Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

UA Linux http://ualinux.com

Украина на 4 месте в мире по количеству исходящих кибератак.

Читайте в этом номере:

- Украина на 4 месте по количеству исходящих кибератак.

- Системы интернет-трейдинга и брокерского обслуживания под угрозой..

- Мобильный банкинг – легкий способ стать жертвой.

- «Яндекс», Google и другие компании объединились против СМС-мошенников.

- Половина украинцев регулярно сталкивается с вредоносным ПО в Сети.

- Обзор Android-угроз в 2012 году: основные риски для пользователей.

- Эксперт «Лаборатории Касперского» рассказал подробности о раскрытии Red October

- Контроль запуска программ как залог безопасности сети. Часть 1.

И многое другое.

Ведущий немецкий оператор связи Deutsche Telekom визуализировал карту стран-источников кибератак, на которой Украина оказалась на 4 месте после России, Тайваня и Германии. За последний месяц с украинских серверов было совершено 566 531 атак.

На портале в реальном времени показаны атаки и страны, из которых они исходят, а также статистика наиболее частых видов атак, срезы по регионам с наибольшим числом активных атакующих серверов. Карта находится в свободном доступе, компания обменивается данными с регуляторными органами и производителями ПО безопасности.

Система глобального мониторинга была разработана в сотрудничестве с ассоциацией BITKOM и Федеральным департаментом информационной безопасности (BSI), и использует более 90 датчиков для регистрации вторжений.

В Deutsche Telekom подчеркивают, что число интернет-угроз постоянно растет — ежедневно обнаруживают около 200 тыс. новых образцов вредоносов. Только в ловушках Deutsche Telekom собираются записи о 450 тыс. атак в день.

Напомним, в хакерских атаках на сайты Facebook, Apple и Twitter, которые участились за последнее время, подозревают украинцев. Как минимум один сервер, который был использован для атаки, находится в Украине.

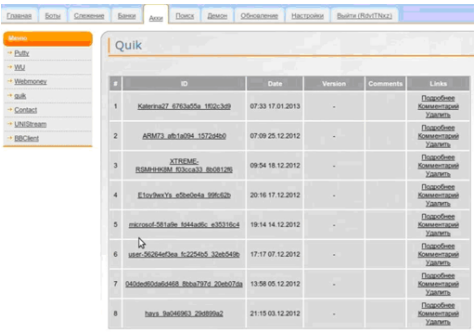
Источник: http://ain.ua

User And Linux

Системы интернет-трейдинга и брокерского обслуживания под угрозой.

С ноября 2012 года специалисты Group-IB фиксируют, что владельцы банковских бот-сетей начали активный сбор информации по пользователям систем интернет-трейдинга и брокерского обслуживания.

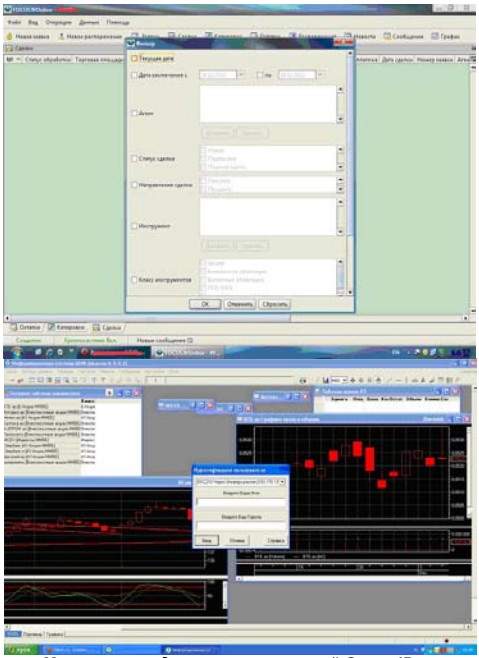
Напомним, что в 2009-2010 годах, преступные группы используя различные троянские программы совершали хищения с банковских счетов именно юридических лиц. Позже, в 2011-2012 году они постепенно начали активно совершать хищения и со счетов не только юридических, но и физических лиц, что значительно увеличило их доходы. Пользователи систем интернет-трейдинга и брокерского обслуживания стали целью злоумышленников недавно.



В Group-IB были обращения по совершению мошеннических операций с использованием скомпрометированных пользовательских данных систем интернет-трейдинга и брокерского обслуживания в 2012 году, но проведённые исследования показали, что в тех мошеннических операциях были замешаны недобросовестные партнёры без использования специализированных вредоносных программ.

Теперь же с уверенностью можно сказать, что следующей целью для киберпреступников станут пользователи различных систем интернет-трейдинга и брокерского обслуживания. Принцип работы злоумышленников остаётся прежним: вредоносная программа попадая на компьютер жертвы определяет, установлено ли программное обеспечение для работы с брокерскими системами. Установлено, что вредоносные программы нацелены на пользователей систем QUICK от ARQA Technologies и FOCUS IVonline от EGAR Technology, крупнейшими клиентами которых являются «Сбербанк», «Альфа-банк» и «Промсвязьбанк».

Если вышеуказанные системы установлены на компьютере, то вредоносная программа начинает активное слежение за действиями пользователей. Собранные данные, логины/пароли и снимки экранов передаются на сервер злоумышленника для последующего анализа и проверки. Ниже опубликованы примеры перехваченных скриншотов, сделанных вредоносной программой.



Материал предоставлен компанией Group-IB

Источник: http://www.xakep.ru

Мобильный банкинг – легкий способ стать жертвой.

Идет активное развитие мобильных технологий, современные требования бизнеса таковы, что доступ к информации должен осуществляться быстро, надежно и из любой точки мира. Платежные приложения не являются исключением, и они постепенно появляются на наших смартфонах и планшетах. Мобильные устройства пока еще недостаточно изучены, и каждая мобильная ОС (Android, iOS, Windows Phone, Symbian, BlackBerry и т.п.) имеет свою специфику, поэтому в каждой из них можно обнаружить большое количество как новых уязвимостей, так и хорошо известных.

Исследовательский центр Digital Security представляет общественности результаты тестирования безопасности приложений для мобильного банкинга. Этичные хакеры в течение года препарировали мобильные платежные приложения более чем от 30 российских банков. «Мы не стоим на месте и стараемся делать сегодня то, что будет востребовано завтра», – говорит Дмитрий Евдокимов, исследователь из Digital Security.

Результаты исследования подтверждают тенденцию, отмеченную экспертами в традиционных ежегодных отчетах по исследовательской работе в области безопасности систем ДБО. Разработчики мобильных банк-клиентов не уделяют достаточно внимания вопросам безопасности приложения, не следуют руководствам по безопасной разработке. Зачастую отсутствуют процессы разработки безопасного кода и архитектуры. В результате все рассмотренные приложения содержат хотя бы одну уязвимость, позволяющую либо перехватить данные, передающиеся между клиентом и сервером, либо напрямую эксплуатировать уязвимости устройства и самого мобильного приложения.

Так, 35% мобильных банков для iOS и 15% мобильных банков для Android содержат уязвимости, связанные с некорректной работой SSL, а это означает возможность перехвата критичных платежных данных с помощью атаки «человек посередине». 22% приложений для iOS потенциально уязвимы к SQL-инъекции, что создает риск кражи всей информации о платежах с помощью нескольких несложных запросов. 70% приложений для iOS и 20% приложений для Android потенциально уязвимы к XSS – одной из самых популярных атак, позволяющей ввести в заблуждение пользователя мобильного банк-клиента и таким образом, например, украсть его аутентификационные данные. 45% приложений для iOS потенциально уязвимы к XXE-атакам, особенно опасным для устройств, подвергнутым столь популярной в России операции jailbreak. Около 22% приложений для Android неправильно используют механизмы межпроцессного взаимодействия, тем самым фактически позволяя сторонним приложениям обращаться к критичным банковским данным.

«У злоумышленников есть множество путей реализации атак. При этом затраты на проведение атаки могут в реальной среде быть весьма низкими по сравнению с возможной выгодой», – предрекают эксперты Digital Security.

«Надеюсь, что результаты этого исследования привлекут внимание банковских CISO к актуальным проблемам безопасности мобильных технологий. Проверка защищенности клиентских приложений методом статического анализа бинарного кода, проведенная нашим исследовательским центром, покрывает в лучшем случае 30% от общего фронта работ по анализу защищенности мобильных приложений, однако серьезные проблемы очевидны уже сейчас. Разработанный нами в процессе исследования внутренний инструмент анализа кода мы планируем в дальнейшем использовать для повышения качества услуг, которые мы предоставляем клиентам», – говорит директор Digital Security Илья Медведовский.

Источник: http://www.anti-malware.ru

«Яндекс», Google и другие компании объединились против СМС-мошенников.

Ведущие интернет-компании договорились сообща бороться с СМС-мошенничеством. Об этом «Ленте.ру» рассказали в компании «Яндекс».

Как отметили в компании, в последнее время участились случаи мошенничества с СМС-подписками с использованием названий «Яндекса» и других известных интернет-ресурсов. Вместе с «Яндексом» в проекте участвуют Google, Group-IB, Mail.Ru Group, «ВКонтакте», «Доктор Веб», «Лаборатория Касперского». Программа получила неформальное название «Операция Мухобойка».

Компании договорились об обмене данными об обнаруженных угрозах. Предполагается, что это поможет антивирусным компаниям оперативно блокировать мошеннические веб-страницы, а интернет-компаниям — предупреждать пользователей об опасности при попытке перехода на такие ресурсы.

Кроме того, участники программы договорились передавать обнаруженные короткие номера, с которых рассылаются недобросовестные сообщения, сотовым операторам. Интернет-компании надеются, что операторы будут блокировать такие номера.

Источник: http://lenta.ru

Кабмин одобрил законопроект о кибербезопасности Украины.

Законопроект направлен на формирование основ государственной политики в сфере обеспечения кибернетической безопасности

На заседании 6 марта Кабинет министров Украины одобрил законопроект "О внесении изменений в Закон Украины "Об основах национальной безопасности Украины" относительно кибернетической безопасности Украины". Об этом сообщает пресс-служба Министерства внутренних дел.

Законопроект направлен на формирование основ государственной политики в сфере обеспечения кибернетической безопасности Украины. Достигнуть этого планируется путем определения основных реальных и потенциальных угроз национальной безопасности кибернетического характера, направлений государственной политики и функций субъектов обеспечения национальной безопасности в этой сфере.

В законопроекте, в частности, оговаривается введение таких основополагающих понятий, как "кибернетическая безопасность (кибербезопасность)" и "кибернетическое пространство (киберпространство)".

Специалисты считают, что принятие законопроекта заложит правовую основу для дальнейшей нормотворческой деятельности на законодательном и подзаконном уровне, направленной на создание и совершенствование национальной системы кибербезопасности и противодействие киберпреступности.

Напомним, в прошлом году Национальная комиссия по регулированию в сфере связи и информации (НКРСИ) предложила изменения в Закон Украины "Об основных принципах развития информационного общества в Украине на 2007-2015 годы". В комиссии считают, что украинское законодательство требует корректировки и дополнения. Кроме того, одной из основных задач внесения изменений в указанный закон является важность обеспечения координации действий государственных органов при его реализации.

