ЖУРНАЛ ОТ КОМЬЮНИТИ ХУЛИГАНОВ

ХАКЕР

ХАКЕР

WWW.XAKEP.RU

№03(75) МАРТ 2005

УДАР ПО ВЕБУ

стр. 60

Новый способ взлома web-сайтов

ВЗЛОМ:

ПРОГРАММА-НЕВИДИМКА

>> стр. 110 Делаем нашу программу невидимой в системе

ПИНГВИН КЛАСТЕРИЗУЕТСЯ

Поднимаем кластер своими руками

>> стр. 94

PC ZONE

ИМПЛАНТ

СЦЕНА

ВЕСЕННИЙ ПОСТЕР INSIDE

ВЕСНА • ЗАГРУЗКА • 99%

3 ВИДЕО ПО ВЗЛОМУ!

НА CD

- Corel Painter IX
- PhotoFiltre 6.1
- PuTTY 0.57
- Scribus 1.2.1
- OpenOffice 1.1.4
- Linux kernel 2.6.11 RC4

НА DVD БОЛЕЕ 4 ГИГАБАЙТ

- NetBSD 2.0 Live
- Corel Painter IX
- Borland Caliber RM 2005
- FLStudio XXL v5.0.1
- Adobe Audition 1.5
- ACDSee 7
- Музыка
- Софт из журнала
- etc.

ISSN 1609-1019

(game)land

INTRO

Какое-то глубочайшее отсутствие умных мыслей, которыми нужно с тобой поделиться. Не чувствую себя Бублосом, поэтому не буду писать о том, как легко положить двадцатерых противников в Мортал Комбате и как тяжело это повторить в обычной жизни. Сошлюсь на весеннее обострение.

Лучше обнадежу тебя. Ведь если ты наш хороший читатель, то этот номер должен был купить еще в марте. И поэтому, надеюсь, читаешь сейчас актуальную для себя информацию. Ха-ха. Дорогой, обрати внимание на колонку ART на этом же развороте. Видишь, там появились новые имена и фамилии? Увидел? А это значит, что нас опять ждет новый дизайн. Сам понимаешь, весна, гормоны, девушки в нужной одежде… Вот тут явление - дизайнотоксикоз…

Но радость на этом не кончается. Теперь мы опять выходим с постером. И это не временное явление, а постоянное. Так что и в следующий номер мы положим тебе что-нибудь интересное.

P.S. Такие вот радости. Больше не буду тебя грузить. Пожелаю лишь направить в нужное русло всю твою весеннюю активность. Приятного чтения.

CuTTer
cutter@real.xakep.ru

CONTENT

НЬЮСЫ

FERRUM

PC ZONE

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

УДАР ПО ВЕБУ

Reverse IP Lookup. Что это? Читай эту статью, и тебе откроется Дао :)

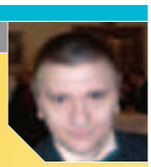
ЖИВОЖУРНАЛЬНАЯ АТАКА

Сказ о том, как ломали украинский ЖЖ, да так и не добрались до аккаунта Хинта

С ВИПАМИ НА «ТОМАГАВК»

Самоделкины против Пентагона. Выигрывает Пентагон

Слава Янсимов aka ANSI (ansi@infos.ru)



С ВИЛАМИ НА «ТОМАГАВК»

Существует красивый миф о том, что крутой хакер может угнать военный спутник, а настоящий патриот рогатиной завалить танк. Желающих насолить Пентагону становится все больше. Каковы шансы в одиночку противостоять современным военным технологиям? Правда ли, что самый великий в мире хакер не Кевин Митник, а простой питерский профессор?

ПАРТИЗАНСКАЯ ВОЙНА ПРОТИВ ОРУЖИЯ ПЕНТАГОНА

В сверхмогущество хакеров многие охотно верят. Способствуют этому не только голливудские боевики, но даже деловая пресса. В феврале 1999-го английская газета Sunday Business сообщила, что хакерам удалось изменить орбиту очень важного британского военного спутника. Они требовали денег за передачу управления спутником обратно военным.

