

## ЗАЩИТА СЕТЕЙ ПРОТИВ БЫСТРО МЕНЯЮЩИХСЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



*Основной проблемой построения надежных систем защиты информационных ресурсов предприятий сегодня становится работа на опережение против быстро распространяющихся по вычислительным сетям угроз безопасности, таких как вирусы, черви, спам и фишинговые компании, программы-шпионы и др. В данной статье будут рассмотрены вопросы использования ресурсов мировой сети лабораторий по предупреждению сетевых атак SophosLabs™, дающей своевременный и адекватный ответ быстро распространяющимся угрозам и позволяющей поддерживать непрерывность бизнеса. Также будут освещены вопросы уникального «генетического» подхода к анализу вредоносного кода и спамовых рассылок – технологии Sophos Genotype™ – обеспечивающей проактивную защиту против неизвестных видов угроз еще до выпуска обновлений сигнатурных баз.*

на определенном этапе письмо из рассылки все-таки достигнет конечного получателя, несмотря на установленный на его почтовом сервере антиспамовый фильтр.

В текущей ситуации, кроме личных амбиций авторы вредоносных кодов и спамовых рассылок получают еще и финансовую мотивацию, подстегивающую их к координации взаимных действий, усугубляющих в итоге опасность информационных атак. Случайные вандальные действия отдельных вирусописателей сегодня переросли в целую криминальную индустрию, которая набирает обороты и с каждым днем генерирует все более изощренные методы. В результате этого вредоносный код, имеющий раньше только деструктивные или показательные цели, перерос в приложения, преследующие совершенно определенные коммерческие интересы, такие как захват контроля над узлами информационных систем компаний, кража конфиденциальной информа-



### Ускорение темпов распространения угроз

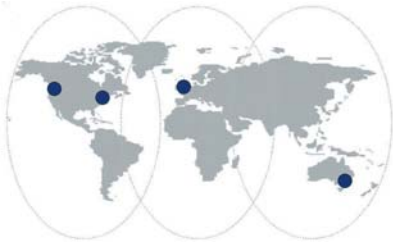
В современном мире существует тенденция к ускорению передачи данных, наращиванию информационных потоков, что одновременно дает возможность быстрее распространяться угрозам информационных систем, таким как вирусные или спамовые рассылки. Обычно, производители систем защиты в ситуации появления новой вредоносной рассылки реагируют на новую угрозу скорейшим выпуском сигнатурных баз или новых алгоритмов распознавания, которые помогли бы противостоять новой угрозе. В ответ авторы вредоносных рассылок видоизменяют тип рассылки (например, модифицируют вирус так, чтобы он не распознавался текущими алгоритмами) настолько быстро, насколько это возможно, и делают это в течение нескольких итераций, производимых в короткое время. В итоге, в какой-то момент из-за некоторой инерционности процесса обновления систем защиты, авторы вредоносных рассылок могут достичь своей цели на определенной итерации, и система защиты будет преодолена. Например, авторы рассылок спама производят рассылку одних и тех же по содержанию писем в несколько потоков, в каждом из которых несколько видоизменяют параметры рассылки, в результате чего

и т.п. Троянские программы и программы-шпионы (spyware), такие как кейлоггеры например, сейчас являются первоочередной угрозой, над анализом и противостоянием которой сосредоточили свои силы специалисты SophosLabs™ – глобальной сети аналитических лабораторий британской компании Sophos™.

### Эффективные методы противостояния новым угрозам

В качестве следующего витка эволюции информационных угроз появились приложения так называемого «нулевого дня». В ответ на это системы эффективной информационной защиты сегодня должны комбинировать в себе как традиционные сигнатурные методы определения новых вирусов и спама, так и превентивные методы, основанные на определении «генотипа» угроз, с целью противостояния их новым модификациям. Также несомненно являются эффективными интеграционные подходы к построению систем защиты, основанные на использовании технологий защиты от разных производителей на разных уровнях информационной системы компаний. Такой метод эффективен потому как не всегда можно полностью определить все деструктивные возможности

той или иной угрозы. Например, рассылка вируса Wofra имела перед собой задачу произвести атаку, используя уязвимости Интернет-браузеров, целью которой было считывание некоторых характеристик конечных рабочих станций, позволяющих организовывать более эффективные вирусные и спамовые атаки в последующем. Однако для эффективного противостояния данной угрозе следовало в информационной системе предусмотреть защиту не только конечных рабочих станций, но и защиту на уровне серверов, которая не позволила бы вредоносному коду в принципе добраться до целевых компьютеров. В результате комбинации интеграционных технологий



совмещенных с экспертными оценками специалистов по информационной безопасности в SophosLabs™ могут предложить серьезный ответ нарастающему уровню угроз вне зависимости от того, насколько сложными и комбинированными они являются.