Источник: http://liga.net

Половина украинцев регулярно сталкивается с вредоносным ПО в Сети.

Украина находится на 8-м месте в мире по количеству угроз, поскольку каждый второй пользователь Интернета регулярно подвергается атакам из Сети.

За прошедшие три месяца количество атак на украинских интернет-пользователей выросло на 5% (составив 50%), а каждый четвертый съемный носитель – инфицирован. В рейтинг наиболее уязвимого ПО попали такое популярные и ши-

роко используемые продукты как: софт компании Adobe, Java, проигрыватель Winamp, браузер Opera и сервис Google Picasa. Об этом рассказал Владимир Заполянский, заместитель руководителя глобального центра исследований и аналитики «Лаборатории Касперского».

«Сегодня эксплойты являются наиболее распространенным методом проникновения вредоносного кода в компьютер пользователя. Они используются как для целевых, так и для крупномасштабных атак через эксплойты, таких, например, как Blackhole. При этом использование традиционных сигнатурных методов для защиты не является достаточным, поскольку они способны блокировать только известные угрозы, – рассказал Владимир Заполянский.

Кроме того, в последнее время все время усложняются хакерские атаки, а такие названия, как Stuxnet, Duqu, Flame и Gauss, уже стали известны многим. В январе «Лаборатория Касперского» объявила об обнаружении еще одной киберугрозы – Red October. На этот раз речь шла не только о целевой атаке, а о сети для кибер-шпионажа за дипломатическими и правительственными структурами, научно-исследовательскими институтами, промышленными предприятиями и др. стратегическими объектами разных стран.

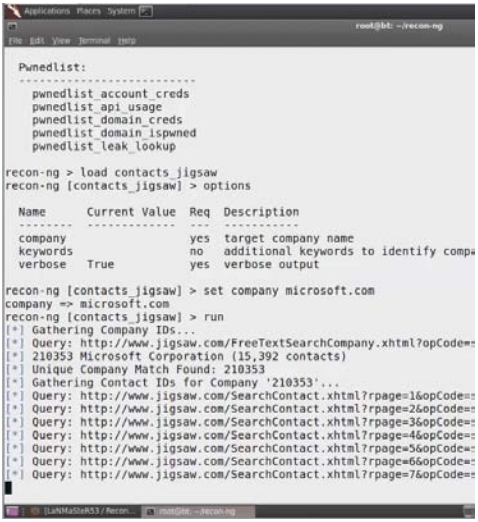
Источник: http://www.imena.ua

Recon-NG: фреймворк для работы с базой 29 млн украденных учётных данных

Пентестер Тим Томс (Tim Tomes) выложил в открытый доступ программу, которой сам успешно пользуется несколько месяцев. Это фреймворк Recon-NG для разведки в открытых источниках, в том числе в базе украденных учётных данных PwnedList.

Об открытии PwnedList сообщалось в марте 2012 года. На этом сайте любой желающий может ввести хэш от своего адреса электронной почты и проверить наличие такого адреса в различных базах украденных данных. Основатели сайта постоянно мониторят более 200 хакерских форумов, скачивают свежие базы с логинами и паролями, а также осуществляют автоматический сбор дампов в интернете. В марте прошлого года у них была база из 12,3 миллионов украденных аккаунтов, сейчас уже 29,6 млн комбинаций почтовых адресов и паролей, а также отдельно 168,6 млн адресов электронной почты и 966,2 млн паролей. Пополнение базы происходит буквально ежедневно.

Фреймворк Recon-NG сделан по образцу Metasploit и поддерживает подключение разных модулей. Один модуль выводит список сотрудников определённой компании, осуществляя поиск в социальных сетях. Другой модуль выводит список всех поддоменов для указанного хоста, осуществляя поиск в Google. Есть несколько модулей и для работы с утёкшими в открытый доступ учётными данными, в том числе с базой PwnedList. На скриншотах показаны команды для получения списка сотрудников и проверки паролей в базе PwnedList.



Источник: http://www.xakep.ru

SearchInform полностью обновила свои продукты

Компания SearchInform, представила ряд существенных обновлений для продуктов, входящих в состав «Контура информационной безопасности SearchInform» - решения, обеспечивающего контроль всех каналов, по которым возможна утечка конфиденциальных данных.

Обновленный SearchInform NetworkSniffer - решение для борьбы с утечками информации в организациях по распространенным протоколам передачи информации через интернет – в новой версии была реализована поддержка интеграции с почтовыми серверами по протоколу IMAP\IMAPS. Также в новой версии решения добавлена возможность перехвата сообщений, переданных с помощью программы Агент Mail.ru через Web-интерфейс по протоколу MMP. В новой версии SearchInform NetworkSniffer стал перехватывать входящую почту с почтового сервера Zimbra и входящую почту mail.lv. Нельзя не отметить и изменения в работе с PCAP-файлами, позволяющими SearchInform NetworkSniffer стабильно работать с большими потоками данных.

Обновился и продукт SearchInform AlertCenter – средство обнаружения нарушений корпоративной политики информационной безопасности и анализа информационных потоков организации. В новой версии повышен уровень защиты программы от несанкционированного доступа: консоль SearchInform AlertCenter теперь требует авторизации, реализовано возможность разграничения прав на доступ к группам алертов. Теперь руководитель отдела безопасности может установить права доступа различных специалистов к разным алертам. Например, одним из них можно разрешить редактирование политик безопасности и просмотр инцидентов, другим дать возможность только просмотра политик и результатов проверки, остальным же запретить просмотр и политик безопасности, и инцидентов. Также в SearchInform AlertCenter появилась возможность создавать «черные списки», позволяющие осуществлять проверку строго по заданному в них перечню пользователей.

В модуле SearchInform Client список алгоритмов поиска, и без того весьма внушительный, пополнился «Поиском по словарю». Теперь специалист по информационной безопасности может использовать тематические словари для анализа перехваченных данных. Словари можно расширять и составлять самостоятельно. Для черновиков HTTP-почты можно ограничить их выведение в результатах поиска – в этом случае в них не будут включены версии документов, созданные при автоматическом сохранении в почтовом клиенте. По умолчанию эта настройка отключена, и черновики выделяются серым цветом.

В новой версии SearchInform DataCenter – продукта для управления поисковыми индексами, создаваемыми приложениями, перехватывающими трафик, - добавлена возможность перекрытия настроек операций над индексами. Это позволяет более гибко управлять индексами благодаря ограничению «родительских» настроек DataCenter и установке новых настроек для создания индексов подобных данных, перехваченных разными компонентами «Контура информационной безопасности SearchInform». Теперь, например, индексы mail могут создаваться по перехваченным данным через SearchInform NetworkSniffer и SearchInform EndpointSniffer.

Новая версия SearchInform EndpointSniffer – продукта для предотвращения утечек конфиденциальных данных и контроля информационных потоков на рабочих станциях персонала и корпоративных ноутбуках – появилась возможность отложенного обновления агентов, что позволяет сделать этот процесс полностью незаметным для конечных пользователей. При активации данной опции загруженные обновления вступят в силу только после перезагрузки системы. Также SearchInform EndpointSniffer теперь может получать список пользователей не только непосредственно из Active Directory, но и из базы данных SearchInform DataCenter. Из этой базы, обновляемой при каждой синхронизации продукта с Active Directory, SearchInform EndpointSniffer считывает домены и поль-

зователей в них, что позволяет снизить количество обращений от компонент «Контура» непосредственно к AD. Среди прочих улучшений, специалисты по информационной безопасности получили возможность осуществлять остановку и запуск агентов через меню EndpointSniffer.

Модуль SearchInform MonitorSniffer, предназначенный для контроля содержимого экрана пользователя в режиме реального времени, получил поддержку разграничения прав доступа к данным мониторинга Liveview. Специалист по информационной безопасности может задать права неограниченного доступа к этой возможности, права доступа по паролю в SearchInform MonitorSniffer и права доступа только для тех пользователей, которые заданы в настройках SearchInform EndpointSniffer. Также в SearchInform MonitorSniffer появилась поддержка поиска по маске процесса.

Как отметил Генеральный директор компании SearchInform Лев Матвеев, «выпуск столь значительного числа обновления для «Контура информационной безопасности SearchInform» поднимает наш продукт, и без того являющийся безоговорочным лидером рынка России, стран СНГ и Балтии, на новую высоту. Благодаря новым возможностям работа специалистов по информационной безопасности станет более продуктивной, а количество инцидентов в этой сфере снизится».

Источник: http://www.anti-malware.ru

«Касперский» выпустит бесплатные антивирусы для мобильных устройств

Известный производитель антивирусного программного обеспечения «Лаборатория Касперского» планируют переформатировать линейку мобильных продуктов компании.

В частности, на Всемирном мобильном конгрессе (Mobile World Congress) в Барселоне, 25-26 февраля 2013 года разработчики антивирусных программ представят обновленную концепцию продуктов.

Новая концепция предполагает создание бесплатно распространяемых версий для мобильных приложений Kaspersky Mobile Security для смартфонов под управлением Android, и Kaspersky Tablet Security для планшетов под руководством все той же операционной системы. Напомним, что до сих пор компания предлагала единственный бесплатный продукт для Android: приложение Kaspersky Mobile Security Lite.

Функциональность новых бесплатных приложений «Лаборатории Касперского» ограничится файловым сканированием «по требованию» и системой «Антивор». Помимо «Антивора» и сканера, решение для смартфонов будет фильтровать нежелательные вызовы и SMS. Интересно, что мобильные приложения Касперского впервые получат собственную антивирусную функциональность – прежняя бесплатная программа для мобильных устройств Kaspersky Mobile Security Lite обладала усеченными антивирусными возможностями, ограниченными проверкой загружаемых материалов.

Источник: http://www.imena.ua

Etersoft

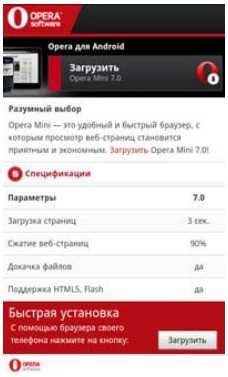
Обзор Android-угроз в 2012 году: основные риски для пользователей.

И хотя многие пользователи поначалу восприняли этот факт скептически, постепенно их сомнения сменились обеспокоенностью за безопасность используемых мобильных устройств, так как число вредоносных приложений продолжало неуклонно расти. Прошедший 2012 год в этом плане не стал исключением. В этом обзоре мы рассмотрим наиболее интересные и заметные прошлогодние события, связанные с Android-угрозами.

СМС-троянцы

Троянцы семейства ***Android.SmsSend***, появившиеся еще в 2010 году и быстро ставшие настоящей головной болью пользователей мобильных Android-устройств, по-прежнему являются наиболее распространенной и массовой угрозой для этой мобильной платформы. Эти вредоносные программы предназначены для отправки дорогостоящих СМС-сообщений и подписки абонентов на различные контент-услуги, что может повлечь за собой серьезные финансовые потери (при этом жертва даже не будет знать, что деньги списаны с ее счета). Чаще всего они распространяются под видом популярных игр и приложений, а также их обновлений, однако могут встречаться и другие каналы распространения.

