Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

UA Linux http://ualinux.com

В хакерской атаке на Apple, Facebook и Twitter заподозрили украинцев

Читайте в этом номере:

Для беспрецедентной атаки хакеры использовали по крайней мере один сервер компании, которая базируется в Украине.

В атаке хакеров на серверы почти 40 американских компаний, включая Apple, Facebook и Twitter, подозревается группировка, которая базируется в Восточной Европе или России. Об этом сообщило агентство Bloomberg.

Хакеры, похоже, стремились получить секретную информацию Apple, покушаясь на ее интеллектуальную собственность, приводит агентство мнение представителей спецслужб США. Такие же атаки были предприняты в последнее время против социальных сетей Facebook и Twitter. По словам источников, хакеры использовали по крайней мере один сервер компании, которая базируется в Украине.

Последними подверглись атаке во вторник, 19 февраля, серверы компании Apple. "У нас нет информации о краже секретных данных, однако атака носит беспрецедентный характер", - говорилось в заявлении пресс-службы Apple.

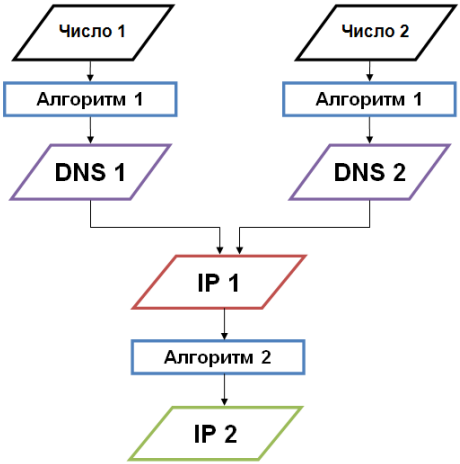
В минувшую пятницу о действиях хакеров сообщила социальная сеть Facebook. "Мы предприняли все необходимые шаги для очистки всех зараженных компьютеров, проинформировали правоохранительные органы и начали масштабное расследование", - отмечалось в сообщении соцсети, насчитывающей свыше миллиарда пользователей.

Источник: http://zn.ua/

And User Linux

Троянец Linux.Sshdkit атакует Linux-серверы.

В связи с участившимися случаями взлома веб-серверов, работающих под управлением операционной системы Linux, компания «Доктор Веб» провела собственное расследование данных инцидентов. Специалисты выяснили, что одним из способов кражи паролей на серверах с ОС Linux стало использование троянца, добавленного в базы Dr.Web под именем Linux.Sshdkit.



Вредоносная программа Linux.Sshdkit представляет собой динамическую библиотеку, при этом существуют ее разновидности как для 32-разрядных, так и для 64-разрядных версий дистрибутивов Linux. Механизм распространения троянца пока еще до конца не изучен, однако имеются основания полагать, что его установка на атакуемые серверы осуществляется с использованием критической уязвимости. Последняя известная специалистам «Доктор Веб» версия данной вредоносной программы имеет номер 1.2.1, а одна из наиболее ранних — 1.0.3 — распространяется на протяжении довольно-таки длительного времени.

После успешной установки в систему троянец встраивается в процесс sshd, перехватывая функции аутентификации данного процесса. После установки сессии и успешного ввода пользователем логина и пароля они отправляются на принадлежащий злоумышленникам удаленный сервер посредством протокола UDP. IP-адрес управляющего центра «зашит» в теле троянской программы, однако адрес командного сервера каждые два дня генерируется заново. Для этого Linux.Sshdkit применяет весьма своеобразный алгоритм выбора имени командного сервера.

Linux.Sshdkit генерирует по специальному алгоритму два DNS-имени, и если оба они ссылаются на один и тот же IP-адрес, то этот адрес преобразуется в другой IP, на который троянец и передает похищенную информацию. Используемый данной вредоносной программой алгоритм генерации адреса командного сервера показан на иллюстрации ниже.

