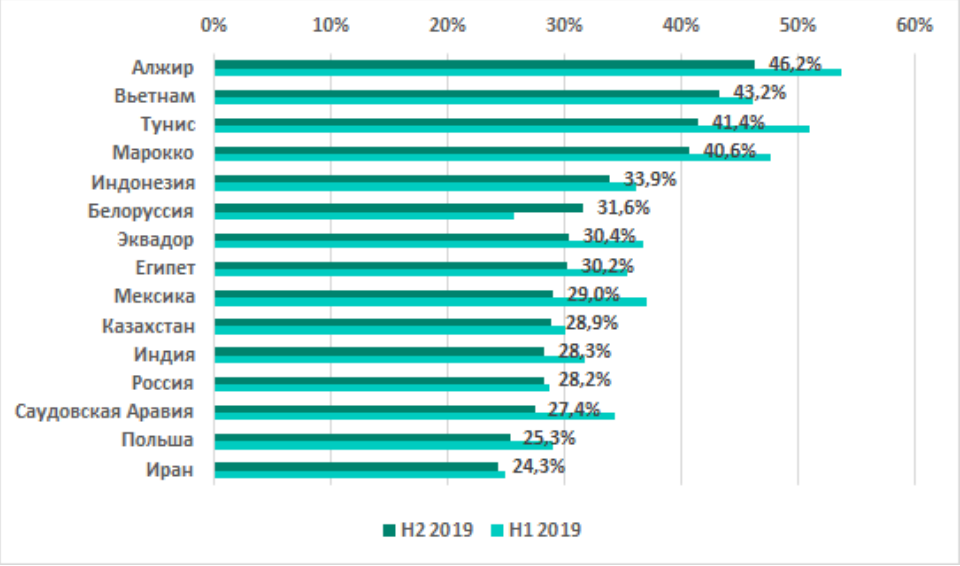
Во всех регионах мира основным источником угроз является интернет. Однако в Северной и Западной Европе и в Северной Америке процент компьютеров АСУ, на которых были заблокированы угрозы из интернета, значительно ниже.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2019



Большая часть стран, входящих в TOP 15 по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, по-прежнему в нем остаются. Покинули рейтинг Чили, Украина и Боливия, в списке их сменили Белоруссия, Россия и Иран.

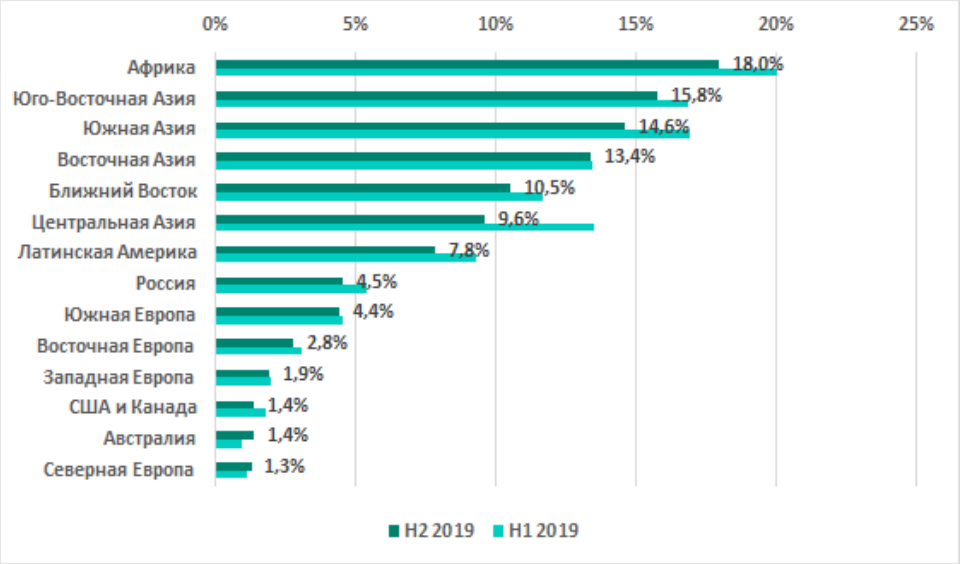
TOP 15 стран по проценту компьютеров АСУ, на которых были заблокированы угрозы из интернета, второе полугодие 2019



Съемные носители

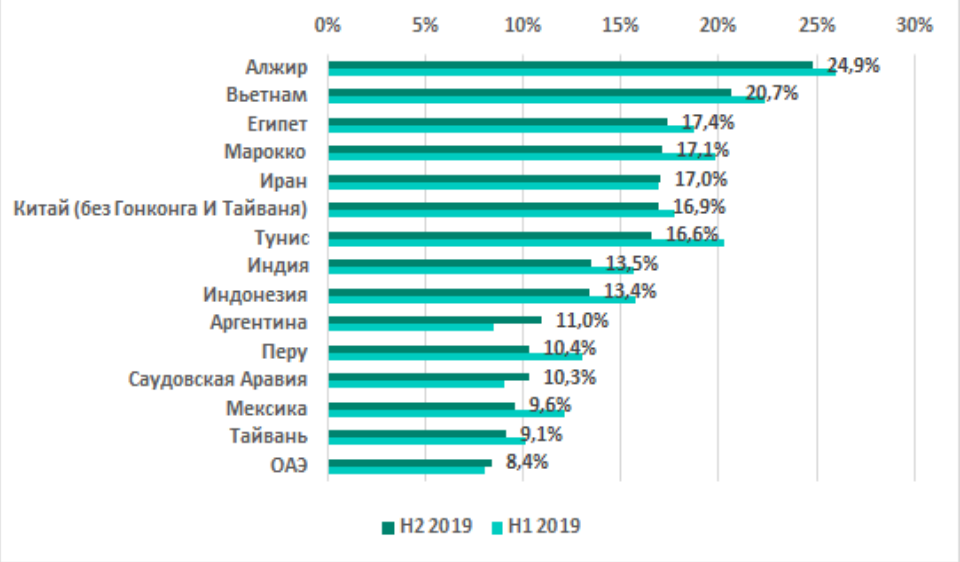
Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, остался без изменений. Максимальный процент компьютеров АСУ, на которых были заблокированы угрозы при подключении съемных носителей, отмечен в Африке, Южной и Юго-Восточной Азии. При этом в Австралии, Северной Европе и Северной Америке этот показатель – минимальный.