Во все времена ломать компьютерные системы Пентагона и NASA было для хакеров предметом особой крутизны. Считалось, что все эти штуки защищены по-военному, поэтому не каждому по зубам.

Между тем бесчисленные сообщения о проникновениях в секретные базы данных и явная утка с угоном спутника имеют много общего. Ни то, ни другое просто невозможно, так как по-настоящему секретные коммуникации и тем более системы управления никак не пересекаются с общедоступными каналами типа интернета или телефонных сетей. Военные уже устали это повторять.

Да, военные ведомства и спецслужбы все больше и больше представлены в глобальной Сети. Однако не надейся, что, получив доступ к сайту британской «МИ-6», ты доберешься до списков внешней резидентуры. Максимум, на что можно рассчитывать, это памятка с грифом «Для служебного пользования» с личного компьютера одного чайника на военной базе. Именно так было и в 1989-м, когда парни из Chaos Computer Club продали КГБ «драгоценную информацию» из правительственных компьютеров США, и в 2002-м, когда спецы из ForensicTec Solutions поперли у генералов личную переписку и списки страховых свидетельств новобранцев. Как правило, «военные тайны», похищаемые хакерами, - это не результат слабой защиты, а закономерное следствие разгильдяйства сотрудников. Для национальной безопасности это вряд ли смертельно и даже не очень ощутимо. Хотя Пентагон вполне серьезно готовится к так называемой «кибервойне», сильно навредить ему через интернет не получится. DoS-атаки не остановят войска, как не сделают этого пацифистские дефейсы или кража «чувствительной» информации.

ВОЙНА И МИР

Если в киберпространстве враг не то чтобы сильно защищен, а по-хорошему не представлен, остается обратить взгляд непосредственно на поле боя. Похоже, и здесь борцов с агрессором ждут те же грабли - иллюзия уязвимости сращивания военных и гражданских систем. «Раскурочим рельсы - ни электричка не пройдет, ни бронепоезд».

Объектом особого внимания последнее время является спутниковая навигационная система NavStar-GPS, которую Пентагон в свое время разрешил использовать всем подряд - от военных в других государствах до геологов и рыбаков. Разнесенные по орбите спутники излучают сигналы, сравнивая которые, GPS-приемник может вычислить свое местоположение в любой точке Земли с точностью до десятка метров. Как только технология позволила создавать малогабаритные приемники с вычислителями, GPS нашла свое применение повсеместно. Сейчас эту модную штучку встраивают во все, что шевелится, - катера, автомобили, бытовые приборы, инвалидные коляски, браслеты для больных и ошейники домашних животных...

Известно, что в марте 2003 года, в самом начале иракской кампании, у всех журналистов, сопровождавших подразделения войск коалиции, были конфискованы сотовые телефоны, снабженные приемниками GPS. Точнее, изъяты были только те телефоны, которые обслуживались одной из арабских телекоммуникационных компаний. Военные заподозрили, что в сигнал таких телефонов

ВЫСТРЕЛИЛ И ЗАБЫЛ

Вся прелесть крылатых ракет в том, что они полностью автономны. Ориентируются ракеты, сравнивая картинку рельефа местности, получаемую от собственного локатора и высотомера, с картами, заложенными в памяти. Это прекрасно проиллюстрировано в фильме, где Стивен Сигал шинкует злодеев на крейсере «Миссури».

Весьма вероятно, что режим наведения по координатам GPS все же имеется в «томагавках» блока 3, ориентированных на морские цели или целиком морские маршруты. В море, как известно, рельеф местности большим разнообразием не отличается. Но даже в ракетах версии 1994 года GPS играет не основную функцию.

Вспомогательные функции приемника глобальной радионавигационной системы в «томагавке» блока 3 следующие:

- повышение достоверности и дополнительный контроль координат;

- координация действий с другими ракетами и самолетами.

