Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

UA Linux http://ualinux.com

Троян ransomlock научился обходить песочницы автоматизированных систем анализа угроз

Читайте в этом номере:

- Обезврежена группа хакеров.

- Фокусы хакеров становятся все изощреннее.

- Киберугрозы выходят из тени.

- Программы-вымогатели начали использовать историю посещенных сайтов пользователя.

- «Мартовские троянцы» и другие угрозы прошедшего месяца.

- Атака на контакт-центр – аналог DDOS.

- Новый вредоносный троянец следит за мышкой и перехватывает данные.

- Контроль запуска программ как залог безопасности сети. Часть 2

- «Яндекс» запустил сервис для защиты от вредоносных и недетских сайтов.

И многое другое.

Эксперты информационной безопасности предупреждают о распространении новой модификации опасного вируса. Согласно сообщению экспертов по информационной безопасности из антивирусной компании Symantec, им удалось обнаружить новую модификацию трояна ransomlock. Среди обновленного функционала вредоносного приложения появилась возможность обхода песочниц, содержащихся в автоматизированных системах анализа угроз.

Symantec проводил проверку образца вредоносного файла на восьми web-сайтах, которые занимаются хостингом автоматизированных систем анализа угроз и получил следующие результаты:

•ThreatExpert зарегистрировал создание файла, изменения в реестре, а также подозрительную сетевую активность.

•Еще три портала зафиксировали появление нового процесса, однако не смогли предоставить дополнительной информации.

•Четыре оставшихся ресурса вовсе не смогли что-либо зафиксировать.

«Symantec продолжит вести мониторинг вредоносного кода и анализировать его функционал. Мы рекомендуем пользователям воздержаться от запуска подозрительных программ и регулярно обновлять свое антивирусное ПО до актуальных версий», - заявили эксперты.

Источник: http://www.securitylab.ru

And User Linux

размещение рекламы - journal@ualinux.com

Обезврежена группа хакеров.

Как стало известно "Ъ", Служба безопасности Украины совместно с Федеральной службой безопасности России пресекла деятельность группы кибермошенников, которые через системы интернет-банкинга за последние пять лет похитили более $250 млн. Хакеры при помощи вируса получали доступ к системам интернет-банкинга, после чего переводили средства компаний на счета подставных фирм. Силовики утверждают, что большую часть средств, похищенных через интернет, удается вернуть "по горячим следам". Но все же, по мнению экспертов, уровень защиты банковских платежей в стране недостаточен.

Операцию по разработке группы кибермошенников департамент контрразведывательной защиты интересов государства в сфере информационной безопасности СБУ проводил около года. "Хакеры создали вирус, который проникал в компьютеры при скачивании фотографий или просмотре видео в интернете. Он получал доступ к данным бухгалтерии, программе 1С, паролям и электронным ключам, после чего передавал их мошенникам. Вредоносная программа постоянно модифицировалась, поэтому антивирусные средства защиты ее не идентифицировали",— рассказал собеседник "Ъ" в спецслужбе. По его словам, после получения данных преступники какое-то время изучали деятельность предприятия, затем от лица компании формировали электронные платежи на счета подставных фирм. Только в Украине от их действий пострадало более 30 компаний.

На территории Украины мошенники действовали с 2009 года, а до этого работали по аналогичной схеме в РФ. Всего в Украине и России им удалось украсть более $250 млн. По данным СБУ, в группе насчитывалось около 20 человек, средний возраст которых от 25 до 30 лет. "Это были программисты, работавшие удаленно в Киеве, Запорожье, Львове, Херсоне и Одессе. Как правило, они не знали друг друга, каждый отвечал за свою часть разработки программного модуля. Потом данные передавались на главный сервер в Одессе, там же работал главный организатор — 28-летний гражданин России", — добавил собеседник "Ъ". Внимание сотрудников СБУ к группе кибермошенников привлекли многочисленные обращения в милицию от пострадавших фирм и системный характер преступлений. Операцию по задержанию хакеров СБУ организовала совместно с ФСБ России.

Сейчас СБУ проводит следственные действия и экспертизу компьютерного оборудования, изъятого у подозреваемых. "Согласно новому Уголовному процессуальному кодексу, экономические преступления не являются тяжкими, поэтому задержанные сейчас находятся под подпиской о невыезде, кто-то отпущен под залог. Если суд докажет их вину, преступникам грозит более пяти лет тюремного заключения",— отметили в СБУ.

Следует отметить, что в феврале немецкий оператор связи Deutsche Telekom опубликовал отчет о том, из каких стран в основном идут кибератаки. В этом списке Украина оказалась на четвертом месте после России, Тайваня и Германии. В отчете говорится, что ежемесячно с украинских серверов запускается более полумиллиона вредоносных программ.

Уровень киберпреступности в Украине действительно растет, подтверждают в МВД. "Это естественный процесс — ежегодно увеличивается число пользователей интернета, а значит, и количество мошенников. В 2012 году зафиксировано 139 фактов несанкционированного списания средств со счетов предприятий, совершенного путем вмешательства в работу систем удаленного обслуживания клиентов на общую сумму свыше 116 млн грн. Нам удалось вернуть 80% от этой суммы, причем значительную часть — по горячим следам, в течение двух часов с момента совершения преступления",— заявил собеседник "Ъ" в МВД.

Исполнительный директор Независимой ассоциации банков Украины (НАБУ), председатель правления Укргазбанка Сергей Мамедов заявил "Ъ", что 36%

случаев мошенничества происходит, когда человек сам дает информацию мошенникам, например, по телефону или через интернет. "В 20% случаях речь идет о потере платежной карты, в остальных — о ее подделке",— уточнил господин Мамедов. В целом, по данным Нацбанка, в 2012 году убытки от мошенничества с картами составили 0,0015% от общего объема убытков банков — около 11 млн грн.

Между тем в Интернет Ассоциации Украины (ИнАУ) считают, что банки зачастую сами экономят на способах информационной защиты. "Украина находится на четвертом месте в мире по уровню подготовки IT-специалистов, понятно, что среди них находятся и любители легкой наживы. При этом уровень защиты банковских платежей в стране недостаточен, клиентам обещают стопроцентную безопасность, но это, как правило, остается на словах,— отметил член правления ИнАУ Иван Петухов.— Банкам следует регулярно обновлять защиту платежных систем, привлекать к этому высокооплачиваемых специалистов и помнить, что хакеры по уровню подготовки на голову выше обычных системных администраторов".

Впрочем, координатор комитета НАБУ по вопросам банковской инфраструктуры и платежных систем Владимир Еременко уверен, что во взломах виноваты не только банки. "Клиент часто сам нарушает правила пользования системой дистанционного управления счетом, пользуется интернетом с компьютера, на котором установлена эта система, тогда как он вообще не должен быть в сети, а запускать его следует электронными ключами. Мошенники в основном взламывают не компьютеры, а мозги клиентов",— утверждает господин Еременко.

Источник: http://www.kommersant.ua

Фокусы хакеров становятся все изощреннее.

Фокус сложных атак сместился: ранее под угрозой была финансовая индустрия, теперь же мошенники начинают все активнее интересоваться другими важными сферами экономической деятельности. При этом в атаках используется целый ряд новых тактик и технологий, которые позволяют обойти стандарты безопасности, принятые в индустрии. Об этом говорится в отчете антивирусной компании McAfee.

Троянцы и комплексные угрозы продолжают сохранять лидерство. Сфера деятельности злоумышленников, которые применяют такие комплексные атаки, расширилась. Теперь в поле зрения мошенников попали государственные организации, производства и инфраструктура компаний, которые занимаются коммерческими транзакциями.

"Это и предприятия, и корпорации, и государственные структуры, и инфраструктура, которая их связывает, - говорит Винсент Вифер (Vincent Weafer), старший вице-президент McAfee Labs. - Мы наблюдаем зарождение нового этапа киберугроз. Создание вредоносных инструментов вместе с возможностью получения незаконной прибыли из привлекательного для мошенников финансового сектора - факторы, которые сформировали новый растущий "черный рынок". Сейчас спросом пользуется кибероружие и новые креативные подходы, которые позволяют обмануть средства безопасности в различных сферах бизнеса".

Рост в группе троянского вредоносного ПО составил 72% за квартал. Самый "лакомый кусочек" конфиденциальных данных пользователей для мошенников в данный момент - это пользовательские логины и пароли. Именно поэтому троянские программы стали весьма доступны, и в данный момент либо появляются в составе как специально разработанных комплексов, так и готовых угроз.

Ботнеты в качестве метода распространения вредоносного ПО сейчас используются реже, нежели ссылки, и эта тенденция сохраняется. Анализ веб-угроз показал, что количество новых ссылок с "подозрительным" контентом в четвертом квартале увеличилось на 70%. Количество новых ссылок такого характера составило 4,6 млн. в месяц - это почти в два раза больше, нежели 2,7 млн. в месяц в двух предыдущих кварталах. При этом ссылки в 95% случаев содержали вредоносный код, программное обеспечение или эксплойты.

В то же время количество зараженных компьютеров, находящихся под контролем бот-сетей, снизилось. Частично это связано с усилиями властей по ликвидации ботнетов, но, скорее всего, основная причина кроется в снижении популярности бот-сетей как бизнес-модели злоумышленников.

Вредоносное ПО, цель которого - загрузочный сектор диска, поставило новый квартальный рекорд: в четвертом квартале 2012 года объем таких угроз вырос на 27%.

В целом в 2012 году эксперты McAfee Labs обнаружили в 44 раза больше образцов вредоносного ПО для мобильных устройств, нежели в 2011. Это означает, что 95% всех существующих мобильных вредоносных программ появилось в прошедшем году.

Киберпреступники прикладывают больше всего усилий к тому, чтобы атаковать устройства на базе Android: только в четвертом квартале 2012 года количество нового вредоносного ПО для этой платформы выросло на 85%. Привлекательность мобильных угроз для злоумышленников кроется в ценности информации, которую можно найти на устройствах пользователей - пароли, адресные книги и многое другое. Кроме того, мобильные платформы открывают новые, недоступные на традиционных компьютерах возможности для "бизнеса" злоумышленников. К таковым относятся, например, троянцы, которые отправляют SMS-сообщения на платные номера без ведома пользователя.

Источник: http://www.finobzor.com.ua

Программы-вымогатели начали использовать историю посещенных сайтов пользователя.

О новом варианте вымогательской программы под названием Kovter рассказал на днях автор блога Malware don't need Coffee. От прочего кода такого класса Kovter отличается тем, что для большей убедительности изучает историю посещения веб-сайтов и использует полученную информацию в составлении сообщения для жертвы.

Как и многие другие подобные программы, Kovter блокирует работу компьютера и демонстрирует пользователю сообщение, якобы исходящее от министерств юстиции и национальной безопасности США, а также ФБР, с заявлением о том, что данный компьютер уличен в скачивании незаконных материалов и что разблокировать его можно, выслав определенную сумму по приведенному адресу.

При этом Kovter проверяет, нет ли в журнале браузера записей о посещении сайтов из заданного списка порнографических сайтов (далеко не все из которых являются незаконными) и, если они найдены, включает их в сообщение. Если же записи не найдены, Kovter выбирает случайный сайт из списка.

За первые месяцы 2013 года число заражений вымогательскими программами успело удвоиться, пишет эксперт «Лаборатории Касперского». В феврале и марте оно достигло рекордного уровня.

Источник: http://cripo.com.ua

Киберугрозы выходят из тени.

Специалистами Cisco развеян популярный миф, согласно которому угрозы возникают главным образом тогда, когда пользователь занимается в сети не вполне приличными делами. А также выявлены необычные интернет-привычки поколения «игрек».

