Kaspersky ICS CERT

kaspersky

Киберугрозы для систем промышленной автоматизации в странах Средней Азии H2 2019

TLP: GREEN

23.04.2020 Version 1.0

Объект исследования

Компьютеры в странах Средней Азии, на которых стоят продукты «Лаборатории Касперского», используемые для конфигурирования, обслуживания и управления оборудованием систем промышленной автоматизации, а именно: компьютеры под управлением Windows, на которых установлены различные программные пакеты автоматизированных систем управления.

Отчетный период

Второе полугодие 2019 года

Краткие итоги

Всего в отчетный период в странах Средней Азии продукты «Лаборатории Касперского» заблокировали вредоносное ПО на 48,8% компьютеров АСУ.

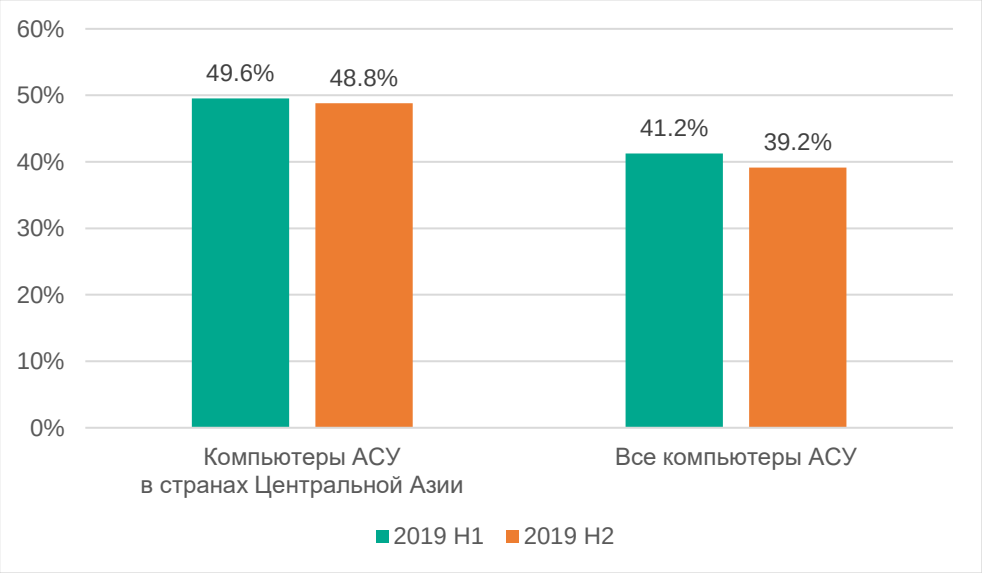
Было заблокировано 575 модификаций вредоносного ПО, относящихся к 266 различным семействам. Среди них особую опасность представляют различные самораспространяющиеся вредоносные программы – черви (6,8%), многофункциональные шпионские программы (4,3%), похищающие данные аутентификации и позволяющие злоумышленникам удаленно управлять зараженным компьютером в автоматическом и ручном режимах, а также программы-вымогатели (1,5%) и майнеры (4,1%), заражение которыми может оказать негативное влияние на доступность и целостность АСУ ТП и систем технологической сети.

Поверхность угроз для компьютеров АСУ в странах Средней Азии значительно больше, чем в среднем по миру. В частности, это относится к угрозам, распространяемым через интернет и съемные носители.

Данные об угрозах, заблокированных на компьютерах АСУ, указывают на недостаточность применяемых мер по защите сетевого периметра технологических сетей, а также на наличие высокой активности самораспространяющегося ПО в отдельных странах региона.

