ЛЕТНЯЯ МАЛВАРЬ 2016: СВЕЖАЯ, ГОРЯЧАЯ, ТВОЯ

Павел Шалин
аналитик,
«Доктор Веб»

ОБЗОР САМЫХ ИНТЕРЕСНЫХ ВРЕДОНОСОВ ЗА ПОСЛЕДНИЕ ТРИ МЕСЯЦА

Большинство вредоносных программ, которые ежедневно попадают в нашу вирусную лабораторию, не представляют для аналитиков особого интереса. Как говорится, все новое — это либо накрытое упаковщиком старое, либо слегка модифицированные образцы, позаимствованные кем-то из паблика. Изредка среди этого бесконечного потока попадается что-то по-настоящему любопытное — семпл, который можно обсудить с коллегами в курилке. Ну или рассказать о нем читателям журнала «Хакер».

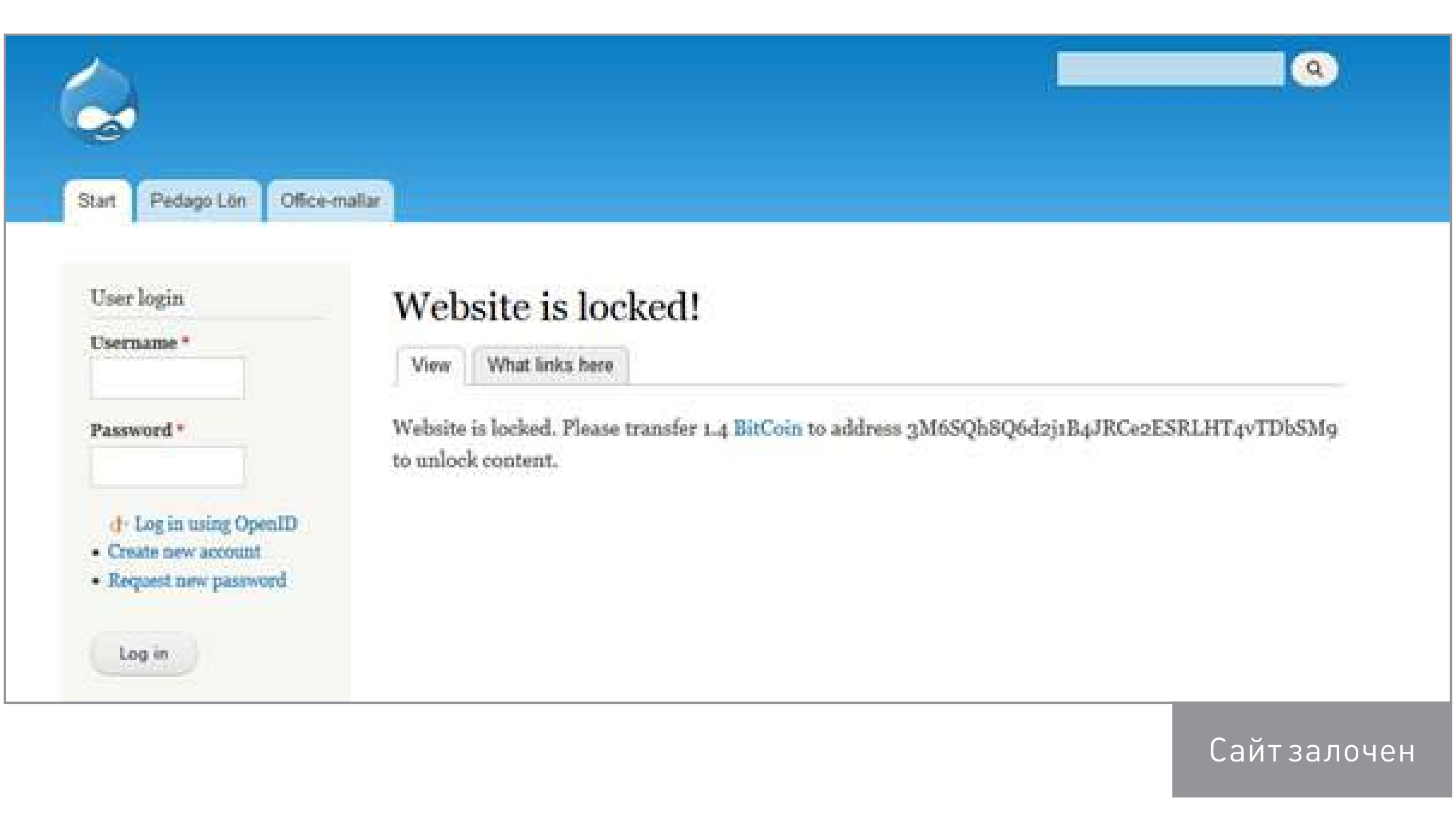
САМОРАСПРОСТРАНЯЮЩИЕСЯ ЛИНУКС-ТРОЯНЫ

Троянами для Linux сейчас никого не удивишь: в последнее время таких становится все больше. Не потому, что бородатые линуксоиды и их личные компы стали вдруг жутко интересны вирусописателям, отнюдь. Разработчики вредоносных программ — ребята прагматичные, их в первую очередь волнует прибыль. А под управлением различных модификаций Linux сейчас работает несметное число всевозможных мелких девайсов: роутеры, телеприставки, сетевые хранилища, мясору... Стоп, мясорубок на Linux я еще не видел. В общем, весь этот электронный зоопарк и оказывается первоочередной целью для создателей троянов. Вторая цель — веб-сайты.

Как создается подавляющее большинство корпоративных сайтов в нашей благословенной стране? Обычно руководитель компании решает открыть представительство своей фирмы в интернете потому, что у конкурентов уже есть, а у него еще нет. Пишет на коленке что-то вроде технического задания (хотя чаще обходится и без этого), обращается