Специалистам компании «Доктор Веб» удалось перехватить один из управляющих серверов Linux.Sshdkit с использованием широко известного метода sinkhole — таким образом было получено практическое подтверждение того, что троянец передает на удаленные узлы похищенные с атакованных серверов логины и пароли.

Сигнатура данной угрозы добавлена в вирусные базы Dr.Web. Администраторам серверов, работающих под управлением ОС Linux, специалисты «Доктор Веб» рекомендуют проверить операционную систему. Одним из признаков заражения может служить наличие библиотеки /lib/libkeyutils* размером от 20 до 35 КБ.

Источник: http://www.chip.ua

Мировой рынок утечек информации в 2012 г. достиг 535 млн долл.

Согласно исследованию Gartner рынка систем предотвращения потери данных (Data Loss Prevention, DLP), его объем в 2012 г. составил 535 млн долл., что на более чем 100 млн долл. превышает значение предыдущего года. Постоянный рост потерь корпоративных данных заставляет усиливать контроль за их передачей и обработкой, в том числе и развертывая системы DLP. Это дает основание аналитикам ожидать, что в 2013 г. объем продаж DLP достигнет 670 млн долл.

К числу лидеров рынка аналитики Gartner относят компании Symantec, Websense, RSA, McAfee, CA Technologies и Verdasys. В группу нишевых игроков наряду с несколькими другими компаниями включена российская InfoWatch.

По данным Gartner, около 35% предприятий установили системы DLP из-за требований сетевой безопасности, 20% руководствовались необходимостью распознавания важных данных, а 45% требовалось защитить конечные точки сети.

Источник: http://www.chip.ua

Как поиграть в Angry Birds на банкомате?

На банковском форуме в Магнитогорске эксперты Positive Technologies продемонстрировали безопасность банкоматов.

В ходе подготовки к банковскому форуму в Магнитогорске команда экспертов Positive Technologies подготовила три короткометражных фильма, посвященных безопасности банкоматов.

Первый из них демонстрирует атаку типа «Jailbreak». Суть атаки заключается в том, что при некорректных настройках ОС или имеющихся уязвимостях в ПО банкоматов возможно возникновение ситуации, в которой длительное нажатие на сенсорный экран (имитация нажатия правой кнопки мыши) приводит к появлению контекстного меню, с помощью которого возможно получить доступ к командам ОС и файловой системе.

В следующем видео «злоумышленник» не только извлек из терминала PAN и срок действия пластиковых карточек предыдущих пользователей банкомата, но и запустил на нем игру Angry Birds.

И в последнем видеоролике - жизненная ситуация, когда мы не уделяем должного внимания уничтожению «продуктов жизнедеятельности» (не забираем и не уничтожаем чеки), разумеется в сочетании с нарушениями требований стандартов безопасности АТМ.

Отметим, что безопасность удаленных банковских терминалов является одной из главных проблем, над которой работают специалисты по ИБ и сотрудники правоохранительных органов. Так, на прошлой неделе правительство США предъявило обвинение по отношению к двум мошенникам, которые похищали информацию о счетах клиентов банков. Мошенники использовали технологию копирования информации с банковских карточек, благодаря которой им удавалось зафиксировать данные порядка 6000 жертв.

Источник: http://www.securitylab.ru

Google попал под «Статью 29»

Евросоюз грозит корпорации Google репрессиями за проблемы с конфиденциальностью пользователей. Компания игнорирует требования контрольных органов и не отвечает на претензии, утверждают защитники персональных данных. Меры будут приняты до лета 2013 года. Аналогичное расследование начинается и в отношении Facebook.

Европейские службы контроля в информационной сфере намерены скоординировать действия в отношении корпорации Google, говорится на сайте Национальной комиссии Франци и по информатике и гражданским свободам (Commission nationale de l'informatique et des libertés, CNIL). «Европейские регуляторы в сфере персональных данных отмечают, что Google не предоставил точных ответов на наши вопросы», — сказано в сообщении. Регуляторы предлагают создать рабочую группу во главе с CNIL, чтобы скоординировать претензии и ответные меры,«которые должны быть приняты до лета».