Обе задачи не принципиальны. Ракета выполнит свою миссию и без них, если система GPS вдруг откажет или не будет работать изначально. Даже с новым дополнительным приемником GPS ракета в базовом боевом применении сохраняет автономность. Она летит на высокой скорости с огибанием рельефа на предельно малой высоте (около 20 м). В «томагавке» все сделано так, чтобы ракету было крайне сложно обнаружить и уничтожить.

может добавляться служебная информация от GPS о точном местонахождении владельца, а следовательно - об оперативных перемещениях войск.

Еще раньше появилась информация о том, что Пентагон начал оснащать средствами GPS не только пехоту и авиацию, но и бомбы, и ракеты.

Благодаря прессе, ситуация вокруг GPS стала обрастать такой ботвой из слухов и фантазий, что барон Мюнхгаузен просто отдыхает.

Так, руководитель одного из наших радиотехнических НИИ в интервью ИТАР-ТАСС договорился до того, что объяснил сбои в работе системы GPS резким увеличением числа пользователей с началом боевых действий в Ираке. В отличие от, например, сотовой связи, приемники GPS полностью пассивны, то есть никакой обратной связи с обслуживающей системой (спутниками) не имеют. С таким же успехом можно было бы объяснять сбои на телецентре увеличивающимся количеством включенных телевизоров, когда начиналась «Масяня».

ПРОФЕССОР-ХАКЕР

В промежутке между югославской и второй иракской кампаниями - году эдак в 2002-м - широкой общественности стал известен главный гений, можно сказать, вождь и отец последних партизан века хай-тек. В его изобретения безоговорочно верят серьезные печатные издания, он шантажирует целые правительства и оценивает свой ущерб Пентагону в таких масштабах, что все хакеры планеты вместе взятые по сравнению с ним - просто дети малые...

Итак, в свое время несколько печатных и онлайновых СМИ рассказали о профессоре из Санкт-Петербурга, докторе наук Валентине Кашинове, который якобы изобрел простую глушилку для GPS. Поначалу не разобравшиеся в объяснениях самого профессора журналисты сходу написали, что устройство, которое можно спаять из доступных деталей в домашних условиях, способно нарушить работу чуть ли не самой спутниковой группы GPS. Новость большого шума не наделала ввиду ее очевидной бредовости. Вмешаться в работу спутников даже с мощными радиотехническими средствами вряд ли возможно, разве что залезть с ножовкой на огромные локаторы НИП и попытаться что-нибудь отпилить.

Вскоре после этого появились более обстоятельные объяснения профессора и даже результаты экспериментов. Речь шла о помехах приемникам GPS в пределах некоторого радиуса действия на местности. Кашинов сообщил, что используемые в GPS фазоманипулированные сигналы оказались неустойчивы к маломощным помехам: «При мощности передатчика помех порядка 1 Вт дальность глушения в свободном пространстве может достигать 500 км».

Профессор Валентин Кашинов. Народных героев нужно знать в лицо

Старт «Томагавка»

ЗАРОЙТЕ СВОИ ТОМАГАВКИ

Свою «помеху» Кашинов придумал достаточно давно, но не стал продавать ее отечественным военным. Профессор, возмущенный политикой Соединенных Штатов, занялся донесением своих метазнаний до всех жертв агрессивной Америки. Он стал открыто рассылать описание своего диковинного устройства и раздавать интервью прессе. По его словам, еще до начала бомбежек Белграда он послал сербам ценные указания, но они поначалу ими пренебрегли. «И вот, когда после первых обстрелов «томагавками» стало ясно, что к чему, мне пришлось через интернет обратиться к прогрессивной общественности, после чего со мной связались их военные представители». Якобы после этого косяки «томагавков» американцев полетели не туда и в массовом порядке стали самоликвидироваться.

Аналогичную историю профессор рассказывает про Ирак. Как пишет Кашинов, за время операции «Лиса в пустыне» в воздухе на пути к Ираку самоликвидировалось более сотни «томагавков».

