Кого обесточат на этот раз?

В ожидании следующего «кибер-блэкаута»

Авторы

Даниэль Тривеллато, руководитель по разработке решений для промышленных систем

Деннис Мёрфи, старший инженер по безопасности ICS

4 февраля 2016 г.

Оглавление

Введение

23 декабря 2015 года впервые в истории крупная кибератака на критическую инфраструктуру одной из стран затронула значительную часть её населения. По сообщениям нескольких источников [1, 5], сотни тысяч жителей Ивано-Франковской области в течение приблизительно шести часов оставались без электричества.

Исследователи и аналитики крупных компаний, занимающихся защитой от кибератак, проводят сейчас детальный разбор данного инцидента [1, 5, 2, 4, 8, 7]. Несмотря на то, что на многие вопросы пока нет ответов, все аналитики сходятся во мнении о том, что отключение электроэнергии стало результатом целенаправленной, хорошо скоординированной атаки хакеров на ряд энергоснабжающих предприятий Украины.

В данной статье изложены результаты расследования инцидента по состоянию на текущий момент и обсуждаются возможности своевременного обнаружения ключевых элементов атаки при условии оснащения основных участков сетей электроснабжения механизмами мониторинга состояния сети.

Скоординированная атака на энергосеть Украины

Начнем анализ атаки на энергосеть Украины с разбора случившегося 23 декабря 2015 года. Между 15:35 и 16:30 по местному времени

было совершено проникновение в ИКТ-инфраструктуру украинского «Киевоблэнерго». Злоумышленникам удалось отключить семь подстанций 110 кВ и двадцать три подстанции 35 кВ, в результате чего около 80000 потребителей различных категорий остались без электроснабжения. «Киевоблэнерго» сообщило о взломе на страницах своего сайта (Рис. 1).


12/242015

Уважаемые клиенты!

23 декабря 2015 года в промежутке между **15:35 и 16:30** посторонними лицами было совершено незаконное проникновение в информационно-технологическую систему удаленного доступа телеуправления оборудованием подстанций 35-110 кВ ОАО «Киевоблэнерго».

В результате было отключено семь подстанций 110 кВ и 23 подстанциии 35 кВ. Это привело к тому, что около 80000 потребителей различных категорий остались без электроснабжения.

Подача электроэнергии была полностью восстановлена в **18:56** того же дня.

Мы приносим свои изменения за инцидент и благодарим вас за понимание.

ОАО «Киевоблэнерго»

Рис. 1. Сообщение о взломе на сайте «Киевоблэнерго».

Согласно информации на сайте компании энергоснабжение было полностью восстановлено три часа спустя, в 18:56 по местному времени. В очередном новостном сообщении «Киевоблэнерго» сообщило также о техническом сбое в работе своего колл-центра, в результате которого потребители не могли связаться с сотрудниками предприятия в течение периода действия блэкаута (Рис. 2).

Одновременно с атакой на сети «Киевоблэнерго» наблюдались проблемы и в работе других украинских предприятий энергоснабжения. В отчете, опубликованном TrendMicro [5], сообщается о том, что атаке хакеров подверглись два других предприятия. А в отчетах SANS ICS [2] и ESET [1] (компании-разработчика ПО для защиты сетей из Братиславы) в частности была упомянута компания «Прикарпатьеоблэнерго».

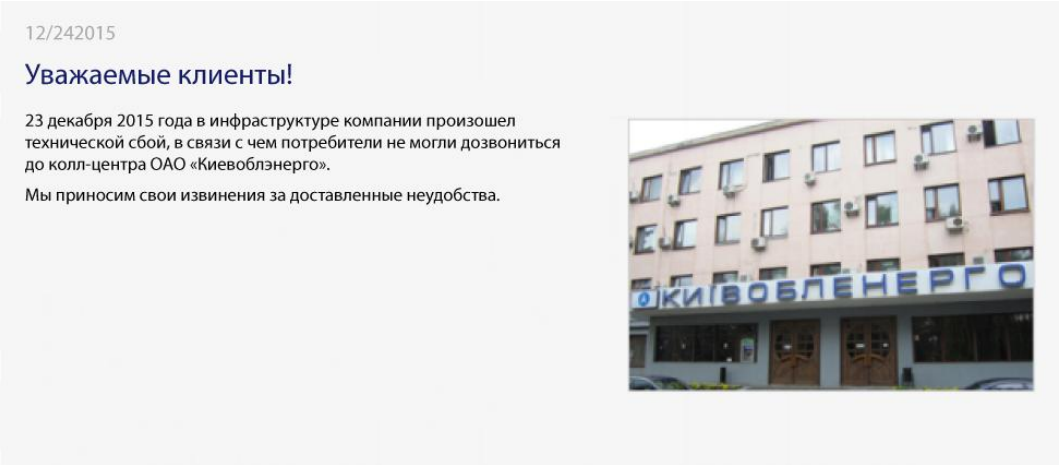

Рис. 2. Информационное сообщение о проблемах с колл-центром «Киевоблэнерго».

