войны юрского периода II –черви возвращаются

крис касперски ака мыщъх noemail

введение

Мы живем в неспокойное время. Интернет содрогается под ударами червей, и их активность стремительно усиливается. Ветер перемен приносит не только обрывки уничтоженной информации, но и свежесть надвигающейся бури. На горизонте собираются тучи, подсвечиваемые сполохами молний и подтверждающие серьезность своих намерений громовыми раскатами. Пять опустошительных эпидемий за три последних года, миллионы зараженных машин. И все из-за ошибок переполнения! Только по счастливой случайности и незлобному настрою вирусописателей, ни один из червей ни уничтожал информацию. А ведь мог бы! Только представьте, что произойдет с земной цивилизаций, если стратегически важные узлы лишатся всех своих данных. А ведь это произойдет… со временем…

утраченное звено

Черви относятся к наиболее независимым обитателям кибернетического мира. История их создания уходит своими конями в глубокую древность, перенося нас мезозойскую эру, когда землей правили динозавры – огромные неповоротливые ламповые ЭВМ, издающие при работе ужасный треск и скрежет. Пионеры компьютерной индустрии, ныне должностные лица респектабельных корпораций, а в прошлом – небритые студены с жаждой деятельности в глазах (кто читал "хроники лабораторий", тот поймет), активно экспериментировали с биокибернетическими моделями, пророча им блестящее будущее. Во время становления информатики как науки Настоящие Программисты (Real Programmer) были насквозь пропитаны духом энтузиазма, казалось еще вот-вот и грохочущее создание приобретет интеллект, а вместе с ними – навыки самосовершенствования и саморазмножения. Термин "вирус" еще не был выпущен из бутылки и никто не видел в биокибернетических механизмах ничего порочного. О них говорили в курилках, они обсуждались на высоком научном уровне, им выделялось драгоценное машинное время…

С приходом к власти корпораций все изменилось. Информатика из науки превратилась в публичную девку капитализма, торгующую собой и не интересующуюся ничем, кроме прибыли. Программное обеспечение раскололось на "правильное" и "неправильное". Правильное – это такое, которым можно торговать. "Неправильное" – написанное не ради денег, не с целью получения научных гарантов, которые сейчас выклянчивает каждый, кто горазд, и даже не под эгидой агрессивной идеологии Open Source, а для собственного удовольствия и удовлетворения программистского зуда, который сжигает вас изнутри, гонит вперед, подбрасывает ночами из постели, подкидывая новые идеи, которые тут же необходимо опробовать. Вот это – настоящее! Это не электронная таблица, и не база данных, созданная для тупых клерков. В каждой сточке кода – частичка вас самих, вашей души, придающая смысл всему происходящему. Это то звено, что отличает ремесло от конвейера, но к сожалению оно сейчас оказалось практически утрачено. Электронно-вычислительные машины перестали вызывать благоговения, сократиливись до "компа", и мистическое чувство единения с ними рассыпалось, исчезло…

явление червя народу

Червями называют разновидность вирусов, размножающихся без участия человека. Если файловый вирус активируется лишь при запуске зараженного файла, то сетевой червь проникает в твою машину *самостоятельно*, достаточно лишь просто войти в Интернет. По сути, черви являются высоко автономными роботами, брошенными в пучину всемирной сети и вынужденными бороться за выживание. Червей можно сравнить с космическими зондами, конструктор которых должен предусмотреть все до мелочей, ведь потом исправить ошибку уже не удастся. Кстати, ошибки проектирования червей обходится намного дороже ошибок проектирования космический станций (сравните стоимость станций и убытки от вирусных атак). Мужики, вы только представьте: какая на вас лежит ответственность! Поэтому, пионерам червей лучше не писать. Учите мат. часть, ассемблер и TCP/IP протоколы. Забудьте о деструкции! Деструктивный код – это плохой код. На вандализм много ума не надо, а вот

ухитриться проникнуть в миллион удаленных узлов, при этом ни один из них не уронив – вот это цель, достойная истинного хакера!