в модное дизайнерское агентство, изучает прайс, шевелит бровями и в конце концов нанимает знакомого студента за пятьдесят долларов. Тот качает бесплатный WordPress, натягивает на него крякнутый шаблон с торрента и заливает все это на хостинг. Хорошо, если догадается сменить дефолтный пароль администратора. Обновления CMS? Не, не слышали. Вывод напрашивается сам собой: такие интернет-ресурсы — лакомый кусок для любого уважающего себя вирмейкера.

Именно взлом сайтов, работающих под управлением движков **Drupal, WordPress, Magento, JetSpeed** и некоторых других, задуман основной функцией троянца Linux.Rex.1. Остальные функции — это рассылка писем с требованием выкупа и организация DDoS-атак. Но обо всем по порядку.

Начнем с того, что этот трой, написанный на языке Go, по-видимому, все еще находится в стадии разработки и активного допиливания. Иначе невозможно объяснить, почему при работе он генерирует значительное количество отладочных сообщений, которые записывает в файл на устройстве `/dev/null`. Троянец имеет несколько модулей. Один из них сканирует сеть в поисках сайтов под управлением популярных движков вроде Drupal, для чего ищет индексную страницу сайта и файл Changelog.TXT, а потом проверяет в них наличие характерных строк. Затем Linux.Rex.1 с использованием уязвимости CVE-2014-3704 выполняет SQL-инъекцию в форму для ввода логина и меняет аутентификационные данные в администраторской учетке. Заходит админ на сайт и наблюдает вот такую прелестную картину:



Website is locked!

Website is locked. Please transfer 1.4 BitCoin to address 3M6SQh8Q6d2j1B4JRCe2ESRLHT4vTDbSM9 to unlock content.