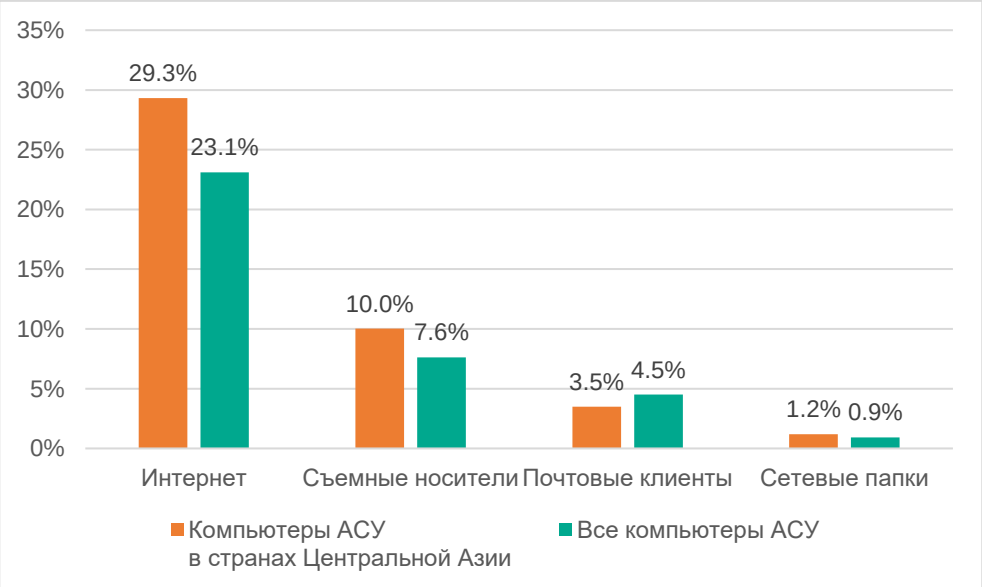
Статистика

В Средней Азии процент компьютеров АСУ, на которых было заблокировано вредоносное ПО во втором полугодии 2019 года (48,8%), сопоставим с аналогичным показателем за первую половину 2019 года (49,6%). При этом, по сравнению с аналогичными данными по всем компьютерам АСУ в мире, в Средней Азии этот показатель был выше на 8,4 п.п. в первом и на 9,6 п.п. во втором полугодии 2019 года.



Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

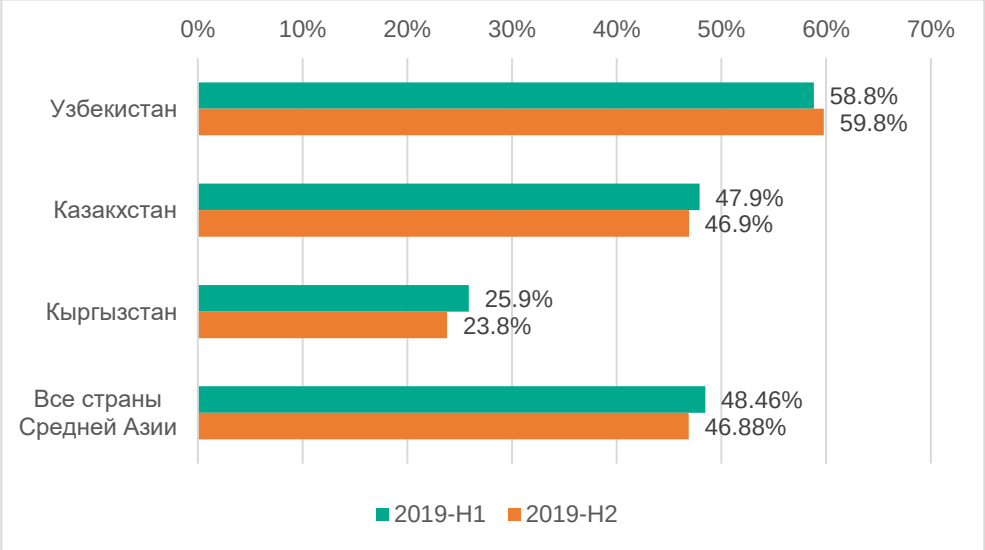
Сравнение данных об источниках угроз на компьютерах АСУ в Средней Азии и на всех компьютерах АСУ в мире показывают, что наибольшая разница в проценте компьютеров АСУ, на которых были заблокированы вредоносные объекты, связана с угрозами, проникающими через интернет и съемные носители. В то же время, компьютеры АСУ в Средней Азии реже сталкиваются с почтовыми угрозами, по сравнению со всеми компьютерами АСУ в мире.