Существует прямая зависимость распространения угроз по информационным сетям от начала рабочего дня в разных часовых поясах. Это объясняется тем, что корпоративные компьютеры, на которые чаще всего организованы атаки, включаются, а значит могут быть атакованы, в основном в рабочее время. Можно даже сказать что угрозы «следуют за солнцем», это означает, что свое начало волны опасных рассылок берут в Японии, Азии и Австралии, затем следуют в Европу и Африку, и заканчивают свой путь в странах Америки. Если лаборатория по отслеживанию информационных атак находится в Европе, то она сможет с определенной долей вероятности своевременно защитить информационную сеть в Европе и Америке, однако в странах Азии ее работа будет менее эффективна. Для решения данной проблемы в SophosLabs™ была реализована стратегическая концепция по разделению карты мира на основные зоны: Азия и страны Тихоокеанского региона, Европа, западное и восточное побережье Северной Америки, как показано на рисунке. Такое распределение аналитических центров дает дополнительный уровень защиты, например, новая вредоносная рассылка может быть распознана центром SophosLabs™ в Австралии и нивелирована еще до того, как в странах Северной Америки и Европы начнется рабочий день и будут включены потенциально атакуемые компьютеры.

В аналитических центрах Sophos ежемесячно анализируются десятки тысяч образцов вредоносного кода и миллионы почтовых сообщений в день для предотвра-

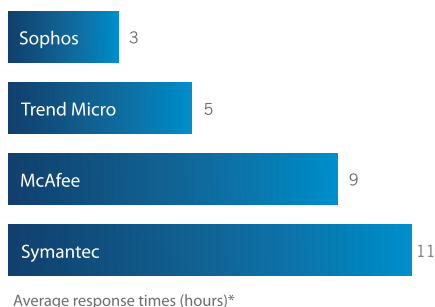
щения спамовых рассылок. В SophosLabs™ используется ряд автоматизированных систем, таких как машина Mentor, которая в автоматическом режиме исследует и распознает вредоносный код, что повышает скорость реагирования на очередную информационную угрозу. База Данных Sophos, содержащая сигнатуры и алгоритмы определения вредоносного кода, пополняется каждый день вот уже более 20-ти лет при помощи распределенной сети аналитических лабораторий, анализирующих общемировую ситуацию в информационном пространстве 24 часа в сутки каждый день. В результате слаженной работы автоматизированных систем и команды опытных экспертов новые спамовые рассылки распознаются несколько раз в час. Такая высокая скорость реакции на рассылки считается наивысшей среди ряда крупнейших производителей средств информационной защиты в мире. В результате система лабораторий SophosLabs™ на сегодня признана наиболее мощным орудием защиты против современного кибер-криминала. Способность анализировать общемировую ситуацию дает возможность Sophos предлагать ряд расширенных сервисов в дополнение к своим продуктам. Сервис Sophos ZombieAlert™ дает возможность организациям-подписчикам с помощью Sophos выявлять случаи, когда произошло заражение троянскими программами их рабочих станций, в результате чего их информационная система становится невольным соучастником спамовых рассылок, или соучастником организованных атак типа «отказ в обслуживании» (Denial of Service, DOS). Сервис Sophos PhishAlert™ означает предоставление дополнительных возможностей для организаций по защите от фишинговых атак, путем прямого отключения фишинговых (поддельных) сайтов, на которых упоминается имя компании-подписчика, либо давая возможность своевременно предупредить клиентов компании-подписчика о том, что данный сайт не имеет никакого отношения к ее деятельности.