Согласно результатам Ежегодного отчета Cisco по информационной безопасности (Cisco 2013 Annual Security Report, ASR) и глобального исследования Cisco Connected World Technology Report (CCWTR), информационная безопасность компаний становится уязвимой из-за того, что сотрудники стремятся к повсеместному использованию мобильных устройств, а граница между работой и личной жизнью все более размывается.

Исследование Cisco в области информационной безопасности развеяло популярный миф, согласно которому угрозы возникают главным образом тогда, когда пользователь занимается в сети не вполне приличными делами. Сегодня сетевые злоумышленники фокусируют внимание не столько на порнографических, фармацевтических и игровых сайтах, сколько на

обычных сетевых ресурсах с массовой аудиторией, таких как популярные поисковые механизмы, розничные магазины и социальные сети. Более того, отчет Cisco показал, что вредоносный контент можно «подцепить» на сайтах интернет-магазинов в 21 раз чаще, а в поисковых механизмах – в 27 раз чаще, чем на сайтах, специально созданных хакерами. Так, вероятность загрузки вредоносного контента при просмотре онлайн-рекламы в 182 раза выше, чем на порнографических сайтах, передает soft.mail.ru.

Информационная безопасность бизнеса попадает под угрозу во многом потому, что сотрудники предпочитают работать в привычной для себя манере, повсеместно используя одни и те же устройства и приемы – в офисе, дома, по дороге на работу и домой. Угрозы, создаваемые этой тенденцией, получившей название «консьюмеризация», усугубляются еще одним трендом, раскрытым в отчете Cisco Connected World Technology Report, где говорится о поведении сотрудников поколения «игрек». Большинство (91%) из них считают, что эпоха повышенного внимания к вопросам конфиденциальности личных данных безвозвратно ушла в прошлое. Треть поколения «игрек» вообще не задумывается о том, где и как хранится их персональная информация. Эти люди охотно сообщают личные данные, чтобы получить доступ в социальные сети. Более того, все больше специалистов из поколения «игрек» из разных стран предоставляют свои данные сайтам интернет-магазинов с большей готовностью, чем IT-отделам компании-работодателя, отвечающим за сохранность и защиту личных данных и устройств.

Окончив колледж и получив работу, представители поколения «игрек» испытывают на прочность корпоративную культуру и политику компании в области безопасности, требуя от работодателя свободы использования социальных сетей, личных устройств и методов мобильной работы. Предыдущие поколения никогда не выдвигали подобных требований. С утра, не вылезая из постели, большинство молодых людей поколения «игрек» заходят в социальные сети, работают с электронной почтой и текстовыми сообщениями (так поступают трое из четырех опрошенных во всех странах, где проводилось исследование). Почти половина респондентов выполняет похожие задачи за обеденным столом, треть – в ванной и одна пятая – за рулем автомобиля. Этот стиль жизни все шире распространяется в корпоративной среде, определяя будущее рабочей среды и новые параметры поиска талантливых сотрудников. К сожалению, исследование показало, что интернет-привычки нового поколения сотрудников создают серьезные угрозы безопасности, с которыми компании никогда раньше не сталкивались.

Основные выводы исследований

Вредоносные программы для ОС Android

•В 2012 году число заражений вредоносными программами для операционной системы Android выросло на 2 577% (ASR).

•При этом доля мобильных вредоносных кодов составляет всего 0,5% от общего объема вредоносных кодов в Интернете (ASR).

•Эти тенденции приобретают особое значение ввиду того, что для поколения «игрек» смартфоны стали самым популярным устройством, использующимся чаще, чем ноутбуки, персональные и планшетные компьютеры (CCWTR).

Распространение вредоносных интернет-кодов в разных странах

В 2012 году географический ландшафт интернет-угроз претерпел значительные изменения. В 2011 году Китай занимал второе место в списке стран, наиболее пораженных вредоносными кодами. В 2012 году Китай опустился на шестое место. Скандинавские страны (Дания и Швеция), наоборот, поднялись в этом списке на третью и четвертую позицию соответственно. Первую строчку в списке по-прежнему занимают Соединенные Штаты.

1.США 33,14%
2.Российская Федерация 9,79%
3.Дания 9,55%
4.Швеция 9,27%
5.Германия 6,11%
6.Китай 5,65%
7.Великобритания 4,07%

8.Турция 2,63%
9.Нидерланды 2,27%
10.Ирландия 1,95%

Тенденции в области спама

•За период с 2010 по 2011 год объем спама уменьшился на 18%. При этом спамеры стали переходить на «стандартную рабочую неделю» (объем спама в выходные дни сократился на 25%) (ASR).

•В 2012 году большинство спам-сообщений передавалось в рабочие дни. Самым «активным» днем с точки зрения спама, стал вторник (ASR).

•Главным мировым источником спама является Индия. В 2011 году США заняли в этом списке шестое место, а в 2012 году – второе. Третье, четвертое и пятое места заняли, соответственно, Корея, Китай и Вьетнам (ASR).

•Главные цели спамеров, на сегодняшний день, – это реклама фармацевтических средств, таких как Виагра и Cialis, и наиболее фешенебельных марок наручных часов (Rolex и Omega) (ASR).

Защита личной информации

•Хотя большинство опрошенных представителей поколения «игрек» (75%) не доверяет веб-сайтам и не считает их надежными хранилищами личной информации, такой как номера кредитных карт и личные контактные данные, недоверие не накладывает никаких ограничений на действия этих пользователей. Они готовы идти и идут на риск, надеясь на «авось» и используя при этом рабочие устройства, подключенные к корпоративной сети, что создает большие проблемы для компаний-работодателей (CCWTR).

•57% представителей поколения «игрек» не возражают против использования их личной информации розничными магазинами, социальными сетями и другими онлайновыми ресурсами, если это приносит какую-то выгоду или удобство (CCWTR).

Выполнение корпоративных IT-правил

•Девять из десяти (90%) опрошенных IT-специалистов указали, что в их компаниях имеются официальные правила использования на работе тех или иных устройств, однако лишь двое из пяти представителей поколения «игрек» знают об этих правилах (CCWTR).

•Хуже того, четверо из пяти сотрудников из поколения «игрек», знающих о корпоративных правилах, не придерживаются этих правил в своей повседневной работе (CCWTR).

•IT-специалисты знают, что многие сотрудники не выполняют правил, но не представляют себе масштаба бедствия. Более половины (52%) IT-специалистов в разных странах считают, что в общем и целом правила безопасности все-таки выполняются. При этом трое из четырех (71%) сотрудников из поколения «игрек» правил не выполняет (CCWTR).

•Двое из троих (66%) опрошенных из поколения «игрек» во всех странах заявили, что IT-специалисты не имеют права следить за их поведением в сети, даже если это поведение связано с использованием корпоративных устройств в корпоративных сетях (CCWTR).

•Неприятие мониторинга сетевого поведения со стороны корпоративного IT-отдела оказалось намного выше, чем неприятие такого же мониторинга со стороны розничных магазинов. Другими словами, поколение «игрек» гораздо спокойнее относится к отслеживанию работы в сети со стороны совершенно незнакомых лиц (сотрудников розничных магазинов), чем со стороны IT-специалистов компании-работодателя, то есть тех, кто по долгу службы обязан защищать сотрудников и корпоративную информацию (CCWTR).

В третьем ежегодном отчете Cisco Connected World Technology Report публикуются результаты исследования, проведенного независимой аналитической компанией InsightExpress из США. В ходе исследования опрашивались две группы респондентов. Одна состояла из студентов колледжей и молодых сотрудников в возрасте от 18 до 30 лет. Во вторую группу входили IT-специалисты, работающие в разных отраслях и разных странах. Всего было опрошено 3 600 респондентов (по 100 респондентов из 18 стран для каждой из двух групп). Исследование проводилось в 18 странах: США, Канаде, Мексике, Бразилии, Аргентине, Великобритании, Франции, Германии, Нидерландах, России, Польше, Турции, ЮАР, Индии, Китае, Японии, Южное Корее и Австралии.

Источник: http://www.anti-malware.ru

ИТ-эволюция приводит к ИБ-революции.

Известный блогер, бизнес-консультант по безопасности компании Cisco Systems Алексей Лукацкий назвал основные тенденции, которые сопровождают эволюцию цифровых устройств и напрямую влияют на деятельность служб информационной безопасности.

В частности, первая тенденция заключается в постепенном замещении используемых корпоративных информационных технологий на их потребительские «аналоги» и активном проникновении последних на ранее закрытый для них корпоративный рынок. Речь идет о стирании границы между двумя ранее независимыми направлениями – рынков корпоративных и потребительских технологий.

Алексей Лукаций приводит несколько примеров проникновения потребителей в корпорации. В частности, сотрудники не желают использовать выданную им на работе оргтехнику (лэптопы, смартфоны и т. п.) по 4–5 лет и диктуют это своему предприятию. В результате жизненный цикл основных ИТ снижается, что уменьшает и жизненный цикл средств защиты.

Вопрос замены рабочих инструментов на привычные касается и замены технологий: таким образом, концепция BYOD («Bring Your Own Device» – «принеси свое устройство») трансформируется в BYOT, то есть «принеси свою технологию» («Bring Your Own Technology»), когда пользователь начинает приносить свои приложения, делающие работу удобней и эффективней. Это ведет к тому, что становится невозможной стандартизация ПО, а также к усложнению работы специалистов по ИБ.

Как следствие, возникают дополнительные риски ИБ, связанные с размыванием границы между личным и корпоративным не только в устройствах или технологиях, но и в действиях, которые пользователи осуществляют в рабочее время с личных устройств или с корпоративных устройств в нерабочее время. В том числе это касается и использования социальных сетей для целей корпоративного маркетинга, привлечения новых клиентов, получения обратной связи от потребителя, формирования community и т.д. В этих условиях службам ИБ приходится отходить от концепции «замкнутой среды» и придумывать что-то более гибкое.

Вторая тенденция – смещение взаимодействия от модели «человек – машина» в сторону модели «машина – машина» (M2M). Обе эти тенденции имеют важнейшее значение особенно с точки зрения информационной безопасности, которая пока не видит происходящих изменений. И то, что в ИТ является эволюцией, в ИБ может стать проблемой № 1 внезапно, приведя к революции. К революции в сознании, в технологиях, в подходах.

Источник: http://www.allcio.ru

Атака на контакт-центр – аналог DDOS.

Пока что рассадником атак на центры телефонного обслуживания остается США, но, как обычно, из Штатов любые тенденции рано или поздно распространяются на Европу и на Россию. Тем временем в Америке многие контакт-центры испытывают TDoS атаки, при которых на номера операторов поступает множество звонков от лиц неопределенной национальности, говорящих с очень сильным акцентом, причем говорящих непонятно что. Даже после детального анализа специалистам не удалось определить, о принадлежности к какой стране говорит данный акцент, так что можно задуматься о специальном искажении голоса.

ФБР и другие службы предупреждают контакт-центры о возможности подобны провокаций, которые могут быть связаны с коммерческими или террористическими целями. Учитывая неткость речи обращающихся, подобный «обзвон» может быть запущен в автоматическом режиме по

UA Linux
open source ■ open future
Эксперт в области безопасности.

нескольким предварительно созданным записям речи – с фразами, паузами и прочими эффектами, характерными для разговора.

Суть такой атаки очень проста – перегружая линии, она делает невозможным дозвон для тех пользователей, которые действительно хотят обратиться в контакт центр. А это чревато потерей имиджа для коммерческих компаний, а также невозможностью оказания услуг для государственных организаций.

Источник: http://www.dlp-expert.ru

Усиленная защита онлайн-платежей и дополнительные облачные функции от ЛК.

«Лаборатория Касперского» объявляет о выпуске обновленной версии продукта для домашних пользователей с максимальным уровнем защиты от информационных угроз – Kaspersky CRYSTAL. В этом году решение дополнено усиленной защитой электронных платежей, а также облачным «Менеджером паролей» и резервным копированием данных в онлайн-хранилище.