Этот план действий был разработан на встрече в Париже в конце января 2013 года и должен быть принят на пленарном заседании рабочей группы «Статья 29» (независимый орган по защите персональных данных, в который входят представители каждой из 27 стран Евросоюза и Еврокомиссии, названный по номеру статьи из Директивы по защите данных) 26 февраля.

Претензии регуляторов вызвали правила Google, введенные около года назад. Тогда корпорация начала собирать данные о пользователях практически со всех своих сервисов, включая почту Gmail, видеосервис YouTube и социальную сеть Google+, и объединять их, чтобы «портрет пользователя был более полным».

В итоге политика приватности для 60 отдельных ресурсов, принадлежащих Google, была объединена в единые для всех сервисов правила. Интегрированная персональная информация, по словам представителей Google, используется, чтобы развивать существующие службы и создавать новые, а также «обеспечивать безопасность Google и пользователей».

Отраслевые эксперты сразу отметили, что такие изменения могут обеспокоить пользователей, которые в течение долгого времени не подозревали, что информация о них может использоваться таким количеством веб-сервисов. Еще до того как новые правила вступили в силу, в феврале 2012 года, регуляторы начали изучать их. Расследование CNIL стартовало 16 марта. 16 октября регуляторы объявили, что новые правила не соответствуют европейскому законодательству о защите данных, и предписали скорректировать их.

«По истечении четырехмесячного срока, предоставленного Google для приведения правил в соответствие с европейским законодательством и выполнения рекомендаций группы, никакого ответа не последовало», — пишет CNIL.

Руководители других европейских комиссий по конфиденциальности персональных данных заявляют, что намерены на примере Google «преподать урок другим». В частности, начинается расследование в отношении Facebook.

Единая рабочая группа, по словам представителя CNIL, — оптимальный вариант для работы в этом направлении. «Мы лучше вооружены когда выступаем

единым фронтом, чем когда каждая страна предпринимает собственные усилия», — заявила глава CNIL Изабель Фальк-Пьерротен, которую процитировал The Wall Street Journal. Она считает, что уточнять, какую именно форму примут репрессии, пока рано, но подчеркнула, что заявление отражает намерение CNIL и других регуляторов пойти на решительные меры.

Штраф за нарушение норм защиты информации во Франции достигает 300 000 евро при повторных нарушениях.

CNIL уже штрафовала Google на 100 тыс. евро в марте 2011 года за незаконный сбор персональных данных автомобилями компании, которые фотографировали улицы крупных городов для сервиса Street View, собирали данные о сетях Wi-Fi, а также через незащищенные сети скачивали персональные данные пользователей.

Сама корпорация придерживается иного мнения. Представитель Google заявил, что политика компании соответствует европейскому законодательству. «Мы оказывали полное содействие CNIL в период расследования и продолжим это делать», — цитирует пресс-секретаря Google WSJ. В начале января компания направила CNIL письмо, где перечислила свои шаги в ответ на октябрьские предписания регулятора, и просила о встрече для личного обсуждения деталей. Но, по словам главы CNIL, письмо не содержало конкретики.

Источник: http://www.gazeta.ru

Мошенники воруют деньги через PoS-терминалы.

Злоумышленники атакуют не только огромные международные корпорации, но и небольшие локализованные компании. Эксперты компании **Sophos** зафиксировали участившееся количество хакерских атак, в которых злоумышленники используют **PoS-терминалы**. По их данным, в последние 15 месяцев вирусописатели разработали несколько дополнительных схем мошенничества, используя некоторые версии троянских программ, которые позволяют извлекать данные напрямую, а не сбрасывать их на диск.- Кроме того, хакеры внесли несколько незначительных изменений в проведение атак. Так, появился новый генератор случайных имен файлов, а, в случае с жестко прописанными именами, вирус сможет их скрывать.