### Современные технологии защиты

Базой в работе сети лабораторий SophosLabs™ является ряд технических новинок и передовых технологий, позволяющих в максимально оперативном режиме реагировать на новые угрозы и выпускать соответствующие обновления:

- Dynamic Code Analysis™ – набор технологий, используемых в движке Sophos, используемом для распознавания вредоносных кодов, а также некоторых их семейств и модификаций;
- Algorithmic pattern-matching – исходный образец проверяется по базе уже известных сигнатур вредоносных кодов, что повышает скорость реакции системы на известные вирусы;
- Эмуляция – новая технология для детектирования полиморфных вирусов, которые весьма сложно определить по сигнатурной базе, так как в них используется технология шифрования одного и того же исходного кода вируса при каждой новой рассылке;
- Специализированные технологии – комбинация частных технологий распознавания по различным косвенным критериям: двойные расширения присылаемых файлов (например .jpg.txt), либо расширение файла не соответствует его реальному формату (например, запускаемый файл приложения, имеющий расширение .txt) и др.

Распознавание спама происходит на базе набора следующих технологических приемов:



Average response times (hours)\*

- Сканирование содержания письма – проверка письма на основе его содержания при помощи сигнатур (в том числе графических);

- Детектирование зашумлений – многие спамеры используют специальные методы зашумления содержаний писем для того, чтобы сигнатурные и более простые методы (например, по ключевым словам) не могли детектировать адекватно письмо; в Sophos используются специальные методы выявления такого рода зашумлений, которые позволяют с большей вероятностью предупредить спамовые рассылки;

- Sender reputation filtering – блокирование писем по IP-адресам отправителя, занесенным в черный список – Sophos IP Block List, содержащим адреса известных источников спамовых рассылок;

- Детектирование по контактной информации/URI-фильтр – обычно компании, использующие спамовые рассылки в качестве рекламы своих продуктов и услуг, оставляют в письмах обратные адреса, телефоны, домены и т.п., по которым с ними можно связаться; в Sophos используется специальный фильтр по такого рода информации;

- Контрольные суммы – в Базу Данных Sophos заносятся контрольные суммы писем, определенных другими методами как спам, это помогает построить эффективную защиту в случае, если рассылка произойдет в несколько этапов; обычно эта технология используется совместно с технологией Sophos Genotype™, позволяющей в данном случае определить, что письмо исходит из очередной волны рассылки, в которой каждое последующее письмо в очередной волне слегка модифицируется и его контрольная сумма меняется;

- Эвристика – набор эвристических правил определения спама помогает отслеживать вредоносные рассылки вне зависимости от языка, на котором написаны сами письма, с минимальной вероятностью ложного срабатывания;

- Автоматическая система настройки – автоматизированная система синтеза различных правил определения спама позволяет гибко реагировать на новые типы рассылок, путем создания новых методик определения вредоносных писем на основе уже имеющегося набора исходных правил.

### Распутывая спирали

Набор описанных методик позволяют системам комплексной защиты от компании Sophos находиться в одном ряду с ведущими мировыми производителями по уровню надежности и скорости реагирования на информационные угрозы. Кроме того, технология Sophos Genotype – используемая как в системах защиты рабочих станций и файловых серверов, так и в системах защиты внешнего периметра корпоративных информационных

### ТЕХНОЛОГИЯ ОПРЕДЕЛЕНИЯ ВИРУСОВ SOPHOS GENOTYPE™ НАЦЕЛЕНА НА ОПРЕДЕЛЕНИЕ СТЕПЕНИ ОПАСНОСТИ АНАЛИЗИРУЕМОГО ОБРАЗЦА ПО ЕГО «ГЕНОТИПУ», ОДНОЗНАЧНО ОПРЕДЕЛЯЮЩЕМУ К КАКОМУ СЕМЕЙСТВУ ВИРУСОВ ОН ОТНОСИТСЯ

систем – позволяет создавать проактивные системы защиты информационных ресурсов компаний. Такие системы представляют собой надежный щит против информационных атак как известных, так и неизвестных типов, образцы которых еще не были обработаны антивирусными лабораториями. Технология Genotype интегрирована

также в ядро продуктов Sophos, позволяющее отслеживать и предупреждать спамовые рассылки. Истоки технологии берут свое начало из самоорганизующегося мира живых организмов в природе. В биологии слово

### ТЕХНОЛОГИЯ SOPHOS GENOTYPE™ ПОЗВОЛЯЕТ ИНФОРМАЦИОННОЙ СИСТЕМЕ ОСТАВАТЬСЯ ЗАЩИЩЕННОЙ ПРОТИВ НОВЫХ УГРОЗ ЕЩЕ ДО МОМЕНТА, КОГДА ЛАБОРАТОРИИ SOPHOS LABS™ УСПЕЮТ СРЕАГИРОВАТЬ НА ЕЕ ПОЯВЛЕНИЕ