Рейтинг регионов по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2019



Во втором полугодии 2019 года в TOP 15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, вместо Турции, Казахстана, Таиланда и Боливии вошли Тайвань, Саудовская Аравия, Аргентина и ОАЭ.

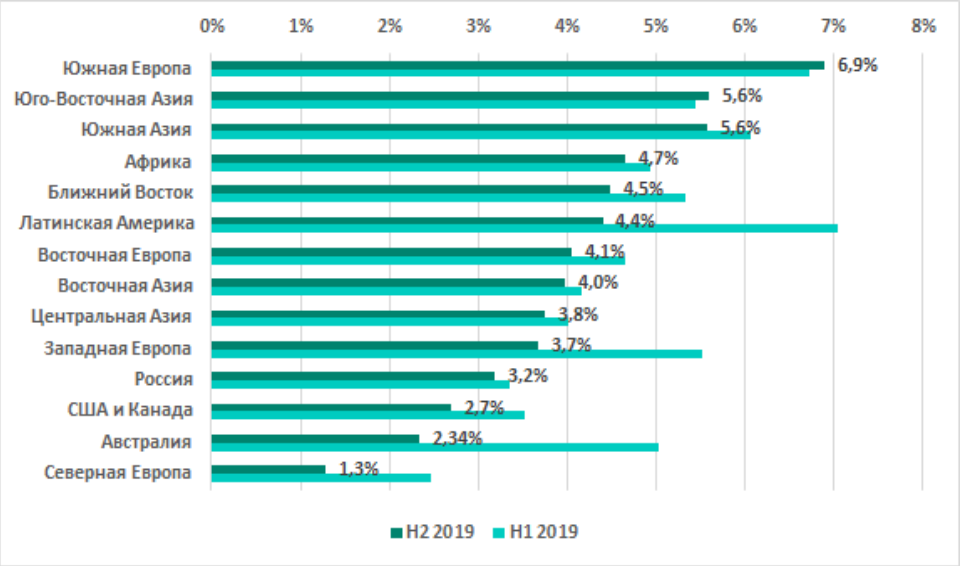
TOP 15 стран и территорий по проценту компьютеров АСУ, на которых было заблокировано вредоносное ПО при подключении съемных носителей, второе полугодие 2019



Почтовые клиенты

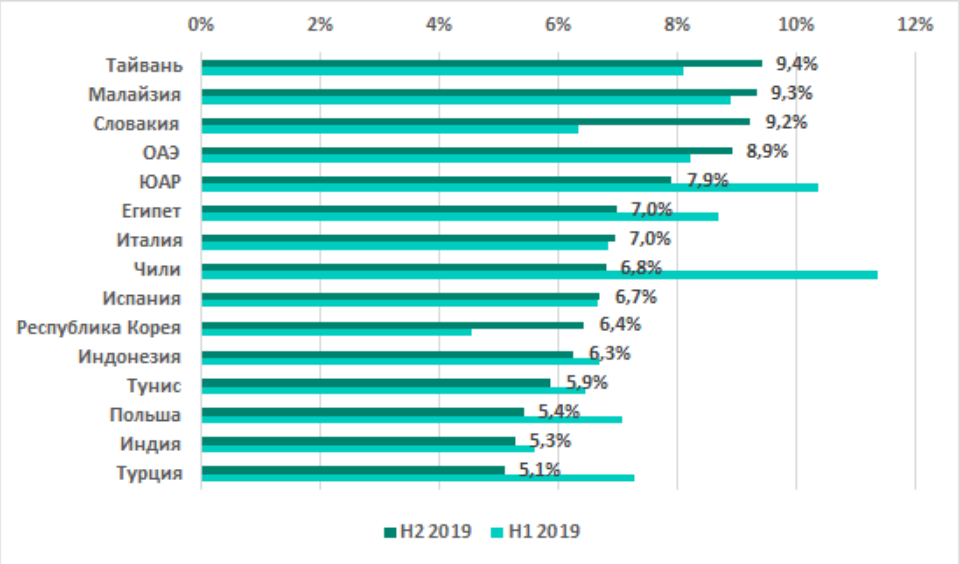
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, по итогам полугодия впервые возглавила Южная Европа.

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2019



Во втором полугодии 2019 года TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, обновился на треть.

TOP 15 стран и территорий по проценту компьютеров АСУ, на которых были заблокированы вредоносные почтовые вложения, второе полугодие 2019



Покинули TOP 15 Германия, Япония, Мексика, Аргентина и Эквадор. В него вошли Словакия, которая оказалась сразу на третьем месте, Испания, Южная Корея, Тунис и Индия.

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