Для создания большинства подобных программ не требуется особых знаний, большого количества времени и средств, а получаемая злоумышленниками прибыль от их использования многократно компенсирует все затраты.



Широкое распространение троянцев обусловлено хорошо развитой сетью партнерских программ, которые предлагают весьма выгодные условия оплаты всем своим участникам. Кроме того, летом 2012 года были зафиксированы многочисленные случаи взлома легитимных веб-сайтов, которые модифицировались злоумышленниками таким образом, что пользователи, посещающие их с мобильных устройств, перенаправлялись на мошеннические ресурсы, распространяющие эти вредоносные программы.

Именно благодаря относительной простоте, высокой окупаемости и эффективности применяемых методов распространения семейство ***Android.SmsSend*** доминировало в прошедшем году среди остальных вредоносных приложений.

Увеличение риска кражи конфиденциальной информации, негласный мониторинг и кибершпионаж

Учитывая возможности мобильных Android-устройств, а также принимая во внимание продолжающийся рост числа их пользователей, неудивительно, что проблема сохранности конфиденциальной информации становится все более

ощутимой. Рискам в этой сфере подвержены все: как простые пользователи, так и представители коммерческого и государственного секторов. Ценные сведения, интересующие злоумышленников, могут быть самыми разнообразными.

Шпионы — пособники спамеров

Сами по себе вредоносные программы, шпионящие за пользователями и крадущие их конфиденциальную информацию, не уникальны и известны достаточно давно. Однако в 2012 году обозначилась четкая тенденция к появлению довольно специфической группы троянцев-шпионов, направленных против жителей Японии.Все они распространялись при помощи спам-писем, в которых пользователям предлагалось установить то или иное «полезное» приложение, начиная от эротической игры и заканчивая оптимизатором расхода аккумулятора.

К этой группе относятся такие вредоносные программы как:

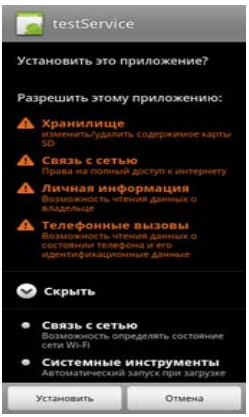
Android.MailSteal.1.origin;
Android.Maxbet.1.origin;
Android.Loozfon.origin;
Android.EmailSpy.origin.

Их основная задача — похищение адресов электронной почты из книги контактов мобильного устройства и отправка их на удаленный сервер. Помимо этого, некоторые троянцы могут отправлять злоумышленникам не только адреса электронной почты, но и всю информацию из телефонной книги, а также идентификаторы устройства, включая номер сотового телефона. Добытая таким образом информация в дальнейшем может быть использована киберпреступниками для организации новых спам-кампаний и для продажи на черном рынке, а для владельцев похищенных адресов это несет потенциальную угрозу фишинг-атак и вероятность заражения их персональных компьютеров самыми разными вредоносными программами, использующими для инфицирования каналы электронной почты.

Узконаправленные атаки — угроза с повышенным риском

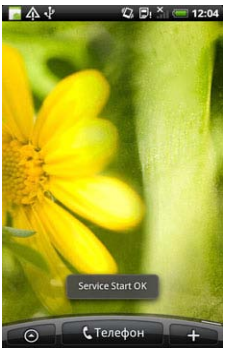
Узконаправленные, точечные или таргетированные атаки несут в себе серьезную угрозу, поскольку они, в отличие от большинства обычных атак, направлены не на максимально возможное число пользователей, а на их ограниченный круг, что снижает вероятность оперативного и эффективного обнаружения используемых при преступлении вредоносных программ.

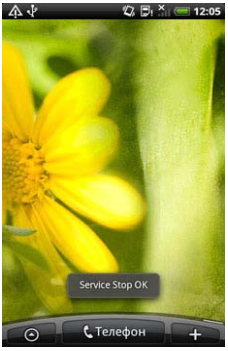
Одним из вариантов точечной атаки является ***Advanced Persistent Threat*** или APT-атака. Ее суть заключается в том, чтобы вредоносная программа как можно дольше оставалась в скомпрометированной системе без обнаружения и получила при этом максимально возможный объем ценных сведений. Жертвами обычно становятся различные компании, организации и государственные структуры.



До сих пор под ударом подобных кампаний находились лишь «большие» компьютерные системы, такие как рабочие станции и серверы. Однако в 2012 году была зафиксирована новая APT-атака, в процессе изучения которой обнаружилась вредоносная программа ***Android.Luckycat.origin***. Функционал троянца включал выполнение команд, поступающих с управляющего сер-

вера, загрузка различных файлов с мобильного устройства и на него, сбор идентификационных данных и некоторые другие возможности.



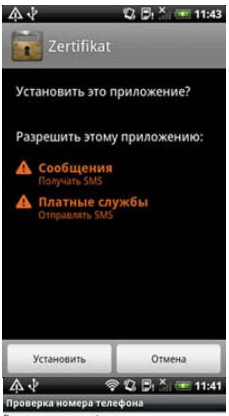


Несмотря на то, что троянец находился в стадии разработки, и свидетельств его применения на практике не было, факт существования такого инструмента дает серьезное основание полагать, что мобильные Android-устройства в скором времени могут стать такой же привычной мишенью APT-атак, как и обычные компьютеры.

Еще одним инструментом проведения таргетированных атак с целью завладения конфиденциальной и ценной информацией стали мобильные банковские троянцы, крадущие одноразовые коды mTAN. Для обеспечения безопасности финансовых операций в сети Интернет банковские системы отправляют СМС-сообщения с этими кодами на привязанный к клиентскому счету номер мобильного телефона. Чтобы успешно завершить транзакцию, пользователь должен ввести в специальную веб-форму полученный код. Мобильные банковские троянцы предназначены для перехвата СМС-сообщений, кражи этих кодов и передачи их злоумышленникам, которые выполняют различные финансовые операции с электронными счетами ничего не подозревающих жертв (например, совершают онлайн-покупки).

Применение подобных вредоносных программ никогда не было массовым явлением, в том числе и для устройств под управлением Android. В 2012 году мы стали свидетелями появления лишь нескольких новых представителей этого класса троянцев, направленных на мобильную операционную систему от Google. Ими стали:

Android.SpyEye.2.origin;
Android.Panda.2.origin;
Android.SmsSpy.6.origin;
Android.FakeSber.1.origin.



Типичный способ распространения таких вредоносных программ — социальная инженерия, когда пользователя вводят в заблуждение, предлагая срочное обновление операционной системы или установку некоего сертификата безопасности, необходимого для дальнейшего получения финансовых услуг. Несмотря на то, что случаи появления банковских троянцев для ОС Android являются редкими, проводимые с их помощью атаки весьма эффективны. Именно благодаря

нешироко распространенности таких приложений и направленности на пользователей конкретных банковских систем снижается вероятность их быстрого обнаружения и обеспечения необходимой защиты от них.

Среди всех этих вредоносных программ стоит особо выделить ***Android.FakeSber.1.origin***: он стал первым банковским Android-троянцем, направленным против клиентов российского банка. До его появления киберпреступников интересовали лишь зарубежные пользователи. Кроме того, в отличие от своих собратьев, распространяющихся при помощи мошеннических сайтов, данный троянец был помещен злоумышленниками непосредственно в официальный каталог приложений Google Play. К счастью, к моменту, когда троянец был удален из каталога, установить его успели немногие. Тем не менее, потенциальная опасность, которую он представлял, была весьма существенной.

Принцип, по которому работал ***Android.FakeSber.1.origin***, был схож со схемами, применяемыми злоумышленниками в других банковских Android-троянцах. Во-первых, для того чтобы заставить пользователей выполнить его установку, была использована весьма распространенная тактика запугивания: на официальным веб-сайте банка посетителям демонстрировалось сообщение о необходимости авторизации при помощи мобильного телефона (это сообщение отображалось благодаря Windows-троянцу, заразившему компьютеры жертв и работавшему в связке с ***Android.FakeSber.1.origin***). Пользователям предлагалось установить специальное приложение, которое на самом деле и было мобильным банковским троянцем. Во-вторых, попав на мобильное устройство, эта вредоносная программа имитировала ожидаемый функционал, усыпляя бдительность пользователя. В конечном итоге ***Android.FakeSber.1.origin*** скрытно перехватывал все входящие сообщения и пересылал полученные из них сведения на удаленный сервер, поэтому помимо mTAN-кодов в руках киберпреступников могли оказаться и другие конфиденциальные сведения, например, частная переписка.

Коммерческое шпионское ПО

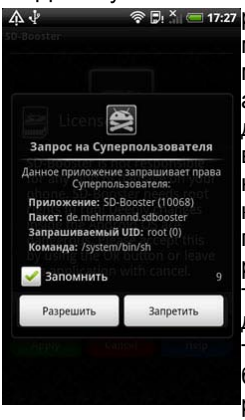
Потенциальную угрозу сохранности персональной информации продолжают нести и различные виды коммерческого программного обеспечения для мониторинга и шпионажа. В 2012 году было обнаружено значительное число не только новых модификаций уже известных программ, но и новые представители этого класса приложений. Большинство подобных шпионов может использоваться как легально, с согласия владельца мобильного устройства, так и без его ведома. Для их установки обычно требуется физический доступ к мобильному устройству, однако после установки данные приложения способны скрывать свое присутствие в системе (например, не создавая иконку на главном экране, а также маскируясь под системное ПО). Наиболее распространенными функциями таких шпионов являются отслеживание СМС-сообщений, получение координат пользователя, перехват совершаемых им звонков, а также запись происходящего вокруг в аудиофайл.

Затруднение анализа, разделение функционала и активное противодействие удалению

Борьба с вредоносными Android-программами при помощи антивирусных средств и постепенное повышение компьютерной грамотности владельцев мобильных устройств на базе ОС от Google заставляет злоумышленников искать способы обхода возникающих трудностей. И если раньше троянцы представляли собой единственный программный пакет, содержащий весь вредоносный функционал, сейчас все чаще встречаются более сложные схемы их построения и работы.

Весьма интересным решением киберпреступников была своеобразная матрешка из трех вредоносных приложений, обнаруженных в мае 2012 года. Дроппер ***Android.MulDrop.origin.3*** содержал в своих ресурсах зашифрованный пакет, который также являлся дроппером

(***Android.MulDrop.origin.4***). Он, в свою очередь, имел в своих ресурсах еще один зашифрованный пакет, представляющий собой троянца-загрузчика ***Android.DownLoader.origin.2***, способного получать с удаленного сервера список приложений для загрузки на мобильное устройство.



Для успешного функционирования разработанной схемы были необходимы root-привилегии, а так как основной дроппер находился в модифицированном злоумышленниками легитимном приложении, для работы которого требовался root-доступ, у пользователей не должно было возникнуть серьезных опасений в связи с необходимостью предоставления ему соответствующих прав. Примененный в данном случае механизм может быть весьма эффективным способом избежать лишних подозрений и увеличить шансы успешного заражения мобильного Android-устройства.