Согласно отчету ESET [1], от блэкаута пострадало около 700000 человек в Ивано-Франковской области Украины (половина местного населения). TrendMicro [5] сообщает о «сотнях тысяч» домов, пострадавших в результате атаки, не приводя точной цифры.

Две фазы атаки

Пока преждевременно говорить о том, как именно развивалась атака. При этом все специалисты, занимающиеся анализом данного инцидента, в один голос заявляют о том, что блэкаут стал результатом превосходно скоординированных действий. Согласно отчету SANS ICS [2], атака включала в себя как минимум три компонента:

- **Вредоносная программа**, которая вероятно открыла злоумышленникам доступ к сети и вывела из строя SCADA-систему объектов нападения с целью замедлить процесс восстановления работоспособности и «запутать следы». Для взлома была использована модификация вредоносного ПО, нацеленная на вывод из строя именно промышленных систем [1, 8].
- Атака на колл-центр коммунальных предприятий типа «**отказ в обслуживании**», в ходе которой злоумышленники блокировали инфраструктуру объектов нападения, чтобы потребители не смогли сообщить о проблеме.
- **Отключение автоматического оборудования** подстанций с целью отключения подачи электроэнергии. Этот компонент пока является наиболее загадочным элементом головоломки. Скорее всего отключение автоматических выключателей произошло в результате прямой команды хакеров, а не действия вредоносной программы, обнаруженной в сетях объектов нападения.

Эти компоненты были тщательно подготовлены и планомерно реализованы хакерами с целью нанести как можно больший ущерб электрораспределительной системе Украины. Возможный сценарий действий хакеров:

1. Злоумышленники смогли разместить вредоносное ПО на главных серверах управления электрораспределительной системы «Киевоблэнгерго» и двух других предприятий.
2. Они преодолели сетевую защиту объектов нападения (предположительно посредством бэкдора) и дали команду на отключение автоматических выключателей различных подстанций.
3. Задачей вредоносной программы было «ослепить и парализовать действия» персонала предприятий энергоснабжения, т.е. скрыть от них и не дать им отреагировать на запущенную хакерами команду, блокировав функции перезапуска некоторых основных служб системы SCADA.
4. Злоумышленники организовали атаку на колл-центр типа «отказ в обслуживании», чтобы не позволить потребителям сообщить о последствиях действий хакеров.

Принимая во внимание сложившуюся ситуацию, специалисты подвергшихся атаке предприятий сумели достаточно оперативно восстановить подачу электроэнергии потребителям. Так как они не могли управлять процессом дистанционно посредством своей SCADA-системы, чтобы восстановить энергоснабжение, им пришлось выезжать на соответствующие подстанции и вручную включать прерыватели. Какое-то время после инцидента предприятия работали в «аварийном режиме», поскольку SCADA-система оставалась инфицированной.

Роль вредоносного ПО

В данном разделе мы излагаем результаты анализа вредоносного ПО, обнаруженного в сетях предприятий-объектов нападения, и его роль в атаке. Согласно отчетам ESET [1] и TrendMicro [5], внутренние сети коммунальных предприятий были заражены вредоносным ПО BlackEnergy посредством электронных писем, содержащих вложение с электронной таблицей Microsoft Excel с макросами (Рис. 3). Активированный макрос загрузил соответствующие компоненты вредоносного ПО на зараженные машины. Для удаления данных с SCADA-серверов предприятий использовалась утилита **KillDisk**. Ниже представлена выдержка из отчета ESET [1]:

«Впервые информация о связи BlackEnergy и KillDisk появилась в отчете украинского агентства по кибербезопасности CERT-UA в ноябре 2015 года. Тогда в ходе местных выборов 2015 атаке подверглось несколько компаний-представителей СМИ. В отчете сообщается о том, результатом атаки стало уничтожение большого количества видеоматериалов и различных документов».

