Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»

Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Испытание «Аврора»: как 30 строк кода разорвали 27-тонный генератор

КІБЕРЗЛОЧИННІСТЬ | ПТ, 2020-10-30 09:20

Версия для печати

Секретный американский эксперимент 2007 года доказал, что хакеры могут сломать оборудование энергосети так, что его уже невозможно будет починить. И для этого потребуется файл размером с типичный gif.

В конце октября министерство юстиции США **рассекретило** обвинительный документ, касающихся группы хакеров, известной как **Sandworm** [песчаный червь]. В документе США **обвинили** шестерых хакеров, работающих на ГРУ, в компьютерных преступлениях, проходивших в последние пять лет по всему миру – от **саботажа зимней олимпиады** 2018 года в Южной Корее до **запуска** самой деструктивной из вредоносных программ на Украине.

Среди этих обвинений упоминается **беспрецедентная атака** на украинскую энергосеть в 2016-м году, которая была разработана с тем, чтобы не только отключить подачу энергии, но и **повредить оборудование энергосети**. Когда один из исследователей кибербезопасности, Майк Ассанте, углубился в подробности этой атаки, он обнаружил, что идею взлома энергосетей придумали не русские хакеры, а правительство США – придумало, и испытало её ещё десять лет назад [никаких доказательств в обвинении традиционно не приводится; энтузиасты при помощи нейросети провели поиски людей по фотографиям, приведённым в документах, и один из них оказался очень похож на **тромбониста из Барнаула** / прим. перев.].

> На эту тему: **Sandworm. Как хакеры ГРУ отключали энергетику в Украине и взламывали избирком США**

Приводим перевод отрывка из книги «Sandworm: новая эпоха кибервойн и охота за самыми опасными кремлёвскими хакерами», опубликованной неделю назад, где подробно описывается тот самый ранний эксперимент по взлому энергосети. Руководил проектом ныне покойный Ассанте, легендарный пионер в области безопасности промышленных систем. Эксперимент позже назвали «Испытание генератора ''Аврора''». Сегодня он служит напоминанием того, как кибератаки могут влиять на физический мир. Он стал жутковатым предсказанием случившихся впоследствии атак Sandworm.

Одним промозглым и ветреным утром марта 2007 года Майк Ассанте прибыл в здание национальных лабораторий Айдахо, расположенное в 50 км к западу от Айдахо-Фолс. Это здание высится над пустынным ландшафтом, покрытым снегом и поросшим кое-где полынью. Он зашёл в большой зал, расположенный в центре для посетителей, где

НОВИНИ

20:00 **Погода в Україні на 8 травня: місцями короткочасні дощі та грози**

19:09 **Павло Казарін: Пастка безстроковості**

18:04 **Олег Чеславський: ЦПК і розкрадання стратегічних активів**

17:10 **Геннадій Левітас: Піхота - рід військ, який зникає**

16:04 **Касьянов: Вони крадуть 4 млн доларів на добу**

15:10 **Батьки очільника столичної прокуратури Сергія Ходаківського та судді Соборного суду Дніпра Максима Ходаківського у 2020 році придбали квартиру в Москві**

14:59 **ВАКС засудив заступника голови Рівненської облради за хабар до 9 років позбавлення волі**

13:01 **2500 гектарів лісу палає на Чернігівщині через російські обстріли**

12:19 **Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех**

11:50 **УПЦ МП має повернути державі споруди Богоявленського монастиря у Кременці - суд**

ПІДПИСКА НА КАНАЛ

уже собралась небольшая группа людей. В неё входили чиновники из министерства внутренней безопасности США, министерства энергетики США, некоммерческой корпорации надёжности энергосетей [North American Electric Reliability Corporation, NERC], директора нескольких энергокомпаний со всей страны. Были там и другие исследователи и инженеры, такие, как Ассанте, которым национальной лабораторией было поручено придумывать различные катастрофические сценарии, угрожающие критически важным американским инфраструктурам.

В передней части комнаты стояли ряды мониторов с видео и таблицами данных, повёрнутые к расположенным полукругом сиденьям в комнате – это было похоже на зал управления полётами в космическом центре. На экранах в прямом эфире с нескольких ракурсов показывали массивный дизельный генератор. Мятного цвета машина была размером с автобус – огромная масса стали весом 27 тонн, почти как современный танк. Она располагалась в полутора километрах от аудитории, на электрической подстанции, непрерывно гудя. Выдаваемого ею электричества хватило бы для обеспечения госпиталя, или военного корабля. На видео было заметно, как в поднимающихся от генератора волнах горячего воздуха колеблется горизонт.