«генотип» означает некоторый набор генов, определяющий индивидуальные характеристики и отличия каждого живого организма. Фактически речь идет о спирали молекулы ДНК, через компоненты которой передается наследственная информация от предыдущих поколений живых организмов последующим. Технология Sophos Genotype позволяет выявить «наследственные характеристики» новых разновидностей вирусов и спама, на основе знаний об их предыдущих реализациях, и таким образом детектировать новые угрозы информационной безопасности несигнатурным методом.

### Детектирование вирусов при помощи Sophos Genotype™

Обычно авторы вредоносных кодов для создания новых вирусов, троянов и т.п. используют уже накопленную базу исходных кодов их более ранних версий. Например, на сегодня существуют тысячи различных вариантов вируса Rbot. В случае если в новую версию добавлена новая функциональность, все равно часть кода вируса сохраняет некоторые характеристики своего прародителя, либо того семейства вирусных программ, на базе которого был создан новый образец. На базе этого постулата и построена основная функциональность механизма Genotype – определение, к какому семейству относится новый образец, при помощи анализа «генотипа» его кода. Принципиальным отличием механизма Genotype от эвристических методов является то, что на стадии разработки самой технологии в неё заложено отсутствие возможности ложных срабатываний.

Не только вредоносные программы имеют свой «генотип», любая программа может быть охарактеризована с использованием данного параметра. Однако, «генотип» вредоносного кода значительной степени отличается от безвредной программы в силу тех функций, которые он призван выполнять. Кроме того «генотип» вируса из одного семейства может серьезно отличаться от «генотипа» вируса из другого семейства, что позволяет определять не только степень его опасности, но и классифицировать его.

Вот некоторые типы «генов», которые могут свидетельствовать в пользу того, что образец тестируемого приложения является вредоносным:

- попытки копировать самого себя в системные директории жесткого диска;
- попытки использовать известные уязвимости операционных систем;
- попытки изменить ключи реестра таким образом, чтобы программа стартовала в автоматическом режиме при каждой авторизации пользователя на рабочей станции;
- попытки сканирования жесткого диска с целью пополнения базы данных адресов электронной почты, которая затем используется для рассылки спама;
- попытки пересылки своей копии в качестве приложения к отсылаемым письмам электронной почты.

Ранжированный набор подобных генов дает возможность практически стопроцентно определить код как вредоносный. А гены, определяющие отношение

#### ПРИМЕРЫ РАБОТЫ ТЕХНОЛОГИИ SOPHOS GENOTYPE™

- 100% ДЕТЕКТИРОВАНИЕ ВСЕХ ВЕРСИЙ APRIBOT
- 100% ДЕТЕКТИРОВАНИЕ ВСЕХ ВЕРСИЙ VABA

тестируемого приложения к одному из семейств вирусов дают однозначное определение его типа и наиболее эффективного метода противостояния ему. В случае если вирус был обнаружен при помощи технологии Genotype, он соответствующим образом маркируется в итоговых отчетах о сканировании (например, W32/Rbot-Gen).

#### Детектирование спама при помощи Sophos Genotype™

Спамеры постоянно разрабатывают новые технологии обхода существующих систем защиты от рассылок.

#### СИСТЕМА ПРОТИВОСТОЯНИЯ СПАМОВЫМ РАССЫЛКАМ НА ОСНОВЕ ТЕХНОЛОГИИ SOPHOS GENOTYPE СПОСОБНА ЭФФЕКТИВНО СНИЖАТЬ СПАМ-ТРАФИК, РАСПОЗНАВАЯ КАК СТАТИЧЕСКИЕ ТАК И ДИНАМИЧЕСКИЕ АТТРИБУТЫ СПАМОВЫХ ПИСЕМ

Один из таких методов заключается в рассылке спама с подменой IP-адреса отправителя на адрес одной из открытых проху-систем в Интернете, обходя таким образом фильтры, использующие технологию блокирования рассылок по IP-адресам. Для обхода так называемых «репутационных» фильтров, спамеры ежедневно регистрируют сотни новых доменов для каждой новой рассылки, осложняя тем самым работу по противодействию данной угрозе. Также используются другие методы:

- использование зашумления содержания писем;
- использование графики в письмах, которая значительно видоизменяется от одной волны к другой, изменяя тем самым контрольную сумму письма;
- использование в тексте писем случайных слов и фраз и т.п.