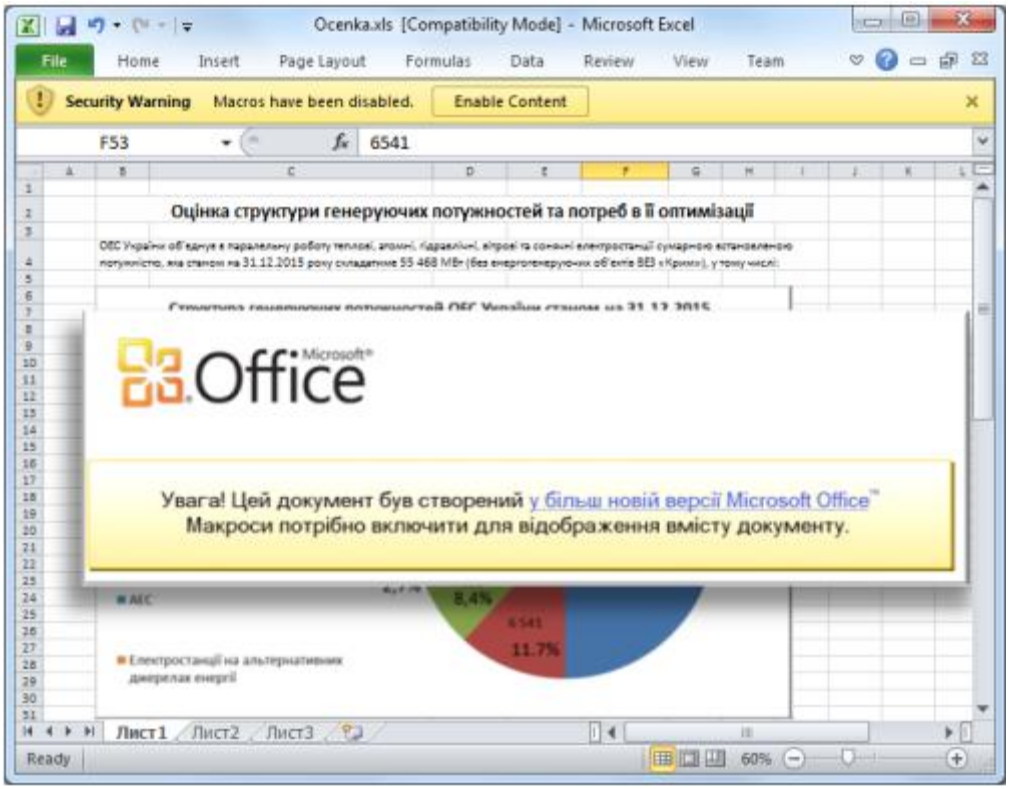

Рис. 3. Зараженный документ Microsoft Excel с активированными макросами [9]

С подробным анализом KillDisk можно ознакомиться в отчете Symantec [8]. Там сообщается о том, что KillDisk (обнаруженный специалистами Symantec троян Trojan.Disakil) считается крайне разрушительным модульным трояном, который полностью выводит из строя зараженную систему путем перезаписи главной загрузочной записи и других ключевых файлов. Но что самое интересное, оказалось, что троян, проникший в систему украинских коммунальных предприятий, содержал код, созданный для атаки именно на промышленные системы. В частности, KillDisk данной модификации

«пытается остановить и удалить службу sec_service. Данная служба относится к ПО Serial to Ethernet Connector, разработанному компанией Eltima. Эта программа обеспечивает дистанционный доступ к последовательным портам по сетевым соединениям. Во многих унаследованных SCADA-системах для связи с дистанционными терминалами до сих пор используются последовательные порты. [...] Если злоумышленники знали, что предприятие использует данное ПО для связи с унаследованными SCADA-устройствами, остановка службы и блокировка линии связи увеличили бы ущерб его системам.»

Тщательный анализ образца вредоносной программы, проведенный SentinelOne [7], показывает, что помимо удаления данных, утилита может перехватывать трафик от сетевых интерфейсов зараженных машин, в т.ч. беспроводных адаптеров. Все собранная информация направляется на командный сервер злоумышленников посредством HTTP-сообщений.