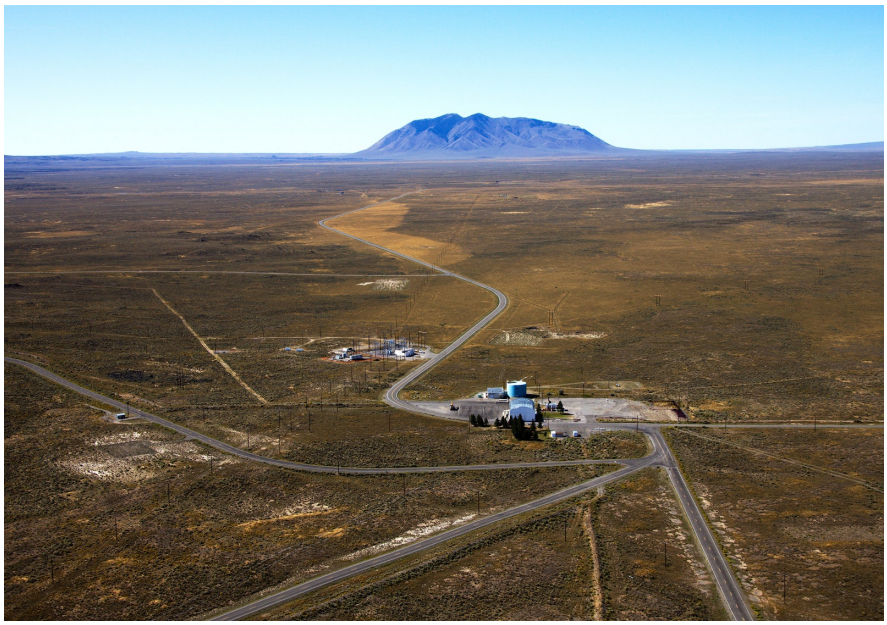
На эту тему: **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб?**

Ассанте и его коллеги, исследователи из лаборатории, купили этот генератор за $300 000 у нефтедобытчиков с Аляски. Они перевезли его за тысячи километров, на полигон в Айдахо – участок земли площадью 2300 кв. км., где у национальной лаборатории была целая энергосеть, предназначенная для испытаний, вместе с сотней километров проводов электропередач и несколькими электрическими подстанциями.

Если Ассанте справился с задачей, генератор получится уничтожить. При этом собравшиеся исследователи планировали разрушить эту дорогую и надёжную машину не каким-то физическим инструментом или оружием. Это должен был сделать файл объёмом 140 кБ – не больше, чем средняя GIF-ка с котятами из твиттера.

За три года до этого Ассанте работал директором по безопасности в компании American Electric Power, поставлявшей коммунальные услуги миллионам потребителей в 11 штатах, от Техаса до Кентукки. Ассант когда-то служил во флоте, а потом стал инженером по кибербезопасности, и давно уже понимал возможность хакерской атаки на энергосеть. Однако он был потрясён тем, насколько его коллеги из других компаний-поставщиков энергии слабо понимали эту угрозу, пусть теоретическую и отдалённую. Тогда было принято считать, что если **хакеры** и заберутся в сеть провайдера достаточно глубоко для того, чтобы начать щёлкать переключателями, то сотрудникам просто придётся выгнать их из сети и снова включить электричество. «Мы сможем справиться с этим, как с последствиями обычного шторма, — вспоминает Ассанте слова коллег. – Считалось, что это будет похоже на аварийное отключение энергии, и что мы просто восстановимся и всё – таковы были пределы модели рисков».

Однако Ассанте, обладавшего уникальной комбинацией знаний об архитектуре энергосетей и компьютерной безопасности, донимали более изощрённые мысли. Что, если атакующие не просто перехватят управление системами, начав щёлкать выключателями, чтобы вызвать кратковременные отключения электричества? Что, если они вместо этого перепрограммируют автоматические элементы сетей, без участия человека принимающие решения о выполнении различных операций?



Электрическая подстанция в национальных лабораториях Айдахо, на испытательном полигоне площадью 2300 кв.км.