Тем самым спамеры создают массовые рассылки в несколько кратковременных волн, в каждой из которых последующее письмо, отправляемое на один и тот же адрес, несколько отличается от предыдущего. Данный метод делает практически бесполезными антиспам-фильтры, работающие на сигнатурных методах или использующих другие простые правила, основанные на анализе содержания письма.

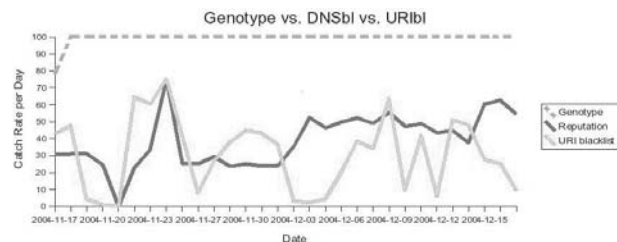
Одним из самых распространенных новых методов создания разных писем одного содержания в рамках одной рассылки, является использование зашумления графических элементов, используемых в письме. Можно изменить буквально несколько пикселей в одной из картинок, при этом изображение все равно останется читабельным, но само письмо изменится. Кроме того, становится все менее популярным оставление в письме обратных координат рекламодателя, использующего массовые рассылки, что снижает эффективность определения спамовых писем по номерам телефонов или адресам веб-сайтов, оставленных в них.

Однако не стоит считать, что «война проиграна» и спам больше нельзя детектировать и блокировать. Все письма в рамках одной рассылки имеют некоторый набор общих атрибутов, по которым их можно классифицировать, например, размеры писем или их контрольные

суммы изменяются незначительно в рамках определенных границ, или заголовки писем могут в некоторой степени совпадать. Основываясь на данных правилах эксперты SophosLabs™ для каждой рассылки создают ее уникальный «генотип», на основе которого все разновидности писем из данной рассылки можно однозначно квалифицировать как спам. Примеры совпадающих атрибутов писем в рамках одной рассылки могут быть такими:

- в письме найдена ссылка на вебсайт, которая заканчивается расширением «.aspx», после которой стоит знак «?» и от 5-ти до 7-ми цифр;
- HTML-часть письма включает в себя таблицу с тремя строками на розовом фоне.

Письма, атрибуты которых совпадают с «генотипом» рассылки, идентифицируются автоматически как спамовые. Некоторые «генотипы» массовых рассылок являются кратковременными и могут эффективно противостоять только одной спамовой рассылке, другие же могут идентифицировать целый ряд рассылок на протяжении длительного времени. Комбинируя «генотипный» метод идентификации писем с другими алгоритмами распознавания, можно снизить спам-трафик на 95%. Технология Genotype используется обычно в тех случаях, когда другие методы идентификации не столь эффективны. Сравнительные характеристики методов Genotype, URI-анализа и «репутационного» фильтра показаны на нижеследующем рисунке. На графике можно



увидеть степень эффективности различных алгоритмов на одном типе массовой рассылки в течение длительного времени. Как видно из рисунка, единожды определив «генотип» рассылки с помощью технологии Genotype можно достичь 100 % эффективности, тогда как другие методы не обладают такой устойчивостью и надежностью определения.

В итоге можно заключить, что на единичных рассылках эффективность алгоритма Sophos Genotype достигает всего 5%, однако при массовой рассылке в несколько волн с видоизменяемыми письмами эффективность Genotype может достигать 100%, в то время как другие алгоритмы в такой ситуации оказываются гораздо менее эффективными.

#### Заключение

Компания Sophos, обладая 20-тилетним опытом разработки эффективных технологий защиты против угроз информационных систем в корпоративном секторе, сегодня может предложить наиболее эффективный подход к построению надежных систем защиты, комбинирующий в себе не только передовые технологии, но и постоянный мониторинг за новыми угрозами, осуществляемый мировой сетью лабораторий SophosLabs™. 35 миллионов пользователей компании Sophos в 150-ти странах мира уже смогли оценить уровень надежности и доверять защите своих данных старейшей компании в мире, работающей в области информационной безопасности.