Несмотря на полученные результаты, точную роль и влияние вредоносного ПО во взломе еще предстоит подтвердить. SANS ICS [1] сообщает, что помимо тех исследователей, которые считают, что атака была реализована

исключительно с помощью BlackEnergy и KillDisk, существует мнение о том, что возможно вредоносное ПО, обнаруженное во внутренних сетях коммунальных предприятий, не связано с блэкаутом (т.е. оно там уже было на момент атаки). SANS ICS придерживается мнения, что: вредоносное ПО лишь дало возможность провести атаку, оно не было ее непосредственным инструментом. Данное ПО позволило хакерам получить доступ к внутренним сетям предприятий и было использовано для вывода из строя SCADA-серверов после атаки. При этом подача электроэнергии была остановлена именно посредством команды, т.е. в результате отключения нескольких автоматических выключателей на подстанциях в течение короткого временного интервала, **вручную запущенной** самими злоумышленниками.

Определение злоумышленников

Мнения аналитиков о том, кто стоит за этой кибератакой, расходятся. Служба безопасности Украины сразу же заявила о причастности России. Такого же мнения придерживаются аналитики компании iSIGHT Partners [4]. Данное мнение основывается главным образом на наличии в сетях подвергшихся нападению украинских предприятий трояна BlackEnergy. За BlackEnergy стоит группировка российских хакеров **Sandworm**, «отличившаяся» атаками на предприятия Украины, некоторых западных стран, и компании энергетического сектора [4, 8]. В отчете SentinelOne [7] Россия напрямую не упоминается, однако аналитики этой компании уверены, что эта последняя модификация вредоносного ПО является плодом деятельности лиц, имеющих поддержку со стороны государственных структур, и «возможно результатом объединенной работы нескольких команд».

Другие аналитики более осторожны в своих оценках причастности к инциденту известных и поддерживаемых государством группировок. Например, SANS ICS в своих отчетах однозначно заявляет [2, 3] о том, что пока еще слишком рано делать выводы о причастности BlackEnergy к кибератаке. Кроме того, в своей рассылке SCADASEC Рей Паркс (Ray Parks) [6] уделяет особое внимание установлению исполнителей атаки. В своем анализе господин Паркс отмечает, что атаки, организованные при поддержке государства, как правило нацелены на решение очень «масштабных» (например, червь Stuxnet, запущенный, чтобы замедлить ход реализации иранской ядерной программы) или узких стратегические задач (напр., вывод из строя критической РЛС). От декабрьской атаки больше всего пострадали украинские предприятия энергетической отрасли, расположенные в западной части Украины. Поэтому маловероятно, что атака была элементом решения стратегических (военных) задач. На основании этого Рей Паркс делает вывод о том, что скорее всего атака была проведена группировкой, имеющей «определенную» господдержку (что подтверждается использованием специальных инструментов), которая тем не менее действовала самостоятельно, исходя из личных мотивов.

Можно ли было предотвратить атаку?

Ответ: наверное, нет. Тем не менее, некоторые признаки атаки и действия злоумышленников можно было обнаружить на более раннем этапе. Так, например антивирусные программы и системы защиты от взлома, такие как системы Symantec [8] уже имеют сигнатуры, способные обнаруживать вредоносный компонент KillDisk. При этом не факт, что они смогли бы выявить конкретную модификацию трояна, использованного на западе Украины.

А вот две фазы атаки несомненно можно было обнаружить. Это: (a) передача данных, полученных в результате перехвата трафика, от зараженных машин на командный сервер злоумышленников; и (b) действие, предпринятое хакерами до дистанционного отключению автоматических выключателей на подстанциях, которое непосредственно вызвало отключение энергоснабжения. Обнаружить их можно было бы, если бы на предприятиях использовалась платформа сетевого мониторинга SilentDefense компании SecurityMatters, которая в реальном времени оповещает о действиях, способных угрожать стабильному выполнению технологических процессов.

SilentDefense

SilentDefense – интеллектуальная контрольно-аналитическая платформа, применяемая операторами критически-важных инфраструктурных объектов по всему миру для защиты своих ICS/SCADA-сетей. SilentDefense осуществляет текущий мониторинг и анализ сетевого трафика, сопоставляет данные с параметрами допустимых/желательных операций и с известными проблемами, описание которых находится в библиотеке данных о промышленных угрозах компании SecurityMatters, и оповещает о проблемах и угрозах для сетей и процессов ICS/SCADA. Некоторые примеры:

- Попытки проникновения извне и состоявшееся проникновение
- Устройства с аномальным поведением и с ошибками в конфигурации
- Подозрительные технологические операции
- Эксплуатационные ошибки
- Известные атаки и атаки нулевого дня