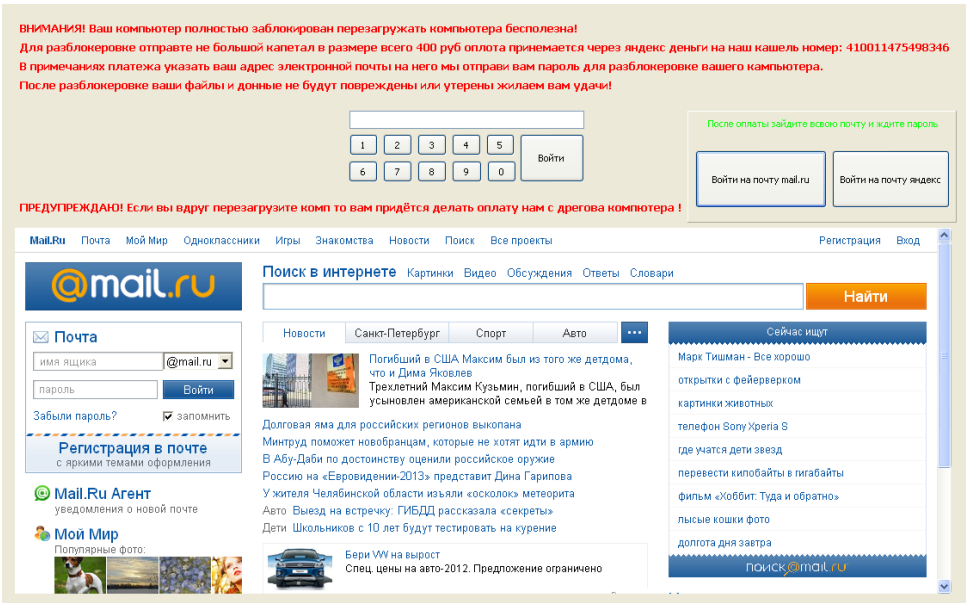
При дополнительном исследовании PoS-терминалов, являющихся целью мошенников, эксперты установили, что злоумышленники изменили вектор нападения, и вместо крупных международных корпораций чаще атакуют небольшие компании.

По мнению исследователей, в последнее время у пользователей легко может сложиться впечатление, что нападениям подвержены только крупные корпорации, однако хакеры чаще используют принцип «легче похитить по $75 у миллиона человек, чем $75 млн у мегакорпорации».

Источник: http://www.securitylab.ru

Новый винлокер насмешил специалистов.

Троянцы-блокировщики семейства Trojan.Winlock демонстрируют своим жертвам требования об оплате на разных языках: например, в феврале 2012 года специалистами компании «Доктор Веб» была обнаружена вредоносная программа Trojan.Winlock.5490, угрожающая шариатским судом арабским пользователям, незадолго до этого в вирусные базы были добавлены винлоки на французском, немецком и итальянском языках. Однако вредоносная программа, получившая обозначение Trojan.Winlock.8026, озадачила вирусных аналитиков «Доктор Веб» прежде всего тем, что они так и не смогли определить, на каком языке написано отображаемое на экране заблокированного компьютера сообщение:



Троянец представляет собой примитивную форму, созданную с использованием среды разработки Delphi, код которой содержит не меньше нелепых ошибок, чем демонстрируемый на экране текст. Форма разработана с помощью стандартного конструктора Delphi, ничем не упакована, исполняемый файл вредоносной программы занимает более 7 Мб, а все ресурсы (включая код разблокировки) хранятся в приложении в открытом виде. По всей видимости, коварный злоумышленник создавал эту грозную вредоносную программу второпях, пока родители не вернулись с работы и не заставили его делать домашнее задание по русскому языку. В качестве альтернативы можно предположить, что перед нами проявление итогов либерализации российского законодательства в области миграционной политики, благодаря которому трудовые мигранты из ближнего зарубежья, пока еще не в достаточной степени владеющие русским языком, постепенно осваивают все новые и новые специальности.

