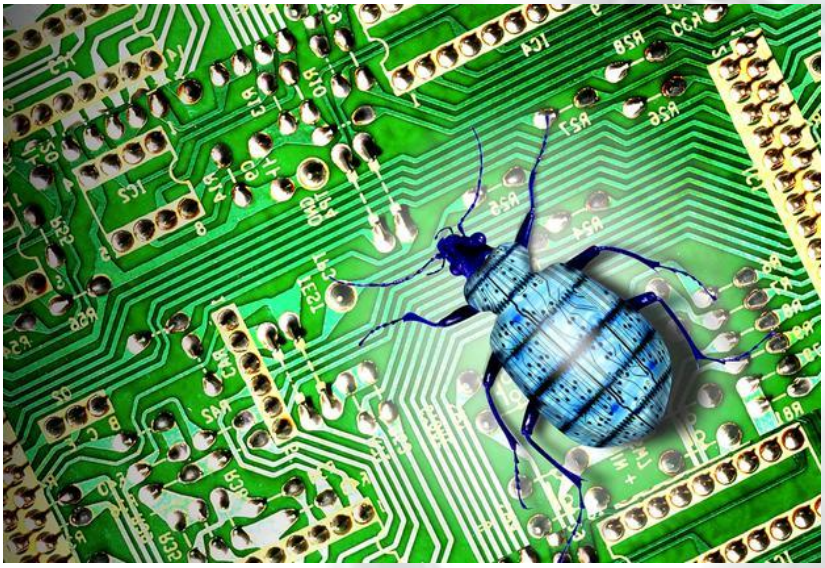
БЕЗОПАСНОСТЬ. НИЧЕГО ЛИШНЕГО

Операция Windigo

Сегодня мы рассмотрим вредоносную кампанию «Windigo», в ходе которой злоумышленники компрометировали тысячи Linux и UNIX серверов. Скомпрометированные серверы использовались для кражи учетных данных SSH, перенаправления пользователей веб-сервисов на вредоносный код и рассылку спама. Эта операция началась предположительно в 2011 г. и привела к компрометации различных крупных серверов и компаний, включая, известную cPanel, которая разрабатывает одноименную известную панель управления хостингом. Другой крупной жертвой этой кампании стал известный ресурс kernel.org, который представляет собой основной репозиторий исходного кода для ядра Linux.



Мы уже частично писали про вредоносные программы, которые использовались в этих кампаниях, в наших отчетах в прошлом и в этом году [1,2], однако, теперь у нас есть более полная картина происходящего, а также анализ других вредоносных программ, которые использовали злоумышленники. Ранее были упомянуты бэкдоры **Linux/Ebury** и **Linux/Cdorked**, которые применялись для кражи учетных данных различных сервисов на сервере, а также для перенаправления посетителей веб-сервисов на вредоносные ресурсы. Кроме них в операцию Windigo была вовлечена вредоносная программа **Perl/Calfbot**, с помощью которой зараженные серверы могли генерировать миллионы спам-сообщений в день.

Ключевые находки

- Операция Windigo началась не позднее 2011 года
- За последние два года были скомпрометированы более 25 тыс. серверов.
- Атакующим удалось скомпрометировать большое количество ОС, включая, Apple OS X, OpenBSD, FreeBSD, MS Windows и Linux.
- Некоторые вредоносные программы являются переносимыми на уровне ОС. Спам-бот Perl/Calfbot может работать на любой ОС, в которой установлен интерпретатор Perl, а SSH бэкдор может работать как на Linux, так и на FreeBSD серверах.
- Как мы отмечали в самом начале, такие крупные организации как cPanel и Linux Foundation стали жертвами этой атаки.

- Windigo отвечает за рассылку около 35 миллионов спам-сообщений в день.
- Более 700 веб-серверов на текущий момент все еще перенаправляют пользователей на вредоносное содержимое.
- Каждый день более полумиллиона посетителей скомпрометированных Windigo веб-ресурсов перенаправлялись на набор эксплойтов.
- Уровень заражений пользователей вредоносным кодом в результате успешного перенаправления составляет около 1%.
- Вредоносные программы Windigo разработаны на достаточно высоком уровне: в них используются техники сокрытия присутствия в системе, переносимость между различными платформами, криптография. Помимо этого, можно отметить высокий уровень знаний атакующих в системе Linux.
- HTTP бэкдор переносим между сервисами Apache httpd, Nginx и lighttpd.
- Атакующие максимально используют возможности ресурсов скомпрометированного сервера, запуская на нем различное вредоносное ПО и другую активность, в зависимости от уровня доступа, который был ими получен.
- Для получения доступа к серверам злоумышленники использовали украденные учетные данные, а также backdoored-apps (изначально скомпрометированные приложения) вместо эксплуатации каких-либо уязвимостей.

Общая информация

Windigo была раскрыта ESET совместно с CERT-Bund, исследовательским центром SNIC и европейской организацией ядерных исследований (CERN). Для получения доступа к серверам атакующими не применялись какие-либо эксплойты для удаленного исполнения кода, вместо этого использовались скомпрометированные вредоносным содержимым дистрибутивы различных программ для Linux, а также изначально полученные аутентификационные данные учетных записей для входа на сервер. В дальнейшем база украденных данных учетных записей для компрометации новых серверов пополнялась за счет вновь зараженных машин.