Профессор утверждает, что при пропадании сигнала от спутников компьютер «томагавка» теряет ориентацию, и на этот случай в нем предусмотрена программа самоликвидации. Весьма убедительно. Фазоманипулированный сигнал действительно неустойчив по отношению к узкополосной помехе на частоте, близкой к несущей, - об этом написано во всех учебниках. Вся штука в том, что крылатые ракеты «томагавк» (Tomahawk) были разработаны General Dynamics аж в 1970 году - намного раньше запуска первого спутника GPS в 1978-м. Поскольку все они до настоящего момента не самоликвидировались, нетрудно догадаться, что в основе их работы лежит иной принцип, а именно автономное наведение по радиолокационному рельефу местности. GPS-приемники на «томагавки» действительно начали ставить, но лишь 10 лет назад. Открою военную тайну Пентагона. «Томагавки» всех поколений не наводятся по GPS. Ни в стратегических, ни в тактических, ни в ядерных, ни в любых других вариантах. GPS играет исключительно вспомогательную функцию.

На одном из сайтов Кашинов пишет: «Из США поступают сведения о начале испытаний новых «томагавков», ориентирующихся по рельефу местности. Конечно, специалистам США ничего не остается, как признать полное фиаско системы GPS NAVSTAR». Вот так. Оказывается, все было наоборот - сначала GPS, а потом системы наведения по

рельефу. Очевидно, профессор слегка запутался в хронологии и причинно-следственных связях. Об истории и технических деталях «томагавков» можно прочитать на официальных сайтах ВМС США. Что касается невозможности модернизации GPS, вообще, жаль, что профессор ничего не слышал о запуске новых поколений спутников GPS Block IIR - IIF.


«Томагавк» в полете

МЫ ВАС ОТКЛЮЧИМ ОТ ВСЕГО

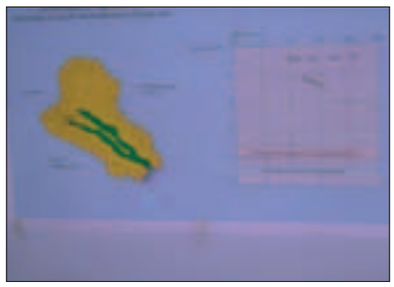
Ладно, с «томагавками» профессор малость напутал, однако существуют более продвинутые, «умные» бомбы и ракеты, на которых GPS действительно используется для наведения на цель. Уж с ними-то простенькая схема питерского инженера наверняка разберется с полпинка. В конце концов, есть инфантри-пехота, поголовно оснащенная средствами GPS. Наверное, если американский пехотинец потеряет сигнал GPS, он должен немедленно застрелиться...

Свой ультиматум Кашинов отправил в НАТО: «Если не прекратите свои бесчинства, опубликую способы, как можно вырубить и другие ваши навигационные системы». Позже в своих более трезвых статьях профессор признавал, что глушить длинноволновую LORAN-C без глобальных международных последствий будет сложно. Для технического решения этой задачи потребуются дополнительные исследования, так же как и для вывода из строя новой перспективной европейской системы Galileo.

В Пентагоне, похоже, действительно изучили страшилки из России, но серьезной опасности в них не обнаружили. В конце марта 2003 года представитель Пентагона заявил, что попытки противника нарушить работу средств, использующих GPS, успеха не имели. При этом было отмечено, что американские военные ожидали применения подобных средств и приняли соответствующие меры. Меры эти, как выяснилось на следующий день, тоже были незатейливы и предсказуемы. Несмотря на то что помехи никому не мешали, шесть обнаруженных источников помех были на всякий случай уничтожены. На них просто сбросили бомбы, оснащенные той самой GPS, что подтвердило ее нормальную работоспособность.

Первоначально американцы заявляли, что помеховые устройства войска Саддама получают из России, где их кустарно собирает некая фирма. На хакерских сайтах и правда встречаются фотографии маленьких коробочек и внутреннего монтажа с пайкой на коленке и русскими надписями. Как утверждает «Российская газета», впервые портативные передатчики помех для подавления систем космической навигации, произведенные российской фирмой, были показаны на Московском международном авиакосмическом салоне в 1997 году. В день, когда в Ираке засекли попытки глушения GPS, президент Буш намекнул президенту Путину на русский след в этом деле. Президент обещал разобраться.