вирус	когда обнаружен	что поражал	механизмы распространения	машин заразил
Вирус Морриса	1988, ноябрь	UNIX, VAX	отладочный люк в sendmail, переполнение буфера в finger, слабые пароли	6.000
Melissa	1999, ???	e-mail через MS Word	человеческий фактор	1.200.000
LoveLetter	2000, май	e-mail через VBS	человеческий фактор	3.000.000
Klez	2002, июнь	e-mail через баг в IE	уязвимость в IE с IFRAME	1.000.000
sadmind/IIS	2001, май	Sun Solaris/IIS	переполнение буфера в Sun Solaris AdminSuite/IIS	8.000
Code Red I/II	2001, июль	ISS	переполнение буфера в IIS	1.000.000
Nimda	2001, сентябрь	ISS	переполнение буфера в IIS, слабые пароли и др.	2.200.000
Slapper	2002, июль	Lunix Apache	переполнение буфера в OpenSSL	20.000
Slammer	2003, январь	MS SQL	переполнение буфера в SQL	300.000
Love San	2003, август	NT/200/XP/2003	переполнение буфера в DCOM	1.000.000 (???)

Таблица 1 Top10 парад сетевых вирусов – от Червя Морриса до наших дней (указанное количество зараженных машин собрано из различных источников и не слишком-то достоверно, поэтому не воспринимайте его как истину в первой инстанции)

конструктивные особенности червя

С анатомической точки зрения, червь представляет собой морфологически неоднородный механизм, в котором можно выделить по меньшей мере три основных компонента: компактную **голову** и протяжный **хвост** с ядовитым **жалом**. Разумеется, это только схема, и черви ей совсем не обязаны подчиняться.

Необходимость дробления монолитной структуры червя на голову и хвост вызвана ограниченным размером переполняющихся буферов, который в подавляющем большинстве случаев не превышает пары десятков байт. Только самым крохотным и примитивным червям удается втиснуться в этот объем целиком, в остальных же случаях, сначала на атакуемую машину забрасывается загрузчик, устанавливающий TCP/IP-соединение и подтягивающий оставшийся хвост, иначе называемый основным телом червя.

Голова червя отвечает за переполнение буфера, захват управления удаленной машиной, установку TCP/IP-соединения и транспортировку хвоста. Образно говоря, голова – это ниндзя, десантирующийся в укрепленный район вражеского подразделения, бесшумно делающий охране харакири, отпирающий ворота и зажигающий посадочный маяк, обеспечивающий приземление основной группы. Как минимум голова червя включает в себя запрос посылаемый серверу, срывающий крышу одному из его буферов, и передающий управление либо на shell-код, либо на секретную функцию root, обеспечивающую удаленный доступ к серверу. Голова червя чаще всего пишется на голом ассемблере, а в наиболее ответственных случаях – непосредственно в машинном коде (трансляторы ассемблера не переваривают многих эффективных трюков и извращений).

Собственно говоря, голов у червя может быть и несколько, тогда он сможет поражать несколько различных типов серверов (например, MS SQL, MS IIS и SendMail сервера), значительно расширяя ареал своего обитания. У червя Морриса было две головы – она поражала finger, другая – sendmai, а MWORM'a целых пять, что позволяло ему распространятся через web, ftp-сервера и дыры в rpc, bind и lpd демонах. Love San, Slapper и Slammer имели по одной голове, что совсем не помешало занять им первые места в TOP10. Как видно, количество голов само по себе еще ни о чем не говорит и одна умная голова лучше трех тупых.

```
GET /default. ida?
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u
8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00= a HTTP 1.0
Content- type: text/ xml,
Content- length: 3379
```