Злоумышленники извлекали выгоду из этой кампании за счет выполнения следующих вредоносных операций:

- рассылка спама;
- заражение пользователей скомпрометированных серверов (drive-by);
- перенаправление пользователей скомпрометированных серверов на рекламные сайты.

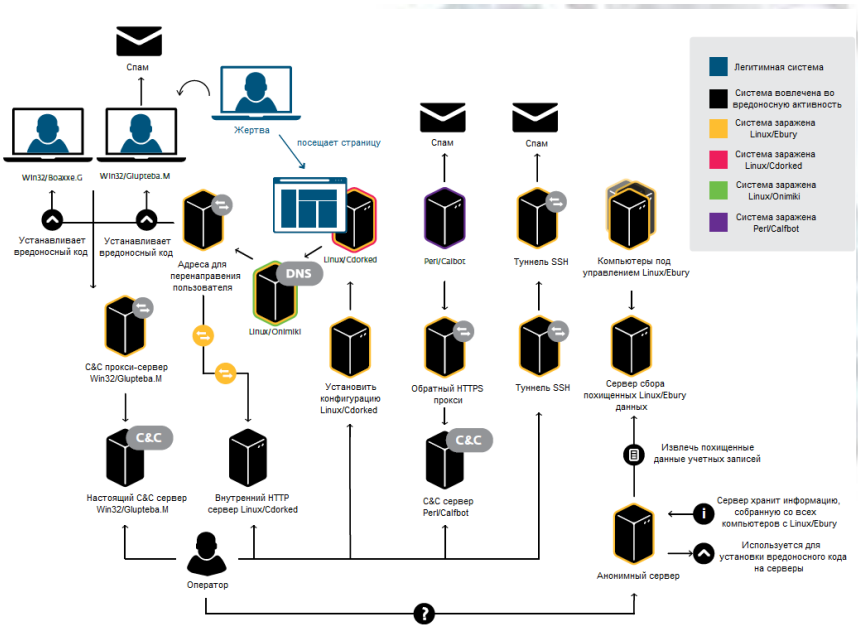


Рис. Взаимодействие различных компонентов вредоносных программ и сервисов, используемых в Windigo.

Следующие вредоносные программы использовались злоумышленниками в операции Windigo:

- **Linux/Ebury** компрометирует серверы под управлением Linux. Предоставляет злоумышленникам полный доступ к системе через командную строку (root backdoor shell), а также имеет возможность кражи учетных данных SSH.
- **Linux/Cdorked** компрометирует веб-серверы под управлением Linux. Предоставляет злоумышленникам полный доступ к системе через командную строку и отвечает за заражение вредоносным кодом пользователей Windows (drive-by).
- **Linux/Omniki** компрометирует DNS-серверы Linux. Отвечает за преобразование доменных имен, которые совпадают с определенным шаблоном, в соответствующие IP-адреса, без необходимости модификации настроек конфигурации на стороне сервера.
- **Perl/Calfbot** компрометирует ОС, которые имеют в своем составе установленный пакет интерпретатора Perl. Отвечает за рассылку спама (спам-бот).
- **Win32/Boaxxe.G** представляет из себя вредоносный код для организации кликфрода, а также **Win32/Glupteba.M**, используемый злоумышленниками как прокси сервис для Windows. Распространяются через drive-by зараженных серверов.

Вредоносная активность	Вредоносный код
Спам	Win32/Glupteba.M, Perl/Calfbot, Linux/Ebury
Drive-by download	Linux/Cdorked
Рекламный кликфрод	Linux/Cdorked, Win32/Boaxxe.G
Кража данных учетных записей	Linux/Ebury

Ниже указана хронология развития событий, связанных с Windigo.

Кража данных учетных записей

Как мы уже упоминали выше, кража учетных данных SSH является единственной обнаруженной методикой, с помощью которой злоумышленники расширяли операцию Windigo и получали доступ к новым жертвам. Существуют два типичных сценария кражи учетных данных SSH. Первый заключается в краже этих данных, когда пользователь совершает успешную операцию входа на зараженном сервер. Другой сценарий подразумевает собой похищение данных, когда пользователь (или администратор) использует зараженный сервер для входа на любую другую систему. Linux/Ebury является основным элементом в операции Windigo, так как отвечает за кражу данных учетных записей.

