POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛОЩАДЬ / Д. 8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

Чем опасны «умные» электросети

Артём Чайкин, руководитель отдела безопасности мобильных приложений Positive Technologies

Электричество дорожает, и глобальная экономика усиленно ищет способы повысить свою энергоэффективность. Помимо солнечных и ветряных установок во всем мире идет активное строительство «умных» сетей распределения электроснабжения, так называемых Smart Grid, которые позволяют использовать энергию рационально. Они обычно автоматизированы и подключены к интернету, что вызывает естественный интерес к уровню их защищенности.

Внимание! Все описанные в статье уязвимости переданы производителям и ими устранены, но могут встречаться в действующих системах.

Китай в 2013 году инвестировал в Smart Grid 4,3 млрд долларов, а общемировые вложения составили 14,9 млрд. По прогнозам Pike Research, к 2015 году на переход к этой технологи будет потрачено свыше 46 млрд долларов, его поддерживают не только экономисты, но и экологи. В «Гринписе», например, уверены, что сети Smart Grid позволят спасти планету.

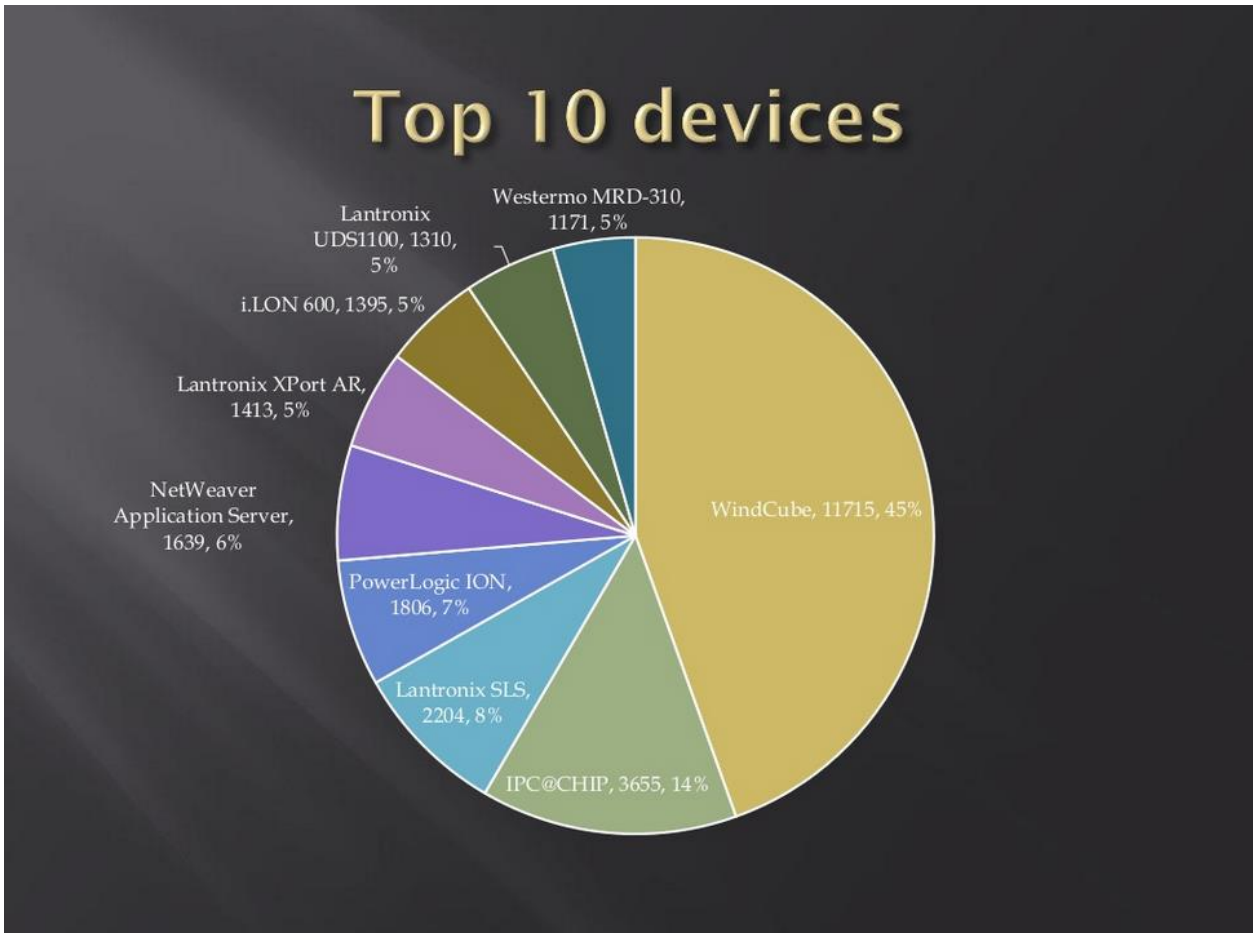
Из чего они сделаны

Технологии Smart Grid только готовятся завоевать мир. Сейчас их применяют главным образом в домашних автоматических системах управления климатом, где внедряются простейшие элементы «умных» электросетей. Подобные устройства позволяют

конечному пользователю осуществлять мониторинг, эффективно использовать энергию ветра и солнца, а в их отсутствие переходить к другим источникам. Опасны ли Smart Grid для прогрессивных домовладельцев? Чтобы ответить на этот вопрос, нужно узнать, из каких управляющих компонентов состоят такие сети.

> **Fingerprint-утилиты** отправляют запросы на удаленный узел с целью определения его принадлежности к тому или иному семейству. Из ответа на запрос можно определить операционную систему либо узнать модификацию устройства.

После короткого fingerprint-исследования мы обнаружили в интернете следы встраиваемых систем минимум девяти различных производителей, на базе которых строятся Smart-Grid-системы.



Статистика по Smart-Grid-микроконтроллерам

Самым распространенным семейством оказалось WindCube, но в качестве полигона для экспериментов были выбраны более «интеллектуальные» девайсы другого производителя, в онлайн-каталоге которого есть контроллер с множеством перспективных особенностей: процессором PowerPC, операционной системой реального времени RTOS, встроенным веб-сервером, поддержкой FTP, Telnet, SSH, TCP/IP, HTTP, PPP.