Другим примером разделения функционала между несколькими вредоносными приложениями являются троянцы ***Android.SmsSend.405.origin*** и ***Android.SmsSend.696.origin***. Первый в различных модификациях распространялся в каталоге Google Play под видом сборника обоев для рабочего стола, доступ к которым пользователь мог получить, нажав кнопку «Далее». В этом случае приложение подключалось к облачному сервису Dropbox и загружало второй программный пакет, который являлся СМС-троянцем. По всей видимости, подобным переносом основного функционала во второе приложение, расположенное вне Google Play, злоумышленники пытались обойти систему Bouncer, которая контролирует каталог на предмет наличия вредоносных программ.

Весьма тревожит появление у вредоносных Android-приложений функционала по противодействию своему удалению. В мае 2012 года был обнаружен троянец ***Android.Relik.origin***, который завершал работу популярных китайских антивирусных средств, а также запрашивал у пользователя доступ к режиму администратора мобильного устройства. В случае активации этого режима другие антивирусные программы уже не смогли бы удалить троянца, однако для избавления от этой вредоносной программы пользователю ничто не мешало убрать вредоносное приложение из списка администраторов.

Идея противодействия удалению в дальнейшем была значительно развита в другом китайском троянце, ***Android.SmsSend.186.origin***. Практически сразу после установки он отображал требование предоставить ему права администратора мобильного устройства, причем в случае отказа требование выводилось вновь до тех пор, пока троянец не получал соответствующие права.

После получения троянцем необходимых прав попытки убрать его из списка администраторов мобильного устройства на некоторых версиях ОС Android заканчивались полным провалом, так как ***Android.SmsSend.186.origin*** препятствовал этому, не давая владельцу мобильного устройства зайти в необходимые системные настройки. Антивирусные средства, не располагающие функционалом по нейтрализации таких угроз, также не могли избавить систему от инфицирования, даже если и детектировали вредо-

носную программу. Самостоятельно же избавиться от троянца было весьма проблематично, поскольку это требовало выполнения ряда нетривиальных действий и определенной доли терпения. Ко всему прочему, эта вредоносная программа распространялась при помощи дроппера, помещенного киберпреступниками в «живые обои», которые при установке не требовали никаких специальных разрешений для своей работы. Таким образом, ***Android.SmsSend.186.origin*** представляет собой одну из самых серьезных за последнее время Android-угроз.

Нельзя не отметить тенденцию к росту использования авторами вредоносных программ обфускации кода, которая призвана затруднить анализ троянцев и помешать их детектированию антивирусными средствами. Например, обфускация встречается в целом ряде представителей семейства ***Android.SmsSend***.

Интересные и необычные угрозы

Весьма интересной вредоносной программой, обнаруженной в 2012 году, стал троянец ***Android.MMarketPay.origin***, который самостоятельно покупал приложения в электронном магазине китайского оператора связи China Mobile. Для этого он перехватывал СМС-сообщения с кодами подтверждения совершения покупки, а также обходил проверку captcha, отправляя на удаленный сервер соответствующие изображения для анализа. Целью создания этого троянца могло стать как желание недобросовестных разработчиков увеличить прибыль за счет подобной незаконной продажи своих приложений, так и обычное желание злоумышленников досадить пользователям и сотовому оператору, репутация которого могла заметно пострадать.

Рынок заказных услуг киберпреступников?

Не секрет, что большая часть современных вредоносных программ создается не из простого любопытства — эта сфера незаконной деятельности уже давно стала источником заработка для самых разнообразных групп киберпреступников. И появившихся в 2012 году Android-троянцев:

Android.Spambot.1.origin и

Android.DDoS.1.origin - вполне обоснованно можно отнести к инструментам осуществления киберкриминальных услуг. ***Android.Spambot.1.origin*** представлял собой троянца, предназначенного для массовой рассылки СМС-спама. Текст сообщений и номера, по которым осуществлялась рассылка, загружались с удаленного сервера, принадлежащего злоумышленникам, поэтому им не составляло большого труда выполнить спам-рассылку для заинтересованных лиц. Чтобы скрыть свою вредоносную деятельность, троянец удалял все сведения об отправляемых СМС, и владельцы инфицированных мобильных устройств могли не сразу обнаружить подозрительную активность. Что же касается ***Android.DDoS.1.origin***, то это — вредоносная программа, предназначенная для осуществления DoS-атак с использованием мобильных Android-устройств. Параметры, необходимые для их проведения, троянец получал посредством СМС-сообщений, в которых указывались имя сервера и требуемый порт. Особенность этой вредоносной программы — в том, что атакуемый сайт мог быть абсолютно любым, поэтому теоретически воспользоваться возможностями этой вредоносной программы могли все, кто проявит должный интерес и заплатит соответствующую цену за оказание незаконной услуги.

Вандализм — редкая, но опасная угроза с деструктивным потенциалом.

На фоне общей массы вредоносных Android-приложений, направленных на получение той или иной материальной выгоды, Android.Moghava, обнаруженный весной 2012 года, держится особняком, будучи троянцем-вандалом. Он распространялся в модифицированной злоумышленниками версии приложения — сборника рецептов иранской кухни. Через определенные промежутки времени троянец выполнял на мобильном устройстве поиск JPEG-изображений в каталоге /DCIM/Camera/ и накладывал на них еще одно изображение. В результате этого

фотографии пользователя безвозвратно портились.

Обычно вирусописатели создают подобные вредоносные программы с целью громко заявить о себе, либо в качестве мести или простого развлечения. Более редкой причиной является попытка совершить диверсию среди определенной группы лиц. Так или иначе, ущерб от подобных приложений может быть весьма существенным.

Выводы

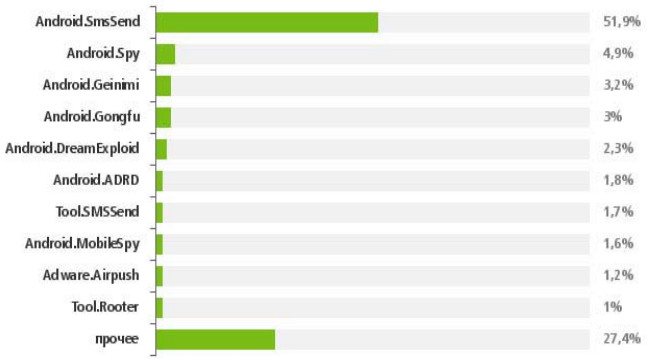
По состоянию на конец 2012 года вирусные базы Dr.Web содержали почти 1300 записей для Android-угроз. Их процентное распределение представлено на диаграмме - «Распределение различных типов угроз для ОС Android».

Следует учитывать тот факт, что специалисты компании проводят постоянную оптимизацию баз, поэтому число соответствующих вирусных записей может со временем уменьшаться.

С ростом популярности мобильных устройств под управлением ОС Android соответственно увеличивается число и разнообразие вредоносных приложений, представляющих опасность для пользователей этой платформы. Описанные выше типы угроз в 2012 году стали наиболее заметными, а также продемонстрировали потенциальный вектор развития вредоносных Android-программ в ближайшем будущем. Одновременно с этим могут появляться и вредоносные приложения, которые сочетают свойства самых разнообразных угроз или же являются «нестандартными» по сравнению с общей массой, что во многом повторяет ситуацию с Windows. Учитывая, что в ближайшие несколько лет мобильная платформа Android будет оставаться среди лидеров рынка, стоит ожидать дальнейшего роста числа созданных для нее вредоносных программ.

Распределение различных типов угроз для ОС Android

по состоянию на 2012 год



Dr.WEB®
www.drweb.com

Источник: http://news.drweb.com

Эксперт «Лаборатории Касперского» рассказал подробности о раскрытии Red October

В январе текущего года широкий резонанс среди экспертов по информационной безопасности вызвала раскрытая российской компанией «Лаборатория Касперского» крупнейшая шпионская сеть Red October, на протяжении пяти лет занимающаяся хищением государственных секретов, о чем ранее сообщал SecurityLab. Ведущий эксперт компании Виталий Камлюк поделился с РИА Новости подробностями о том, как происходило исследование шпионской сети.

Как сообщил эксперт, все началось с того, что в октябре прошлого года в «Лабораторию Касперского» обратился один из ее зарубежных партнеров с просьбой проанализировать подозрительный файл, обнаруженный в их компьютерной сети. «Сами они в организации изначально думали, что эта целевая атака против них конкретно, но в итоге оказалось, что список жертв не ограничивается одной организацией» - сообщил Камлюк.

Исследователи провели первичный анализ исполняемого файла, однако это ничего им не дало. Тем не менее, файл содержал в себе IP-адрес сервера в интернете, за что и «зацепились» эксперты.

С помощью специального программного обеспечения, эксперты создали виртуальную копию обычного компьютера и запустили на ней исполняемый файл, чтобы посмотреть, как он взаимодействует с сервером.

Вскоре в виртуальную систему были заброшены «первичные» модули, собиравшие и отсылавшие злоумышленникам информацию об установленных в ней программах, флэш-накопителях и мобильных устройствах, подключаемых к ней, и прочее, после чего, в зависимости от результата, на компьютер забрасывались новые вредоносные модули под более узкие задачи.

Как сообщил Камлюк, исследователи «ЛК» предположили, что модулей существует гораздо больше тех, что были загружены на виртуальный компьютер, поэтому они создали виртуальную сеть компьютеров, якобы принадлежащую администрации некоей городской службы. Это было именно то, что искали злоумышленники.

В виртуальную сеть несуществующей городской службы стали загружаться вредоносные модули под самые разные задачи. Тогда исследователи создали еще несколько подобных сетей, после чего получили более тысячи уникальных вредоносных файлов.

Сначала эксперты объяснили такое большое количество вредоносных программ тем, что они являются несколькими программами, но по-разному зашифрованными. Тем не менее, поскольку файлы сильно отличались по размерам, эксперты отказались от данного предположения.

Анализ обнаруженных файлов длился несколько недель, в результате чего исследователи выявили 34 различных вредоносных модуля, собирающих статистику, осуществляющих поиск информации, а также взламывающих сетевое оборудование, смартфоны на операционных системах Windows Mobile, iOS, Symbian и пр. Таким образом, исследователи определили анатомию, цели и масштабы Red October и пришли к единственно возможному выводу – «Красный октябрь» является крупнейшей шпионской операцией.

На компьютер жертвы посылался файл Word или таблица Excel с внедренным вредоносным кодом, который исполнялся как только пользователь открывал такой файл. Названия файлов подбирались таким образом, чтобы заинтересовавшийся пользователь обязательно его открыл. Заразив один компьютер, с помощью дополнительных модулей злоумышленники углублялись в атакуемую сеть.

Виталий Камлюк отметил, что промежуточный анализ собранных Red October данных проводили люди. Так, модули, используемые преступниками, были не всегда активны. В один день регистрировалась активность, а потом несколько дней

ничего не происходило. Это значит, что злоумышленникам требовалось время на обработку данных.

По словам эксперта, штат высококвалифицированных специалистов, проводивших операцию, должен насчитывать около 20 человек. Авторы вредоносного ПО, использовавшегося при атаке, вообще не похожи на «обычных» вирусописателей, отмечает Камлюк. Поскольку в коде двух модулей были обнаружены слова Proga и Zakladka, эксперты сделали вывод, что специалисты являются русскоязычными. Происхождение преступников, а также их имена пока остаются неизвестными.