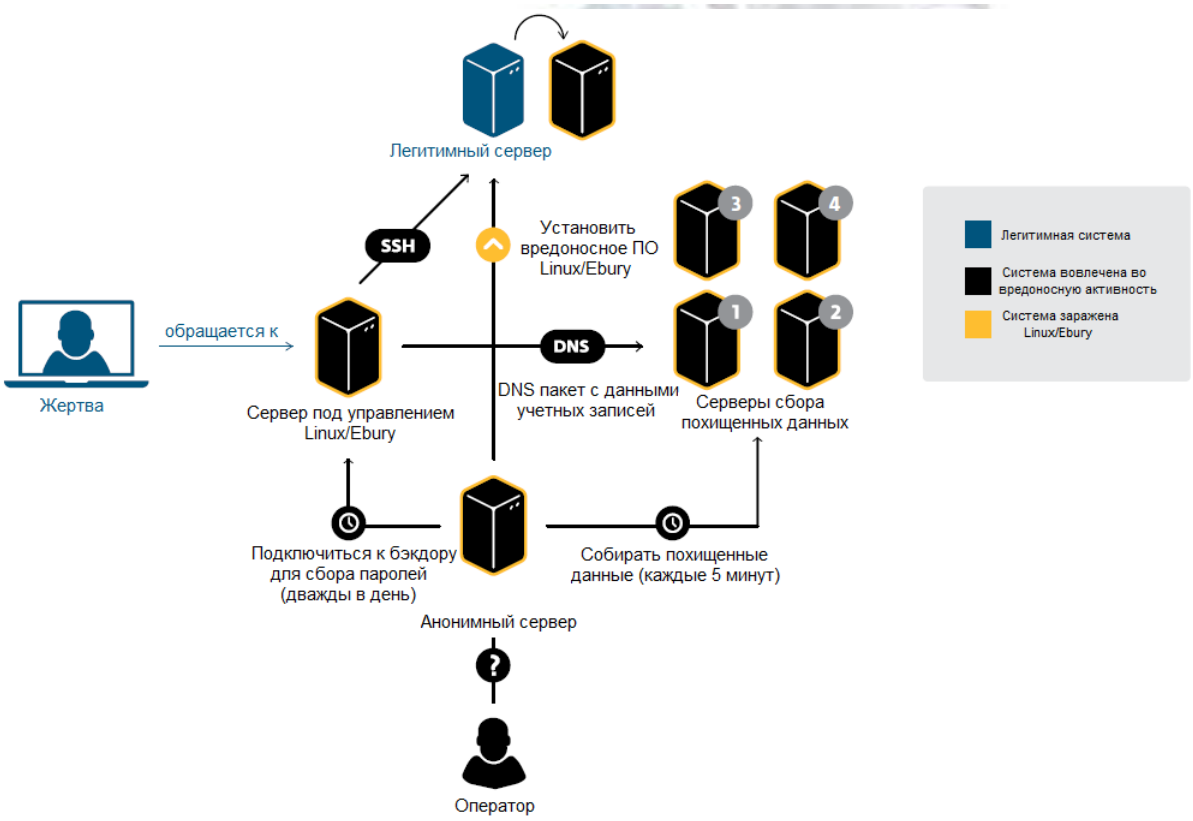


Рис. Схема кражи данных учетных записей с помощью Linux/Ebury.

Перехваченные Linux/Ebury данные отправляются на специальные серверы сбора похищенных данных (exfiltration servers) через специальные DNS-запросы. Эти учетные данные потом будут использоваться атакующими для дальнейшего распространения заражений. Группа атакующих использует специальные анонимные туннельные сервисы (anonymizing tunnel services) на одном из скомпрометированных серверов, для выполнения операции подключения к серверам, от которых были получены данные учетных записей. Это позволяет им оставаться незамеченными больше времени. Упомянутый сервер также используется для извлечения похищенных данных учетных записей.