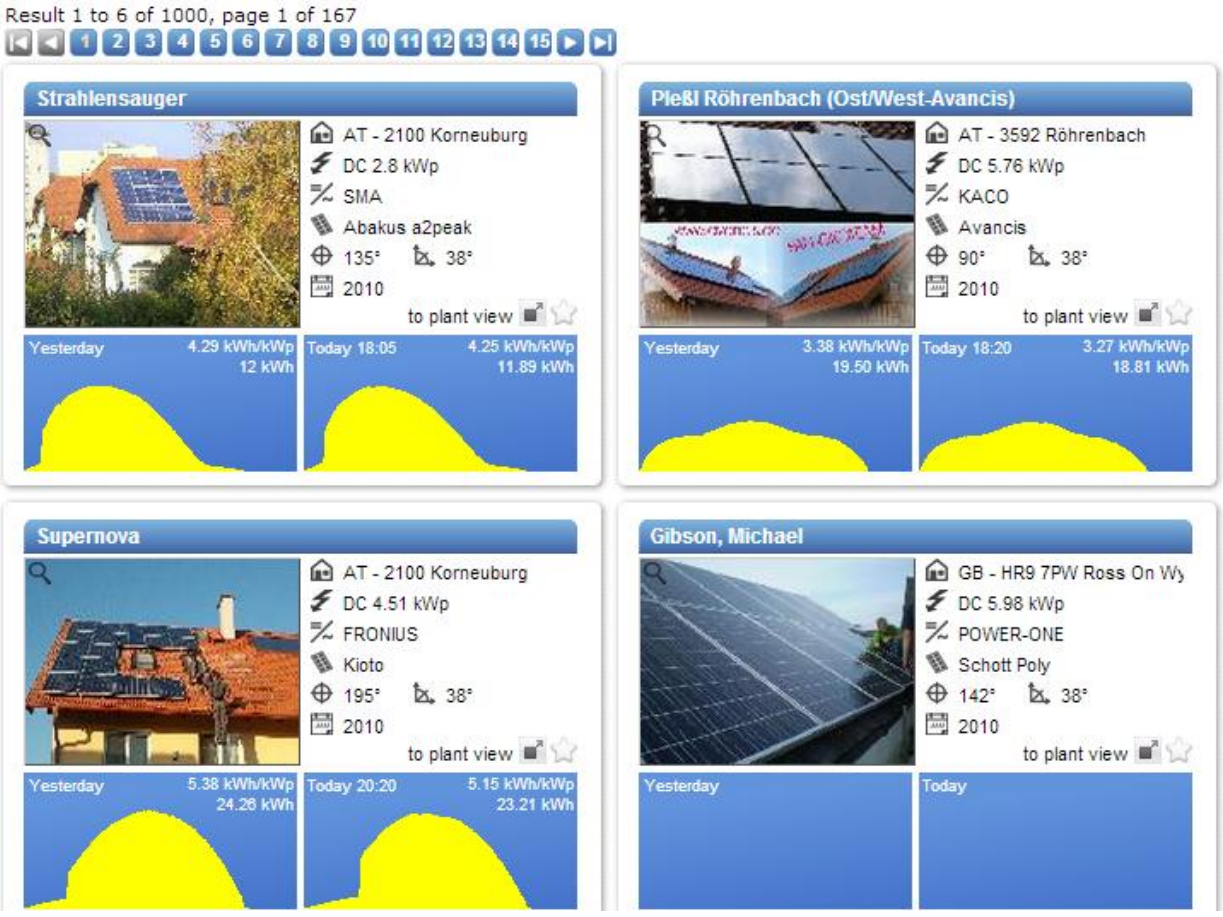
Ищем самых умных

Поиск в интернете систем Smart-Grid на базе выбранных контроллеров не вызвал больших затруднений. Вновь спасибо официальному сайту производителя, на котором указано название

операционной системы и вывешена инструкция, согласно которой с настройками конфигурации устройства из семейства его владелец может ознакомиться по адресу http://...../ZZZ. После этого мы отправились на Google, где воспользовались модификатором inurl, позволяющим искать информацию в подкаталогах сайта, и ввели комбинацию из названия ОС и ZZZ. В итоге мы получили несколько страниц с IP-адресами, масками подсети и серийными номерами конкретных устройств. Но в составе каких систем работают эти микрокомпьютеры?