Источники угроз* для компьютеров АСУ в Средней Азии и в мире, второе полугодие 2019 года

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

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в странах, которые оказывают наибольшее влияние на статистику по региону, различен. В Узбекистане он выше среднего показателя для региона. Для сравнения – в Киргизии данные показатель значительно ниже.

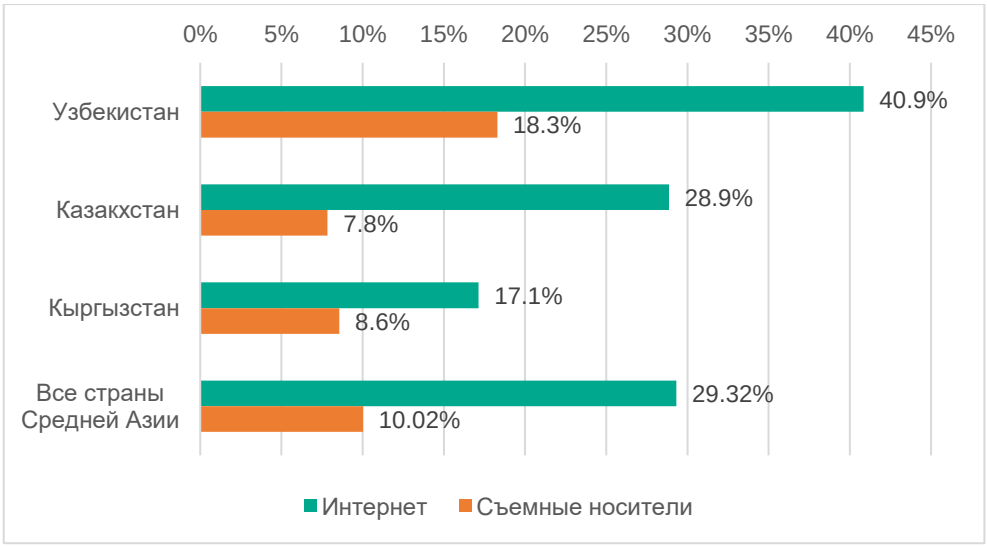


Процент компьютеров АСУ, на которых были заблокировны вредоносные объекты, в странах Средней Азии

Столь значительные различия в показателях обусловлены различиями в ландшафтах угроз для компьютеров АСУ в странах Средней Азии.

В частности, в Узбекистане процент компьютеров АСУ, столкнувшихся с угрозами в интернете во второй половине 2019, на 11,7 п.п. выше аналогичного показателя по региону, а с угрозами на съемных носителях – выше на 8,7 п.п.

В Казахстане процент компьютеров АСУ, столкнувшихся с угрозами в интернете, во втором полугодии 2019 сопоставим с аналогичным показателем по региону. В Киргизии компьютеры значительно реже сталкиваются с угрозами, распространяемыми через интернет. И в Казахстане, и в Киргизии процент компьютеров АСУ, сталкивающихся с вредоносным ПО на съемных носителях, ниже среднего показателя по региону и сопоставим с аналогичным показателем для всех АСУ в мире.



Источники угроз для компьюетров АСУ* в странах Средней Азии во втором полугодии 2019,

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

Угрозы из интернета

Большинство интернет-угроз, заблокированных на компьютерах АСУ в странах Средней Азии, были связаны с веб-сайтами, распространяющими вредоносное ПО под видом легитимных программ и медиа-контента (музыка, фильмы и пр.). В ряде случаев перенаправления на вредоносные сайты происходили с небезопасных легитимных веб-ресурсов (информационного и медийного содержания), которые использовали популярные JavaScript компоненты разработки веб-сайтов, размещенные на сторонних серверах (например, bootstrap.js, JQuery.js и пр). Заражение таких модулей на сторонних серверах, с которых они динамически загружались небезопасными сайтами, и позволило распространять вредоносное ПО, среди которого чаще всего встречались:

- шпионские программы (Glupteba, TrickBot)
- банковские троянцы (Emotet, Stealer.Generic)
- загрузчики рекламных модулей (Generic)
- майнеры (CoinMiner, Generci)

Реже сами легитимные веб-сайты были заражены вредоносными скриптами. Среди зараженных встречались веб-сайты промышленного характера (оборудование, материалы и пр.). В большинстве таких случаев вредоносное ПО было предназначено для скрытого майнинга криптовалюты в контексте браузера.