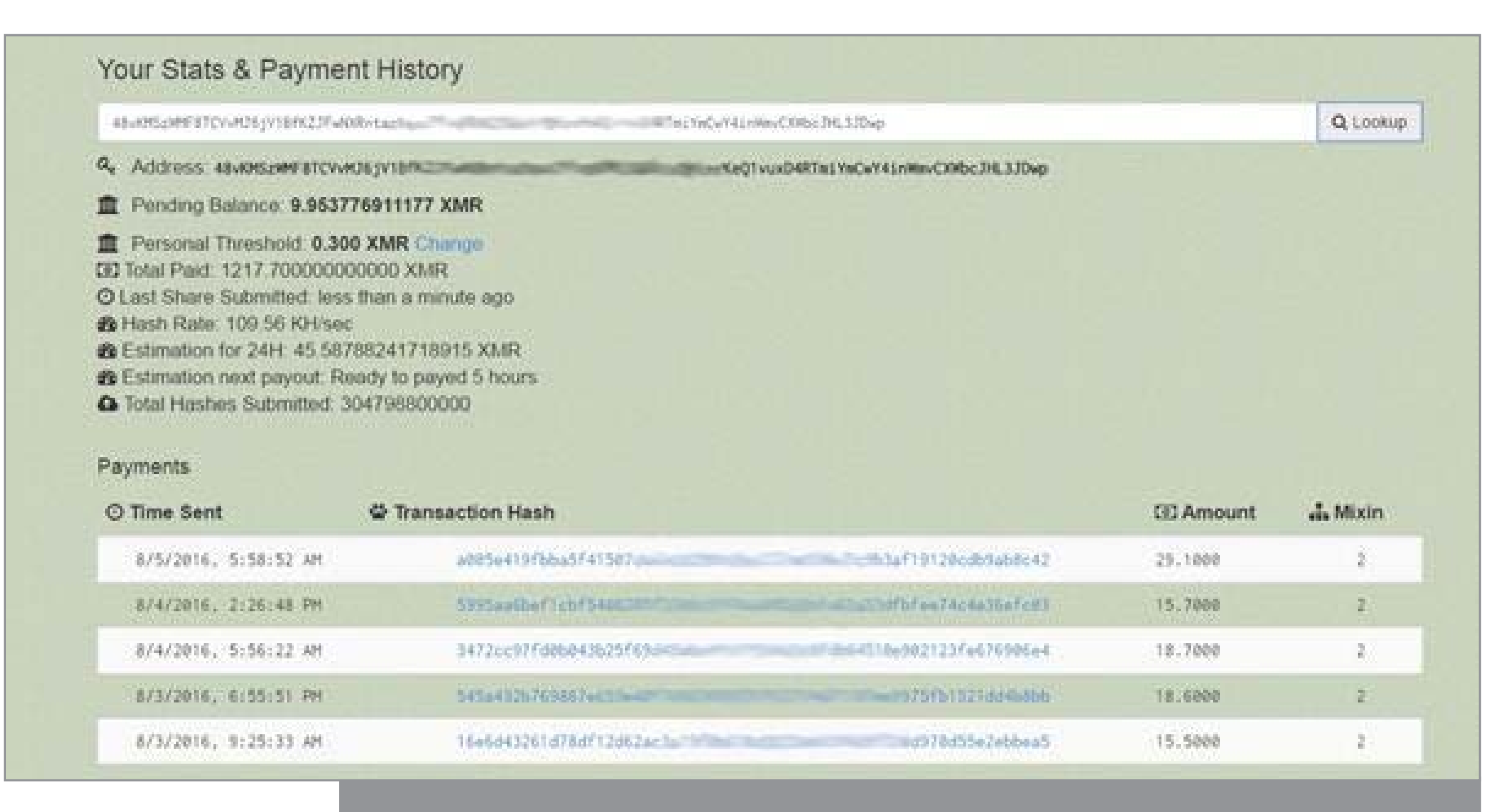
Сайт залочен

Если взлом удался, трой загружает на сайт бинарный файл с собственной копией и запускает его на исполнение. Таким образом, Linux.Rex.1 реализует механизм саморепликации, то есть умеет распространяться автоматически, без участия пользователя.

Помимо этого, данная малварь может рассылать по электронной почте письма с угрозами. Например, обещает владельцам сайтов организовать DDoS-атаку. Чтобы избежать этой участи, потенциальная жертва должна заплатить выкуп в биткойнах. В своих сообщениях трой даже просит получателя переслать письмо ответственному сотруднику компании, если оно пришло не по назначению. Причем угрозы эти не пустые: Linux.Rex.1 умеет проводить DDoS-атаки методами **HttpFlood, HttpPost, slowLoris, tlsThc и DnsAmp**. Но самое интересное заключается в том, что он способен организовываться в одноранговые децентрализованные P2P-ботнеты. Для этого в его архитектуре предусмотрена собственная реализация протокола DHT. Одним словом, не троянец, а самый настоящий вредоносный комбайн. Хранящий логи в `/dev/null` :).

Вообще, складывается впечатление, что придуманный парнями из Google язык Go очень популярен среди разработчиков малвари под Linux. Например, троянец под названием Linux.Lady.1 написан на нем же. Этот трой предназначен для скачивания и запуска на зараженном устройстве программы — майнера криптовалют и тоже обладает своеобразным механизмом самораспространения, правда весьма примитивным и хромым на обе ноги. Он обращается к одному из интернет-сайтов, чтобы определить свой IP-адрес, на основе полученного значения вычисляет маску подсети External_ip\8 (маска 255.0.0.0) и пытается подключиться к удаленным узлам через порт 6379, используемый Redis. Если подключение удалось, троянец предпринимает попытку авторизоваться без пароля.

Разумеется, это возможно только в том случае, если «редиска» настроена, мягко говоря, неправильно. И тем не менее кошельки, на которые Linux.Lady.1 сливает намайненное, вполне себе живые. Что однозначно подтверждает: интернет до сих пор не оскудел грамотными и талантливыми админами.