Сигнатура Trojan.Winlock.8026 успешно добавлена в вирусные базы, и потому троянец не представляет опасности для пользователей антивирусного ПО Dr.Web. Впрочем, он не представляет серьезной опасности и сам по себе: если по ошибке или в силу роковой случайности вы запустили данную вредоносную программу на своем компьютере, то, хорошенько от-

смеявшись, воспользуйтесь кодом 141989081989 для его разблокировки.

Источник: http://news.drweb.com

McAfee предлагает унифицированную систему управления ИБ.

Компания McAfee объявляет о выпуске нового программного обеспечения McAfee Real Time for ePolicy Orchestrator —системе управления безопасностью, позволяющей предприятиям мгновенно находить информацию о любом компьютере, развертывать продукты или обновлять конфигурации за считанные секунды.

Кроме того, теперь решение McAfee Enterprise Security Manager имеет активное подключение к платформе McAfee ePolicy Orchestrator (McAfee ePO), решению McAfee Vulnerability Manager и платформе McAfee Network Security Platform, что позволяет автоматически изменять политики безопасности конечных точек и сети благодаря мощному механизму сопоставления, используемому в данном решении. В совокупности эти решения устанавливают новый отраслевой стандарт для времени реагирования, ситуативной осведомленности и операционной эффективности.

«Мы стремимся постоянно совершенствовать наши средства защиты», — рассказывает Бен Шекелфорд (Ben Shackelford), управляющий по информационной безопасности компании Cobham North America. — Подход Security Connected компании McAfee позволяет интегрировать разрозненные продукты и улучшает управление. Мы с удовольствием используем преимущества новейших разработок в этой области, которые позволяют совершенствовать сбор информации об угрозах и сократить время реагирования. При управлении операциями защиты и системой мониторинга мы полагаемся на такие решения, как McAfee ePolicy Orchestrator и McAfee Enterprise Security Manager, а теперь и на Real Time for ePO. Активная интеграция этих решений с системой SIEM позволяет нам еще лучше выполнять нашу работу».

Решения по управлению безопасностью:

1) Решение McAfee Real Time for ePO добавляет функции расследования событий безопасности в режиме реального времени к возможностям передовой платформе управления безопасности McAfee ePolicy Orchestrator. McAfee Real Time for ePO помогает администраторам систем безопасности за считанные секунды выполнять запросы по тысячам различных активов всего предприятия, позволяя администраторам принимать решения о защите, зная о том «что происходит сейчас», а не о том «что произошло раньше». Эта революционная технология в сочетании с функцией обнаружения активов в реальном времени, предлагаемой в решении McAfee Asset Manager, заметно повышает ситуационную осведомленность, снижает подверженность угрозам, уровень риска и затраты на обеспечение безопасности. Платформа McAfee ePO представляет наиболее комплексное масштабируемое решение для управления безопасностью. Обновленная платформа оставляет далеко позади себя прочие системы управления операциями защиты, которым на сбор данных о конечных точках порой требуются часы и дни, а потом еще несколько дней, чтобы установить исправления на незащищенных системах.

2) Сегодня McAfee Enterprise Security Manager обеспечивает активную интеграцию с ПО ePolicy Orchestrator, платформой McAfee Network Security Platform и решением McAfee Vulnerability Manager. McAfee Enterprise Security Manager — единственная система SIEM, которая может быть одновременно и «умной», и «скорой», когда речь идет о сборе в режиме реального времени информации об

угрозах, необходимой для принятия точных мер. В результате выпуска новой версии система SIEM превращается из системы пассивного мониторинга в платформу автоматического реагирования на инциденты безопасности. Мощное ядро сопоставления угроз позволяет выявлять угрозы и мгновенно реагировать на них, в автоматическом режиме отправляя команды управления политиками программным продуктам McAfee и интегрированным решениям партнеров.