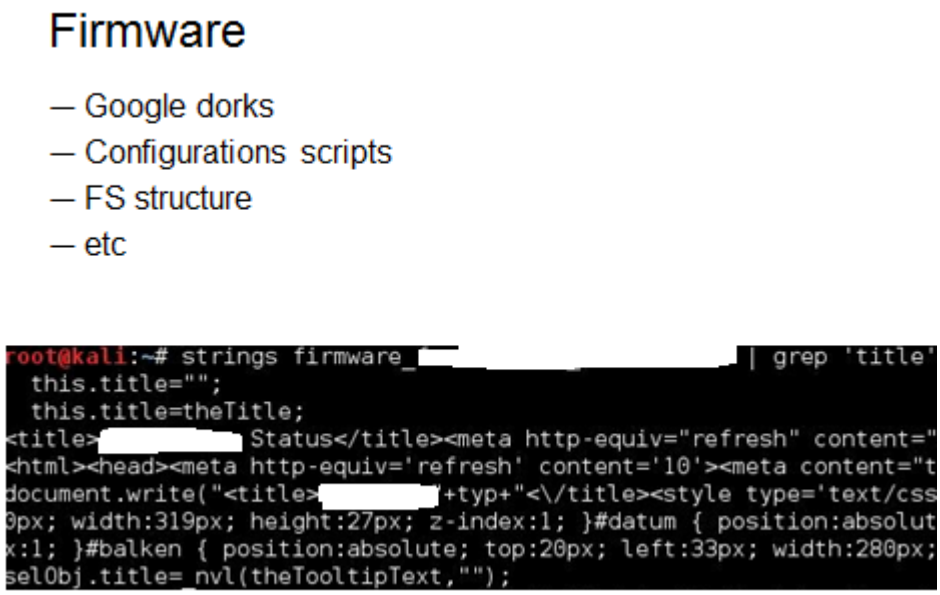
> **Дорки (Dorks)** — ключевые слова, URL-адреса или их составляющие, позволяющие с помощью поисковых систем или веб-сканеров найти путь к панели администратора или к странице с ошибками.

Как выяснилось на одной из обнаруженных страниц, исследуемая платформа трудится, в частности, в составе систем мониторинга фотогальванических установок Solar Sail (название производителя изменено), которые оказались чрезвычайно распространенными. Согласно сведениям разработчика, в мире функционирует более 200 тысяч солнечных электростанций и почти 1 млн инверторов, подключенных к веб-серверу этой компании.