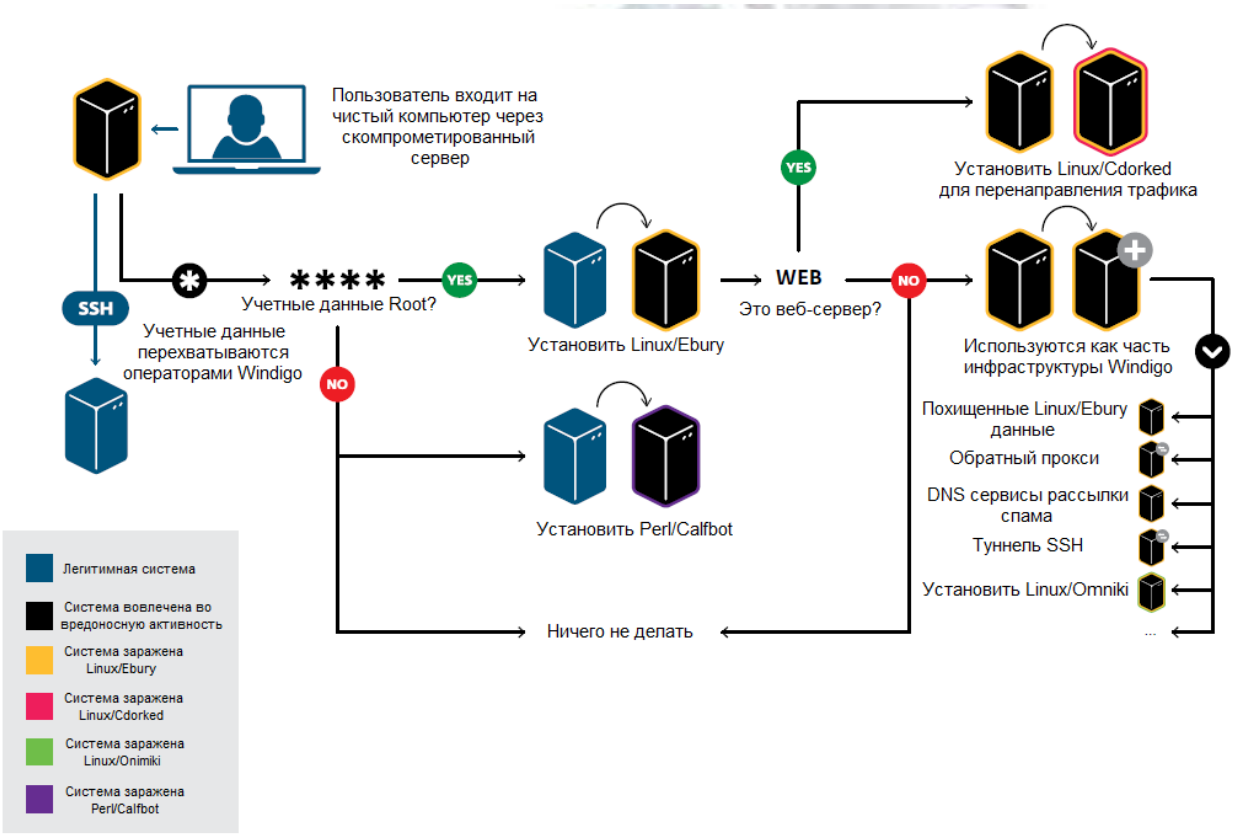


Рис. Схема кражи данных учетных записей операторами Windigo.

После того как украденные данные учетных записей оказались в руках операторов Windigo, они проверяются на уровень доступа, который они предоставляют в случае успешного входа. В случае, если учетная запись не предоставляет права root, сервер может остаться нетронутым, т. е. не подвергнутся компрометации, либо на него будет установлена вредоносная программа Perl/Calfbot. Если учетная запись предоставляет доступ root, то на сервер устанавливается Linux/Ebury, с помощью которого атакующие получают доступ к серверу для удаленного управления. В некоторых случаях атакующие устанавливают Perl/Calfbot даже при полученных правах root, но это скорее исключение.

Перенаправление трафика и заражение пользователей

Если на скомпрометированном сервере функционирует один или несколько веб-сайтов, то в такую систему будет установлен Linux/Cdorked. Кроме этого, злоумышленники могут развернуть на сервере другие вредоносные сервисы. Например, если сервер обслуживает 443-й HTTPS порт и он доступен из Интернета, тогда на этот сервер будет установлен экземпляр обратного прокси nginx, он будет использоваться как звено между ботом Perl/Calfbot и настоящим C&C сервером.

Веб-серверы, зараженные Linux/Cdorked, перенаправляют пользователей на серверы наборов эксплойтов, которые пытаются заразить их вредоносным кодом. Ниже представлена схема того, как это происходит.