Листинг 1 голова червя Code Red, приходящая в первом TCP-пакете запроса

Хвост червя решает намного более общие задачи. Оказавшись на территории вероятного противника, спецназ должен первым делом окопаться, укоренившись в системе. Некоторые черви зарываются в исполняемые файлы, прописывая путь к ним в ключе автоматического запуска, некоторые довольствуются одной лишь оперативной памятью, погибая после выключения питания или перезагрузки. И, знаете, это правильно! Настоящий червь должен вести кочевую жизнь, блуждая от машины к машине – в этом и есть его предназначение. Как говориться, мавр сделал свое дело и может уходить, а сделать червю предстоит не так уж и много: найти по меньшей мере две жертвы, пригодные для внедрения, и забросить в них свою голову (точнее, копии своих голов, ну чем вам не ракета носитель с разделяющейся боеголовкой?). Теперь, даже если червь умрет, численность его популяции будет расти в геометрической прогрессии. Ввиду высокой алгоритмической сложности и отсутствию ограничений на предельно допустимый размер, хвост червя чаще всего разрабатывается на языках высокого уровня, например, языке Си, хотя Форт или Алгол подошли бы ничуть не хуже, но это уже дело вкуса, о котором не спорят (но Си все равно лучше).

```
rt_init()/* 0x2a26 */
{
        FILE *pipe;
        char input_buf[64];
        int l204, l304;

        ngateways = 0;
        pipe = popen(XS("/usr/ucb/netstat -r -n"), XS("r"));
        /* &env102,&env 125 */
        if (pipe == 0) return 0;
        while (fgets(input_buf, sizeof(input_buf), pipe))
        { /* to 518 */
                other_sleep(0);
                if (ngateways >= 500) break;
                sscanf(input_buf, XS("%s%s"), l204, l304);/* <env+127>"%s%s" */
                /* other stuff, I'll come back to this later */

        }/* 518, back to 76 */
        pclose(pipe);
        rt_init_plus_544();
        return 1;
}/* 540 */
```

Листинг 2 хвост червя Морриса (по соображениям экономии места здесь приведен лишь его крошечный фрагмент)

Подавляющее большинство червей не ядовито и весь вред от них сводится к перегрузке сетевых каналов из-за неконтролируемого размножения. Лишь у немногих на конце хвоста расположено ядовитое жало или в более общем случае полезная нагрузка (читай – боевая начинка). Например, червь может устанавливать на атакуемой машине терминальный shell, предоставляющий возможность удаленного администрирования. До тех пор пока эпидемия такого червя не будет остановлена, в руках его создателя окажутся рычаги управления нашим миром и он в любой момент сможет прервать его бренное существование. Нет, атомные электростанции взорвать не удастся, но вот подорвать экономику, уничтожив банковскую информацию сможет даже начинающий хакер и скажу вам по секрету, знающие люди утверждают: такая угроза возникала уже неоднократно и лишь грубые ошибки, допущенные при проектировании червей не позволили ей воплотиться в реальность. Так что учите мат. часть!

Последний писк моды – модульные черви, поддерживающие возможность удаленного конфигурирования и подключения плагинов через Интернет. Только прикиньте, насколько усложняется борьба в условиях непрерывно изменяющейся логики поведения червя. Администраторы ставят фильтры, а червь их успешно преодолевает! Запускают антивирус, червь подхватывает брошенный ему щит и, воспользовавшись замешательством противника, со всей дури бьет его по голове. Правда и проблем здесь тоже хватает. Система распространения плагинов должна быть не только полностью децентализовна и еще и уметь при случае постоять за себя, иначе администраторы подкинут плагин-бомбу, ко всем чертям разрывающую червя на куски. В общем, тут есть еще над чем подумать и поработать!

долг перед видом или рожденный, чтобы умереть

Считается, что естественная цель всех живых организмов (и червей в том числе) это неограниченная экспансия или попросту говоря, захват всех свободных и несвободных территорий. На самом деле, это неверно. Чтобы не подохнуть от голода, каждый индивидуум должен находится в гармонии с окружающей средой, поддерживая баланс численности своей популяции в равновесии. Нарушение этого правила оборачивается неизменной катастрофой.