Высокий процент компьютеров АСУ, сталкивающихся с угрозами из интернета, указывает на недостаточность мер по защите периметра сети АСУ (наличие свободного доступа в интернет). Важно отметить, что мобильные рабочие станции, так же как и стационарные, входят в периметр сети и должны быть защищены. Защите мобильных устройств следует уделять даже больше внимания – возможность использования таких устройств вне физического периметра предприятия делает их наиболее частым вектором проникновения вредоносного ПО внутрь периметра промышленной сети.

Примеры индикаторов компрометации для описанных угроз представлены ниже и актуальны на момент выявления угрозы.

Адреса URL зараженных веб-ресурсов и ресурсов, использующих внешние JavaScript компоненты:

- irstar[.]kz/assets/components/tickets/js/web/default.js
- maksvel[.]kz/assets/templates/template/libs/jquery/jquery-2.1.3.min.js
- promanalyt[.]kz/assets/templates/default/js/jquery.min.js
- telon[.]kz/assets/templates/template_1/js/libs.min.js
- www.kr-elprof[.]ru/bitrix/js/main/public_utils.js
- www.trubotvod[.]ru/bitrix/js/main/core/core_loader.js
- www.trubotvod[.]ru/bitrix/js/main/public_utils.js
- opc-servers[.]ru/program/modbus-master

Адреса URL хостингов вредоносного ПО и майнинговых сервисов:

- 134.249.116[.]78/jquery.js
- wmtech[.]ml
- coinhive[.]com
- www.hostingcloud[.]racing/FACg.js
- citygame[.]xyz/app.exe

- enemyunknown[.]club/app/app.exe
- kktoade[.]pw/q/seescenicelfq.exe
- www.ydncg[.]pw/b/wyfdggb.exe
- 47.88.87[.]118

MD5 хеш суммы вредоносных объектов

- 1CAE0711ECCB3A109FB3FB29C3880A9D
- 0D204EA9A5F8EDB4F371EAF423193602
- 55A2F1238D77375191D46B8993378405
- FF3663D31C586A3B7B5BAE02E158FB33
- F64E527C35C182272D9D8BFC7520C8B2
- 84B89FD7569BB818342FAEB3E74EC14A

Полный список индикаторов компрометации доступен в отдельном IoC файле.

Угрозы на съемных носителях

Во второй половине 2019 года на съемных носителях, подключаемых к компьютерам АСУ в средней Азии, встречалось:

- шпионское ПО (в том числе бэкдоры и ботнет-агенты) с действующими серверами управления (TeviRat, Phorpiex)
- банковские троянцы (Emotet)
- майнеры (CoinMiner, Generic)

Отметим, что по-прежнему есть и компьютеры АСУ, зараженные старыми версиями вирусов и червей (таких как Kido и Sality), которые продолжают распространяться через съемные носители.

Примечательно, что распространяющиеся через съемные носители вредоносные майнеры также имеют модули для распространения по сети с использованием известной уязвимости MS-17-010.

Модификации шпионского ПО и программ-вымогателей, заблокированных на съемных носителях, также встречались в различных фишинговых рассылках, темы которых не специфичны для промышленных компаний (оплата счетов, доставка, и т.д.). Таким образом, вероятнее всего вредоносное ПО, проникнув на компьютеры в корпоративной сети через электронную почту, заражало съемные носители, которые впоследствии использовались на компьютерах АСУ в промышленной сети.