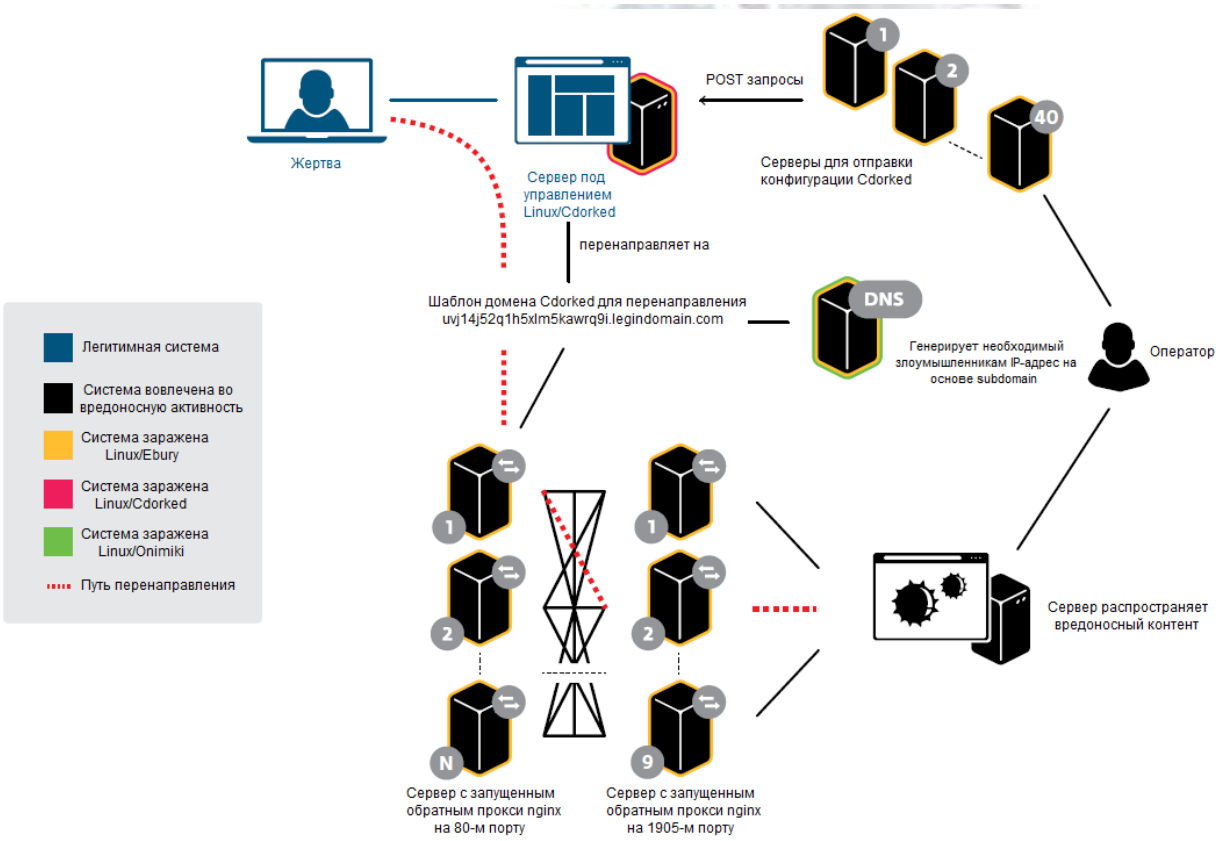


Рис. Инфраструктура атакующих, которая используется для организации перенаправления трафика.

Логика перенаправления основана на трех этапах:

1. Пользователь посещает легитимный сайт, размещенный на зараженном Linux/Cdorked сервере, который затем перенаправляет его на специальный вредоносный домен, который формируется на основе оригинального домена (новый subdomain). Это перенаправление осуществляется через набор зараженных серверов Linux/Ebury и зависит от определенных условий, предусмотренных операторами.
2. Прежде доверенный DNS-сервер уже заражен одним из компонентов Windigo, который называется Linux/Onimiki, и возвращает соответствующий IP-адрес для последующего перенаправления (необходимый IP-адрес кодируется в subdomain, который был добавлен на предыдущем этапе). Так как в результате перенаправления используется легитимный домен, это позволяет скрывать факт подмены адреса на вредоносный, что делает обнаружение этой операции более сложной задачей. Возвращенный IP-адрес принадлежит обратному прокси-серверу.
3. Этот сервер является точкой входа в цепочку обратных прокси-серверов, которая обрывается на сервере, обслуживающим набор эксплойтов. Он отвечает за установку вредоносного кода на компьютер пользователя и может перенаправлять его на рекламные сайты.

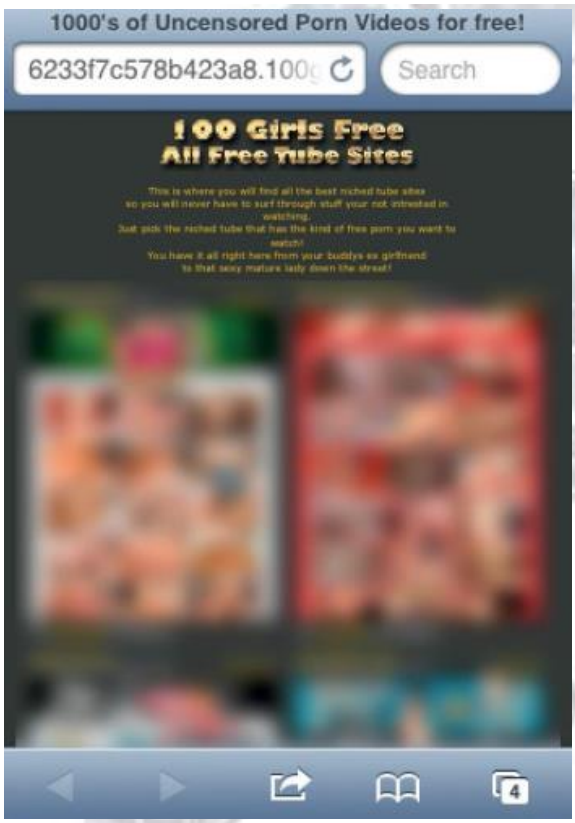


Рис. Если жертва работает под iOS (iPad, iPhone, iPod), она перенаправляется на порно-контент (Linux/Cdorked).

В следующей таблице приведена статистика по IP-адресам зараженных веб-серверов за последние три месяца с момента составления отчета, а именно, ноябрь 2013, декабрь 2013 и январь 2014.

Дата получения информации	Количество уникальных IP-адресов зараженных компьютеров
Ноябрь 2013	1,593
Декабрь 2013	831
Январь 2014	771

Таким образом за эти три месяца мы наблюдали 2,183 уникальных IP-адреса, которые были замечены в распространении вредоносного содержимого (заражены Linux/Cdorked). При этом 221 из этих адресов были активны все три месяца с начала момента отслеживания. Следующая карта показывает географическое распределение заражений Linux/Cdorked.