Кроме того, Kaspersky CRYSTAL предоставляет широкие возможности по шифрованию данных, централизованному управлению всеми компьютерами в доме с одного ПК, а также настройке функций «Родительского контроля». К выходу продукта «Лаборатория Касперского» запускает специальную акцию, которая дает шанс любому пользователю этого решения поболеть с трибун на гонке в Италии за легендарную команду Ferrari.

Согласно исследованию «Лаборатории Касперского»*, 53% российских пользователей совершают покупки в Интернете. При этом данные огромного количества банковских карт могут с легкостью стать добычей киберпреступников. По итогам прошедшего года облачная система мониторинга угроз Kaspersky Security Network (KSN) задетектировала, что около 70% всех фишинговых писем завлекают пользователей на вредоносные сайты, хитроумно имитирующие легитимные ресурсы. Также по данным KSN, каждый день взламывается более 5000 вебсайтов, среди которых сайты популярных интернет-магазинов и систем онлайн-банкинга. Kaspersky CRYSTAL специально создан для тех, кто ценит свои данные.

В решении Kaspersky CRYSTAL реализован самый полный набор защитных функций среди продуктов «Лаборатории Касперского» для домашних пользователей. Одна из уникальных функций продукта – создание и хранение разнообразных, устойчивых к взлому паролей. В среднем у каждого интернет-пользователя есть по пять учетных записей, которые защищены комбинациями из различных сочетаний букв и символов. Помнить их – достаточно непростая задача. В обновленной версии модуль «Менеджер паролей» дает возможность держать все учетные записи в едином защищенном облачном хранилище, доступ к которому возможен с любого ПК с установленным Kaspersky CRYSTAL.

Поскольку на компьютерах пользователей хранится множество важных документов, фотографий и других ценных данных, важно учитывать возможность физической потери, повреждения или кражи персональных компьютеров. Для таких случаев в Kaspersky CRYSTAL предусмотрен еще один уникальный инструмент - автоматическое резервное копирование и восстановление данных. В новой версии впервые появилась возможность хранить резервные копии не только на жестком диске, съемном носителе или FTP-сервере, но и с помощью популярного сервиса Dropbox. При этом пользователи могут получить доступ к резервным копиям своих файлов с любого компьютера, подключенного к Интернету.

Особое внимание в обновленном решении уделено защите личных данных пользователя при совершении любых банковских операций онлайн. Поэтому в новый Kaspersky CRYSTAL интегрирован специальный модуль «Безопасные платежи», который проверяет подлинность всех веб-сайтов при совершении онлайн-транзакций. Это позволяет защитить пользователей от ввода личных данных на поддельных ресурсах. Для еще более высокого уровня безопасности в этот модуль включена функция «Защита данных при вводе с аппаратной клавиатуры», что

позволяет исключить перехват личных данных клавиатурными шпионами при вводе с обычной клавиатуры. Новый Kaspersky CRYSTAL также дополнен «Автоматической защитой от эксплойтов». Такая технология предотвращает и блокирует атаки с использованием уязвимостей в популярных программах, таких как Adobe Acrobat, Java и др.

В Kaspersky CRYSTAL традиционно доступны другие функции для тех, кому необходима расширенная защита. «Централизованное управление безопасностью домашней Сети» и средства очистки компьютера пригодятся пользователям, которые привыкли держать под контролем все до мелочей. Кроме того, благодаря возможностям «Родительского контроля» пользователи могут быть уверены в полной безопасности своих чад в Сети. Например, взрослые могут заблокировать доступ к нежелательным вебсайтам, установить ограничения на использование Интернета по времени или исключить возможность передачи какой-либо конфиденциальной информации через социальные сети.

Источник: http://www.anti-malware.ru

Спамеры используют Google Translate для обхода антиспамовых фильтров.

Спамеры и борцы с ними продолжают игры в высокотехнологичные кошки-мышки. На сей раз компания Barracuda Networks, производитель систем фильтрации интернет-трафика, сообщила о новом спамерском приеме, направленном на введение антиспамовых фильтров в заблуждение и пропуск рекламных сообщений в ящики пользователей.

В Barracuda говорят, что компания зафиксировала волну спама, в котором для маскировки рекламных сообщений отправители используют систему Google Translate, полагаясь на ее репутацию для различных генераторов черных списков и антиспам-фильтров, передает cybersecurity.ru.

Спамеры здесь рассылают сообщения, в которых гиперссылки маскируются при помощи переводчика Google Translate, переадресовывающего потенциальных получателей на целевой сайт с объявлением через собственный встроенный обработчик и для большинства веб-фильтров сообщение выглядит, как контент от непосредственно Google Translate.

Помимо этого, Barracuda сообщает, что ее инженеры зафиксировали примеры спама, в котором рекламщики применяли URL-маскировщик компании Yahoo - y.ahoo.it. До недавнего времени подобный прием для рассылки спама на y.ahoo.it не использовался.

Также в компании говорят, что сейчас регистрируют попытки рассылки рекламных псевдо-сообщений, где мошенники маскируют через Google Translate гиперссылки на вредоносное ПО, которое в конечном итоге предлагается пользователю через сеть редиректов. "Ранее в Google велись разработки, направленные на то, чтобы блокировать прием Frame Busting, однако они либо были свернуты, либо реализованы не полностью, чем и пользуются злоумышленники", - говорит Шон Андерсон из Barracuda Networks.

Источник: http://www.anti-malware.ru

Компания UALinux представляет новый продукт - Ubuntu BussinesPack!

Ubuntu BussinesPack это:

✓ простая установка операционной системы не требующая особых знаний;

✓ уверенность в том, что на компьютере установлено только лицензионное программное обеспечение;

✓ это низкая цена по сравнению с аналогами

✓ создание рабочего места без дополнительных финансовых затрат. Это существенно экономит бюджет организаций.

✓ идеальное решение для перехода на Linux с Windows, если вы все еще используете windows-приложения и игры;

✓ полная поддержка в системе русского, украинского и английского языков;

✓ отсутствие необходимости затрат на антивирусную защиту.

UA Linux
open source ■ open future

Эксперт в области безопасности.

Новый вредоносный троянец следит за мышкой и перехватывает данные.

Поставщик решений для обеспечения ИТ-безопасности FireEye сообщил об обнаружении нового вредоносного кода, использующего различные методы для перехвата данных, вводимых пользователем на зараженном компьютере. Вредоносный код может перехватывать не только нажатия клавиш, но и отслеживает действия мыши и применяет иные способы получения сведений о том, что именно делает пользователь за компьютером.

Код Trojan.APT.BaneChat распространяется через специально сконструированный документ Word и доставляется пользователям посредством мошеннических электронных писем. В большинстве случаев имя зараженного документа, рассылаемого по почте, - Islamic Jihad.doc. "Мы подозреваем, что вредоносный документ был первично использован для атаки правительственных режимов стран Центральной Азии и Ближнего Востока", - говорит ИТ-эксперт FireEye Чонг Рон Ва.

Атака работает в несколько шагов: злонамеренный документ скачивается и открывается на целевом компьютере, далее в код запускается анализатор, который определяет, не является ли операционная система виртуализованной, не запущен ли Word в "песочнице" (изолированной среде) и нет ли на ПК автоматизированной системы детектирования вредоносов. Если эти условия выполняются, запускается вторая стадия атаки: запускается система слежения за курсором мыши, способная перехватывать данные о кликах и положении курсора. BaneChat пропускает первые три клика, после чего пытается подгрузить новое вредоносное ПО на компьютер, которое уже замаскировано под JPG-файл.

Сам по себе вредонос использует несколько методов ухода от антивирусов. К примеру, во время первой стадии атаки код пытается сбросить на компьютер дроппер, путь к которому зашифрован через сервис анонимизации URL ow.ly. Использование URL-анонимайзера нужно, чтобы путь к дропперу не попал в черные списки систем фильтрации и позволяет загрузить вредоносный код в сеть. Аналогично этому, вредоносный код JPG грузится с сервера с динамической системой IP-адресов.

В системе код также пытается ввести пользователя в заблуждение, создавая для своих нужд файлы GoogleUpdate.exe в папке C:\ProgramData\Google2\, а чтобы запускаться при старте системы код размещает свои ярлыки в Автозапуске. Напомним, что легальные файлы программ Google расположены по адресу C:\Program Files\Google\Update\.

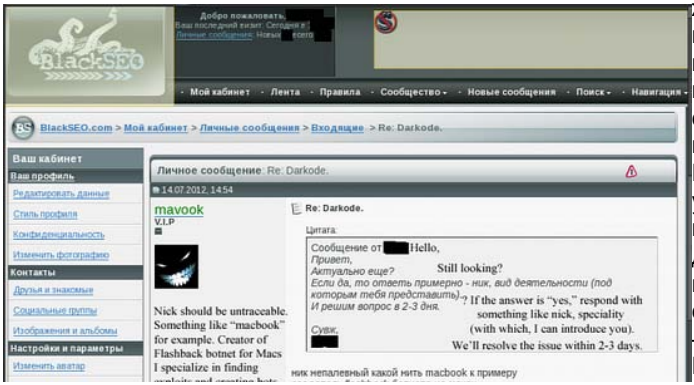
Все собираемые данные вредоносный код передает на удаленный контрольный сервер, находящийся под контролем злоумышленников. Кроме всего прочего, у BaneChat есть поддержка нескольких команд для выполнения нестандартных действий.

Источник: http://www.cybersecurity.ru

Эксперт установил личность предполагаемого создателя трояна Flashback.

Эксперт в области ИБ Брайан Кребс (Brian Krebs) заявляет, что ему удалось установить личность предполагаемого создателя трояна Flashback. Использовав данный вредонос, злоумышленники создали бот-сеть из более чем 600000 Маков. Личность автора вредоносной программы оставалась неизвестной. Однако данные, полученные Брайаном Кребсом, возможно, помогут разрешить эту загадку.По словам Кребса, один из пользователей популярного закрытого форума BlackSEO.com, под ником Mavook, заявил, что является создателем бот-сети из более чем 600000 Маков, обнаруженной специалистами компании Dr.Web в июле 2012 года.

Признание прозвучало в процессе общения с одним из старожилов форума, которого Mavook убеждал выдать ему приглашение на Darkode.com, другой сайт, также популярный среди киберпреступников.



Проанализировав активность Mavook, Брайан Кребс выяснил, что под этим ником может скрываться Максим Дмитриевич Селиханович, 30-летний россиянин из Саранска, Республика Мордовия.

При этом Кребс не исключает, что Mavook мог просто хвастать перед более уважаемым участником форума, желая поднять себе репутацию.

Источник: http://www.anti-malware.ru

Энергетические компании стали главными целями хакеров.

Министерство национальной безопасности США недавно выпустило отчет ISC-CERT Monitor, в котором подробно рассказывается об основных целях киберпреступников, которые интересуют их на территории Соединенных Штатов. Самое интересное в этом документе заключается в том, что в зоне потенциального риска значится 11 компаний из энергетического сектора.

Чтобы осуществлять атаки на отдельных людей, связанных с энергетическим сектором нападающие использовали информацию, которая доступна на сайтах компаний. Они использовали имена сотрудников, их email-адреса и названия должностей при оформлении писем, чтобы послания казались максимально аутентичными и легитимными.

«Вредоносные электронные письма сообщали получателям о том, что у отправителя появился новый адрес. Их также просили нажать на предлагаемую ссылку, которая отправляла их на сайт, хранящий в себе вредоносное программное обеспечение. Кроме того, иногда злоумышленники присоединяли к письмам опасные дополнения, которые при открытии атаковали систему пользователя», – говорится в отчете DHS.