Источник: http://www.bezpeka.com

Результаты исследования AV-TEST: WINDOWS 8 нуждается в дополнительной защите.

Очень приятно когда твои результаты подтверждаются авторитетным источником. Я писал о том, что в Windows 8 обеспечивается только базовая защита и вот подтверждение!

В декабре 2012 года независимая исследовательская лаборатория AV-Test провела сравнительный анализ нового Kaspersky Internet Security и защитных компонентов, встроенных в операционную систему Windows 8, для определения эффективности защиты от вредоносного ПО. Продукт “Лаборатории Касперского” для домашних пользователей оказался практически безупречным, в то время как результаты встроенного решения Microsoft оказались значительно скромнее.

Для проведения тестирования эксперты AV-Test подготовили “чистый” образ операционной системы Windows 8 Pro, который использовался на нескольких идентичных компьютерах. Перед испытанием на каждом новом вредоносном образце тестовые системы возвращались в исходное (чистое) состояние. На каждом из компьютеров было установлено либо защитное ПО “Лаборатории Касперского”, либо решение Windows Defender 4. Оба продукта использовались со стандартными настройками, заданными по умолчанию. Защитные продукты имели доступ в Интернет и могли использовать “облако” как элемент своей защитной стратегии, но при этом вредоносные программы также имели возможность подключения к “Облаку”/Интернету для доступа на другие сайты и дальнейшей загрузки файлов с целью заражения системы. В этом случае предпринимались меры по обеспечению безопасного доступа вредоносных образцов в “облако”, чтобы предотвратить риск заражения тестовых систем.

В ходе исследования были проведены четыре отдельных теста – тестирование в “реальных” условиях (динамическое), два статических теста для определения уровня обнаружения вредоносных программ и статический тест на количество ложных срабатываний. Kaspersky Internet Security заблокировал все вредоносные URL-адреса, а также вложения в сообщениях электронной почты, и обнаружил 99% образцов вредоносных программ, не допустив при этом ни одного ложного срабатывания. Компоненты защиты Windows 8 пропустили 11,9% атак и смогли обнаружить только 90% вредоносных образцов. Как и Kaspersky Internet Security, решение Microsoft не допустило ни одного ложного срабатывания.

Это доказывает, что продукты, демонстрирующие высокий уровень обнаружения вредоносного ПО и высокую степень защиты, могут работать безложных срабатываний.

Существенные отличия в результатах тестирования Kaspersky Internet Security и компонентов защиты Windows 8 позволяют сделать вывод, что Windows Defender и защитные функции, реализованные в решении компании Microsoft, обеспечивают лишь базовую защиту. В условиях, когда ежедневно появляются 200 000 новых вредоносных образцов, домашним пользователям требуется испытанное и гораздо более надежное решение – Kaspersky Internet Security.

“Появление дополнительных средств антивирусной защиты в новой операци-

онной системе Windows 8, безусловно, положительно сказалось на степени защищенности этой системы, – комментирует Никита Швецов, руководитель управления исследования угроз "Лаборатории Касперского". – Однако проведенное AV-Test исследование наглядно продемонстрировало, что сегодня этих средств уже недостаточно для полноценной защиты пользователей от нового и неизвестного вредоносного ПО – наиболее серьезной из современных киберугроз. По-настоящему высокий уровень безопасности обеспечивает новый Kaspersky Internet Security, который полностью совместим с Microsoft Windows 8″.

Автор: Безмалый Владимир.
Источник: http://www.dlp-expert.ru

Зарубежные правообладатели недовольны работой российской полиции.

Международный союз по защите интеллектуальной собственности (IIPA) опубликовал предварительные материалы для отчёта 2013 Special 301 Report с анализом нарушений прав интеллектуальной собственности в разных странах мира. Организация традиционно выделяет в «список наблюдения» те страны, в которых ситуация особенно неудовлетворительна и требует неотлагательных мер. Россия находится в «приоритетной» части списка с 1997 года. В свежем отчёте список главных стран-нарушителей составят Аргентина, Чили, Китай, Коста-Рика, Индия, Индонезия и Россия.

Особняком стоит Украина, где нарушения интеллектуальных прав настолько вопиющи, что это государство пришлось выделить среди главных стран-нарушителей в особую категорию. Эксперты отмечают увеличение уровня использования нелицензионного ПО украинскими компаниями и частными пользователями. Ситуация в этом отношении значительно ухудшилась за последние два года. Значительно распространилось скачивание нелицензионной музыки через интернет. Украину также считают одним из основных источников пиратских копий фильмов («экранок»), которые появляются в торрентах. По информации разведчиков, нелицензионные фильмы, музыка и программное обеспечение открыто продаются на улицах городов. Специалисты считают, что действия украинских властей ведут к ещё большему ухудшению ситуации.

В России тоже проявляются негативные тенденции в области охраны интеллектуальной собственности. По данным IIPA, за весь 2012 год российская полиция смогла провести лишь один рейд против интернет-пиратов вместо 22 таких операций годом ранее. Аналогично, значительно снизилось количество рейдов против конечных пользователей нелецензионного ПО: в 2012 году проведено 506 таких рейдов против 554 в 2011 году. Количество заведённых уголовных дел против пользователей нелицензионного ПО составило 97 (в 2007 году было 200), но количество обвинительных приговоров — всего лишь 24 (в 2007 году было 83).

В числе главных сайтов, где процветает криминальный обмен контентом, эксперты называют Rutracker.org и «Вконтакте». По данным Entertainment Software Association, Россия поднялась на первое место в мире по количеству интернет-пользователей, скачивающих пиратский контент из торрентов.

Ещё 25 стран, в том числе Беларусь и Казахстан, попадут в обычный «список наблюдения», если ситуация не изменится в ближайшее время. Окончательная версия отчёта 2013 Special 301 Report будет опубликована в конце апреля 2013 года.

Международный союз по защите интеллектуальной собственности объединяет интересы более 3200 американских компаний, крупнейших владельцев интеллектуальной собственности, и отстаивает их интересы через дипломатические каналы и торговые представительства США.

Источник: http://www.xakep.ru

Контроль запуска программ как залог безопасности сети. Часть 1.

Введение

Безопасность корпоративных сетей является одной из наиболее острых проблем современных компаний. Вредоносные программы наносят значительный урон бизнесу, и репутация фирмы страдает не в последнюю очередь. Компании, специализирующиеся на IT-безопасности, предлагают различные дорогостоящие решения, однако во многих случаях внедрение этих решений ведет к значительному увеличению затрат на обслуживание и поддержку сети. А обеспечить гарантированную защиту от неизвестных угроз, особенно от целевых атак, традиционные решения могут далеко не всегда.

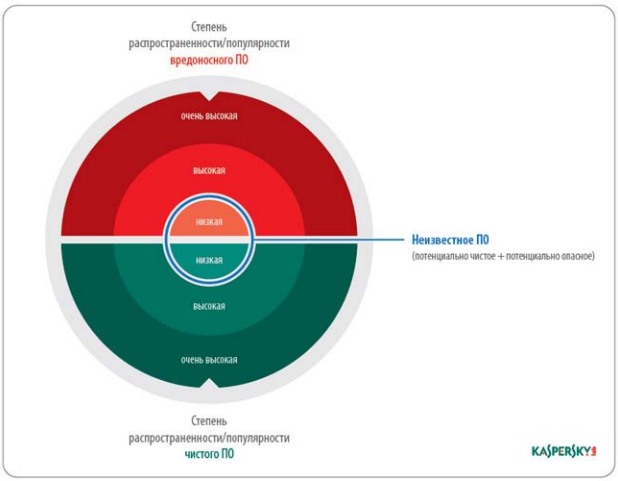
Наша статья посвящена альтернативному подходу к защите корпоративных сетей, который мы назвали Whitelist Security Approach.

Этот подход является продолжением развития технологии контроля запуска и исполнения программ (Application Control), дополненной реализацией развитой поддержки режима «Запрет по умолчанию» (Default Deny), а также инновационной технологии белых списков (Dynamic Whitelist).

Мы в «Лаборатории Касперского» считаем Whitelist Security Approach одним из ключевых элементов средств защиты корпоративных сетей будущего. Продукты, в которых реализован такой подход, способны не только защитить от неизвестных угроз, но и предложить системным администраторам сетей, инженерам по информационной безопасности развитые средства учета и контроля программного обеспечения, включая посторонние (не имеющие отношения к производственным задачам), нежелательные и нелицензионные программы.

Предпосылки поиска альтернативных подходов к защите

Количество нового ПО стремительно растёт с каждым годом. Для обеспечения качественной защиты пользователей антивирусные компании должны оперативно анализировать гигантские потоки информации и ежедневно обрабатывать терабайты данных, классифицируя десятки миллионов файлов. Если говорить о классификации, то все программное обеспечение можно разделить на три категории: известное вредоносное, известное чистое и неизвестное ПО.



ПО, которое однозначно не классифицировано антивирусной компанией как чистое или вредоносное, считается неизвестным.

Часть неизвестного ПО содержит вредоносный код, и именно такие программы являются самыми опасными для пользователя и самыми проблемным для детектирования АВ-продуктами, именно отсюда стоит ждать угрозы, поскольку вирусописатели постоянно оттачивают своё мастерство и появляются все новые и новые и новые вредоносные программы.

В большинстве случаев антивирусным компаниям приходится играть роль догоняющих: за появлением новой технологии вирусописателей следует новый виток развития средств защиты. В настоящее время для повышения уровня безопасности используются не только тради-

ционные сигнатурные технологии, но и целый арсенал современных технологий защиты. Это и проактивные эвристические методы (как статические, так и динамические), и облачные технологии, которые не только обеспечивают практически мгновенную реакцию на новые угрозы, но и расширяют стандартные мощности «коробочных» средств защиты мощностью ранее недоступной инфраструктуры online-сервисов.

Традиционный подход к защите предполагает блокирование известных угроз, в том числе известных шаблонов вредоносного поведения. Однако истории с троянцами Stuxnet, Duqu и Flame показывают, что против некоторых новых угроз и целевых атак традиционная защита предлагаемых на рынке решений практически бессильна. Следствием этого являются постоянно растущие требования к безопасности корпоративных сетей.

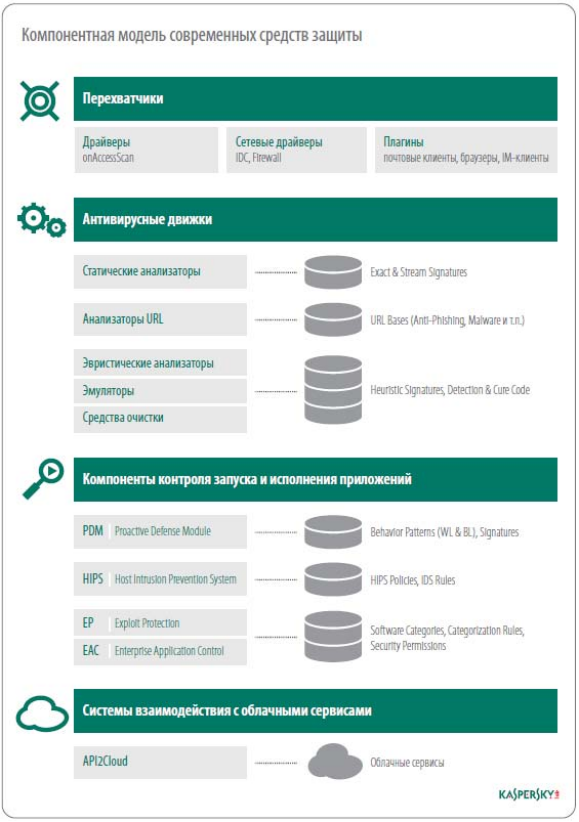
В сложившейся ситуации перед разработчиками ПО в области IT-безопасности стоит задача поиска альтернативных решений, способных существенно повысить уровень защиты корпоративных сетей. Предлагаемый в данной статье альтернативный подход – Whitelist Security Approach – не только обеспечит соответствующий современным требованиям уровень защиты, но и позволит антивирусным компаниям перестать быть догоняющими и начать играть по своим правилам.