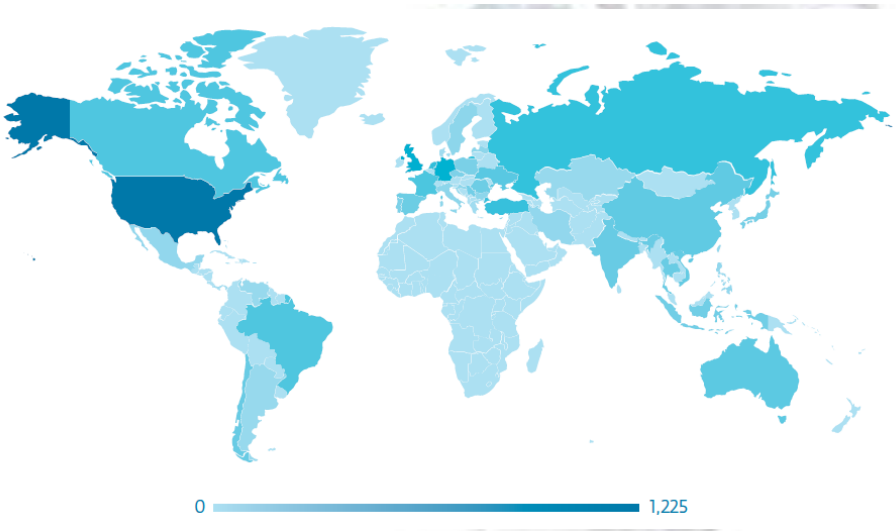


Рис. Распределение заражений серверов Linux/Cdorked по странам.

В таблице ниже показаны страны с наибольшим количеством заражений Linux/Cdorked.

Позиция	Страна	Количество IP-адресов
1	США	1,225
2	Великобритания	151
3	Германия	129
4	Голландия	65
5	Турция	61
	Другие	552
Всего		2,183

Рассылка спама

Одним из основных способов, с помощью которого операторы Windigo получают прибыль от установки вредоносных программ, является рассылка спама через электронную почту. Спам рассылается либо через серверы, зараженные Perl/Calfbot, либо через ПК пользователей, которые заражены Win32/Glupteba.M. Ниже мы рассмотрим случай рассылки спама вредоносной программой Perl/Calfbot.

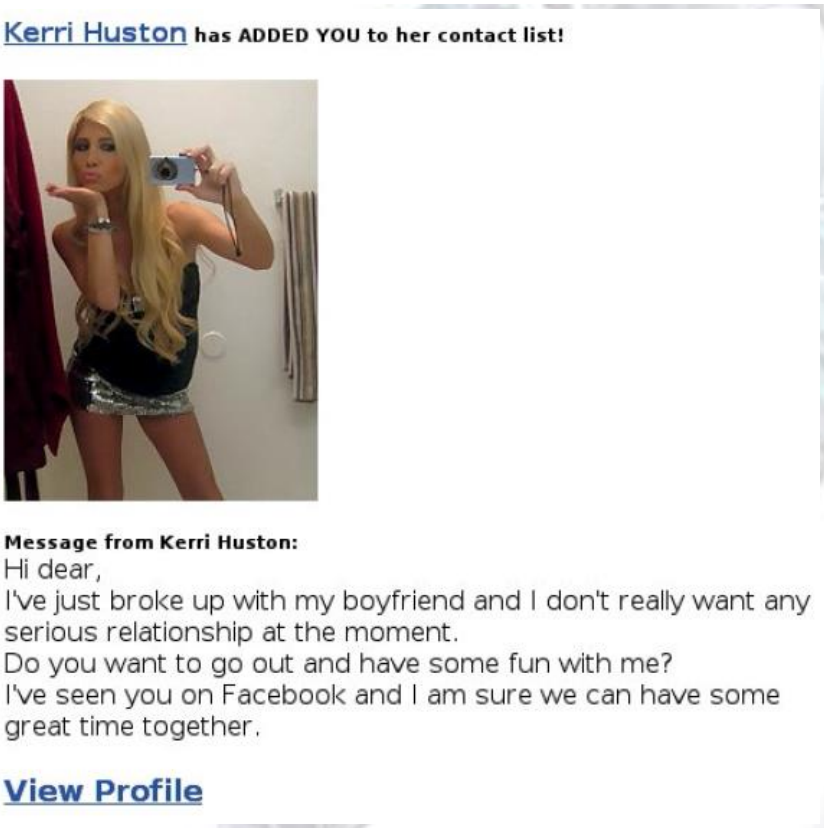


Рис. Пример спам-сообщения.

Мы использовали два различных подхода для понимания объемов и типов рассылаемого спама, генерируемого ботами Perl/Calfbot. Первый подход заключается в создании поддельного бота, который реализует соответствующий протокол работы с C&C сервером. Используя второй подход, мы обрабатывали захваченный сетевой трафик, полученный в январе 2014 г. на одном из обратных C&C прокси-серверов (C&C reverse proxy server) и, далее, экстраполировали эти результаты.