На эту тему: **ГРУ РФ проводить безрозсудні та невибіркові кібератаки, — Великобританія та Австралія**

В частности Ассанте размышлял о таком оборудовании, как защитное реле. Реле должны работать в качестве механизма безопасности, защищая электросети от опасных физических условий. Если линии электропередач перегреваются, или генератор теряет синхронизацию, то именно такие защитные реле обнаруживают эту

аномалию и разрывают цепь, отключая проблемное место, спасая ценное оборудование и даже предотвращая пожары. Защитное реле работает спасателем для энергосети.

Но что, если это же самое защитное реле получится парализовать – или ещё хуже, испортить так, чтобы оно стало орудием атаки злоумышленника?

Именно с таким вопросом Ассанте, работавший у провайдера электричества, пришёл в национальные лаборатории Айдахо. И сейчас в центре для посетителей на испытательном полигоне, они с коллегами собирались воплотить эту жуткую идею на практике. Секретному эксперименту дали кодовое название, которое затем станет синонимом возможных цифровых атак, имеющих физические последствия: «Аврора».

Директор испытаний объявил время: 11:33. Он уточнил у инженера по безопасности, что на территории близ дизельного генератора отсутствуют зеваки. Затем он подал одному из исследователей в офисе в Айдахо-Фолс команду начинать атаку. Как и любой реальный цифровой саботаж, эту атаку проводили с большого расстояния и через интернет. Игравший роль хакера сотрудник отправил программу в тридцать строк кода со своей машины на защитное реле, подключённое к дизельному генератору размером с автобус.

До момента атаки внутренности генератора исполняли невидимый и идеально сбалансированный танец с энергосетью, к которой он был подключён. Дизельное топливо в камерах распылялось, и детонировало с нечеловеческой скоростью. Оно двигало поршни, вращавшие стальной стержень в недрах двигателя со скоростью около 600 об/мин. Это вращение передавалось через гасящую колебания резиновую втулку на другую деталь, непосредственно генерирующую ток. Это был стержень с ответвлениями с медной намоткой, вращавшийся между двумя массивными магнитами. Каждый оборот возбуждал в проводах электрический ток. Если вращать эту кучу меди достаточно быстро, можно получить переменный ток с частотой 60 Гц, энергия которого будет передаваться в гораздо более крупную энергосеть.

Защитное реле, подключённое к генератору, должно было не давать ему подключаться к остальной энергосети без точной синхронизации с этим ритмом в 60 Гц. Однако «хакер» Ассанте из Айдахо-Фолс только что перепрограммировал это спасательное устройство, поставив всю его логику с ног на голову.

В 11:33:23 защитное реле получило информацию об идеальной синхронизации генератора с сетью. Но затем его испорченный мозг сделал нечто противоположное его первоначальной цели: разорвал цепь, отсоединив машину.

Когда генератор отключился от более крупной энергосети и перестал делиться своей энергией с этой обширной системой, он сразу же начал ускоряться, будто лошадь, освободившаяся от повозки. Как только защитное реле обнаружило, что скорость генератора выросла настолько, что тот полностью рассинхронизировался с сетью, его вредоносная логика сразу же подсоединила генератор обратно к сети.

Как только дизельный генератор вновь подключился к крупной сети, на него обрушилась вся мощь всех остальных генераторов, подключенных к сети. Всё это оборудование насильно замедлило относительно небольшую массу вращающихся компонентов, приведя её обратно к частоте соседей.

На экранах собравшиеся наблюдали, как гигантская машина началась трясти с невероятной силой, испустив звук, напоминающий щелчок гигантского кнута. Весь процесс, от момента запуска вредоносного кода до первого толчка, занял лишь долю секунды.

> На эту тему: **Carderplanet и убийство Дмитрия Завгороднего: дело российских спецслужб? Часть 2**

Исследователи оставили панель, дававшую доступ внутрь генератора, открытой, чтобы иметь возможность наблюдать за тем, что происходит внутри. И теперь из неё начали вылетать чёрные обломки. Это начала рваться на части чёрная резиновая втулка, связывавшая две половины вала генератора.

Через несколько секунд машина снова затряслась – код защитного реле снова вошёл в свой цикл саботажа, отсоединив машину, и позже снова подсоединив её после рассинхронизации. На этот раз из генератора начал идти серый дым – возможно, из-за сгорания кусочков резины.

Несмотря на то, что на атаку, за которой следили собравшиеся, было потрачено несколько месяцев и несколько миллионов долларов из бюджета, Ассанте даже испытывал какую-то симпатию к машине, которую в этот момент разрывало изнутри. «Ты вдруг понимаешь, что болеешь за него, как за тот **паровозик, который смог**, — вспоминал Ассанте. – Я думал: давай, ты справишься!»