Червь должен бережно относится к "природным" ресурсам кибернетического мира – оперативной и дисковой памяти, процессорному времени и пропускной способности сетевых каналов, по братски разделяя их с остальными обитателями "глубины". Предоставленные сами себе черви размножаются в геометрической прогрессии и численность их популяции взрывообразно растет. А ведь толщина магистральных Интернет-каналов не безгранична! Рано или поздно, сеть насыщается червями и "встает", не только препятствуя их дальнейшему размножению, но и поднимая с постели матерящихся администраторов, устанавливающих свежие заплатки и перетирающих червей в труху. Поймите же вы наконец, что администраторы объявляют войну лишь тем червям, которые им сильно досаждают. Ведите себе скромнее! Будьте тише травы и ниже радаров!

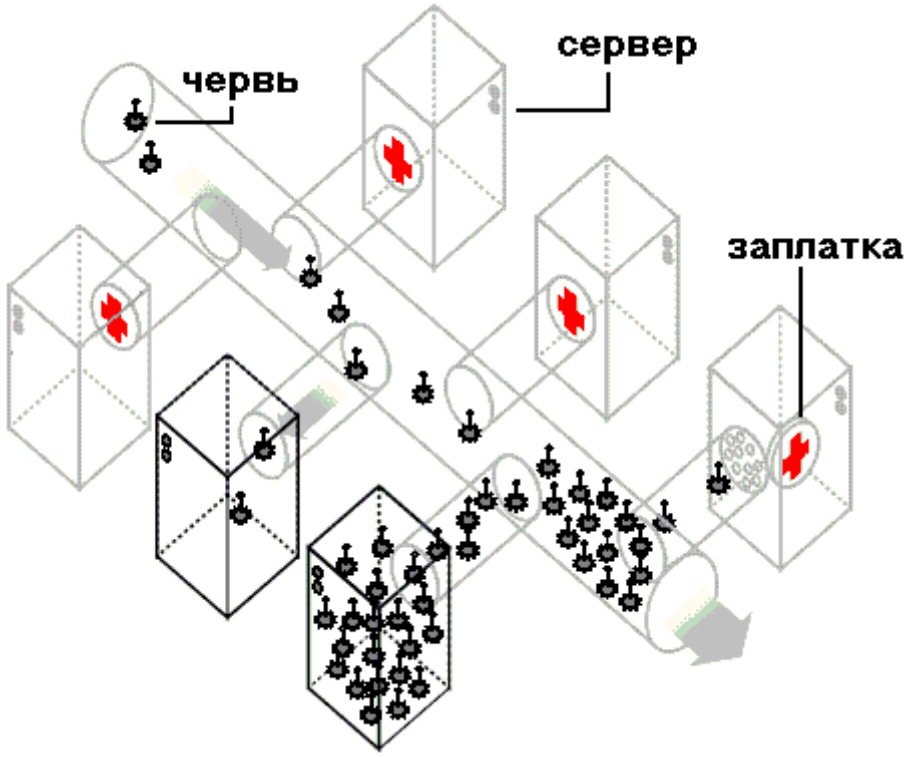

Рисунок 1стремительное размножение червей вызывает запор

тактика и стратегия инфицировано

Основные враги ниндзя это: темнота, неизвестность, колючая проволока фрайволов и волкодавы, снующие по охраняемой территории.