Whitelist Security Approach базируется не только на нашем знании принципов развития и распространения корпоративных угроз, но и на понимании бизнес-потребностей компаний-заказчиков, а также того, какие средства защиты требуются для реализации надежного, и при этом сбалансированного решения. Рассматриваемое ниже решение отличается простотой интеграции и управления и, что тоже важно, относительно невысокой стоимостью его владения (TCO) при достигаемом высоком уровне информационной безопасности.

Реализация данного подхода потребовала не только пересмотра десятилетней «парадигмы преследования», но и инициировала принципиально новый этап развития технологии контроля запуска и исполнения программ (Application Control).

Компонентный состав современных продуктов безопасности

Надежная информационная защита требует комплексного подхода. Современные средства защиты состоят из нескольких компонентов, каждый из которых выполняет определенные задачи.



Компонентная модель современных средств защиты

В данной модели можно выделить четыре основных группы компонентов: перехватчики, антивирусные движки, компонент контроля запуска и исполнения приложений, облачные сервисы.

Рассмотрим функциональные задачи каждого из компонентов.

Перехватчики — это некие «сенсоры», которые позволяют антивирусным продуктам встраиваться в процесс работы

ОС так, чтобы другие компоненты АВ-защиты имели возможность проверять объекты и события в нужный момент времени.

В качестве перехватчиков работают:

•Драйвер, осуществляющий перехват обращения приложений к файлам. Перехватив обращение к файлу, АВ-продукт может проверить этот файл на наличие вредоносного кода или проверить допустимость такой операции согласно правилам контроля активности приложений (HIPS). В случае наличия вредоносного кода или противоречия правилам активности приложения, драйвер может запретить либо обращение к файлу, либо запуск приложения.

•Сетевой драйвер позволяет осуществлять контроль сетевой активности приложений (предотвращение утечек данных по сети, блокировка сетевых атак и т.д.).

•Плагины – библиотеки (модули), встраиваемые в популярные приложения (в почтовые клиенты, браузеры, IM-клиенты и т.д.), обеспечивающие проверку передаваемых данных.

Движки — это модули продукта, предназначенные для проверки потенциально вредоносных объектов. Методов проверки может быть несколько, и их перечень и названия у каждого АВ-вендора могут быть свои.

Можно выделить основные типы движков:

•Статические анализаторы позволяют детектировать вредоносные объекты по каким-либо характерным статическим признакам (чаще всего это связано со структурой файлов специфичных форматов).

•Анализаторы URL проверяют, есть ли URL-адрес, на который переходит пользователь или который ему прислали по почте, в базах вредоносных или фишинговых URL, в базе URL-адресов сайтов определенных тематических категорий (компонент «Родительский контроль»).

•Эвристические анализаторы – технология, которая дает возможность одной сигнатурой детектировать множество вредоносных файлов, в том числе и ранее неизвестные модификации вредоносного ПО, одновременно позволяя добиться повышения качества детектирования и уменьшения размера антивирусных баз.

•Эмуляторы – модули, которые осуществляют исполнение программного кода в изолированной среде для последующего анализа его поведения.

В большинстве современных антивирусных продуктов одной из составляющих информационной защиты является набор технологий, реализованных в компоненте Контроль запуска и исполнения приложений (Application Control). Контроль запуска и исполнения приложений (Application Control) работает с использованием событий от «перехватчиков», обработка этих событий осуществляется с помощью разных компонентов:

•PDM (Proactive Defense Module). Поиск и обнаружение известных вредоносных моделей поведения программ (последовательностей, паттернов) по базам вредоносных паттернов поведения.

•HIPS (Host Intrusion Prevention System). Проверка каждого потенциально опасного действия программы (чаще атомарного действия) по перечню правил, определяющих допустимые для этой программы действия. Причем эти правила могут создаваться разными для разных категорий ПО. Например «доверенным» программам можно делать «все», а «неизвестным и подозрительным» что-то можно запрещать.

•Exploit protection. Предназначен для защиты от вредоносного ПО, использующего уязвимости в программах и операционной системе.

В настоящее время Exploit Protection есть в арсенале лишь некоторых компаний, но мы считаем этот уровень защиты необходимым. У «Лаборатории Касперского» соответствующий набор технологий называется Automatic Exploit Prevention (AEP). В его основе лежит анализ поведения эксплойтов, а также особый контроль приложений, которые чаще других подвергаются атакам злоумышленников. AEP препятствует срабатыванию эксплойтов и развитию вредоносного поведения, если эксплойт всё-таки сработал.

•EAC (Enterprise Application Control). Запуск программ разных категорий и/или

версий ПО в соответствии с разными правилами.

Взаимодействие с облачными сервисами (CLOUD Services) позволяет расширить возможности как движков, так и технологий контроля активности программ. Использование облака позволяет скрыть часть логики проверки (чтобы осложнить злоумышленникам процесс реверс-инжиниринга и обход логики проверки вредоносных программ) и уменьшить размер обновлений баз сигнатур и баз поведенческих шаблонов на стороне пользователя/клиента.

Application Control как ключевой инструмент контроля приложений в корпоративных сетях

В описанной выше компонентной модели Application Control позволяет гибко регулировать активность приложений с помощью HIPS-политик, изначально задаваемых производителем AB-решений. Приложения, рассматриваемые в контексте Application Control, делятся на четыре категории: безопасные, опасные, с сильными ограничениями и слабыми ограничениями. В соответствии с данными категориями определяется уровень накладываемых на приложения ограничений (HIPS-политик). Для каждой категории приложений определяются правила, в соответствии с которыми регулируется доступ приложений к различным ресурсам (файлам, папкам, регистрам, сетевым адресам). Например, если приложению требуется доступ к определенному ресурсу, Application Control проверяет, имеет ли оно соответствующие права, и далее осуществляет операцию в соответствии с заданными правилами.

Application Control позволяет также протоколировать запуски приложений. Эта информация может использоваться в ходе расследований инцидентов и различных проверок. Имея в своём арсенале подобную функциональность, инженер информационной безопасности или администратор оперативно и в структурированной форме получает ответы на следующие вопросы:

•Какие приложения запускались и когда именно в заданный интервал времени?

•На каких ПК и под какими учетными записями?

•Как давно используется та или иная программа?

Именно от функциональных возможностей (мощности и удобства использования) данного компонента зависит, насколько эффективно администраторы сети смогут внедрять и поддерживать различные политики безопасности.

Баланс между свободой действий и безопасностью

При выборе модели информационной защиты важен разумный баланс свободы и безопасности.

Для домашних пользователей важна возможность устанавливать и использовать любое ПО без ограничений. И хотя риск заражения в таком случае больше, чем при жестком режиме запретов, домашний пользователь распоряжается только своей персональной информацией и самостоятельно принимает решение с учетом существования риска разглашения или утраты информации.

Корпоративный пользователь, напротив, оперирует информацией, собственником которой он не является. Чем жестче контроль, тем меньше риски информационной безопасности: утечка/потеря критически важных для бизнеса данных, нарушение бизнес-процессов компании и, как следствие, финансовые и репутационные потери.

Для компаний баланс безопасности и свободы действий означает баланс возможного риска и удобства, которое получают корпоративные пользователи. Если для небольших компаний приоритетом, как правило, является удобство пользователей и, как следствие, минимум ограничений для них, то в случае больших корпоративных сетей на первый план выходит обеспечение максимального уровня защищённости. В крупных компаниях внедряются централизованные политики безопасности — единые правила использования корпоративных информационных ресурсов. Удобство конечных пользователей уступает место унификации ПО и максимальной прозрачности процессов для системных администраторов.

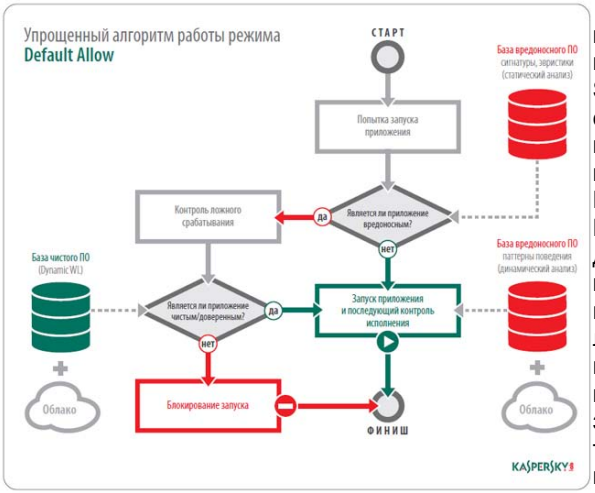
Для выполнения рабочих задач сотрудникам компании, как правило, достаточно использовать определенный набор

программ. Возможность ограничить состав используемого ПО только теми приложениями, которые определит администратор, и заблокировать остальные нежелательные программы (неавторизованное, нелегитимное и нецелевое ПО) — чрезвычайно важная опция для корпоративной сети, не говоря уже об управляющих центрах, промышленных объектах, финансовых организациях, военных предприятиях и устройствах специализированного назначения (например, банкоматы и различного рода терминалы).

Максимальное удобство пользователей обеспечивает режим «Разрешение по умолчанию» (Default Allow), а максимальную защиту – режим «Запрет по умолчанию» (Default Deny).

Традиционный подход к защите: Default Allow

При традиционно используемом и в персональных, и в корпоративных продуктах режиме «Разрешение по умолчанию» (Default Allow) пользователь может запускать любые приложения, за исключением заблокированных или таких, на запуск которых установлены ограничения. Применение данной парадигмы обусловлено тем, что предлагаемые на рынке решения ориентированы на максимальное удобство пользователя.



Очевидно, что возможность запуска любых приложений требует качественных технологий детектирования. В режиме Default Allow все представленные выше компоненты защиты участвуют в анализе исполняемых программ. Это позволяет детектировать не только известные, но и некоторые неизвестные угрозы. Качество детектирования при этом зависит от производителя антивирусного решения.

Однако, как было сказано выше, антивирусные компании, как правило, идут за вирусописателями и являются догоняющими, то есть всегда существует вредоносное ПО, еще не детектируемое антивирусной защитой. При этом в режиме Default Allow, если программа не попала в число запрещенных, то ее запуск и исполнение по умолчанию разрешены. А это значит, что режим Default Allow предполагает определенный риск: допущенный к запуску код может нести еще не идентифицированную угрозу.