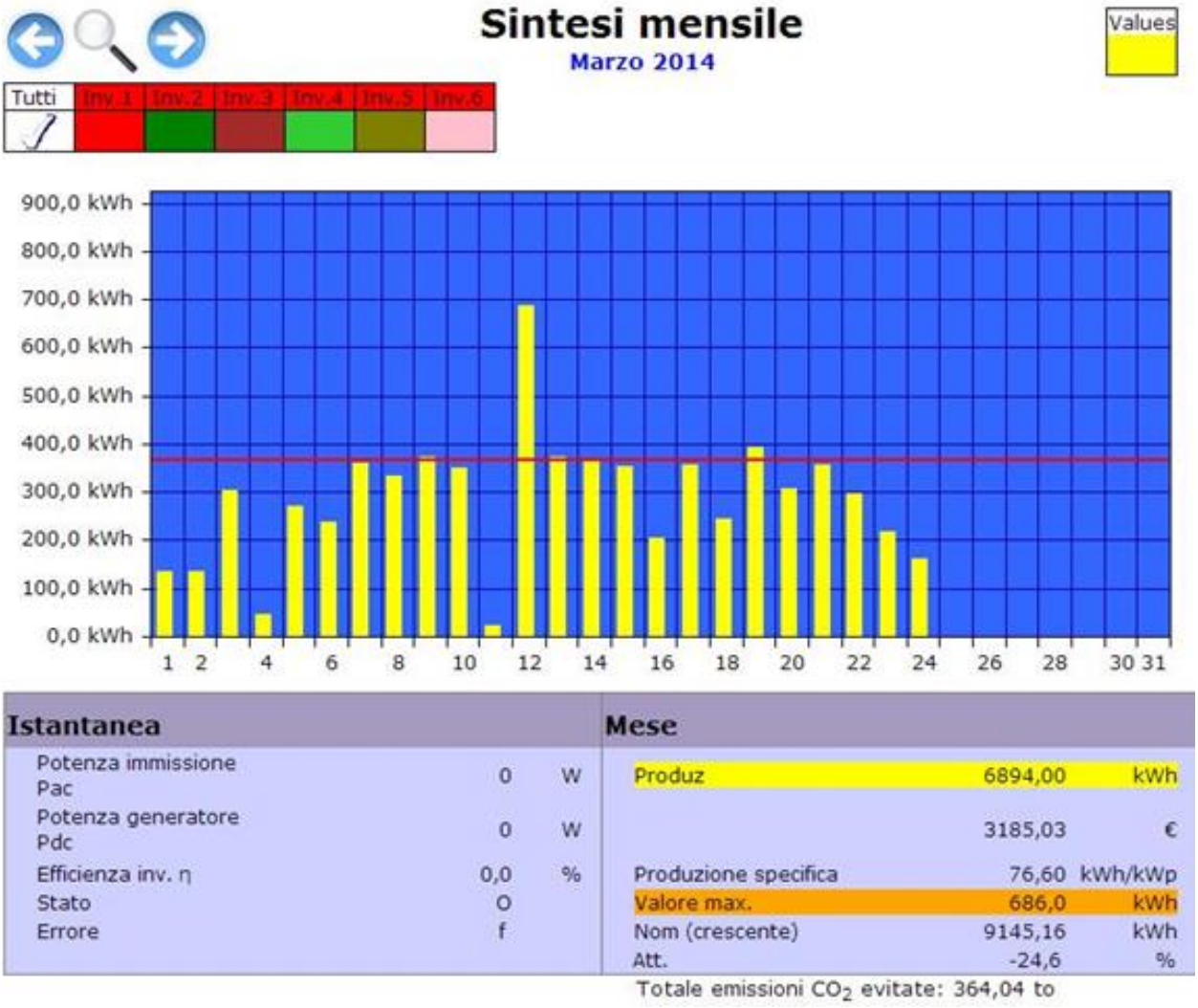
Солнечные батареи, подключенные к веб-серверу Solar Sail

Разбираем прошивку Solar Sail



Прошивка Solar Sail «в разрезе»