Подготовка к заброске shell-кода начинается с определения IP-адресов, пригодных для вторжения. Если червь находится в сети класса C, три старших бита IP-адреса которой равны "110", то ее можно и просканировать (распотрошите любой сканер, если не знаете как). Сканирование сетей остальных классов занимает слишком много времени и немедленно привлекает к себе внимание администраторов, а вниманием администраторов черви предпочитают не злоупотреблять. Вместо этого они выбирают пару-тройку случайных IP-адресов, выдерживая каждый раз секундную паузу, дающую TCP/IP пакетикам время на рассосаться и предотвращающую образование "запоров". Червь Slammer, поражающий SQL сервера, не делал такой паузы и поэтому сдох раньше времени, а вот Love San жив и поныне. Nimda и некоторые другие черви, не играют в кости и определяют целевые адреса

эвристическим путем: анализируя содержимое жесткого диска (перехватывая проходящий сквозь них трафик), они ищет url'ы, e-mail'ы и прочие полезные ссылки, занося их в список кандидатов на заражение.

Затем кандидаты проходят предварительное тестирование. Червь должен убедиться, что данный IP-адрес действительно существует, удаленный узел не висит и на нем установлена уязвимая версия сервера или операционная система, известная червю и совместимая с shell-кодом одной или нескольких его голов.

Первые две задачи решаются предельно просто: червь отправляет серверу легальный запрос, на который тот обязан ответить (для WEB-сервера это запрос GET), и если сервер что-то промычит в ответ, значит, жив курилка! Заметим, что отправлять серверу эхо-запрос, более известный в народе как "ping", неразумно, т. к. его может сожрать недружелюбно настроенный брандмауэр (помните историю про Красную Шапочку?).

С определением версии сервера дела обстоят значительно сложнее и универсальными решениями здесь и не пахнет. Некоторые протоколы поддерживают специальную команду или возвращают версию сервера в строке приветствия, но чаще всего информацию приходится добывать по косвенным признакам. Различные операционные системы и сервера по разному реагируют на нестандартные пакеты или проявляют себя специфическими портами, что позволяет осуществить грубую идентификацию жертвы. А точная червю нужна как зайцу панталоны, а собаке пятая нога – главное отсеять заведомо неподходящих кандидатов. Если забросить голову червя на неподходящий укреп район, ничего не произойдет. Голова, точнее копия головы погибнет, только и всего.