«Учитывая, что атаки постоянно усложняются, нашим клиентам требуются более простые, оперативные и эффективные способы управления безопасностью», — говорит Кен Левин (Ken Levine), старший вице-президент и генеральный менеджер по управлению безопасностью компании McAfee. — Благодаря выпуску обновления теперь конечные точки, сети и средства управление безопасностью объединены в тесно интегрированную, интеллектуально взаимодействующую систему. Компания McAfee — единственный поставщик решений в области информационной безопасности, способный предложить продукт, отражающий всю полноту и глубину нашего решения, в сочетании с мощью управления системой безопасности, предлагаемой программным обеспечением McAfee ePO и решением McAfee Enterprise Security Manager».

Источник: http://www.anti-malware.ru

Сформирован Совет по безопасности центров сертификации.

Крупнейшие центры сертификации, включая Symantec, Trend Micro, GlobalSign, Go Daddy, Comodo, DigiCert и Entrust, объявили о формировании Совета по безопасности центров сертификации (Certificate Authority Security Council, CASC).

Новая организация займётся изучением наиболее актуальных проблем в безопасности нынешней инфраструктуры сертификации, помощью в разработке стандартов, а также улучшением всей экосистемы за счёт образования. Заявленная миссия CASC — улучшать безопасность интернета, в том числе продвигая правильные способы использования публичных сертификатов. Организация ставит своей целью также развенчать существующие мифы:

- отсутствует система регулирования центров сертификации;
- центры сертификации не нужны;
- все выдаваемые сертификаты одинакового типа;
- центры сертификации — изолированные и закоснелые организации, которые не готовы принимать необходимые изменения в протоколе SSL;
- протокол SSL не пригоден для использования и нужно найти альтернативный метод аутентификации в онлайне;
- SSL устарел и содержит слишком много уязвимостей, чтобы полагаться на него в долговременной перспективе;
- поскольку существует более 600 центров сертификации, выдавать сертификаты SSL может практически кто угодно, так что они ничего не гарантируют;
- процедура отзыва сертификатов или не нужна, или не работает, а её преимущества не перевешивают потенциальных проблем с производительностью браузеров;
- у центров сертификации нет стимула для инноваций и осуществления необходимых изменений.

Все эти мифы новый Совет будет развенчивать в меру своих сил, распространяя обучающие материалы и программы образования пользователей.

Первой практической задачей, которой займётся Совет, будет продвижение протокола Online Certificate Status Protocol (OSCP) и стандарта Certificate Status Request для выдачи сервером статуса сертификата в процессе SSL-рукопожатия, описанного в RFC 6066, раздел 8.

Источник: http://www.xakep.ru

В России заведено 895 уголовных дел за пиратский Photoshop.

Компания Adobe Systems сообщила о результатах своей деятельности по защите авторских прав в Российской Федерации. За минувший год ее юристы инициировали открытие 895 уголовных дел.

За прошедший год в Москве и регионах по инициативе юристов Adobe было открыто 895 уголовных дел по факту использования нелицензионных продуктов компании. По информации Cybersecurity, это составило 24% от общего количества нарушений, выявленных Министерством Внутренних дел РФ в 2012 году.

Наибольшее количество судебных исков пришлось на продавцов пиратского программного обеспечения, и пользователей, которые установили взломанные продукты Adobe на свои компьютеры. Иски против конечных пользователей, под которыми подразумевались компании и предприниматели, использующие программное обеспечение для работы, составили 16% от общего количества. Дела, возбужденные против пользователей, распространявших продукцию Adobe в Сети, составили 2%.

Большинство дел были возбуждены против дизайн-студий (12%) и индивидуальных предпринимателей, работающих в области рекламы (11%). Среди новых средств защиты авторских прав, внедренных в практику Adobe Systems стоит отметить «гражданский обыск» – проведение проверки с участием судебного пристава-исполнителя и представителя правообладателя без привлечения полиции.