Помимо вредоносных программ, существует легитимное, но нежелательное для конкретной сети ПО. Оно не подпадает под политику блокирования, поэтому в режиме Default Allow, если нет специального запрета, такое ПО также можно запустить в корпоративной сети без каких-либо ограничений.

Приведем два примера того, как программа, не заблокированная политиками безопасности, может нанести ущерб компании.

Сотрудник устанавливает на компьютер программу мгновенного обмена сообщениями – Skype. Отличительной особенностью Skype является шифрование данных, передаваемых по каналам связи. Это значит, что DLP-системы (Data Loss Prevention) не способны отследить передачу конфиденциальной информации за пределы защищаемого периметра и вычислить получателя данной информации. Антивирусные технологии также не запрещают использование данного приложения, так как оно не является вредоносным. Злоумышленник, вступив в сговор с сотрудником компании, имеет возможность получать от сотрудника конфиденциальную информацию, используя Skype в качестве средства передачи данных.

Другой пример. Сотрудники «Лаборатории» оказывали помощь в расследовании инцидента в одной компании. Вредоносных программ обнаружено не было, а причина инцидента была в том, что IT-специалист установил на ряд ПК легитимную утилиту удаленного администрирования. Специалист этот был уволен более года назад, про утилиту никто не знал – тем не менее, она продолжала работать, открывая уволенному сотруднику несанкционированный доступ к корпоративной сети и хранящимся в ней данным.

Таким образом, при максимальном удобстве для конечного пользователя режим Default Allow оставляет корпоративную сеть уязвимой для неизвестных угроз и нежелательного ПО. При этом контроль за всеми исполняемыми программами требует существенных ресурсов.

Однако в большинстве случаев для выполнения своих задач сотрудникам компаний достаточно использовать ограниченный, конкретный набор программ. А это значит, что логичным было бы простое решение: все необходимое и чистое ПО занести в белые списки, а запуск в сети всех остальных программ запретить по умолчанию. Такой режим работы называется Default Deny.

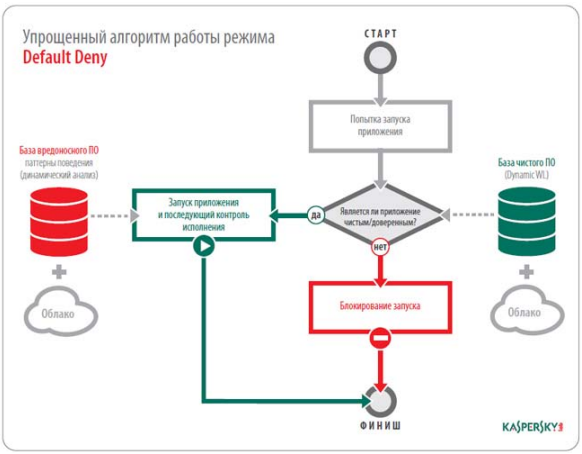
Режим Default Deny

В противоположность Default Allow, режим Default Deny запрещает выполнение любого ПО, не занесенного в доверенные (белые) списки. Таким образом, никакое неизвестное или нежелательное ПО не допускается к запуску.

По сути в режиме Default Deny корпоративная сеть работает в изолированной программной среде, в которой разрешен запуск только тех программ, которые необходимы и достаточны для выполнения бизнес-задач компании.

В дополнение к этому запрет запуска вредоносного, нецелевого, нелицензионного, неизвестного ПО снижает затраты на анализ тех программ, которые в случае режима Default Allow были бы разрешены к запуску. При работе в режиме Default Deny существенно снижаются требования к производительности контролируемых систем и к объему ресурсов, необходимых для анализа программ. Как следствие, снижается влияние системы безопасности на работу сети в целом.

Как видно на рисунке, в отличие от традиционной модели защиты, в режиме Default Deny контроль и мониторинг приложений осуществляется не в процессе исполнения, а в момент запуска разрешенных программ. Тем самым риски информационной безопасности минимизируются на самых ранних этапах обеспечения защиты.



Основные преимущества Default Deny:

1.Минимизация рисков запуска вредоносного и нежелательного ПО:

•Блокирование неизвестных приложений, включая новые разновидности вредоносных программ, в том числе используемых при целевых атаках. Как следствие, обеспечение безопасной среды.

•Возможность блокировать установку, запуск и исполнение нелегитимного/нелицензионного и не связанного с рабочими задачами ПО — разнообразных интернет-пейджеров, игр, заведомо уязвимых версий ПО, «оптимизаторов» и «ускорителей» системы. Как следствие, ориентация персонала на конкретные должностные обязанности и улучшение производственных показателей.

2.Снижение требований к производительности ресурсов, необходимых для

анализа приложений. Как следствие, уменьшение влияния системы безопасности на штатную работу контролируемых систем.

3.И последнее, но не менее важное — снижение затрат, а в конечном итоге снижение совокупной стоимости сопровождения и поддержки системы безопасности в целом: меньше сбоев, меньше жалоб, меньше нагрузка на службу технической поддержки.

Таким образом, применяя альтернативный подход, реализованный в мощных средствах мониторинга и контроля запуска и исполнения приложений, можно существенно повысить уровень информационной безопасности корпоративной сети, при этом значительно снизив затраты на её обеспечение и последующую поддержку. Как мы уже писали выше, это принципиально другой, проактивный подход к защите, который, по мнению экспертов «Лаборатории Касперского», в ближайшем будущем может перевернуть традиционное представление о безопасности корпоративных сетей.

Авторы выражают благодарность Владиславу Мартыненко за помощь в подготовке главы «Компонентный состав современных продуктов безопасности».

Источник:

http://www.securelist.com

Биометрическая проверка личности с помощью смартфона

Скоро для проверки личности человека не нужно будет смотреть его паспорт и подпись. Идентификация будет осуществляться с обычного смартфона, который имеет доступ к биометрической базе данных. Достаточно навести на человека камеру — и через несколько секунд агент увидит на экране его досье.

Министерство обороны США заключило двухлетний контракт на сумму $3 млн с калифорнийской компанией AOptix на разработку мобильных сканеров нового поколения для идентификации личности (Smart Mobile Identity). Через два года компания обязуется предоставить действующий прототип периферийного аппаратного устройства и программное обеспечение, пригодное для установки на коммерчески доступные смартфоны. Система должна уметь сканировать сетчатку глаза, лицо, отпечатки пальцев и голос человека, передавая информацию в удалённую базу данных для идентификации.

На сегодняшний день американцы используют для биометрической идентификации устройства Handheld Interagency Identity Detection System (на фото внизу).

Такие устройства позволяют сканировать радужную оболочку глаза, фотографировать лицо и снимать отпечатки пальцев, но они весьма дороги и неудобны в обслуживании. Если удастся разработать аналог в виде съёмного модуля для смартфонов, то можно значительно сэкономить.

Источник: http://www.xakep.ru

Японская полиция арестовала предполагаемого создателя «вируса-террориста»

Японские власти арестовали предполагаемого создателя вредоносной программы, рассылавшей по доскам объявлений и электронным ящикам различных организаций и отдельных интернет-пользователей Японии объявления и электронные письма с угрозами похищений и террористических актов. При этом угрозы высказывались от имени пользователей инфицированных вредоносом компьютеров.По информации Bangkok Post, полиция подозревает в создании вируса 30-летнего жителя Токио Юсукэ Катаяму (Yusuke Katayama).

Правоохранительные органы Японии

обнаружили вредоносную программу еще в октябре прошлого года, после ареста владельцев нескольких компьютеров, с которых, якобы, рассылались тексты с угрозами. В рассылаемых текстах содержались угрозы совершения террористических актов в торговом центре; угрозы взорвать самолет, полученные одной из авиакомпаний; а также угрозы в адрес императорской семьи, в частности, угрозы проведения террористического акта в школе, посещаемой членами императорской семьи.

В декабре 2012 года в СМИ появилась информация, что японская полиция разыскивает человека, достаточно хорошо разбирающегося в языке программирования C#. Тогда же стало известно, что для анонимной публикации текстов с угрозами в Интернет, подозреваемый использует так называемый метод “Syberian Post Office”.

Власти Японии объявили награду в размере $36000 за любую информацию, которая бы позволила поймать создателя вируса. Ранее японские власти предлагали подобные вознаграждения лишь за информацию о людях, разыскиваемых по подозрению в умышленных убийствах и поджогах.

Хакер сам дал правоохранительным органам подсказку, позволившую им выйти на его след, предложив им сыграть в игру. Найти кота на одном из островов близ Токио. На ошейнике кота была карта памяти, содержащая, как оказалось, часть кода «вируса-террориста».

Проанализировав содержимое карты памяти, а также материалы с ближайших к месту находки камер видеонаблюдения, полицейские вышли на след Катаямы и арестовали его.

Источник: http://www.anti-malware.ru

Вредоносные JAR с цифровыми подписями.

В декабре 2012 года вышло обновление Java SE 7 Update 10, в котором компания Oracle представила новую систему уровней безопасности. При рекомендуемых настройках безопасности выполнение неподписанных апплетов в браузере автоматически блокируется.

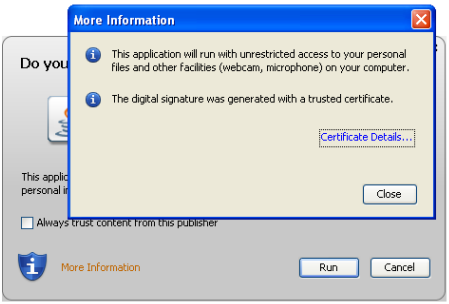
Злоумышленники предприняли вполне логичные ответные меры — и начали подписывать апплеты, используя цифровые сертификаты третьих фирм. Об этой практике рассказывает в своём блоге специалист по безопасности Эрик Романг (Eric Romang).

Вредоносный JAR, оснащённый валидным цифровым сертификатом, обнаружен на немецком сайте hxxp://dict.tu-chemnitz.de/ — это онлайновый словарь, заражённый с помощью g01pack Exploit Kit. Прямую ссылку на вредоносный файл можно взять на :

http://pastebin.com/BiND6qZt.

Java-приложение не распознаётся ни одним из антивирусов, по информации VirusTotal, оно запускается на компьютере как ClearWeb Security Update.

Как видно, в качестве владельца сертификата указана компания Clearesult Consulting Inc., это реальная фирма с юридическим адресом в Техасе. Цифровая подпись приложения сгенерирована с помощью нормального доверенного сертификата.



Источник: http://www.xakep.ru

Backdoor.Barkiofork бьет по оборонной и авиационно-космической индустрии.

Корпорация Symantec сообщает об обнаружении ряда кибератак, нацеленных на предприятия оборонной и авиационно-космической промышленности. Злоумышленники заманивали жертв письмом с вредоносным содержимым, используя в качестве приманки отчет о перспективах развития оборонной и авиационно-космической индустрии.

Несколько недель назад эксперты Symantec стали свидетелями кибератак с применением направленного фишинга, направленных на организации авиационно-космической и оборонной промышленности. СпециалистамиSymantec было выявлено, по меньшей мере, 12 различных организаций, попавших под удар. Среди них оказались компании, связанные с авиацией и управлением воздушным движением, а также выполняющие государственные заказы, в том числе оборонные.