Эти угрозы фиксируются и представляются оператору в двух основных форматах:

- **Наглядная аналитика**: Графическое представление всех аспектов сети посредством различных схем и диаграмм (см. рис. 4). Данные схемы и диаграммы позволяют отслеживать наиболее важные аспекты текущей сетевой активности. Все настройки доступны для изменения. Платформа наглядной аналитики работает на базе исчерпывающего хранилища данных, благодаря чему оператор может в любой момент времени проконтролировать интересующие его параметры сети, увидеть, что сейчас происходит, выявить признаки аномальной сетевой активности, а также проследить, что произошло ранее (напр., в отношении подозрительного события).
- **Оперативные оповещения**: Как только в сети происходит какое-то нештатное событие, SilentDefense направляет оператору уведомление и предоставляет ему данные, необходимые для принятия соответствующих мер. Сюда входит информация об источнике проблемы, список устройств, затронутых проблемой, характер проблемы (напр., неизвестное устройство внезапно начинает обмениваться данными с устройствами на объектах, SCADA-сервер направляет подозрительную команду, устройства на объектах перестают отвечать или выдают нетипичные значения, и т.п.) и даже захват трафика, имеющего отношение к событию. Последний тип уведомлений имеет ключевое значение в случае изощренных атак, таких как атаки нулевого дня, когда полученные данные трафика можно переслать поставщикам систем компьютерной защиты, таким как Symantec, McAfee, и т.п., и может стать основой для последующего анализа.

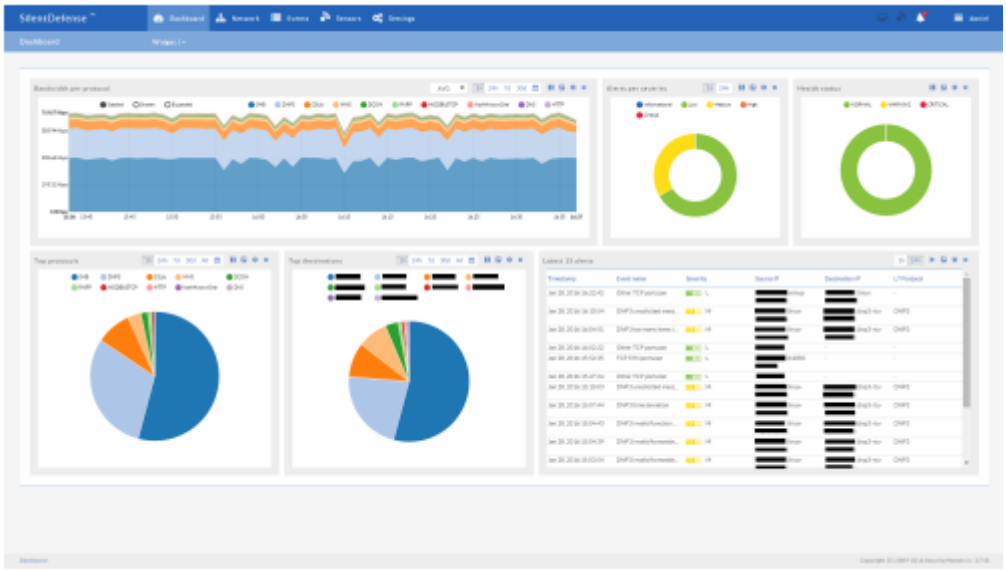

Рис. 4. Инструментальная панель SilentDefense имеет ряд заранее настроенных виджетов

Платформа SilentDefense доказала свою эффективность в предотвращении попыток взлома и обнаружении проблем, связанных с ICS/SCADA, в ходе эксплуатации на объектах ряда клиентов. Два последних примера проблем, выявленных в ходе эксплуатации системы у наших клиентов: успешное обнаружение взлома сети нашего клиента (к чему привело неправильное конфигурирование сетевого экрана), когда злоумышленники были выявлены во время передачи на сервер SCADA искаженных протокольных сообщений, и выявление угрозы вывода из строя электросети крупного города в результате неправильной настройки устройств, которая не была обнаружена системой SCADA.