Министерство национальной безопасности предупреждает, что доступная в широком доступе информация, которая публикуется на официальных сайтах компаний и социальных сетях, может быть использована киберпреступниками для достижения зловещих целей.

Чиновними советуют организациям ограничить доступ к деловой информации, которая выкладывается на их сайты. Кроме того, самим пользователям стоит быть чрезвычайно острожными в разглашении личной и деловой информации, которую они распространяют по социальным сетям.

Источник: http://www.anti-malware.ru

Каждые три минуты какая-то компания подвергается вирусной атаке.

Аналитики подсчитали, что раз в три минуты какая-то компания в мире подвергается вирусному нападению. Этот показатель постоянно растет за счет технического прогресса.

Антивирусные эксперты из компании FireEye подсчитали, что примерно раз в три минуты совершается вирусная атака. При этом большинство из таких атак остается незамеченными из-за постоянно совершенствующихся технологий скры-

тия вредоносной активности.

Выводы аналитиков основываются на информации, которую они собирали в течение второго полугодия 2012 года. FireEye собирали сведения с нескольких тысяч продуктов безопасности, которые были установлены в корпоративных сетях по всему миру.

Проанализировав собранную информацию, эксперты установили, что в Сети в последнее время наблюдается четкая тенденция к повышению «интеллектуальности» вируса. В частности, последнее поколение вредоносного программного обеспечения легко обходит современные антивирусные программы.

Например, один из изученных аналитиками образцов вирусной программы умел останавливать все свои процессы до тех пор, пока за компьютер не садился человек. Вирус определял присутствие пользователя, реагируя на повышающуюся частоту кликов мышки.

Источник: http://www.imena.ua

Британские спецслужбы будут отслеживать киберугрозы совместно с бизнесом.

Спецслужбы Великобритании, в частности МИ5 и Управление правительственной связи Великобритании (GCHQ),объединили усилия с рядом частных бизнес-структур, создав новый информационный центр (“Fusion Cell”). В рамках данного центра спецслужбы и сотрудничающие с ними частные коммерческие структуры будут обмениваться информацией о киберинцидентах и киберугрозах.

По замыслу организаторов проекта, это должно помочь властям и бизнесу Великобритании защитить информационные сети страны от киберугроз. По информации The Telegraph, штаб-квартира “Fusion Cell” находится в Лондоне (её точное местоположение неизвестно). Известно, что обмен информацией о киберугрозах между участниками проекта будет осуществляться посредством специального веб-портала, работающего по принципу Facebook.

“Fusion Cell” призван помочь британским спецслужбам получить более полную картину угроз для киберпространства страны. Представители спецслужб также отмечают, что обобщая имеющиеся разведданные и информацию, получаемую от коммерческих структур, спецслужбы помогут последним лучше защитить свои информационные сети от киберугроз.

По имеющимся данным, на сегодняшний день в проекте “Fusion Cell” готовы принять участие более 160 бизнес-структур, работающих в области фармацевтики, финансов, энергетики, телекоммуникаций и обороны. Информация о том, какие именно компании намерены участвовать в проекте, не разглашается.

Источник: http://www.anti-malware.ru

Coleman Parkes: при переходе на электронный документооборот в 26% банков снизился уровень защиты данных.

После перехода на электронный документооборот лишь треть банков и страховых компаний полностью контролируют доступ к конфиденциальным документам – к такому выводу пришли аналитики агентства Coleman Parkes в ходе исследования, проведенного по заказу компании Ricoh. По данным опроса, только 47% руководителей финансовых организаций считают, что уровень информационной безопасности в их компаниях повысился за последние три года, а более 26% респондентов уверены, что ситуация с безопасностью в их банках за это время, напротив, серьезно ухудшилась.

Как отмечают аналитики Ricoh, сфера финансовых услуг, где бумажная документация традиционно обрабатывалась вручную, столкнулась с проблемой растущего объема данных, необходимостью перехода на взаимодействие с клиентами с помощью электронных систем и внедрения новых технологий. При этом процессы документооборота в финансовом секторе по-прежнему жестко регулируют-

ся сложным набором внутренних и международных норм и законов, предусматривающих полную прозрачность и строгую отчетность.

При проведении исследования также выяснилось, что 80% руководителей отметили серьезные изменения в процессах документооборота за счет активного проникновения мобильных технологий, и 86% при этом подчеркнули влияние на работу банков проблемы Больших Данных. Исследователи также обнаружили, что 69% банков и страховых компаний обновляют систему решений не реже, чем раз в год, при этом 81% топ-менеджеров признались, что принимают решение о внедрении новых технологий, не осознавая до конца потенциала уже используемых решений.

Источник: http://www.osp.ru

Исходный код AMI-BIOS и ключи подписи UEFI попали в открытый доступ.

Это должно было случиться рано или поздно. Тайваньский производитель JetWay случайно выложил на FTP-сайте ftp://ftp.jetway.com.tw/CODE исходный код AMI-BIOS, ключи подписи UEFI и много другой информации, которая явно не предназначалась для широкой публики. Почти целые сутки доступ ко всем этим файлам был возможен с логином и паролем ftp:ftp. Об утечке информации сообщил специалист по ИТ-безопасности Брэндон Уилсон в блоге своего друга.

Чужие ключи подписи UEFI можно использовать для подписи любого загрузчика, в том числе произвольного Linux-дистрибутива. Этот случай наглядно показывает, что внедрение цифровой подписи на самом деле имеет мало смысла с точки зрения информационной безопасности, если ключи настолько просто можно достать. Разработчики могут купить их за 99 долларов, а мошенники — перекупить или украсть. Главное, что пользователь теперь и сам может подписать любую ОС, какую хочет установить на свой компьютер.

Правда, когда об утечке становится всем известно, производитель может обновить UEFI-прошивку, так что старый ключ перестанет действовать.

Сейчас пароли к FTP-серверу поменяли, но поздно: информация уже ушла в открытый доступ.

Компания AMI сейчас готовит пресс-релиз с объяснением произошедшего.

Источник: http://www.xakep.ru

Лидерами по вредоносной активности стали Россия, Беларусь и Украина

Некоммерческая организация HostExploit измерила вредоносную активности в Интернете в IV квартале 2012 г. В своем отчете организация отобразила списки Топ-10 стран и Топ-50 хостов и сетей с высокой концентрацией вредоносного контента.

По результатам исследования, первое место по совокупной вредоносной активности снова досталось России, которая обогнала всех в категориях «Зараженные сайты» и «Badware» (шпионское ПО, программы показа рекламы, лжеантивирусы). Далее следует Беларусь, ставшая лидером по спаму и отмеченная большим количеством зараженных и фишинговых сайтов. Третье место досталось Украине, которая ранее занимала пятую строчку. Мы оказались вторыми в мире по спаму, плюс, как и Россия, имеем много центров управления ботнетами.

Что касается списка топ-50, то первую строчку здесь в который раз заняла небольшая голландская сеть Ecatel. На втором месте – российский хостинг-провайдер Ideal Solution, ресурсы которого злоумышленники используют для рассылки спама и управления ботнетами, в том числе ZeuS. Также в первую десятку вошли крупные операторы «Белтелеком» (Беларусь, 3 место), OVH Systems (Франция, 5 место) и Hetzner Online (Германия, 6 место). Также в этот список попал хостинг российского портала Mail.ru, кото-

UA Linux
open source ■ open future

рый отличился настолько большим количеством вредоносных ссылок, что сразу попал в Топ-50 на 10-е место.

Интересно, что лидером по вредоносности среди украинских провайдеров оказался некий FOP Smovskaya Valentina Ivanovna, за которым замечена очень высокая спам-активность. Этот хост занял восьмое место в общем списке.

По мнению исследователей, провайдеры часто оказываются непричастны к криминальной активности. Цель ежеквартальных отчетов – скорее обратить внимание на проблемы сети, о существовании которых провайдеры могут не подозревать.

Источник: http://www.imena.ua

«Яндекс» запустил сервис для защиты от вредоносных и недетских сайтов.

Крупнейшая российская интернет-компания «Яндекс» запускает бесплатный сервис «Яндекс.DNS», который призван помочь пользователям компьютеров и мобильных устройств предотвратить доступ на вредоносные, мошеннические или «взрослые» сайты, говорится в сообщении на сайте компании.

Сервис «Яндекс.DNS» представляет собой контентный интернет-фильтр, который ограничивает доступ на «вредные» сайты. Сайты проверяются специалистами «Яндекса», при этом использование нового сервиса, как утверждают в компании, на скорость доступа в интернет не влияет, пишет digit.ru.

Пользователи могут настроить «Яндекс.DNS» в трех режимах — «Без фильтрации», «Безопасный» с блокировкой мошеннических и вредоносных сайтов, «Семейный» с фильтрацией не только вредоносных ресурсов, но и сайтов с «взрослым» контентом. Инструкции по настройке сервиса можно получить на сайте dns.yandex.ru.

Сервис можно использовать на настольных компьютерах, ноутбуках, мобильных устройствах или точках доступа Wi-Fi (доступны прошивки для точек доступа ZyXEL, но список поддерживаемых устройств будет расширяться).

Проблема блокировки как вредоносных сайтов, так и ресурсов с вредной для детей информацией получает все большую актуальность в последнее время. Подобные фильтрующие сервисы есть у антивирусных компаний, операторов связи, крупных интернет-компаний. В настоящий момент законодатели обсуждают законодательную инициативу, которая обяжет интернет-провайдеров информировать пользователей о наличии различных решений для блокировки «вредных» сайтов при подключении им доступа в интернет.

Источник: http://www.anti-malware.ru

35% компаний не шифруют корпоративные данные.

Треть компаний, функционирующих на международном рынке, не уделяют внимания защите корпоративной информации.

Данные примерно трети присутствующих на рынке компаний может похитить практически любой мало-мальски грамотный хакер. Современные предприятия просто не уделяют шифрованию данных никакого внимания. Такие данные опубликовала «Лаборатория Касперского», после проведенного совместно с B2B International исследования рынка.

Так, согласно результатам исследования, всего половина компаний во всем мире уделяют должное внимание шифрованию собственных данных как на уровне файлов, так и полностью зашифровывая жесткие диски.

Более того, только в аэропортах США еженедельно теряется 12 тыс. ноутбуков, чья суммарная стоимость за год составляет в среднем $987 млн. Наконец, стоимость утечки корпоративных данных, предварительно оценивается в $25 млрд. убытков в год. Отметим, что это данные только для одной страны.

Любопытно, что ознакомившись с данной информацией, примерно 17% компаний заявили, что все равно не намерены тратить деньги на шифрование корпоративной информации.

Отметим, что шифрованием данных пренебрегают даже крупные банковские

организации.

В начале марта мы писали о том, как хакерская группировка Anonymous осуществила взлом Bank of America, Bloomberg, Thomson Reuters и некоторых других компаний. Дабы не быть голословными, хакеры тогда выложили в Сеть 16 Гб документов, программного обеспечения и исходных кодов.

Источник: http://www.imena.ua

Twitter оказался настоящим кладезем персональных данных.

Независимый эксперт доказал, что с помощью Twitter можно собрать массу личной информации – включая пин-коды к личным счетам.

Программист из США Колин Кейгер (Colin Keigher) исключительно от безделья вознамерился узнать, какую информацию о человеке можно собрать, изучив его Twitter. Результат превзошел все ожидания программиста.

Для начала Кейгер запустил в Сеть бота @PhoneNumberTwit, который отыскивал в Twitter номера телефонов и публиковал их на своей учетной записи, уведомляя программиста о находке. Этот аккаунт заблокировали в течение 36 часов после начала работы.

Тогда программист написал скрипт Avivore – программу для сбора данных в Twitter, которая искала в сети микроблогов три вида информации: телефоны, пинкоды Blackberry и IPv4-адреса. Вся эта информация тщательно накапливалась в базе данных.