Your Stats & Payment History

Address: 48vKMSzMMF8TCVvM26jV1B[redacted]KeQ1vuxD4RTm1YmCwY4inWmvCXWbcJHL3JDwp
Pending Balance: 9.953776911177 XMR
Personal Threshold: 0.300 XMR
Total Paid: 1217.700000000000 XMR
Last Share Submitted: less than a minute ago
Hash Rate: 109.56 KH/sec
Estimation for 24H: 45.58788241718915 XMR
Estimation next payout: Ready to payed 5 hours
Total Hashes Submitted: 304798800000

Payments

Time Sent	Transaction Hash	Amount	Mixin
8/5/2016, 5:58:52 AM	a085e419fbba5f41507[redacted]fb3af19120cdb9ab8c42	29.1000	2
8/4/2016, 2:26:48 PM	5395aa6bef1cbf5468[redacted]dfbfee74c4a36efc83	15.7000	2
8/4/2016, 5:56:22 AM	3472cc97fd0b043b25f69[redacted]db64518e902123fe676906e4	18.7000	2
8/3/2016, 6:55:51 PM	545a492b769887ec5[redacted]e975fb1521dd4b8bb	18.6000	2
8/3/2016, 9:25:33 AM	16e6d43261d78df12d62ac3[redacted]d978d55e2ebbea5	15.5000	2

Даже такое кривое самораспространение находит свою аудиторию

ВАШ ПЕРСОНАЛЬНЫЙ «МЕНЕДЖЕР»

Если говорить о платформе Microsoft Windows, то здесь хитом сезона стали троянцы, использующие для своих вредоносных целей популярную утилиту удаленного администрирования под названием **TeamViewer**. Таковых на сегодняшний день известно очень много (проект **Spy-Agent**, к которому относится значительная их часть, развивается аж с 2011 года).

Как работают подобные троянцы? Здесь мы должны вспомнить одну характерную конструктивную особенность винды. Если какому-либо процессу требуется для работы динамическая библиотека, Windows сначала попытается найти нужный файл в папке, откуда был запущен сам процесс, и лишь потом обратится к системным директориям. Это и поворачивают к собственной выгоде вирусописатели: приложение TeamViewer действительно использует стандартную библиотеку avicap32.dll, по умолчанию живущую в `%SYSTEMROOT%/System32/`, однако злодеи сохраняют на диск вместе с настоящими файлами TeamViewer и поддельную библиотеку с тем же именем, причем хранится она в папке самого приложения. В результате при запуске TeamViewer загружает в память вредоносную копию avicap32.dll вместо подлинной.

Раньше вирусописатели этим и ограничивались (вся функциональность была сосредоточена в самой библиотеке), однако создатели троянца под названием BackDoor.TeamViewerENT.1 решили, что негоже добру пропадать, и стали использовать возможности TeamViewer на полную катушку.

Трой отключает показ ошибок для приложения TeamViewer и устанавливает хуки в его адресном пространстве. Кроме того, в нем хранится список контрольных сумм файлов TeamViewer, и BackDoor.TeamViewerENT.1 регулярно проверяет их с помощью функции API `MapFileAndCheckSumA`. Если для нормальной работы TeamViewer на атакованном компьютере не хватает каких-либо файлов, троянец скачивает их со своего управляющего сервера. Благодаря этим ухищрениям бэкдор может выключить и перезагрузить компьютер, записать звук с микрофона и включить трансляцию через веб-камеру, запустить и перезапустить TeamViewer, скачать и выполнить любые приложения, подключиться по указанному адресу, после чего запустить cmd.exe с перенаправлением ввода-вывода на удаленный хост — и это далеко не все.

В отличие от многих других бэкдоров, наш подопытный рассчитан не на массовое распространение, а, скорее, на индивидуальную работу с каждой жертвой. Распространители этого троянца атакуют в основном жителей ряда определенных стран и регионов. Судя по комментариям, которые злодеи оставляют в предназначенных для управления зараженными машинами админках, BackDoor.TeamViewerENT.1 используется в основном для кражи денег с банковских счетов и счетов электронных платежных систем, а также для выполнения несанкционированных транзакций. Комментарии эти говорят еще и о том, что распространители вирусов развлекаются с зараженными машинами и отжигают на полную катушку. На иллюстрации мы скрыли их только из соображений человеколюбия и гуманности.