Передатчик помех приемникам спутниковых навигационных систем GPS/ГЛОНАСС. Дальность действия 150-200 км. Масса передатчика 8-10 кг


Так работают передатчики помех

ПОВИМ РАКЕТЫ САЧКОМ ДЛЯ БАБОЧЕК

На исследованиях GPS любознательные партизаны не остановились. Они научились бороться с настоящим «злом» - так можно перевести название американской ракеты HARM. На самом деле это аббревиатура High-speed Anti-Radiation Missile - противорадиолокационной самонаводящейся ракеты класса «воздух - РЛС». Ей противопоставили обычную микроволновую печку. Об этой идее можно найти много упоминаний в интернете, но доктор Кашинов и данное открытие приписывает себе.

«Когда англичане вошли в Косово, они с удивлением обнаружили, что во дворах валяются микроволновые печки. Ничего удивительного здесь нет. Например антирадарная

УМНЫЕ БОМБЫ

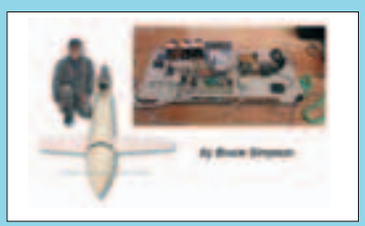
GPS как основное средство наведения используется в так называемых умных бомбах. По нему ориентируются управляемые авиабомбы JDAM (Joint Direct Attack Munition), планирующие бомбы JSOW и управляемые (не крылатые) ракеты JASSM. К последним относится 1000-килограммовая ракета AGM-158 с дальностью полета 185 км. Смысл всех этих наворотов состоит в том, чтобы попасть в цель с высокой точностью с как можно большего расстояния от нее.

Теоретически помехи радионаведению данных боеприпасов поставить можно. Однако не следует забывать, что современное оружие создается для эффективного применения в условиях полномасштабной войны с высокотехнологичным противником. Это означает применение мощнейших профессиональных средств радиоэлектронной борьбы (РЭБ), а не самопальных поделок юных техников. Ракеты и бомбы всегда делались с полным запасом автономности, и открытая система GPS используется в них, как правило, в качестве вспомогательной системы. Как заявил представитель Пентагона в интервью New Scientist, помеховые устройства GPS не являются «серебряными пулями» против бомб и ракет, даже если их воздействие окажется хоть сколько-нибудь эффективным. Если в районе цели действует помеха GPS, это не означает, что самолеты и наземные войска «плюнут на все, развернутся и уйдут».

Использование GPS в ракетах и бомбах не является технологическим прорывом в точности поражения. Это лишь один из способов удешевления высокоточного оружия. Старые добрые бомбы с лазерным наведением, точность которых гораздо выше, никуда не делись. Однако значительно дешевле оказалось установить пассивную систему с GPS-приемником и слегка увеличить мощность заряда. Но если с использованием радиоэлектроники будет совсем беда, а в случае войны с высокотехнологичным противником именно так и будет, можно вернуться к лазерному наведению.

Читай о профессоре Кашинове:
- **www.laboratory.ru/person/kashinov/rstart.htm**
- **www.laboratory.ru/articl/rad/rar020.htm**
- **www.globalresearch.ca/articles/BOG211A.html**

ПРОДЕЛКИ СИМПСОНОВ



Брюс Симпсон и его «почти готовый» самодельный «томагавк»

Летом 2003 года, когда с Саддамом было покончено, тема крылатых ракет была все еще очень популярна. Фанаты буквально помешались на «томагавках». Один 49-летний новозеландец сообщил на своем сайте www.aardvark.co.nz/pjet, что собирает в гараже «томагавк» из купленных на аукционе eBay деталей, при этом планирует уложиться в $5 000.