Источник: imena.ua

Разоблачили 38 серверов с порнографией.

38 серверов с порнографией изъяли у 22-летнего жителя Ровенской области.

Оперативники отдела по борьбе с киберпреступностью УМВД Украины в Ровенской области разоблачили 22-летнего жителя областного центра, который занимался распространением аудиовизуальных произведений порнографического характера. Об этомУНН сообщили в пресс-службе МВД.

"Молодой парень в арендованном помещении создал техническую площадку, на которой разместил веб-ресурсы с противоправным контентом. Во время проведения санкционированного обыска в помещении, правоохранители обнаружили и изъяли 38 системных блоков (серверов) на общую сумму около 160 тысяч гривен.

Пользователям сети Интернет злоумышленник предлагал порнографию, за просмотр которой они перечисляли средства на указанные счета. Таким образом молодой человек ежемесячно зарабатывал от трех до четырех тысяч условных единиц", - говорится в сообщении.

Сейчас открыто уголовное производство по ч. 2 ст. 301 "Ввоз, изготовление, сбыт и распространение порнографических предметов" Уголовного кодекса Украины. Мужчине грозит до пяти лет лишения свободы с конфискацией порнографической кино-и видеопродукции и средств ее изготовления и демонстрирования.

Сейчас прекращена деятельность 15 интернет-ресурсов, а изъятая компьютерная техника направлена для проведения экспертиз.

Источник: http://telegraf.com.ua

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.

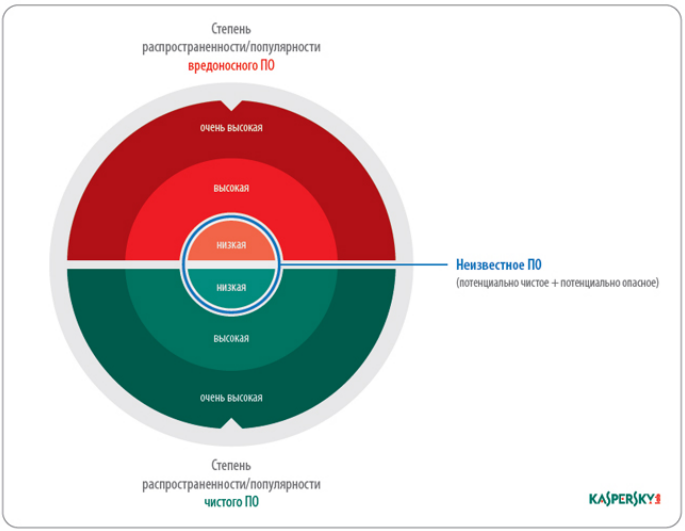
Наша статья посвящена альтернативному подходу к защите корпоративных сетей, который мы назвали Whitelist Security Approach.

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 традиционные 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.

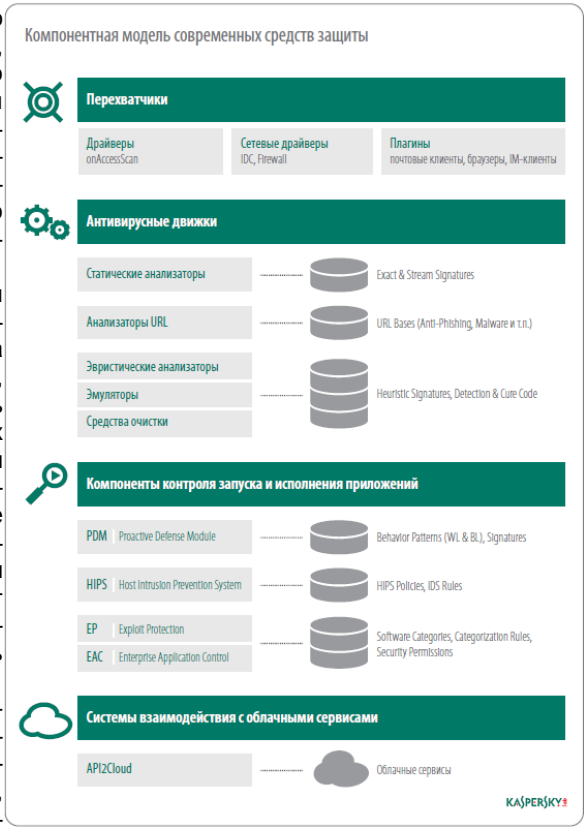
В сложившейся ситуации перед разработчиками ПО в области IT-безопасности стоит задача поиска альтернативных решений, способных существенно повысить уровень защиты корпоративных сетей. Предлагаемый в данной статье альтернативный подход – Whitelist Security Approach – не только обеспечит соответствующий 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» соот-