Обнаружение атаки на украинские предприятия

SilentDefense использует различные дополнительные механизмы обнаружения для выявления вышеописанных проблем и угроз. В частности:

- **Встроенные модули обнаружения** для выявления атак на ранних этапах (напр., сканирование портов или выявление вмешательства в соединение) и проверки протоколов на соответствие.
- Автоматически создаваемые **коммуникационные схемы** для определения допустимых сетевых устройств, шаблонов взаимодействия, протоколов и команд и обнаружения присутствия неизвестных сетевых устройств, небезопасных протоколов и подозрительных операций.
- Автоматически генерируемые **схемы протоколов** для определения желательных технологических операций и выявления подозрительных отклонений в последовательности технологических операций.
- **Информационная база**, состоящая из библиотеки данных о промышленных угрозах, позволяет конфигурировать обязательные проверки сети на лету (напр., обнаружение клапанов, открытых в то время, когда они должны быть закрыты, проверка, чтобы, когда определенной разъединитель подстанции был отключен, другой в это время был включен, и т.д.)

Благодаря оперативному анализу сетевого трафика и сопоставлению текущего трафика с ранее утвержденными коммуникационными схемами, SilentDefense сразу же обнаружила бы факт обмена данными между зараженными машинами и командным сервером хакеров и оповестила об этом. В частности, система уведомила бы персонал украинских предприятий об обмене данными между локальным сервером и неизвестным внешним устройством (рис. 5) Можно, конечно, утверждать, что угрозы такого рода предотвращаются существующими сетевыми экранами и системами защиты от взлома. Однако, мы в нескольких случаях наблюдали, что эти системы были неправильно настроены, либо им не уделялось должного внимания.

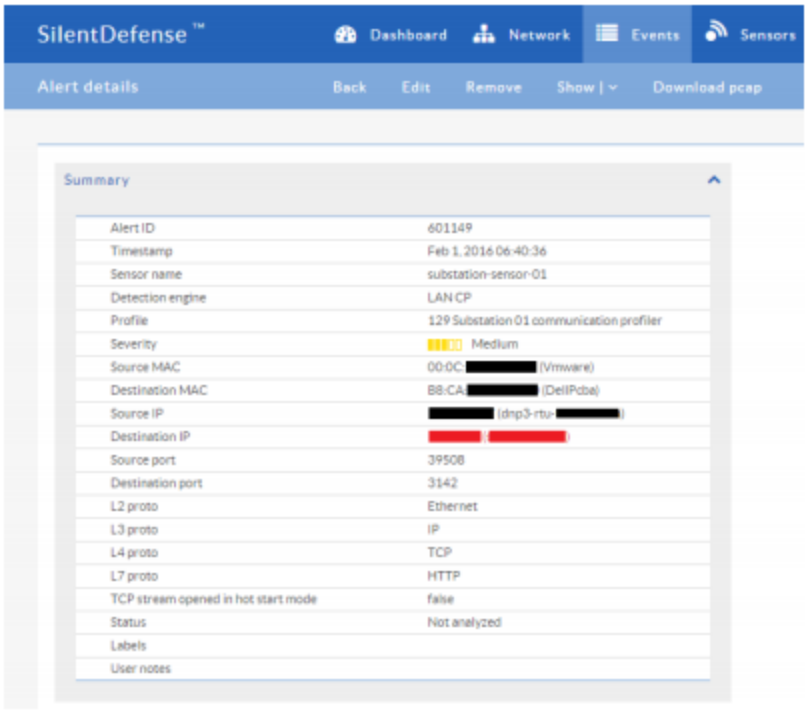

Рис. 5. Оповещение, генерируемое в случае несанкционированного обмена данными с неизвестным устройством

Однако наиболее актуальным механизмом SilentDefense для данной цели является информационная база. Данный механизм доказал свою эффективность в обнаружении большого количества проблем в сетях наших клиентов. Библиотека данных о промышленных угрозах SecurityMatters является базой знаний и практического опыта, полученного из предыдущих реализаций системы, которые учитываются в ходе мониторинга сетевой активности с уведомлением оператора о любых отклонениях от штатной ситуации.

Одна из проверок по библиотеке данных о промышленных угрозах **сразу же выявила и оповестила бы о том, что хакеры** пытаются отключить автоматические выключатели на подстанциях. Данная проверка была реализована после запроса клиента сообщить, когда их автоматизированная система обнаружения неисправностей даст сбой, после чего она была внедрена повсеместно, при этом она обеспечивала отработку в том числе той ситуации, которая как раз возникла на Украине. На самом деле система обнаружения неисправностей действовала бы так же, как и злоумышленники, взломавшие энергосеть Украины, т.е. она бы за короткое время отключила/включила прерыватели ряда подстанций. На рис. 6 показан пример оповещения, генерируемого по результатам проверки.