Но машина не справилась. После третьего удара она испустила большое облако серого дыма. «Двигателю кирдык», — сказал инженер, стоявший рядом с Ассанте. После четвёртого удара из машины вырвалось облако чёрного дыма, поднявшееся на десяток метров вверх, когда генератор сотрясла последняя предсмертная судорога.

Директор испытаний закончил эксперимент и в последний раз отсоединил от сети испорченный генератор, стоявший совершенно неподвижно. Во время последовавшего анализа происшедшего исследователи из лаборатории обнаружили, что вал двигателя столкнулся с его внутренней стенкой, оставив глубокие вмятины, и присыпал все внутренности металлической стружкой. С другой стороны генератора намотка и изоляция оплавились и сгорели. Машина была совершенно испорчена.

> На эту тему: **«Хакеры ГРУ действуют как стратегическое оружие российского государства»**

Над центром для посетителей повисла тишина. «Это был отрезвляющий момент», — вспоминает Ассанте. Инженеры неоспоримо доказали, что хакеры, атакующие

электрического провайдера, могут не просто временно помешать работе жертвы. Они могут повредить критически важное оборудование так, что его потом невозможно будет восстановить. «Это было очень наглядно. Можно было представить, как это происходит с машиной на настоящей электростанции, и это было ужасно, — говорит Ассанте. – В итоге получилось, что всего несколько строк кода могут создать условия, физически опасные для машин, на бесперебойную работу которых мы полагаемся».

Однако Ассанте вспоминает, что осознал нечто ещё более важное сразу после окончания эксперимента «Аврора». Словно **Роберт Оппенгеймер**, наблюдавший за испытаниями первой атомной бомбы в другой американской лаборатории за шесть десятилетий до этого, он наблюдал рождение чего-то как исторического, так и невероятно мощного.

«Я ощутил огромную тяжесть в желудке, — говорит Ассанте. – Я будто бы заглянул в будущее».

—

Автор: Andy Greenberg

Перевод: Вячеслав Голованов SLY_G; опубликовано в издании Хабр

На эту тему:

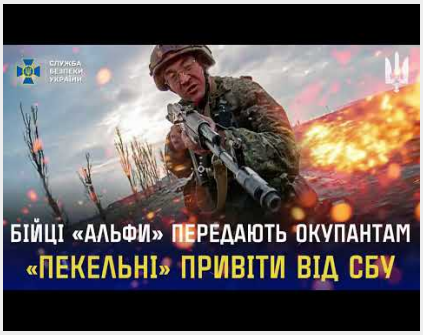
- **Как выглядит кибервойна с Россией**
- **Киберхиросима или Удивительные малвари и где они обитают**
- **Как «хакер» из Беларуси был осуждён в США: приключенческая и поучительная история**
- **«Всемирноизвестный кибермошенник», разыскиваемый ФБР, идет на выборы от блока Петра Порошенко**
- **Взлет и падение CarderPlanet глазами участника движения**

Читайте «Аргумент» в **Facebook** и **Twitter**

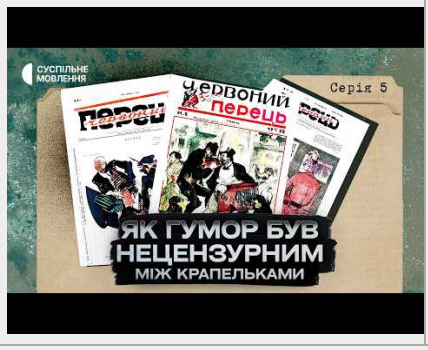
Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

Коментарі

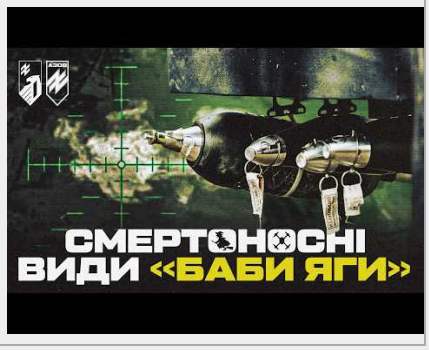
Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні



Про що не можна було жартувати в СРСР



HEAVY SHOT, VAMPIRE, NEMESIS: як «Баба Яга» б'є ок*пантів



Контакт: ***uargumentum@gmail.com***