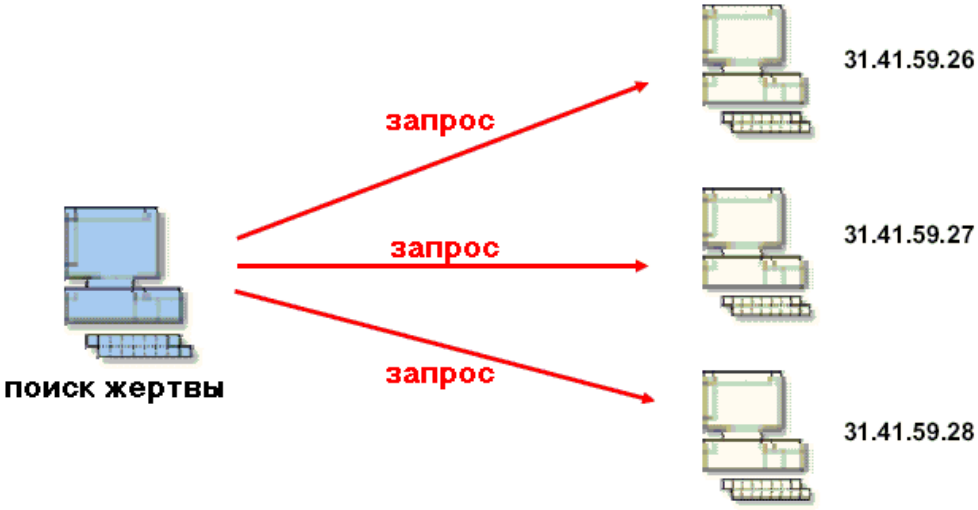

Рисунок 2 червь рассылает запросы по различным IP-адресам

На завершающей стадии разведывательной операции червь посылает удаленному узлу условный знак, например, выпускает две зеленые ракеты (отправляет TCP-пакет с кодовым посланием внутри). Если узел уже захвачен другим червем, он должен выпустить в ответ три фиолетовых. Это наиболее уязвимая часть операции, ведь если противник (администратор) пронюхает об этом, вражеский узел без труда сможет прикинуться "своим", предотвращая вторжение. Такая техника антивирусной защиты называется "вакцинацией" и для борьбы с ней черви раз в несколько поколений игнорируют признак заражения, и захватывают узел повторно, чем и приводят свою популяцию к гибели, ибо все узлы инфицируются многократно и через некоторое время начинают кишеть червями, сжирающими все системные ресурсы со всеми отсюда вытекающими последствиями.

Выбрав жертву, располагающую к вторжению, червь посылает серверу запрос, переполняющий буфер и передающий бразды правления shell-коду, который может быть передан как вместе с переполняющимся запросом, так и отдельно от него. Такая стратегия вторжения называется многостадийной и ее реализует в частности червь Slapper.

При подготовке shell-кода следует помнить о брандмауэрах, анализирующих содержимое запросов и отсекающих все подозрительные пакеты. Этим, в частности, занимаются

фильтры уровня приложений. Чтобы избежать расстрела, shell-код должен соответствовать всем требованиям спецификации протокола и быть синтаксически неотличимым от нормальных команд. Ведь фильтр анализирует отнюдь ***не содержимое*** (на это у него кишка тонка), а лишь ***форму*** запроса. Типа – за Штирлецем тащился парашют…

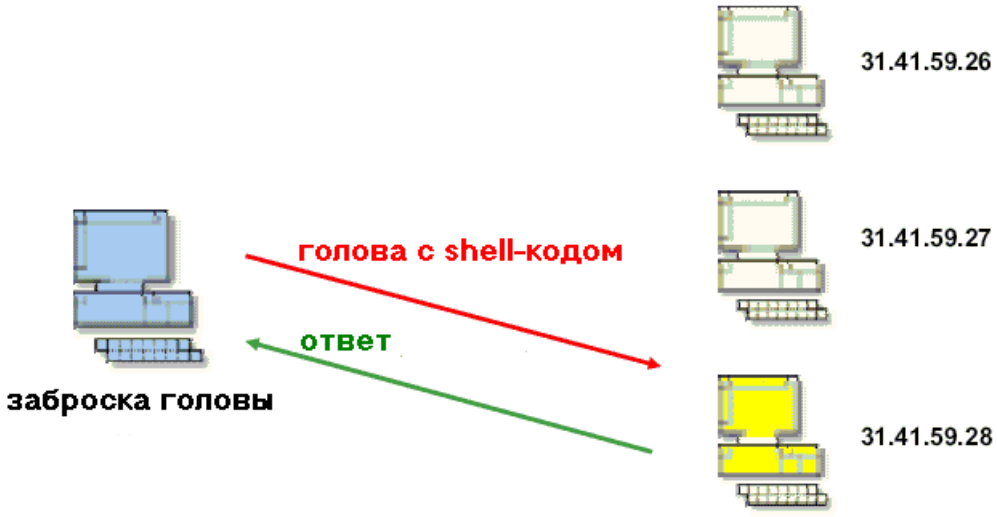

Рисунок 3 червь получает ответ, идентифицирующий подходящую жертву, и забрасывает голову, начиненную shell-кодом

Если захват управления пройдет успешно, shell-код должен найти дескриптор TCP/IP соединения, через которое он был заслан и подтянуть оставшийся хвост (этом можно сделать лобовым перебором всех сокетов через функцию getpeername). Проще конечно было бы затащить хвост через отдельное TCP/IP соединение, но если противник окружил себя грамотно настроенным брандмауэром, хрен вы через него пробьетесь, скажу я вам. А вот использовать уже установленные TCP/IP соединения никакой брандмауэр не запрещает.