Всего за 24 часа программа собрала 12,4 тыс. записей, которые позволили Кейгеру получить доступ к личной переписке свыше девяти тысяч пользователей. Программист прервал эксперимент, чтобы не быть уличенным в преступной деятельности. Тем не менее, вышеописанный эксперимент более чем убедительно доказывает, что Twitter представляет собой неисчерпаемый кладезь персональных данных.

Источник: http://www.imena.ua

Контроль запуска программ как залог безопасности сети. Часть 2

Все гениальное – просто?

Идея Default Deny очень проста и логична. Однако до настоящего момента этот подход был ориентирован на исключительно узкую аудиторию. В первую очередь, это связано с техническими трудностями, возникающими на пути реализации решения, приемлемого для широкого использования и снимающего ряд критических ограничений.

Новый этап развития Application Control

Использование режима Default Deny означает смещение приоритетов при выборе политики безопасности: от свободы действий и удобства конечных пользователей в сторону выполнения главной задачи любой системы защиты информации – сведения к минимуму риска утечки и/или потери критически важных для бизнеса данных.

Однако ранее внедрение жесткого режима контроля запуска и исполнения приложений приводило к возникновению серьезных функциональных ограничений, что делало использование такого режима практически невозможным. Обеспечение качественной поддержки режима Default Deny требует дополнительного функционала, без реализации которого переход на этот режим может нарушить нормальную работу корпоративной сети.

№	Задача	Решение
1	Определить весь состав ПО корпоративной сети	• Инвентаризация ПО
2	Классифицировать все ПО как авторизованное и неавторизованное	• Категоризация ПО • Application Management • Dynamic Whitelist
3	Избежать блокирования при переходе в режим Default Deny необходимого для работы ПО и, как следствие, нарушения бизнес-процессов компаний	• Dynamic Whitelist • Доверенные пользователи, источники ПО (Trusted Users & Sources) • Тестирование и поддержка режима опытной эксплуатации
4	Обеспечить регулярное и бесперебойное обновление популярного ПО: компонентов ОС (системных библиотек, драйверов различных периферийных устройств), офисных приложений и т.д.	• Безопасные механизмы обновлений ПО (Trusted Updaters) • Dynamic Whitelist
5	Разграничивать права и уровень доступа пользователей/групп пользователей на запуск и исполнение приложений	• Категоризация ПО • Application Management
6	Осуществлять мониторинг, а также вести аудит системных событий на случаи необходимости проведения служебных расследований	• Мониторинг и аудит (репортинг)
7	Оперативно реагировать на возникающие потребности конечных пользователей, разрешать возникающие конфликты, связанные с установленными ограничениями/запретами на использование того или иного ПО	• Обеспечение обратной связи и поддержки пользователей

При переходе в Default Deny перед системными администраторами встает ряд задач, и, чтобы облегчить им решение этих задач, Application Control как основной компонент, осуществляющий управление приложениями корпоративной сети, должен был претерпеть существенные изменения.

Итак, использование режима Default Deny стало возможным только после внедрения следующего функционала:

•Инвентаризация – сбор информации обо всем ПО, установленном в корпоративной сети, - на всех компьютерах и сетевых ресурсах.

•Категоризация – деление идентифицированного в сети ПО на функциональные группы: компоненты ОС, браузеры, мультимедиа, игры и т.д.

•Конфигурирование, или Application Management – введение для пользователей/групп пользователей ограничений на запуск и исполнение приложений определенных категорий (собственно, определение политик безопасности).

•Dynamic Whitelist – база знаний обо всём многообразии выпускаемого в мире ПО. Актуальная и регулярно обновляемая информация о приложениях, их репутации, категориях и популярных/рекомендованных аналогах. Это экспертные данные, которые поставляются производителями решений по безопасности.

•Безопасные механизмы обновления ПО – автономные средства поддержки регулярных обновлений популярного ПО, избавляющие администраторов от необходимости повторно проводить утомительную процедуру идентификации и легализации обновлённых в сети приложений.

•Поддержка списков доверенных пользователей, источников ПО – инструментарий, предоставляющий администра-

торам сетей, инженерам информационной безопасности простые и удобные способы легализации ПО. В частности, создание списков доверенных сетевых ресурсов в интернете и в локальной корпоративной сети (HTTP/FTP/Shared folders/etc.) - источников чистых приложений, которые разрешено устанавливать и использовать.

•Тестирование и поддержка режима опытной эксплуатации – средства статического или динамического обнаружения системных коллизий, возникающих в ходе внедрения тех или иных политик безопасности (несовместимости/неработоспособности различных приложений), в результате которых могут быть нарушены бизнес-процессы.

•Обратная связь и поддержка пользователей – инструменты управления возникающими инцидентами для максимального облегчения процесса сопровождения и поддержки пользователей.

•Мониторинг и аудит – развитые средства для сбора, агрегации и систематизации отчётности.

Остановимся на ключевой составляющей Whitelist Security Approach – динамической базе чистых файлов (Dynamic Whitelist). Интерес к Dynamic Whitelist обусловлен не только ее техническими, но и организационными составляющими, без которых невозможно обеспечить максимальную эффективность базы Whitelist.

Dynamic Whitelist: динамическая база знаний о ПО

Что же такое база Dynamic Whitelist? Это база знаний обо всём многообразии легитимного ПО. С технической точки зрения Dynamic Whitelist представляет собой огромную базу «чистого» программного обеспечения, которая непрерывно пополняется новыми дистрибутивами, различного рода файлами, а главное – знаниями о данных объектах. Качество и полнота данных в такого рода источниках экспертных данных зависит от их поставщиков. Ведущие компании – производители решений по безопасности сами формируют базы Dynamic Whitelist.

Dynamic Whitelist является компонентом, который необходим для решения трёх из семи задач, стоящих при реализации Default Deny (см. таблицу выше). Очевидно, что качество предлагаемого вендором решения будет напрямую зависеть от качества используемой в нем базы знаний.

Для решения перечисленных выше задач база должна содержать:

1.Базовую информацию о ПО: производитель, название продукта, версия последнего, прочая информация, главным образом извлекаемая из атрибутов самих объектов.

2.Расширенную информацию (экспертные знания):

•данные о степени риска – классификация ПО, его репутация: доверенное, недоверенное, сомнительное и т.п.;

•категория ПО: системное ПО, браузеры, игры, офисные приложения и т.д.;

•бизнес-ориентация приложений: бухгалтерия и финансы, маркетинг, HR, CRM, логистика и т.д.;

•альтернативное ПО – информация об аналогах ПО;

•статистические данные – например, популярность ПО, его распределение по регионам и т.д.

Какие ещё требования, помимо состава данных, предъявляются к таким базам знаний?

Прежде всего, база Dynamic Whitelist должна быть динамичной, что, собственно, и отражено в её названии. Ежедневно в свет выходит множество новых легитимных приложений и обновлений к уже существующему ПО, а это означает, что поставщики решений по безопасности должны незамедлительно реагировать на любые изменения в мире ПО, оперативно обновляя свои базы знаний. А для этого следует обеспечить регулярное и своевременное пополнение базы чистого ПО из множества источников из разных регионов мира. И это обновление должно происходить в автоматическом режиме, ведь речь идет о гигантских объемах информации (терабайты данных в сутки). Для этих целей поставщики баз Dynamic Whitelist разворачивают в Сети так называемые краулеры (от англ. crawler) – поисковые агенты, которые осуществляют мониторинг нового ПО и при необходимости – загрузку новых приложений.

Для поддержки актуальности базы

данных необходимо также развитие технологических партнерских отношений вендора с крупными производителями и дистрибуторами ПО (Independent Software Vendors). Цель такого партнерства — получение, обработка и анализ (классификация и категоризация) нового ПО до выхода его публичных релизов с целью минимизации ложных срабатываний: случаев несовместимости решений по безопасности и ПО вендора-партнера.

Еще один возможный источник пополнения базы — глобальная информационная сеть, созданная вендором на базе сообщества его пользователей. Отметим, что такая информационная сеть является серьёзным конкурентным преимуществом. Она позволяет отслеживать метаданные о ПО, запускаемом на компьютерах пользователей, и снабжать базу знаний информацией о появлении новых приложений и выпуске различных обновлений ПО.

У «Лаборатории Касперского» есть все перечисленные компоненты пополнения базы Dynamic Whitelist. В настоящее время развитая партнерская программа, насчитывающая несколько сотен международных партнеров, десятки миллионов участников глобальной информационной сети Kaspersky Security Network во всём мире, а также обширная сеть автоматических поисковых агентов обеспечивают беспрерывное пополнение динамической базы знаний «Лаборатории Касперского» — в среднем более чем на 1 миллион новых файлов в сутки.

Качество динамической базы Whitelist «Лаборатории Касперского» было доказано в независимом тесте, проведенном компанией West Coast Labs. Согласно результатам тестирования в нашей базе содержится информация о 94% всего чистого ПО, выпущенного в мире.

Необходимо внимательно контролировать все поступающие в базу Dynamic Whitelist объекты, а главное, поддерживать репутацию о них в актуальном состоянии. Ведь ПО, которое сегодня может быть классифицировано как «чистое», завтра, при более тщательном анализе, может оказаться носителем опасного вредоносного кода.

Надо отметить, что регулярное сканирование базы Dynamic Whitelist — весьма нетривиальная задача. Для ее решения, кроме автоматических средств обработки и анализа информации, необходима команда выделенных экспертов, способная в случаях возможных логических коллизий анализировать программный код и выносить финальный вердикт. Маленькие компании или производители «бесплатных» антивирусных продуктов позволить себе такой выделенной антивирусной лаборатории не могут. Кроме того, специфика обработки вредоносного и чистого ПО разная. В идеале компания должна располагать не только антивирусной, но и специализированной Whitelisting лабораторией, которая будет отслеживать входящие информационные потоки, заниматься обучением интеллектуальных систем, а также незамедлительно реагировать в экстренных случаях (такая Whitelisting лаборатория есть у «Лаборатории Касперского»).

От теории к практике: Endpoint 10 «Лаборатории Касперского»

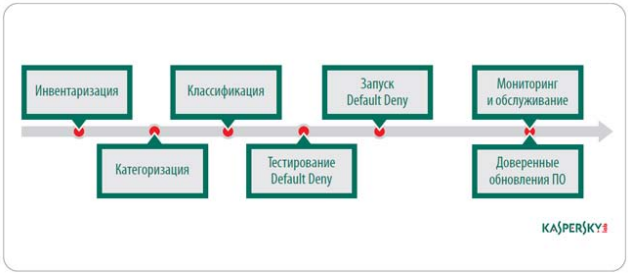
Администраторы корпоративных сетей выполняют сложные, часто повторяемые задачи по обслуживанию множества рабочих станций различного назначения. Использование подхода Whitelist Security Approach (режима Default Deny) гарантирует значительно более высокий уровень безопасности в корпоративной сети. При этом внедрение режима Default Deny с его жёсткой системой ограничений требует реализации в соответствующих продуктах серьёзных средств автоматизации задач, которые встают перед администратором.

Рассмотрим, как осуществляется переход от теории к практике на примере продуктах класса Endpoint Security «Лаборатории Касперского», последовательно проследив все этапы жизненного цикла от инвентаризации ПО до поддержки корпоративной сети (после внедрения продукта).