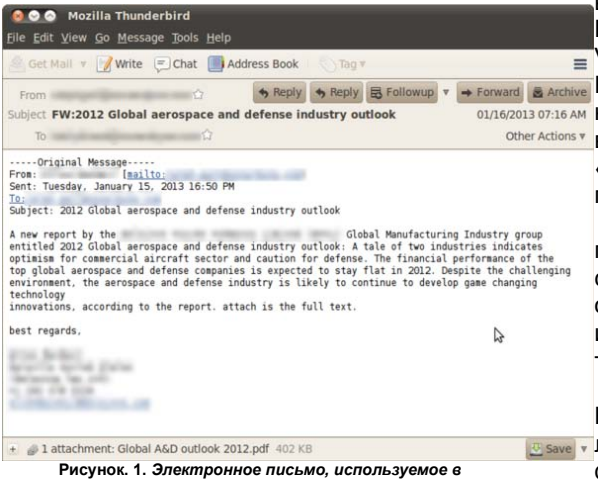


Рисунок. 1. *Электронное письмо, используемое в данной фишинговой кампании*

В качестве жертв злоумышленники выбирали значимых лиц: топ-менеджеров, директоров и вице-президентов. Содержание всех электронных писем было идентичным. В качестве приманки злоумышленники использовали опубликованный в 2012 году отчет, касающийся перспектив оборонной и авиационно-космической индустрии. Злоумышленники попытались создать впечатление, что это письмо было отправлено компанией, которая первоначально его составила. К тому же письмо было написано таким образом, чтобы казалось, что оно пришло от сотрудника компании, либо от специалиста, занятого в одной из указанных отраслей.

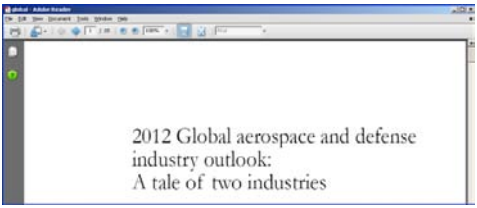


Рисунок. 2. Пользователю открывается «чистый» PDF-файл

Когда жертва открывала прикрепленный к письму вредоносный pdf-файл, срабатывал эксплойт, пытавшийся использовать уязвимость ‘SWF’ File Remote Memory Corruption Vulnerability (CVE-2011-0611). Если попытка оказывалась удачной, в систему загружались вредоносные файлы, а также «чистый» pdf-файл с целью усыпить бдительность пользователя.

Используемый в качестве приманки pdf-файл представляет собой обзор перспектив отрасли, однако злоумышленники слегка изменили оригинал, убрав некоторые брендинговые элементы.

Помимо записи «чистого» PDF-файла, в систему устанавливалась вредоносная версия файла svchost.exe, который затем размещал в папке Windows вредоносную версию библиотеки ntshrui.dll. Угроза использует технику проникновения через механизм поиска DLL (ntshrui.dll не защищён средствами операционной системы, как известный dll-файл). Когда файл svchost.exe запускает explorer.exe, то последний подгружает вредоносный файл ntshrui.dll из папки Windows вместо легитимного, расположенного в систем-

ной папке Windows. Продукты Symantec определяют вредоносные файлы svchost.exe и ntshrui.dll как Backdoor.Barkiofork.

Изученная версия Backdoor.Barikiofork обладает следующей функциональностью:

•Производит переучёт дисков;

•Связывается со своим сервером управления через osamu.update.ikwb.com;

•Похищает системную информацию;

•Скачивает и устанавливает свои обновления.

Эта кампания нацеленного фишинга продолжает демонстрировать изощренность и высокий уровень подготовки злоумышленников при проведении атак с целью хищения информации, и особенно использование приемов социальной инженерии, наиболее эффективно воздействующих на жертву.

Источник: http://www.anti-malware.ru

Исландия хочет блокировать интернет-порно.

Министерство внутренних дел Исландии выступило с инициативой блокировать порнографию в интернете. По сведениям от осведомлённых источников, идея уже получила одобрение в парламенте и у разных организаций, они близки к консенсусу, а законопроект должен появиться ближе к лету. Таким образом, Исландия может стать первым государством в западном мире, которая запустит файрвол по образцу китайского.

Борьба с «вредоносным контентом» в Исландии проводится под лозунгом защиты детей. По информации правоохранительных органов, несовершеннолетние граждане массово скачивают порнографию на свои персональные компьютеры, игровые приставки и смартфоны, из-за чего возрастает количество случаев сексуального насилия в стране.

Министр внутренних дел Огмундур Йонассон (Ögmundur Jónasson, на фото) организовал рабочую группу, которая должна найти наиболее приемлемое техническое решение для блокирования фотографий и видеороликов на всех упомянутых устройствах.

Это непростая задача. Многие эксперты сомневаются, что она в принципе реализуема хоть каким-либо способом, кроме создания «белого списка» сайтов, на которые разрешено ходить. Такой вариант, естественно, неприемлем.

Тем не менее, чиновники смотрят в будущее с оптимизмом: «Если мы можем запустить человека на Луну, то мы сможем и решить проблему порнографии в интернете», — сказала политический советник министерства внутренних дел Хелла Гуннарсдоттир (Halla Gunnarsdóttir).

В лунной миссии цель была понятна каждому без каких-либо разночтений. Было ясно, куда запускать человека и как определить, что он прибыл на место назначения. Фильтрация порнографии — задача совершенно иного плана. Её выполнение особенно осложняется тем, что у каждого жителя Исландии своё понимание, что такое порнография. У экспертов нет единого мнения на этот счёт. То, что для одного может показаться невинным образом, для другого — совершенно непристойное изображение.

Впрочем, маленькая Исландия с населением 319 тысяч человек — одновременно и первая в мире парламентская демократия (по крайней мере, они сами в этом убеждены) — твёрдо намерена защитить моральные устои общества. Два года назад женщина премьер-министр инициировала полный запрет на стрип-клубы в стране из-за нарушения в них гражданских прав женщин и вреда для общества. Очевидно, порнография в интернете представляет не меньшую угрозу морали.

Источник: http://www.xakep.ru

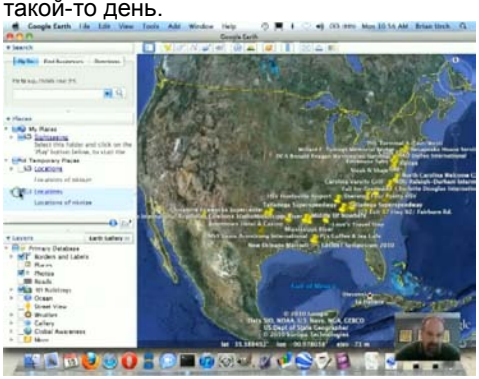
RIOT: программа для слежки за гражданами через социальные сети.

Специалисты по безопасности давно предупреждали, что власти могут начать использовать социальные сети для высокотехнологичной слежки за гражданами. Похоже, что впервые появились доказательства подобных действий. Издание Guardian получило в своё распоряжение

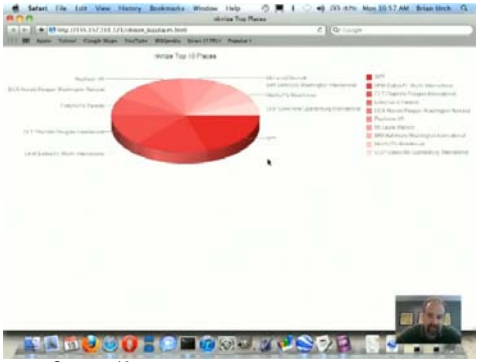
видеозапись презентации программного обеспечения под названием RIOT (Rapid Information Overlay Technology), которое разработал американский военный подрядчик Raytheon ещё в 2010 году. Это система, созданная для быстрого извлечения информации о подозреваемых гражданах из социальных сетей, в том числе Facebook, Twitter и Foursquare.

Буквально в несколько щелчков мыши следователь получает сведения об активности подозреваемого: о его социальных контактах, карте перемещений и др. Информация извлекается в том числе из EXIF-заголовков фотографий, опубликованных в личных фотоальбомах на разных сайтах.

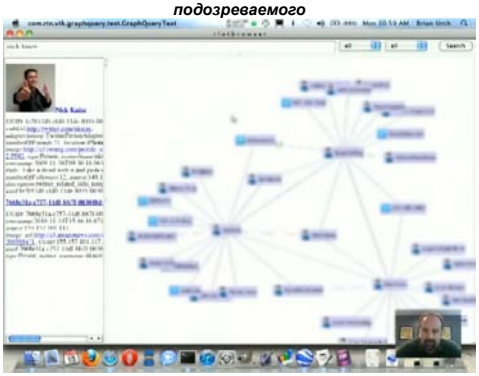
Представители Raytheon сообщили, что программа сделана только в демонстрационных целях и её не передавали для использования ни одному клиенту. Но у журналистов есть сведения, что разработка всё-таки была передана правительственным агентствам США, которые использовали её для создания «системы национального масштаба», способной не только собирать информацию, но якобы даже предсказывать действия граждан. Например, следователь выводит на экран информацию о подозреваемом человеке по имени Ник. Система сообщает, что Ник посещает спортзал обычно в 6 утра, чаще всего по понедельникам, судя по его чекинам в Foursquare и данным GPS с мобильного телефона. Таким образом, если нужно установить бэкдор на ноутбук Ника, то агенты легко получают нужные сведения: нужно всего лишь зайти в раздевалку конкретного спортзала в 6-20 в такой-то день.



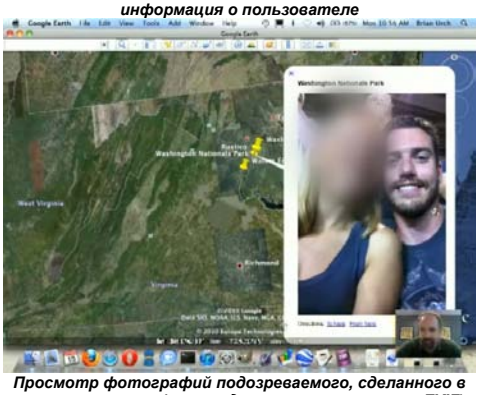
Карта перемещений подозреваемого и интерфейс программы



Список 10-ти самых часто посещаемых мест подозреваемого



Социальный граф со списком контактов подозреваемого. При наведении мыши на каждое имя демонстрируется номер телефона и другая информация о пользователе



Просмотр фотографий подозреваемого, сделанного в указанном месте (по координатам из заголовков EXIF)

Источник: http://www.xakep.ru

Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

{
Адрес журнала в интернете:
http://ualinux.com/index.php/journal

Обсуждение журнала на форуме:
http://ualinux.com/index.php/forum
}

{
Адрес редакции:

Украина, 03040, г.Киев, а/я 56
email: journal@ualinux.com
}

Тип издания: электронный/печатный
Тираж: *более 15 000 копий.

*указано суммарное количество прошлого выпуска журнала с первичных источников, а также загрузок с других известных ftp, http и torrent серверов.