Поддельный клиент (бот) был разработан на основе реального бота Perl/Calfbot. Он используется для извлечения заданий по рассылке спама с C&C-сервера. Задания по рассылке спама представляют собой несколько шаблонов электронных сообщений и список адресатов. Мы проанализировали данные начиная с августа 2013, заканчивая февралем 2014. За этот период времени наш поддельный клиент получил 13,422 различных заданий по рассылке спама для его генерации на 20,683,814 уникальных email адреса. Следующая гистограмма показывает домены сервисов электронной почты, которые чаще всего использовались в качестве email адресов для рассылки спама.

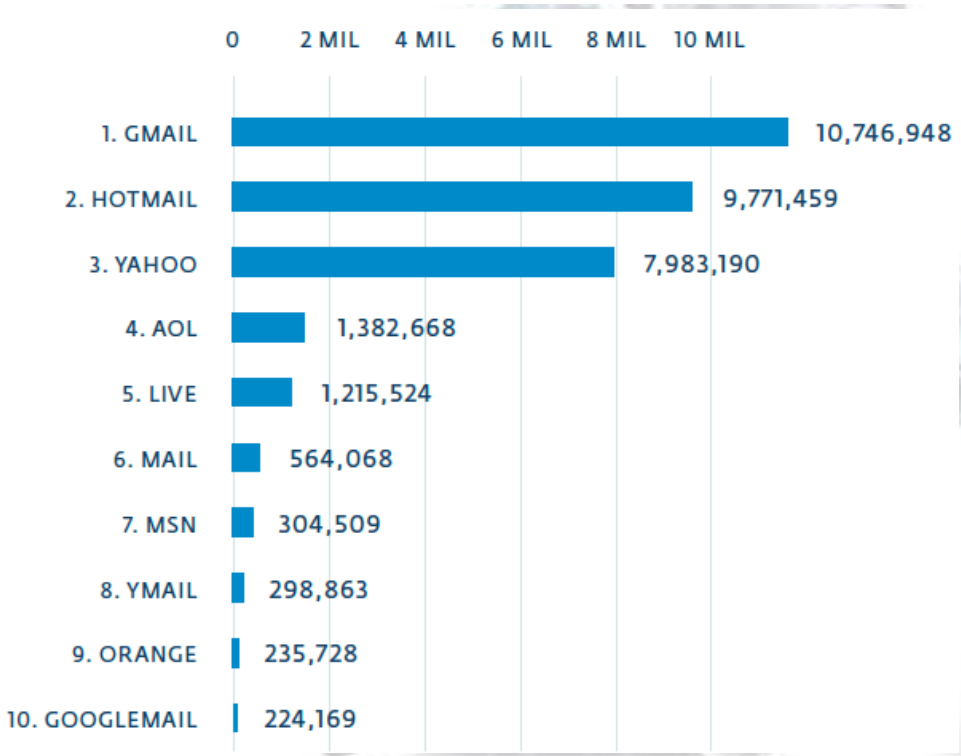


Рис. Сервисы электронной почты, пользователям которых чаще всего рассылался спам.

В результате анализа содержимого спам сообщений, мы выяснили, что в них есть несколько видов содержимого. Большинство из шаблонов сообщений посвящены тематике казино, бонусов и онлайн-знакомств. Многие сообщения содержат в тексте такие слова, замаскированные под ссылки, как «unsubscribe» (отписаться) и «report» (отчет), вероятно, это использовалось для того, чтобы избежать обнаружения спам сообщений со стороны средств безопасности. Возможно, злоумышленники фиксировали адреса тех пользователей, которые нажимали на эти ссылки, помечая их адреса как активные и использовали их в последующих рассылках.

Рис. Форма ввода email для «отписки» от рассылки.

Обычное задание на рассылку спама, которое доставлялось боту, содержит список из 3,000 адресов электронной почты и использует шаблоны сообщений на английском языке, хотя мы также наблюдали используемые французский, немецкий, испанский и русский языки. Все

шаблоны сообщений спама содержат URL-адреса, указывающие на домены, которые обслуживаются скомпрометированным сервером TinyDNS.

Drive-by

В сентябре прошлого года нам удалось получить сетевой трафик с одного из обратных прокси-серверов Linux/Cdorked. Несмотря на то, что эти данные были получены только с одного прокси-сервера, анализ этого трафика позволили нам оценить масштабы перенаправлений пользователей на вредоносный контент с зараженных серверов. Только за несколько дней мы наблюдали более миллиона различных IP-адресов, которые обращались к этому серверу, т. е. непосредственно до того как пользователь перенаправлялся на страницу набора эксплойтов. Часть из этих пользователей, которые были перенаправлены на вредоносный контент, подверглись заражению. Нам удалось получить статистику по ОС и браузерам пользователей, которые перенаправлялись на вредоносный контент за эти несколько дней.