Впервые Whitelist Security Approach

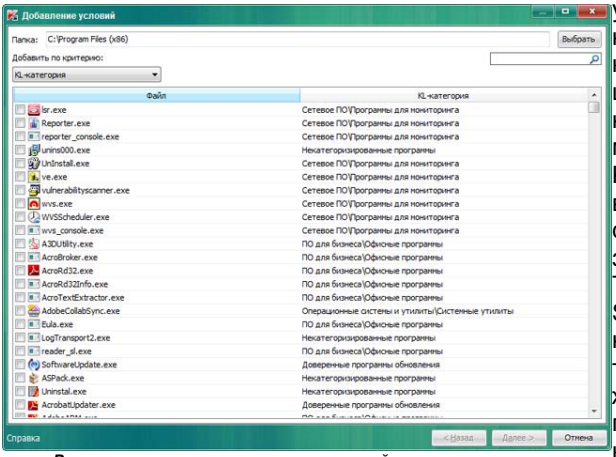
UA Linux
open source ■ open future

был реализован в Kaspersky Endpoint Security 8 for Windows в 2011 году. В 2013 году Kaspersky Endpoint Security 10 for Windows представит еще более широкую функциональность, в том числе в области Application Control.



Этапы жизненного цикла (Default Deny)

•Инвентаризация. В самом начале, после установки продукта, администратор должен провести автоматическую процедуру инвентаризации всего ПО, установленного в корпоративной сети. В рамках этой задачи Kaspersky Endpoint Security собирает информацию обо всем ПО, установленном на компьютерах сети и сетевых ресурсах.



Результат инвентаризации приложений в указанной директории

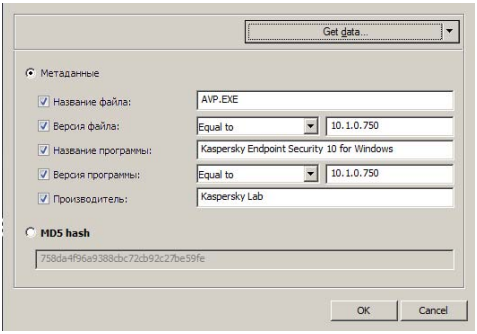
•Категоризация (автоматическая, на базе Dynamic Whitelist). По окончании инвентаризации автоматически проходит категоризация всего ПО — разбиение на соответствующие группы согласно правилам, заложенным в продукте (ОС, мультимедиа, периферия, игры, браузеры и т.д.). Отметим, что такой функционал есть не у всех вендоров, реализовавших Application Control. Однако мы сочли, что для удобства управления огромным разнообразием ПО, установленного в корпоративной сети, он просто необходим. Поэтому разделили нашу базу Whitelist на 16 категорий верхнего уровня и 96 листовых категорий (см. наш каталог категорий).

Для определения критически важных компонентов ОС и драйверов в Kaspersky Endpoint Security реализована особая категория файлов ОС — Golden Image. В нее входят все необходимые компоненты для Win XP, Vista, Win7, Win8 (32 и 64) и более 15 локализаций для каждой (всего более 100 версий и локализаций). Администратору достаточно добавить в категорию Golden Image файлы из локальной Whitelist базы — и конфигурация Default Deny готова.

•Категоризация (ручная). Важно учитывать, что белый список любого производителя защитных решений не может содержать информацию обо всем ПО, установленном в сети конкретной компании. Например, компании нередко имеют специализированный проприетарный софт, разработанный на месте или по заказу. В новом Kaspersky Endpoint Security 10 в Application Control администратор имеет возможность создать локальный белый список. Также в Kaspersky Endpoint Security 10 добавлена функциональность мультивекторной категоризации. Т.е. одно приложение может одновременно принадлежать сразу нескольким категориям.

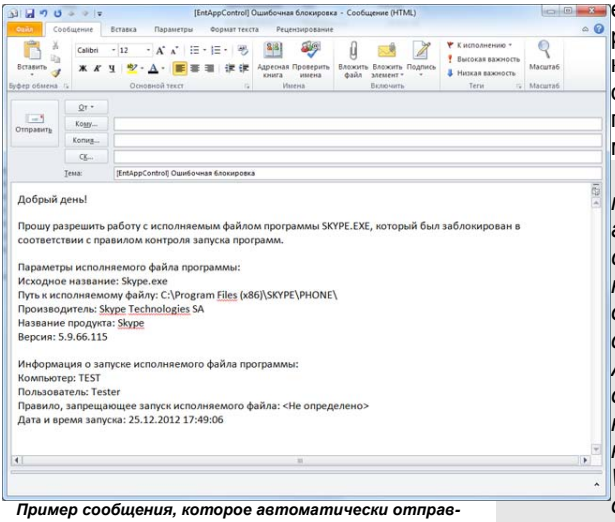
•Конфигурирование. В Kaspersky Endpoint Security существует возможность управлять категоризированным ПО в зависимости от пользователей и групп пользователей. К примеру, можно разрешить использовать ПО категории «Accounting» только бухгалтерии, чтобы никто больше не имел доступа к финансовой информации компании. Именно на этом этапе можно ограничить использование нелицензионного и не связанного с

работой ПО. Т.е., к примеру, запретить использование любого ПО, лицензиями на которое не располагает компания, или запретить все IM, кроме Skype например. Также можно запретить использование конкретных версий ПО, например, запретить все браузеры, кроме указанной версии Internet Explorer.



Возможности пользовательской категоризации файлов

•Безопасные механизмы обновлений ПО. Режим автоматического обновления ПО в Kaspersky Endpoint Security обеспечивает технология Trusted updaters. Она позволяет реализовать безопасную процедуру обновления продуктов, учитывающую сложные цепочки программных вызовов, выполняемых в процессе обновления.



Пример сообщения, которое автоматически отправляется системному администратору в случае блокировки запуска приложения

•Тестирование и поддержка режима опытной эксплуатации. Поскольку внедрение жестких политик в сети достаточно ответственное дело, мы предусмотрели специальный режим Test Mode, который администратор может использовать для моделирования и оценки работы любого правила. Реальная блокировка приложений в режиме Test Mode не происходит, но администратор по отчётам системы видит, что было бы, если бы данный режим работал. Это позволяет внести соответствующие коррективы в правила перед боевой реализацией, не вызывая негативной реакции со стороны пользователей и не нарушая бизнес-процессов компании в случае некорректной работы отлаживаемых правил.

•Обратная связь и поддержка пользователей. IT-среда компании динамична, поэтому пользователь всегда должен иметь возможность запросить у администратора разрешение на запуск нового ПО, а администратор должен иметь возможность простым нажатием кнопки в удобном интерфейсе запретить или разрешить соответствующий запрос. В нашем продукте реализованы обе возможности. Для обеспечения гибкости работы даже в режиме Default Deny мы внедрили возможность обслуживания администратором пользовательских жалоб. В случае если какое-либо приложение оказалось заблокированным, а пользователь считает, что оно необходимо ему для работы, ему достаточно нажать кнопку «Отправить запрос», и соответствующая нотификация поступит администратору автоматически.

Последний год независимые тестовые лаборатории активизировались в новом для себя направлении тестирования Application Control. Сразу две компании проверили эффективность технологии Application Control для защиты от целевых атак и управления неавторизованным ПО. В начале 2012 года компания West Coast Labs опубликовала отчет по результатам первого в индустрии независимого теста, где технология «Лаборатории Касперского» заняла первое место. Позднее компания Dennis Labs также провела сравнительное тестирование и в нача-

ле 2013 года предоставила результат публике. Наше решение второй раз подряд получило высшую оценку.

Заключение

Увеличение количества и, главное, усложнение угроз заставляет производителей антивирусного ПО искать новые решения для эффективной защиты корпоративных сетей. Новый подход — Whitelist Security Approach — позволяет запуск и исполнение в системе только проверенного ПО из белых списков. Соответственно, запрещается запуск любого неизвестного или неавторизованного ПО. В результате любая вредоносная программа просто не может запуститься в системе. Такой подход позволяет обеспечить защиту от сложных и неизвестных угроз, в том числе целевых атак.

Whitelist Security Approach является новым витком 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).

Реализация режима повышенной безопасности Default Deny требует внедрения дополнительного функционала. Сценарий работы Application Control должен предусматривать несколько простых механизмов, таких как инвентаризация, категоризация, конфигурирование (Application Management), гибкое управление политиками локального белого списка и возможность использовать облачную базу Dynamic Whitelist, которая способна незамедлительно реагировать на регулярные изменения в мире ПО. А такой функционал как тестирование и поддержка режима опытной эксплуатации необходим для грамотного перехода в режим Default Deny.

Whitelist Security Approach помогает системному администратору выполнять ряд задач:

•Контролировать (разрешать, запрещать, гибко ограничивать и осуществлять аудит) запуск на рабочих станциях чистых программ в соответствии с политикой безопасности, действующей в компании.

•От поставщика решения получать экспертизу о чистоте файлов из базы Dynamic Whitelist.

•Гарантировать нормальную работу чистого и разрешенного ПО.

•Управлять категориями ПО, а не отдельными программами.

•На этапе промышленной эксплуатации осуществлять мониторинг, контроль и реагировать на проблемы, возникающие вследствие блокирования того или иного ПО.

•Оптимизировать использование IT-ресурсов компании и повышать их производительность за счет контроля использования постороннего и нелицензионного ПО в сети.

Application Control в совокупности с поддержкой Default Deny является мощным и удобным инструментом, который упрощает системному администратору задачу обслуживания рабочих станций в корпоративной сети и обеспечивает ее безопасность.

Мы в «Лаборатории Касперского» считаем Whitelist Security Approach одним из ключевых средств защиты корпоративных сетей будущего. В то же время мы полагаем, что не существует панацеи или единственной технологии, способной обеспечить защиту от всех угроз. Поэтому для корпоративных сетей целесообразно использование мощного endpoint-продукта, сочетающего различные технологии защиты. Только многоуровневая система защиты и контроля позволяет обеспечить максимально возможный уровень защиты корпоративной сети. Авторы выражают благодарность Владиславу Мартыненко за помощь в подготовке главы «Компонентный состав современных продуктов безопасности».

Источник:

http://www.securelist.com

UA Linux
open source ■ open future

Эксперт в области безопасности.

Рынок цифрового оружия принимает угрожающие масштабы.

Авторитетный журнал Economist выступил с пространной статьей о рынке кибероружия, который сегодня стал проблемой международного масштаба. В этой статье приведены высказывания множества людей, имеющих самое прямое отношение к проблеме черного рынка кибероружия.

Как считает Венкатрамана Субрахманиян (Venkatramana Subrahmanian), эксперт по нелегальному обороту хакерских инструментов из Мэрилендского университета, преступники и террористы ведут торговлю опасными программами на множестве (более 20) специализированных форумов или через специальных посредников (их число оценивается в несколько десятков).

Р. Рагхаван (R.K. Raghavan), бывший глава Центрального бюро расследований Индии, сообщает, что еще десять лет назад в Индии не было зафиксировано ни одной связи между авторами эксплойтов и организованной преступностью, а сегодня такие факты стали обыденностью. Полковник Джон Адамс (John Adams) из отдела интеграции разведслужб при корпусе морской пехоты США, считает главной опасностью то, что хакеры снабжают кибероружием агрессивные режимы, которые не имеют достаточных собственных ресурсов на атаки против компьютерных систем в развитых странах.

Сами по себе эксплойты, на которых строится современное кибероружие, вполне легальны. В мире есть немало компаний, которые ищут уязвимости в программных системах и продают средства для их использования (то есть, эксплойты). Одна из таких фирм, Netragard, за прошлый год продала более 50 эксплойтов компаниям и государственным ведомствам США по цене от 20 до 250 тыс. долларов за штуку. Продаваемые эксплойты фирма покупает у тридцати с лишним «вольных хакеров» – их тщательно проверяют, чтобы они не продавали свои секреты на сторону, а особенно преступным элементам и враждебным государствам.