Очевидно, что классы угроз (т.е. шпионсое ПО, вымогатели и майнеры), распространяемых через съемные носители, а также высокий процент компьютеров АСУ, сталкивающихся с этими угрозами, указывает на недостаточность мер защиты систем промышленной автоматизации. Не только неконтролируемое использование съемных носителей, но и наличие в течение длительного времени в инфраструктуре компьютеров, зараженных вредоносным ПО (скорее всего, ввиду отсутствия адекватных мер антивирусной защиты и контроля за состоянием защищенности), способствуют распространению вредоносного ПО в сети промышленной автоматизации и подвергают системы АСУ риску отказа в обслуживании.

Адреса URL C&C и майнинговых сервисов:

- coinhive[.]com
- sasakiguitarschool[.]com
- zugzdwl[.]ua/single.php
- 185.176.27[.]132

MD5 хеш суммы вредоносных объектов

- 3AFEB8E9AF02A33FF71BF2F6751CAE3A
- CCEDB6A05639FF5CA2D1DD67581D4EDE
- D80462A8FD80ECC99F6F45C4FAD1BAFA
- 0BCF08501969A9BBC7E7C2E32FD90A19
- 4962CB536D87973BD61402C75A7E95FA

Полный список индикаторов компрометации доступен в отдельном IoC файле.

Рекомендации

Для обеспечения адекватной защиты систем АСУ необходимо:

- Убедиться, что организация хорошо защищена от фишинговых атак, включая целевые атаки, в частности, при помощи современных технологий обнаружения фишинга – как на уровне сетевого периметра / сервера электронной почты, так и на всех конечных точках внутри периметра (или, по крайней мере, на всех компьютерах, где разрешена электронная почта).
- Регулярно обучать сотрудников, как распознать подозрительные сообщения электронной почты и вложения.
- Использовать технологии sandbox для проверки всех новых файлов, обнаруживаемых на компьютерах в сети, особенно – файлов на съемных носителях, вложений электронной почты и файлов, загружаемых из интернета.
- Использовать и регулярно обновлять системы обнаружения вредоносных URL и IP-адресов;
- Максимально ограничить использование SMB на компьютерах АСУ, разрешать использование SMB только с ограничениями доступа и только в случаях, когда это абсолютно необходимо. Постоянно контролировать использование SMB и проверять предоставляемый доступ на соответствие требованиям политики безопасности.
- Настроить ОС так, чтобы всегда отображались расширения файлов для всех типов файлов.
- Своевременно устанавливать ОС и все обновления программного обеспечения приложения, уделяя особое внимание обновлениям безопасности, или применять обходные меры защиты, когда установка обновлений невозможна. Убедиться в том, что уязвимости MS-17-010, CVE-2017-2636 и CVE-2018-14847, широко используемые вредоносными программами на компьютерах ICS, исправлены на всех инфраструктурах АСУ и корпоративных сетей.

- Убедиться, что на всех компьютерах в организации правильно настроено и запущено антивирусное программное обеспечение.
- Обеспечить своевременную установку обновлений баз и программных модулей для антивирусного программного обеспечения и других решений безопасности.
- Контролировать использование программ на системах АСУ, в частности, – использовать контроль приложений.
- Использовать разные учетные записи для разных пользователей. Управлять правами учетных записей пользователей и служб таким образом, чтобы предотвратить распространение инфекции по всему предприятию в случае взлома учетной записи. Вести журнал событий и контролировать использование функций администратора.
- Ограничить права пользователей в системах, которые они используют, а также права доступа к корпоративным услугам: оставить минимальный набор прав, требуемый для выполнения определенной работы определенными сотрудниками.
- Максимизировать гранулярный контроль доступа. Ограничить использование привилегированных учетных записей. Когда это возможно, администраторы должны использовать учетные записи с правами локального администрирования или с правами администратора для определенных служб и избегать использования учетных записей с правами администрирования домена.
- Проверять использование привилегированных учетных записей и регулярно проверять права доступа.
- Использовать групповые политики, которые требуют, чтобы пользователи регулярно меняли свои пароли. Ввести требования к надежности пароля.

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