Последняя запись на сайте сделана 6 июля 2004 (www.interestingprojects.com/cruisemissile/diary.shtml). Результат года работы, действительно, похож на ракету с крылышками и каким-то хитрым ускорителем в хвосте. Электроникой наведения парень из страны хоббитов сильно заморачиваться не стал, ограничившись карманным GPS-приемником. Своими действиями конструктор пожелал привлечь внимание властей к проблеме доступа к высокотехнологичному оружию. Мол, каждый может наклепать себе «томагавков». Местные власти угрозе не внемлют и озабочены лишь тем, чтобы конструктор не взлетел на воздух вместе со своим домом.

ракета HARM идет на любой мощный источник радиоизлучения в диапазоне от 400 до 10 000 МГц, а в микроволновках стоит магнетрон на 500-800 Вт. Если открыть дверцу печки и перемкнуть блокировку, то около 200 Вт она может излучать». Этот рецепт Кашинов рассказал по телефону своему приятелю из Белграда. Подтверждение тому, что НАТО обстреливала исключительно микроволновые печки, неискушенный в английском юморе профессор нашел в британской газете «Гардиан».

На самом деле пассивная головка самонаведения HARM AGM-88 не пойдет на любой мощный источник радиоизлучения, хотя и может его зафиксировать. Ракета способна различать различные типы РЛС по их сигналу. С какой из них она могла бы спутать микроволновку, непонятно. Возможно, «хармы» принимают микроволновки за танки, что, наверное, неудивительно - в танке всегда очень жарко, особенно когда танкисты жарят сосиски.

Вообще, боевое применение микроволновки выглядит весьма странно. Вынести печку во двор, чтобы в нее влетело 66 кг осколочно-фугасного заряда? При том что на вооружении любой мало-мальски приличной ПВО имеются достаточно простые и дешевые штатные постановщики активных помех, имитирующие РЛС.

НАДУВНЫЕ РЕЗИНОВЫЕ... ТАНКИ

Сели партизаны кумекать: если «томагавки» летят по рельефу, то, может быть, стоит изменить сам рельеф? Не то чтобы умело варьировать радиус Земли в математических формулах, а буквально: разжигать рядами костры, надувать баллоны и резиновые танки, покрытые радиоотражающей краской, по барханам раскидать надувных женщин и плюшевых мишек.

Как ни странно, именно надувная техника сумела подтвердить свою неплохую эффективность. Так, во время первой войны в Заливе получили распространение муляжи самолетов, танков, мостов, телецентров, всяческих оборонительных сооружений и даже химических заводов. Весь этот надувной арсенал был произведен и продан Ираку туринской компанией MBM. Макеты светились, излучали тепло и имитировали прочую активность. От себя добавлю, что в пустыне барханы движутся со скоростью 100 м в месяц, поэтому «рельеф» - понятие сильно текучее.

Противорадиолокационная самонаводящаяся ракета HARM класса «воздух - РЛС»

А, ПУСТЬ СТРЕЛЯЮТ!

Все промазавшие последнее время «томагавки» доктор Кашинов относит на свой счет. Вот что он пишет: «Ущерб подсчитать не представляет труда. Если каждый «томагавк» стоит около 1 300 000 долларов, просто умножьте эту цифру на 300 самоликвидаций. Но это мелочь, так как оценивать нужно стоимость всей системы GPS NavStar, которая теперь практически выведена из строя. А это не менее 80 миллиардов долларов и 20 лет работы специалистов высокой квалификации». Вот какой уверенный в себе западлостроитель живет и потирает ручки в Санкт-Петербурге.

Стараниями партизан века хай-тек эта девушка угодила в болото

Конечно, даже самая современная и очень ответственная техника иногда дает сбои. Случается даже, что космические шаттлы разваливаются на куски. Ну а на войне бывает всякое. «Томагавки» теряют ориентацию, пушки палят по своим, вертолеты падают сами по себе. Но это не означает, что буржуи - полные дураки, что танки можно разгонять ивовым прутиком, а самолеты - ветряными мельницами. И все же человечество приблизилось к той стадии технического развития, когда сумасшедший ученый в своей лаборатории может если не взорвать Земной шар, то изрядно потрепать его. За такими ноу-хау нужен глаз да глаз.