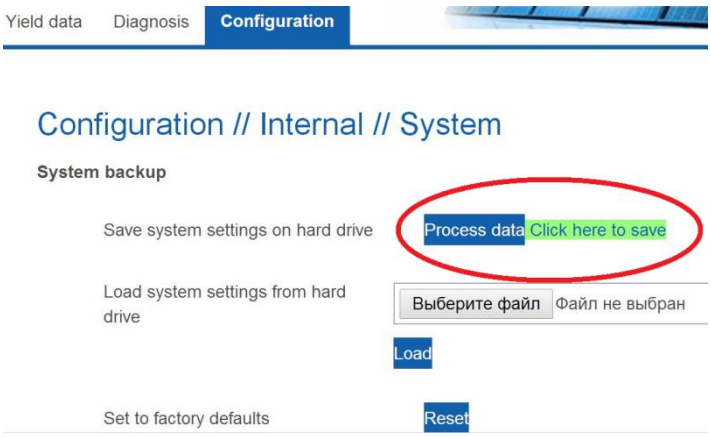
Скачав firmware для систем Solar Sail, мы посмотрели, как выглядит ее файловая структура, поискали «дорки» (Google dorks) и конфигурационные скрипты, которые позволяют управлять системой. С помощью команд strings и grep в прошивке был обнаружен заголовок Solar Sail Client, что натолкнуло на мысль загуглить URL-адрес inurl: Solar Sail-Client. В итоге мы обнаружили множество систем частных пользователей и страниц с данными о потреблении электроэнергии различных Smart-Grid-систем от Solar Sail. Но эта информация может представлять интерес разве что для надзорных органов, но не для злоумышленника.



Данные о выработке электроэнергии различных Smart-Grid-систем от Solar Sail

Можно и без пароля

Более любопытные вещи были найдены в панели администратора. При изучении админок Solar Sail выяснился интересный факт: примерно 5% систем не требовали пароля для входа на страницу конфигурации. У остальных 95% систем пароль был установлен, но толку от него было мало. Сформировав простой запрос к одному конфигурационному скрипту, можно было заставить панель администратора Solar Sail спокойно отдать резервную копию конфигурации, загрузить ее к себе на локальный компьютер и извлечь пароль.



Панель администратора Solar Sail

С расшифровкой пароля, который всегда находился под индексом 222, возникли некоторые трудности. Редактор HEX выдавал какую-то белиберду, поэтому мы пошли обратным путем: заглянули на устройство, которое было без пароля, ввели произвольный пароль (1234567890), сохранили его, потом скачали файл конфигурации и посмотрели, как он выглядит в зашифрованном виде.

```
191;
192;username
193;^d5c7d4dbdec5d9c8
194;
195;0
196;0
197;0
210;1
211;1
220;0
221;1
222;^9494949c9c9c9c94949e
230;[Denominazione impianto]
231;[Nome gestore]
```

Резервная копия файла конфигурации

Точно так же можно составить список соответствия всех необходимых паролей их зашифрованным вариантам.

Идем дальше

Попасть на страницу конфигурации Solar Sail, как можно было заметить, оказалось совсем несложно. С этой страницы доступна загрузка прошивки устройства, где поискать в ней любопытные артефакты. Кстати, в официальной документации Solar Sail указано, что процесс обновления прошивки защищен паролем. Однако мы столкнулись с необходимостью вводить пароль только на одной из систем, причем он был весьма несложным («Solar Sail»), совпадал с логином и был недоступен для изменения обычному пользователю.

Что завтра?

Пользователи «умных домов» и мини-офисов, подключенных к альтернативным источникам энергии, выступают, по сути, бета-тестерами систем Smart Grid. И разработчики не слишком щадят экономных владельцев, допуская серьезные ошибки в механизмах защиты. В нашем случае любой желающий мог выбрать одного из сотен тысяч владельцев установок Smart Grid от Solar Sail в интернете, обойти авторизацию (иногда и она не требуется), удаленно установить дефектную прошивку, завладеть доступом к управлению параметрами системы, проникнуть в другие сегменты сети. Возможны и физические воздействия, вплоть до выведения из строя инверторов, пожара и других неприятных событий.

Если сети электроснабжения критически важных объектов будут интеллектуализироваться с той же поспешностью, уровень рисков может оказаться не ниже, чем в случае со SCADA-системами, а сюжет, когда злоумышленники с помощью компьютера отключают от электросети целый город, — станет вполне реалистичным.

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована ФСТЭК и ФСБ, продукция сертифицирована ФСТЭК, «Газпромом» и Минобороны РФ. Более 1000 организаций в 30 странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, выполнения требований регуляторов и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня по вопросам защиты SCADA- и ERP-систем, крупнейших банков и телекомов. Согласно исследованиям IDC, в 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями. Подробнее о компании — на сайте ptsecurity.ru.