ветствующий 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 вы-

ходит 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

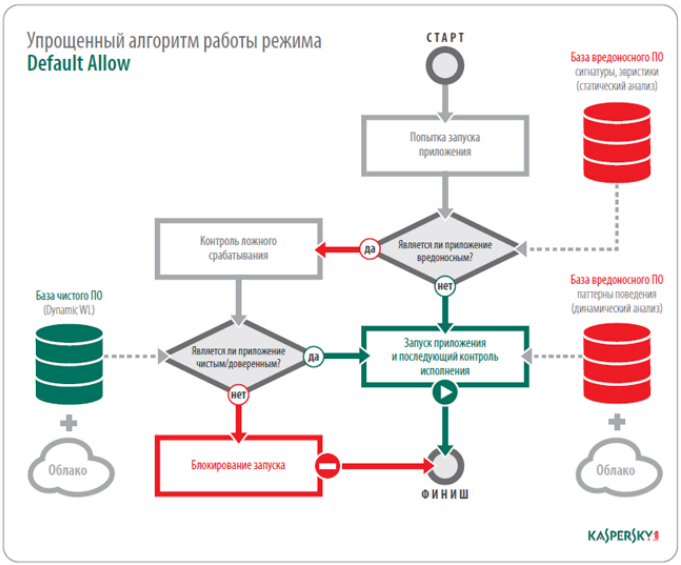
При традиционно используемом и в персональных, и в корпоративных продуктах режиме «Разрешение по умолчанию» (Default Allow) пользователь может запускать любые приложения, за исключением заблокированных или таких, на запуск которых установлены ограничения. Применение данной парадигмы обусловлено тем,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

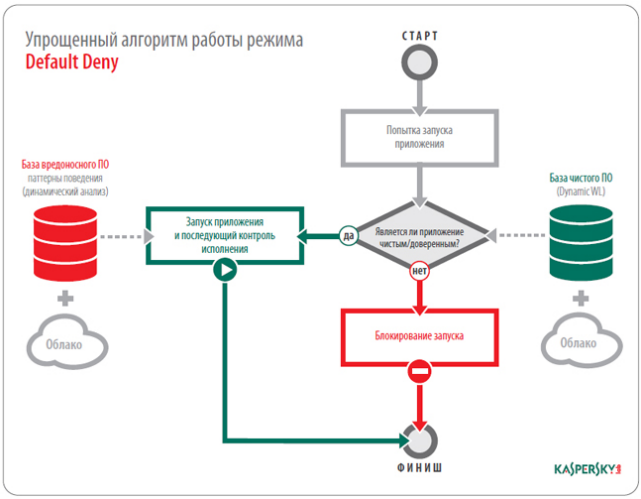
Таким образом, при максимальном удобстве для конечного пользователя режим Default Allow оставляет корпоративную сеть уязвимой для неизвестных угроз и нежелательного ПО. При этом контроль за всеми исполняемыми программами требует существенных ресурсов.

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

Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

Тут может быть Ваша информация!

Заявите о себе!

И про Вас узнают Все...

{
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.