ID	ID TV	IP	Вебкамера	Комментарий	Статус
№ 94	[redacted]	104.240.120.218	No	[redacted]	Offline
№ 95	[redacted]	68.185.181.96	No	[redacted]	Online !!!
№ 98	[redacted]	50.38.192.71	No	[redacted]	Offline
№ 99	[redacted]	174.198.10.196	No		Offline
№ 100	[redacted]	208.54.90.187	No	[redacted]	Offline !!!
№ 104	[redacted]	67.87.194.109	No	[redacted]	Offline
№ 105	[redacted]	216.113.160.71	No		Offline
№ 106	[redacted]	70.212.42.229	No	[redacted]	Online
№ 107	[redacted]	71.239.74.116	No	[redacted]	Online !!!
№ 109	[redacted]	184.20.40.25	No	[redacted]	Offline !!!
№ 110	[redacted]	70.166.150.116	No		Offline

Не хотелось бы увидеть свой айпишник в таком списке

СТАРЫЕ ДОБРЫЕ ГРАББЕРЫ

Никуда не исчезли и троянцы, предназначенные для хищения конфиденциальной информации. Например, такие, как **Trojan.PWS.AlphaLeon.1** и **Trojan.PWS.AlphaLeon.2**. Эти вредоносные программы реализуют функции граббера — они перехватывают вводимую пользователями информацию в окне браузера и передают ее злоумышленникам. Если покопаться в коде Trojan.PWS.AlphaLeon.2, можно даже отыскать зачатки модуля, предназначенного для выполнения веб-инжектов, но он, судя по всему, еще не допилен. В остальном троянцы семейства Trojan.PWS.AlphaLeon на первый взгляд не представляют собой ничего необычного: регистрируются через реестр в автозагрузке, передают на управляющий сервер сведения об инфицированной машине и ОС, пытаются определить наличие в окружении виртуальных машин, перехватывают содержимое заполняемых пользователями форм... Примечательна разве что одна пасхалка, спрятанная вирусописателями в ресурсах троянца:

Привет, Кребс!

Хорошенько приглядевшись к этой своеобразной пиксельной графике, мы можем различить на картинке надпись Krebs Security, а также портрет человека, напоминающего старину Брайана Кребса. Такой вот «привет» от вирмейкеров экспертам по информационной безопасности.

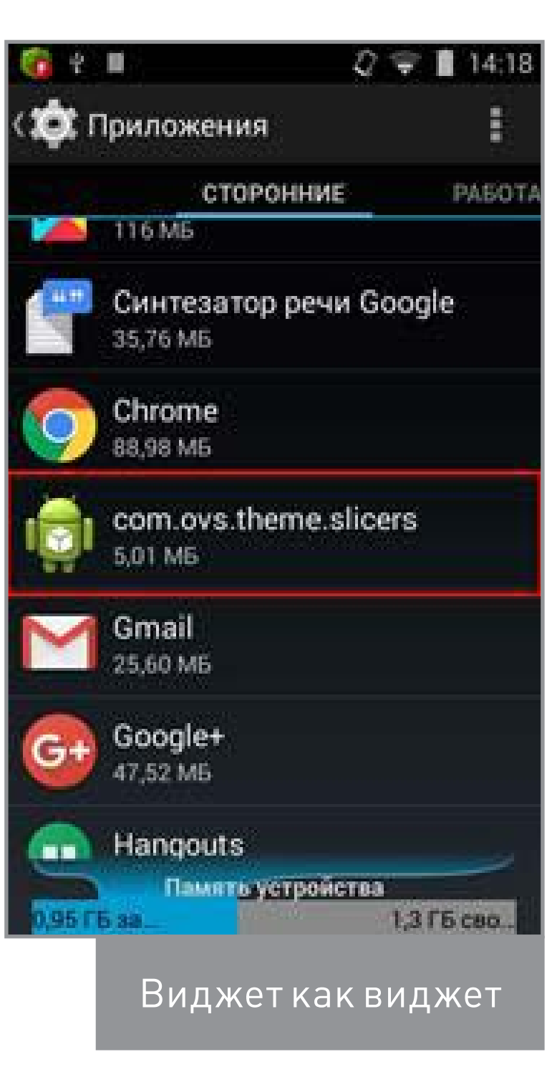
МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ ПОКУПАЮТ ДРУЗЕЙ

Растет количество угроз и для мобильной платформы Android. Оно и неудивительно: с точки зрения вирусописателей, среднестатистический владелец Android-смартфона или планшета — это ходячий кошелек, к содержимому которого обязательно нужно приобщиться. Способов для этого есть много: можно втихаря рассылать платные эсэмэски, можно показывать пользователю рекламу, можно воровать деньги из банковского приложения, а то и вовсе заблокировать экран смартфона и потребовать выкуп.