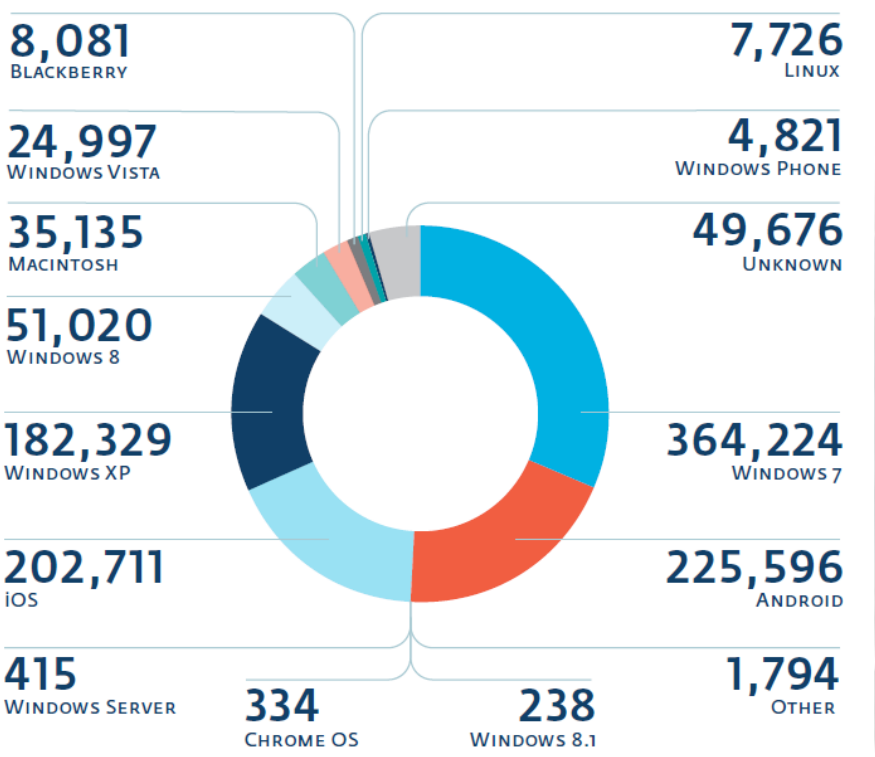


Рис. Распределение ОС пользователей, которые стали жертвами веб-сайтов, скомпрометированных Linux/Cdorked.

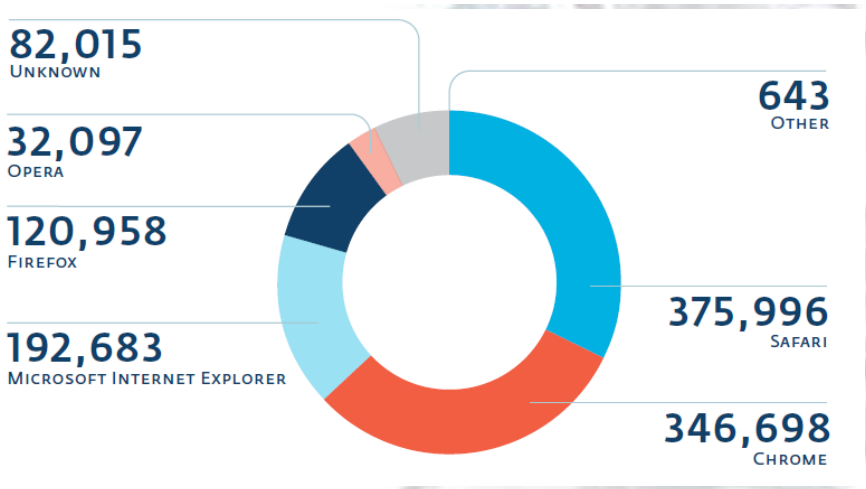


Рис. Распределение браузеров пользователей, которые стали жертвами веб-сайтов, скомпрометированных Linux/Cdorked.

Когда компьютер пользователя перенаправляется на внешний интерфейс обратного прокси-сервера, последний начинает цепочку перенаправлений на сервер набора эксплойтов, который таким образом скрыт за прокси-серверами, которые используются для этих перенаправлений. Конечным результатом такого перенаправления будет попадание пользователя на страницу с набором эксплойтов, откуда ему будет установлен вредоносный код (в случае уязвимости ОС/ПО для одного из применяемых эксплойтов).

На момент нашего анализа, операторы Windigo использовали набор эксплойтов Blackhole. В ноябре 2013 операторы переключились на набор эксплойтов Neutrino, скорее всего это произошло из-за ареста автора Blackhole, когда «клиенты» Paunch начали переходить на новые средства автоматической дистрибуции вредоносных программ. Мы подсчитали, что из 1,1 млн. перенаправленных пользователей, количество зараженных составило 11,108, т. е. около 1% (infection ratio).

Мы наблюдали два различных семейства вредоносных программ, которые таким образом распространялись злоумышленниками. Пользователи из США, Великобритании, Канады и Австралии были заражены вредоносным кодом Win32/Boaxxe.G, тогда как другие оказались заражены Win32/Leechole – вредоносной программой, которая представляет из себя установщик в систему Win32/Glupteba.M. Злоумышленники постоянно использовали эти семейства вредоносных программ для заражения Windows пользователей, по крайней мере, за все время нашего отслеживания этой кампании.

Полный анализ вредоносных программ, используемых в кампании Windigo, индикаторы компрометации (IOC) и другую полезную информацию вы можете найти в нашем детальном отчете.