Уже ведутся разговоры о принятии законов против торговли эксплойтами. Например, Марьете Шааке (Marietje Schaake), депутат Европарламента от Нидерландов, выступила с инициативой о включении эксплойтов в список продукции, подпадающей под экспортные ограничения. В то же время, по ряду очевидных причин контроль за распространением кибероружия вряд ли будет эффективным.

Технически эксплойты представляют собой научное знание, облеченное в форму программного кода, а препятствовать распространению знаний очень тяжело, тем более, в век максимально свободного перемещения информации. Кроме того, эксплойты нелегко отслеживать: расследование громкого скандала с червем Stuxnet показало, что в нем используется четыре эксплойта, а один из них по всем признакам был открыт в недрах правительственных организаций. Предположительно, этот «государственный» эксплойт был создан в США или Израиле.

Не в последнюю очередь из-за спроса на эксплойты со стороны государственных органов цены на черном рынке кибероружия растут завидными темпами. Как сообщает Эрик Фильоль (Eric Filiol), отставной подполковник компьютерной разведки Франции, со ссылкой на секретные документы, средняя цена нового эксплойта с 2004 г. выросла более чем в пять раз. Цена каждого конкретного образца зависит от трех основных факторов: 1) сложности обнаружения, 2) количества компьютеров, к которым эксплойт открывает доступ, и 3) ценности этих компьютеров. Например, эксплойт для незаметного получения прав администратора на удаленном ПК под управлением ОС Windows XP стоит около $40 тыс. Эксплойт для популярного браузера Internet Explorer может стоит до полумиллиона долларов.

Некоторые эксперты выступают с резким осуждением практики по покупке эксплойтов официальными организациями.

Дело в том, как считают противники черного рынка эксплойтов, что эта практика фактически стимулирует опасные исследования. В итоге потенциальные жертвы в лице развитых стран и их спецслужб сами финансируют разработку оружия против себя. Выход из ситуации стал вполне логичным: сегодня спецслужбы развитых стран все чаще склоняются к проведению собственных дорогостоящих исследований, а не приобретают новые эксплойты «на стороне». Такие приемы уже используются в США, аналогичные действия предпринимает и КНР.

Внутренняя разработка эксплойтов снижает риски, связанные с возможностью использования оплаченных эксплойтов против заказчика. Тем не менее, даже с учетом полной «эксклюзивности» эксплойтов, найденных официальными организациями, черный рынок даже не собирается исчезать. По мнению профессиональных торговцев эксплойтами, эта торговля будет процветать до тех пор, пока люди готовы платить большие деньги за гонку вооружений между разработчиками, оставляющими в своих продуктах возможность удаленного контроля, и хакерами, которые пытаются найти и продать способ для использования этих возможностей.

Источник: http://internetua.com

«Мартовские троянцы» и другие угрозы прошедшего месяца.

По наблюдениям аналитиков компании «Доктор Веб», одна из наиболее отчетливых тенденций марта — временное снижение и новый виток роста темпов массового распространения среди пользователей Интернета вредоносных программ семейства Trojan.Hosts. Пик этой эпидемии пришелся на начало 2013 года. Также март был отмечен ростом числа заражений троянцами-энкодерами в Европе и появлением рекламных троянцев для операционной системы Mac OS X. Общий размер ботнета Win32.Rmnet.12 с начала года увеличился на 2 млн инфицированных компьютеров, достигнув в марте рекордной отметки в 8,5 млн зараженных машин.

Вирусная обстановка

По данным, полученным с использованием лечащей утилиты Dr.Web CureIt!, в марте 2013 года наиболее распространенной угрозой стали вредоносные программы семейства Trojan.Hosts. В течение месяца было зафиксировано 186 496 случаев изменения данными троянцами системного файла hosts, ответственного за трансляцию сетевых адресов в их DNS-имена, что составляет более 10% от общего числа выявленных угроз.

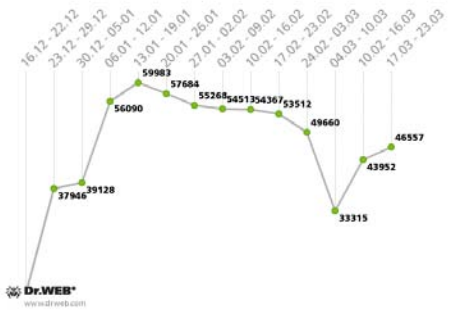
Причины данного явления уже подробно рассматривались в опубликованном компанией «Доктор Веб» новостном материале. Одним из наиболее популярных способов распространения этих троянцев является взлом веб-сайтов с целью размещения специального командного интерпретатора, с помощью которого злоумышленники модифицировали файл .htaccess и помещали на сайт специальный вредоносный скрипт-обработчик. При обращении к такому интернет-ресурсу скрипт-обработчик выдает пользователю веб-страницу, содержащую ссылки на различные вредоносные приложения. Альтернативный способ распространения угроз семейства Trojan.Hosts — использование бэкдоров и троянцев-загрузчиков. При этом наиболее популярной модификацией данной вредоносной программы согласно статистике является Trojan.Hosts.6815.

В начале 2013 года распространение угроз семейства Trojan.Hosts приняло масштабы эпидемии: ежедневно антивирусное ПО Dr.Web фиксировало более 9 500 случаев заражения. Пик распространения троянцевTrojan.Hosts пришелся на январь и середину февраля, в начале марта эта волна понемногу пошла на спад, а во второй половине месяца количество случаев инфицирования вновь начало расти. Динамика этого процесса показана на представленной ниже диаграмме.

Среди других наиболее распространенных угроз, обнаруженных на компьютерах пользователей в марте 2013 года, следует отметить сетевого червя Win32.HLLW.Phorpiex.54. Эта вредоносная программа, распространяясь с ис-

пользованием рассылок по каналам электронной почты, а также путем самокопирования на съемные носители, способна предоставлять злоумышленникам несанкционированный доступ к инфицированному компьютеру.

Динамика распространения троянцев Trojan.Hosts в 2012 - 2013 годах



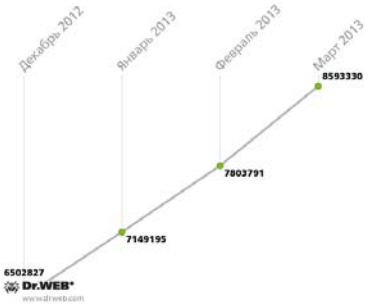
На четвертом месте в статистике заражений расположился один из платных архивов, детектируемых антивирусным ПО Dr.Web как Trojan.SMSSend.2363, за ним следуют троянцы BackDoor.IRC.NgrBot.42 и Win32.HLLP.Neshta. Мартовская двадцатка наиболее распространенных вредоносных программ по данным, полученным от пользователей лечащей утилиты Dr.Web CureIt!, представлена в следующей таблице:

Название	%
Trojan.Hosts	10.96
Trojan.Hosts.6815	1.62
Win32.HLLW.Phorpiex.54	1.11
Trojan.SMSSend.2363	1.02
BackDoor.IRC.NgrBot.42	0.91
Win32.HLLP.Neshta	0.80
Trojan.StartPage.48148	0.69
Trojan.Click2.47013	0.66
Trojan.MayachokMEM.4	0.59
Win32.Sector.22	0.56
Trojan.Mayachok.18024	0.56
BackDoor.Andromeda.22	0.55
Trojan.Mayachok.18582	0.54
BackDoor.Butirat.245	0.51
Trojan.Winlock.6426	0.47
Exploit.CVE2012-1723.13	0.43
Trojan.Popuper.42548	0.41
Trojan.PWS.Panda.368	0.40
Trojan.Hosts.6708	0.40
Trojan.Rmnet	0.39

Ботнеты

В конце 2012 года аналитики компании «Доктор Веб» высказывали предположение, что размер ботнета, состоящего из инфицированных файловым вирусом Win32.Rmnet.12 рабочих станций, будет расти. По данным на декабрь 2012 года, общее количество зараженных компьютеров составляло 6,5 млн, а на 27 марта 2013 года их численность составила 8 593 330, увеличившись за первые три месяца 2013 года на 2 млн. Таким образом, среднесуточный прирост ботнета Win32.Rmnet.12 в январе составил порядка 15–25 тыс. инфицированных компьютеров, а в феврале и марте — 20–22 тыс. Динамику данного процесса можно проследить на представленном ниже графике.

Динамика роста ботнета Win32.Rmnet.12 в начале 2013 года

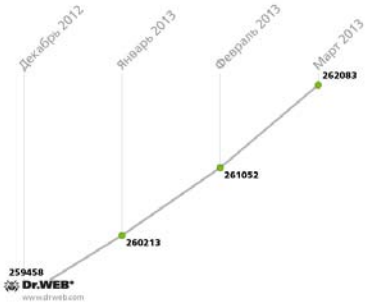


Файловый вирус Win32.Rmnet.12 может реализовывать функции бэкдора, выполняя поступающие от удаленного сервера команды. Также он способен красть пароли от популярных FTP-клиентов, которые могут быть использованы для организации сетевых атак или заражения сайтов. Вредоносный функционал вируса позволяет встраивать в просматриваемые веб-страницы посторонний контент (веб-инжекты), перенаправлять пользователя на указанные злоумышленниками сайты, а также передавать на удаленные

узлы содержимое заполняемых жертвой форм. Как и другие файловые вирусы, Win32.Rmnet.12 обладает способностью к саморепликации и может заражать файловые объекты.

Продолжается постепенный рост ботсети Win32.Rmnet.16 — еще одной модификации файлового вируса семействаWin32.Rmnet. В декабре численность этого ботнета составляла 259 458 инфицированных машин, а в конце марта их число достигло 262 083, увеличившись за три месяца всего на 2 625 узлов. Среднесуточный прирост ботнета составил 20–30 заражений. Проследить динамику роста ботнета можно с помощью представленного ниже графика.

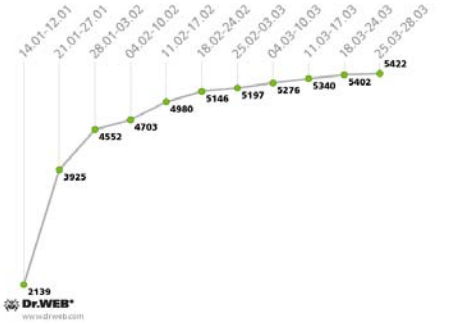
Динамика роста ботнета Win32.Rmnet.16 в начале 2013 года



К сожалению, несмотря на многочисленные публикации и предупреждения со стороны компании «Доктор Веб», фармацевтические компании по-прежнему подвержены заражению опасным троянцем BackDoor.Dande, ворующим информацию из программ электронного заказа медикаментов, таких как специализированная конфигурация «Аналит: Фармация 7.7» для платформы 1С, «Система электронного заказа» СЭЗ-2 производства компании «Аптека-Холдинг», программа формирования заявок компании «Российская Фармация», система электронного заказа фармацевтической группы «Роста», программа «Катрен WinPrice» и некоторые другие. Поскольку данное вредоносное приложение способно работать только на компьютерах, где установлена одна из названных программ, можно смело говорить о том, что ботнет BackDoor.Dande состоит большей частью из рабочих станций, принадлежащих фармацевтическим компаниям и аптекам. По данным на конец 2012 года, в этой бот-сети числился 3 031 инфицированный компьютер; на 27 марта 2013 в России таких компьютеров насчитывается уже 3 066, и еще порядка 800 инфицированных узлов находятся за пределами Российской Федерации. В среднем ежесуточно к ботнету BackDoor.Dande присоединяется 1–2 зараженных узла.