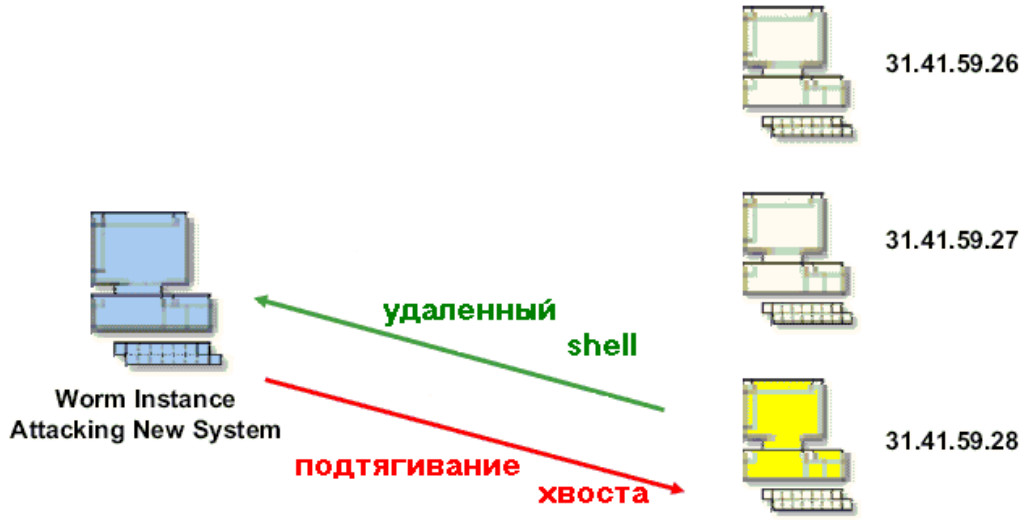

Рисунок 4 голова переполняет буфер, захватывает управление и подтягивает основной хвост

И вот вся группа в сборе. Роем окопы от меня до обеда! Самое идиотское, что только может предпринять спецназ, это сгрузить свою тушу в исполняемый файл, затерявшийся в густонаселенных трущобах Windows\System32 и автоматически загружающийся при каждом старте системы по ключу HKLM\Software\Microsoft\Windows\CurrentVersion\Run. Хорошее же

вы место выбрали для засады, молодцы, нечего сказать! Стоит дотянуться администратору до клавиатуры, как от червя и мокрого места не останется. А вот если червь внедряться в исполняемые файлы на манер файловых вирусов, тогда его удаление потребует намного больше времени и усилий.

Для проникновения в адресное пространство чужого процесса червь должен либо создать в нем удаленный поток, вызвав функцию CreateRemoteThread, либо отпатчить непосредственно сам машинный код, вызвав WriteProcessMemory (разумеется, речь идет лишь об NT-подобных системах, UNIX требует к себе принципиально иного подхода).

Как вариант, можно прописаться в ветке реестра, ответственной за автоматическую загрузку динамических библиотек в адресное пространство каждого запускаемого процесса: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs, тогда червь получит полный контроль над всеми событиями, происходящими в системе, например, блокируя запуск неугодных ему программ – интересно, сколько штанов поменяет администратор, прежде чем разберется в чем дело?

Окопавшись в системе, червь приступает к поиску новых жертв и рассылке своей головы по подходящим адресам, предварительно уменьшив свой биологический счетчик на единицу, а когда тот достигнет нуля – вызывающий процедуру самоликвидации.

Таков в общих чертах жизненный цикл червя, такого его карма.

Рисунок 5 захваченный узел становится новым бастионом, продолжающим распространение червя

заключение

Черви приходят из мрака небытия, рождаясь в подсознании их создателей и уходят ту да же. Черви не умирают. Они трансформируются в новые идеи. Первым известным червем был вирус Морриса. Последним – Love San. Будущее всемирной сети в ваших руках и мозгах, друзья.