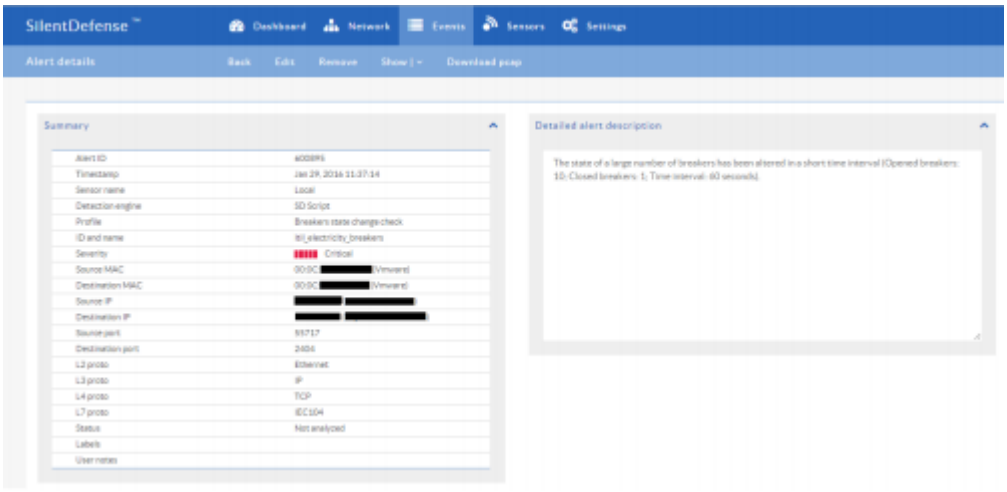

Рис. 6. Оповещение, генерируемое когда состояние нескольких прерывателей изменяется за короткое время

Обратите внимание: здесь мы предполагаем наиболее вероятный вариант действий, когда хакеры с удаленной рабочей станции направляют команду на отключение автоматических выключателей на всех подстанциях. Если предположить менее вероятную ситуацию, например, что хакеры подключаются к соответствующим подстанциям и последовательно отключают автоматические выключатели, SilentDefense в любом случае оповестила бы о присутствии подозрительных подключений к устройствам на объектах, так же как она бы оповестила об обмене данными с командным сервером злоумышленников (рис. 5).

Как было сказано во вступительной части данного раздела, скорее всего даже при своевременном обнаружении действий хакеров, это не смогло бы предотвратить отключение электричества. Тем не менее, диспетчеры имели бы всю информацию, необходимую для оперативного установления причины отключения электроснабжения и определения, какие именно подстанции поверглись атаке, что позволило бы незамедлительно направить специалистов на объекты для проведения восстановительных работ. Кроме того, при наличии системы мониторинга состояния сети, такой как SilentDefense, украинские коммунальные предприятия не оказались бы в полном неведении о том, что происходит в их сетях, даже после выхода из строя системы SCADA.

Выводы и рекомендации

Украинский инцидент стал первым случаем кибератаки на операторов объектов критической инфраструктуры, в результате которой пострадало гражданское население. До этого возможность такого сценария допускалась лишь в теории. Несмотря на своей небольшой масштаб, инцидент показал, что злоумышленникам вполне по силам нанести серьезный удар по экономике и энергобезопасности целой страны. Наибольшую озабоченность вызывает факт, что операторы объектов критической инфраструктуры не уделяют должного внимания вопросам защиты сетей ICS/SCADA, возможно не вполне осознавая, что помимо очевидных преимуществ, четвертая промышленная революция принесла с сбой множество угроз.

Думая о том, что следует сделать следующим этапом, мы соглашаемся с мнением, изложенным в последнем отчете SANS ICS [3]: Объекты ICS во всем мире должны **усилить свою защиту**, и в частности свои возможности по мониторингу сетей ICS/SCADA и реагированию на угрозы. Прежде всего, в каждой организации должны формироваться команды специалистов, обладающих необходимыми навыками и знаниями, позволяющими провести быстрый анализ подозрительной активности и принять соответствующие меры, и разработать четкую схему действий с указанием, к кому обращаться за помощью в случае усугубления проблемы. Во-вторых, такие команды должны быть оснащены необходимыми инструментами, осуществляющими мониторинг состояния сети и оповещающими о любой подозрительной активности. Использование стандартных решений защиты для этой цели не поможет. Возможность обнаружения целенаправленных атак на ранних стадиях их реализации обусловлена внедрением решения, ориентированного именно на ICS/SCADA, такого как SilentDefense.