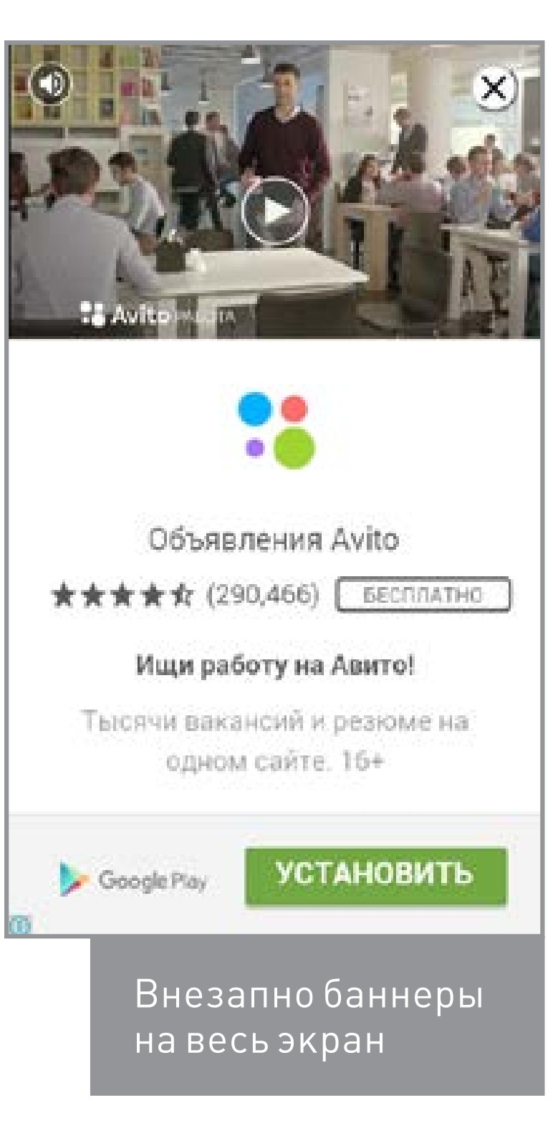
Больше всего среди Android-троянцев рекламных программ. Вот, например, Android.Slicer.1.origin. Вроде бы полезная утилита — может показывать информацию об использовании оперативной памяти и завершать работу ненужных процессов, позволяет включать и отключать беспроводные модули Wi-Fi и Bluetooth. Ан нет, скрыта в ней, как в пресловутой лукасовской Силе, и темная сторона. Этот троянец передает своим хозяевам сведения о зараженном телефоне, а потом по команде показывает на экране навязчивую рекламу, открывает в браузере или в каталоге Google Play различные ссылки или помещает ярлыки на главный экран Android.

Приложение как приложение

Имитация бурной деятельности



Виджет как виджет



Внезапно баннеры на весь экран

Поверх всех приложений или ОС можно даже крутить видео

Этот троянец можно посчитать типичным для Android, но отличительная черта Android.Slicer.1.origin заключается в том, что он может не только рекламировать программы в Google Play, но и покупать и устанавливать их. В этом ему помогает другой троянец под именем Android.Rootkit.40, который живет в системном разделе `/system/bin`. Эта «сладкая парочка» умеет находить в коде открытых страниц элементы управления, например кнопки с идентификатором `com.android.vending:id/buy_button` («Купить» и «Установить») и `com.android.vending:id/continue_button` (кнопка «Продолжить»). Потом троянец определяет координаты середины этих кнопок и нажимает на них, пока они не исчезнут с экрана. Для этого используется стандартная утилита **uiautomator**, предназначенная для тестирования графического интерфейса Android. Правда, проделать эти фокусы Android.Slicer.1.origin и Android.Rootkit.40 могут только в Android 4.3, так как идентификаторы нужных кнопок встречаются лишь в этой системе (и выше), а Android.Rootkit.40 не может работать на устройствах с активным **SELinux** (Android 4.4 и выше).

ЗАКЛЮЧЕНИЕ

Как мы видим, вирусописатели всегда найдут способ обхитрить простого пользователя, поэтому нужно постоянно быть начеку. Ну а мы искренне желаем здоровья вам, вашим компьютерам, смартфонам, планшетам и прочим гаджетам. ⌶

→