В январе 2013 года компания «Доктор Веб» сообщила о распространении (преимущественно на территории США) троянца BackDoor.Finder, подменяющего поисковые запросы пользователей браузеров Microsoft Internet Explorer, Mozilla Firefox, Maxthon, Google Chrome, Safari, Opera, Netscape или Avant. На сегодняшний день к контролируемым специалистами «Доктор Веб» управляющим серверам подключилось 5 422 бота, при этом динамика роста ботнета BackDoor.Finder выглядит следующим образом:

Динамика роста ботнета BackDoor.Finder в 2013 году



Угроза месяца

В течение марта было отмечено широкое распространение троянцев-шифровальщиков, среди которых следует особо отметить Trojan.ArchiveLock.20 — вредоносную программу, упаковывающую пользовательские файлы в защищенный паролем архив WinRAR. Если до недавнего времени этот троянец был знаком только нашим соотечественникам, то в марте были зафиксированы многочисленные случаи заражения компьютеров пользователей европейских стран, в том числе Испании и Франции. Только в период с 23 по 26 марта в службу технической поддержки компании «Доктор Веб» обратилось 150 итальянских пользователей,

пострадавших от данной вредоносной программы, и их количество продолжает расти.

Для распространения троянца злоумышленники пытаются получить доступ к атакуемой машине по протоколу RDP методом подбора пароля. Запустившись на инфицированном компьютере, Trojan.ArchiveLock.20 удаляет содержимое «Корзины» и хранящиеся на компьютере резервные копии данных, после чего помещает пользовательские файлы по заранее составленному списку в защищенные паролем самораспаковывающиеся архивы с использованием консольного приложения WinRAR. Исходные файлы при этом уничтожаются с помощью специальной утилиты, вследствие чего их восстановление становится невозможным.

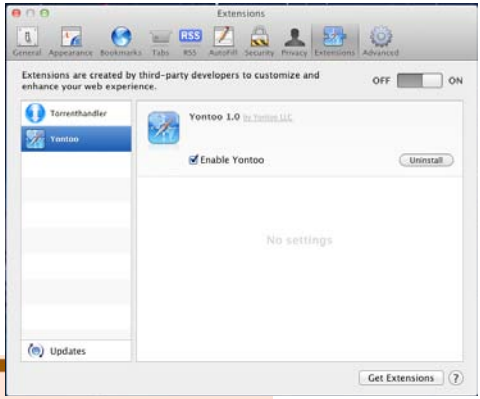
Подробности об этой вредоносной программе можно узнать в опубликованной на сайте компании «Доктор Веб» обзорной статье.

В некоторых случаях специалисты компании «Доктор Веб» могут восстановить файлы, заархивированные троянцем Trojan.ArchiveLock.20: для этого следует создать заявку в категории «Запрос на лечение».

Рекламный троянец для Mac OS X

Троянскими программами, предназначенными для демонстрации рекламы на компьютерах пользователей Windows, уже давно никого не удивить, однако в последнее время подобные приложения стали появляться и для других платформ, в частности, Mac OS X. Одним из таких троянцев является Trojan.Yontoo.1.

Распространяясь под видом кодеков для просмотра видео, а также иных программ, таких как медиаплееры, программы для улучшения качества просмотра видео, «ускорители» загрузки файлов из Интернета и т. д.,Trojan.Yontoo.1 устанавливает на инфицированный «мак» плагины для браузеров Safari, Google Chrome и Mozilla Firefox.



Этот плагин получает от злоумышленников специальный файл, позволяющий встраивать в просматриваемые пользователем веб-страницы различные рекламные модули от сторонних партнерских программ, а также передает на удаленный сервер данные о том, какие веб-страницы открывает пользователь в своем браузере. Узнать больше о принципах работы этой вредоносной программы можно, ознакомившись с опубликованной на сайте «Доктор Веб» аналитической статьей.

Android-угрозы

Для ОС Android в области вирусных событий март оказался весьма насыщенным периодом. Так, в начале месяца в вирусную базу Dr.Web была внесена запись для довольно примитивного троянца, получившего имя Android.Biggboss. Эта вредоносная программа распространялась на различных сайтах-сборниках ПО в модифицированных злоумышленниками приложениях и предназначалась

для пользователей из Индии. Будучи установленным на мобильное Android-устройство, Android.Biggboss загружался в качестве системного сервиса при запуске ОС и демонстрировал диалоговое окно, в котором говорилось о получении важного сообщения из некоего отдела кадров. В случае согласия пользователя просмотреть это «сообщение» троянец открывал в веб-браузере специальный URL, по которому осуществлялась загрузка изображения, содержащего поддельное обращение от отдела кадров компании TATA India Limited, не имеющей никакого отношения к настоящей корпорации TATA. Наряду с заманчивым описанием потенциальной должности, обращение содержало призыв перевести определенную денежную сумму на банковский счет мошенников с целью гарантировать кандидату получение вакантного места.

http://v T...

TATA

Dear Candidate,

It is our good pleasure to inform you that your Resume has been selected online for company's direct recruitments. The Company has selected 168 candidates for IT, Administration and Production Department. TATA urgently requires candidates as Executives and Managers. You are selected according to your resume in which Project you have worked. TATA is recruiting the Staff for new plant.

Your Appointment Process will do at our Company office on 28 - february - 2013 You will be pleased to know that Company has advised you in the selection panel that your application can be progress to final stage. Your offer letter with air ticket will be send to you by courier. The Company can be offering you as best salary 2 LAKH to 50 LAKHS ANNUAL +DA+HRA+BENEFITS for this post, Designation and job location will be fixed by Company at the time of final. You have to come with all documents.

Regarding your interview management by company, you have to deposit an initial refundable security amount in favor of Company for the sum of Rs. 8,150/-. This is refundable interview security against your interview management. Company will pay all the expenditure to you at the time of face-to-face meeting. Job profile and salary offered by Company will be mention in your call letter. Your call letter and Air ticket will be dispatched very shortly after receiving your confirmation of security deposited in bank.

The Company will provide you hotel facilitates and local conveyance. One extra person is allowing with all candidates. Kindly give the information by email after submitted the security amount in bank. The last date of security deposited in bank on 22/02/2013.

After deposited the security amount in to bank. Kindly send the scan copy of bank deposit slip to our email - tatad.companyhrdonline.com. We wish you the best of luck for the subsequent and remaining stage.

Regards,

Prakash Mehta - (HR Manager)

TATA INDIA LIMITED
Unit-2, D – 142, G.T. Kamal Road,
Industrial Area, Near Hydro Power House,
New Delhi - 91
Contact - +919582617367,+919582619120

Также в марте получили распространение новые представители троянских программ-шпионов, направленных против японских пользователей и предназначенных для кражи конфиденциальной информации из телефонной книги их мобильных Android-устройств. В вирусную базу Dr.Web они были внесены под именамиAndroid.EmailSpy.2.origin, Android.EmailSpy.3.origin и Android.EmailSpy.4.origin. Как и прежде, троянцы распространялись под видом самых разнообразных приложений, например видеоплеера, эмулятора игр и фотоаппарата-рентгена.

После запуска эти вредоносные программы имитируют инициализацию настроек или начало процесса работы, затем демонстрируют сообщение, говорящее об ошибке или невозможности выполнить запрошенное действие. Одновременно с этим троянцы выполняют сбор информации из телефонной книги пользователя и незаметно для него отправляют полученные данные на удаленный сервер.

Примечательно, что некоторые модификации этих новых вредоносных программ получили возможность рассылать по обнаруженным в телефонной книге номерам СМС-сообщения, содержащие ссылку на загрузку соответствующих версий троянцев, что, в свою очередь, увеличивает скорость их распространения и число пострадавших пользователей.

Кроме того, в марте было выявлено несколько новых модификаций вредоносных программ семействаAndroid.SmsSend, а также очередные представители коммерческих шпионских приложений, в частности,Android.Recon.3.origin и Program.Childtrack.1.origin.

Вредоносные файлы, обнаруженные в почтовом трафике в марте

01.03.2013 00:00 - 31.03.2013 23:00		
1	Trojan.Packed	1.32%
2	Trojan.Inject2.23	1.28%
3	Trojan.Necurs.97	1.27%
4	JS.Redirector.155	1.07%
5	Trojan.PWS.Stealer.1932	0.92%
6	Win32.HLLM.MyDoom.54464	0.63%
7	BackDoor.Slym.1498	0.54%
8	Win32.HLLM.MyDoom.33808	0.48%
9	Trojan.PWS.Panda.547	0.44%
10	JS.Redirector.186	0.41%

11	Trojan.Packed.196	0.40%
12	SCRIPT.Virus	0.33%
13	BackDoor.IRC.NgrBot.42	0.33%
14	Trojan.PWS.Panda.655	0.31%
15	Trojan.Siggen5.528	0.30%
16	Trojan.DownLoader1.64229	0.28%
17	Exploit.CVE2012-0158.19	0.26%
18	Trojan.KillProc.22394	0.26%
19	Win32.HLLM.Graz	0.26%
20	Win32.HLLM.Beagle	0.25%

Вредоносные файлы, обнаруженные в марте на компьютерах пользователей

01.03.2013 00:00 - 31.03.2013 23:00		
1	SCRIPT.Virus	0.65%
2	Adware.Downware.915	0.63%
3	Tool.Unwanted.JS.SMSFraud.26	0.54%
4	JS.IFrame.387	0.44%
5	Adware.Downware.179	0.44%
6	Tool.Unwanted.JS.SMSFraud.10	0.37%
7	JS.Redirector.175	0.34%
8	Trojan.Fraudster.407	0.33%
9	Trojan.Fraudster.394	0.33%
10	Adware.Webalta.11	0.33%
11	Trojan.Fraudster.424	0.31%
12	Adware.Downware.910	0.30%
13	Win32.HLLW.Shadow	0.28%
14	Adware.InstallCore.99	0.28%
15	Trojan.PWS.SpySweep.389	0.27%
16	Tool.Skymonk.12	0.26%
17	Win32.HLLW.Autoruner.59834	0.26%
18	Adware.InstallCore.53	0.26%
19	Tool.Skymonk.11	0.25%
20	JS.Redirector.179	0.24%

Источник: http://news.drweb.com

Хакеры похитили и опубликовали персональные данные, принадлежащие директору Секретной службы США.

Секретная служба США, отвечающая за охрану первых лиц государства, ведет расследование по факту хищения персональной информации, принадлежащей ее директору Джулии Пирсон. Как заявил сегодня представитель этого ведомства, в настоящее время оно проводит проверку появившихся сообщений о том, что группа хакеров взломала личные данные Пирсон и опубликовала их в Интернете. Об этом сообщило агентство ИТАР-ТАСС.

Сведения о личной информации Пирсон, включающей номера телефонов, кредитных карт и социального страхования, появились в открытом доступе на сайте www.exposed.re. Ранее на ресурсе с таким же названием, но расположенном в другой доменной зоне, были выложены персональные данные вице-президента США Джозефа Байдена, первой леди Мишель Обамы, министра юстиции Эрика Холдера, директора ФБР Роберта Мюллера, экс-госсекретаря Хиллари Клинтон, бывшего губернатора штата Калифорния Арнольда Шварценеггера и некоторых других известных американцев.

В пресс-службе минюста США подтвердили, что по факту случившегося соответствующее расследование также начало ФБР.

В данный момент неизвестно, является ли обнародованная в Интернете информация подлинной. Как удалось выяснить некоторым СМИ, опубликованные на сайте номера телефонов далеко не всегда принадлежат тем владельцам, которых указали хакеры.

Президент США Барак Обама объявил о назначении Пирсон директором Секретной службы на прошлой неделе. Она стала первой женщиной-руководителем в истории ведомства.

Источник: http://www.bezpeka.com

отдел по размещению рекламы
journal@ualinux.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.

Все права на материалы принадлежат их авторам и опубликованы в открытых источниках.
Адреса на оригинальные источники публикуются.

{
Для размещения рекламы обращаться

по тел.:
+38 (048) 770-0425
+38 (094) 995-4425

Или на email: journal@ualinux.com
}