Отзывы

Фрэнк из американской компании-независимого системного оператора:

«Мы обнаружили ошибки в конфигурации, что напрямую влияло на чистую прибыль. Таким образом, SilentDefense окупалась уже за первые несколько дней работы.»

Джери из крупной компании-интегратора систем защиты АСУТП:

«Система защиты и мониторинга технологических процессов должна быть способной адаптироваться к быстрым изменениям, должна быть самодостаточной и быстро и незаметно для пользователя приносить результаты. SilentDefense обеспечивает все это нашим клиентам.»

О компании SecurityMatters

SecurityMatters – международная компания, работающая в сфере защиты критически-важных объектов и систем промышленной автоматизации. Платформа мониторинга состояния сети SilentDefense ICS в течение нескольких лет находится в эксплуатации у клиентов из разных стран, защищая их сети от все новых киберугроз.

Об авторах

Даниэль Тривеллато Даниэль Тривеллато в 2012 году получил степень доктора философии по компьютерной безопасности в Технологическом университете Эйндховена. При подготовке к защите работал в тесном сотрудничестве с Thales Netherlands над разработкой и внедрением системы контроля доступа для защиты конфиденциальных данных в динамических распределенных системах. В 2012 году Даниэль пришел в компанию SecurityMatters на должность руководителя проекта. В его обязанности входило: маркетинг и сбыт, работа с клиентами и подготовка и реализация проектов внедрений систем в компаниях клиентов. С 2014 года Даниэль является ответственным за развитие и коммерциализацию линейки продуктов для промышленных систем управления.

Деннис Мёрфи Деннис Мёрфи – старший инженер по компьютерной безопасности в Security Matters. Он 12 лет занимался проектированием, разработкой и внедрением систем SCADA и ICS и 10 лет работал в области компьютерной защиты сетей критически-важных инфраструктурных объектов. Господин Мёрфи руководил проведением ряда испытаний безопасности систем SCADA в Национальных лабораториях Айдахо во время своей работы в должности руководителя программ в подразделении компании BAE Systems, занимающемся вопросами киберзащиты, расположенном в г. Мерримак, НГ. Во время своей работы в компании-дистрибьюторе Wonderware в Новой Англии он занимался проектированием, установкой и поддержкой десятков различных систем SCADA для компаний из следующих отраслей: энергетика, водоснабжение, биофармацевтика, нефть и газ, пищевая и бумажная промышленности. Он защитил степень магистра по системотехнике в Университете Джона Хопкинса. Является членом бостонского филиала программы партнерства между ФБР и частным сектором,.а также членом Рабочей группы по передовой практике в области кибербезопасности Ассоциации интеграторов управляющих систем.

Список использованных источников

[1] ESET. Eset видит связь между кибершпионажем и отключением электроэнергии на Украине. http://www.eset.com/int/about/press/articles/malware/article/eset-finds-connection-between-cyber-espionage-and-electricity-outage-in-Ukraine/.

[2] SANS ICS. Подтверждение скоординированной атаки на энергосеть Украины.

https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

[3] SANS ICS. Стало понятно, какое вредоносное ПО могло быть использовано в ходе кибератаки на Украине. https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.

[4] iSIGHT Partners. Группировка Sandworm и атаки на энергосистему Украины. http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/.

[5] Trend Micro. Первое в истории Украины отключение энергоснабжения в результате атаки с использованием вредоносного ПО. http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/first-malware-driven-power-outage-reported-in-Ukraine.

[6] Список рассылки SCADASEC Infracritical. Новая волна атак на электроэнергетику Украины. http://news.infracritical.com/mailman/listinfo/scadasec.

[7] SentinelOne. Sentinelone раскрывает новую тактику инфицирования трояном blackenergy 3.

https://www.sentinelone.com/blog/sentinelone-discovers-a-new-delivery-tactic-for-blackenergy-3/.

[8] Symantec. Троян disakil, причастный к блэкауту на Украине, также использовался против компаний отрасли СМИ. http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-Ukraine-power-outages-also-used-against-media-organizatior

[9] ESET welivesecurity. Новая волна кибератак на электроэнергетику Украины.

http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/.