Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с.78-85.

Поступила: 20.09.2017
Окончательный вариант: 10.10.2017

© УлГУ

УДК 004.056

Прогнозирование угроз информационной безопасности путем анализа хакерских форумов

Смагин А. А. [1,*]***, Полетаев В. С.*** [1]

[*] smaginaa1@mail.ru
[1]УлГУ, Ульяновск, Россия

В данной статье представлены анализ актуальных угроз информационной безопасности в 2016-2017 годах и методика определения угроз. Проанализированы наиболее популярные программные платформы для создания интернет-форумов. Определены тематики хакерских интернет-форумов, осуществлено их сопоставление с актуальными угрозами информационной безопасности.

Ключевые слова: *угрозы, информационная безопасность, интернет-форум, программная платформа.*

Введение

В настоящее время глобальные информационные сети оказывают растущее влияние на все новые и новые сферы нашей жизни. Происходит стремительное развитие единого глобального информационно-телекоммуникационного пространства, формируются новые социальные группы, оказывается существенное влияние на традиционный образ жизни людей по всему миру. К сожалению, на сегодняшний день наблюдается стремительный рост не только новых технологий, обеспечивающих информационную потребность человечества, но и разнообразия компьютерных атак, осуществляемых с их помощью.

В данной статье речь идет об общедоступных источниках данных об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, а также результатах специально проведенных исследований по выявлению угроз безопасности информации. Целью рассмотрения указанного вопроса является прогнозирование новых угроз информационной безопасности.

Актуальность темы определяется несколькими группами факторов. С одной стороны, системы обнаружения атак на компьютерные сети уже давно применяются как одно из средств защиты информации. С другой стороны аналитические обзоры компаний, специализирующиеся в сфере интернет-технологий и защиты информации, такие как Symantec, Trustware, KasperskyLabs показывают, что за последние несколько лет количество атак на различные информационные системы продолжает расти, а средства, которыми пользуются злоумышленники, превращаются из простых хакерских инструментов в серьезное информационное оружие. [1, 2, 3]

На сегодняшний день системы обнаружения атак представляют собой программные и аппаратно-программные решения, которые автоматизируют процесс сбора, хранения, анализа и контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализируют эти события в поисках признаков нарушения информационной безопасности. [4].

1. Анализ угроз информационной безопасности в 2016-2017 годах

По прогнозам экспертов компании Positive Technologies в 2017 году ожидается на 30% больше по сравнению с 2016 годом инцидентов по информационной безопасности в финансовой сфере и более эффективные сценарии социальной инженерии.

Эксперты Positive Technologies ежедневно изучают и анализируют инциденты в различных организациях. Нет ни одной сферы общественной деятельности, которая не была бы интересна хакерам. На одни компании нападают в поисках конфиденциальной информации, на другие - с целью нанесения финансового ущерба, а кто-то и вовсе становится случайной жертвой массовой атаки.

Positive Technologies получена статистика по отраслям компаний, пострадавшие от компьютерных атак в 2016 и 2015 годах:

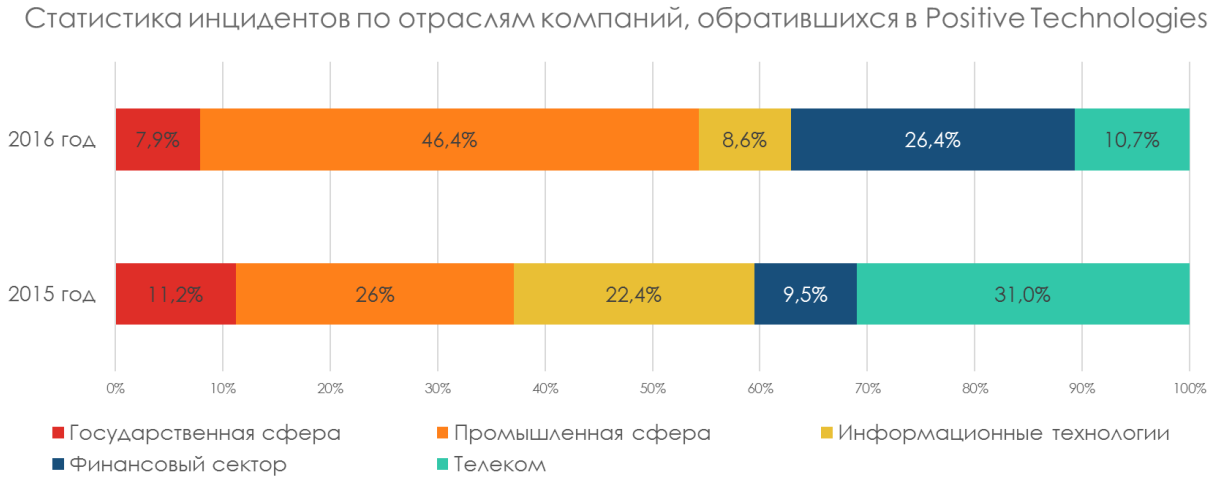

Рис. 1 Сравнительный график (по отраслям) компаний — жертв компьютерных инцидентов

В 2016 году пострадало почти в три раза больше промышленных компаний, столкнувшихся с инцидентами информационной безопасности, чем было в 2015 году. Причем компьютерные атаки на промышленные объекты составили около 37% от общего числа произошедших инцидентов за последние два года.

Злоумышленники атаковали объекты критической инфраструктуры целенаправленно, причем атаки отличались тщательностью подготовки. Они использовали передовые технологии и сложные вредоносные программы, а инструменты разрабатывались с учетом специфики конкретной целевой системы. Такие атаки требуют значительных финансовых и временных затрат.

Целевые атаки на объекты критической инфраструктуры могут приводить к серьезным последствиям и даже потенциально к человеческим жертвам, но наиболее частым последствием является утечка конфиденциальной информации.

В 2016 году Positive Technologies отметила новый всплеск компьютерных атак, направленных на организации финансовой сферы. Такие инциденты заняли более 26% от общего числа инцидентов, случившихся в 2016 году. Более того, в 2017 году прогнозируется 30% рост числа инцидентов в банках, процессинговых и брокерских компаниях, а также организациях, занимающихся денежными переводами.

Если при атаках на промышленные организации злоумышленникам, как правило, нужна была ценная информация, то атаки на компании финансовой сферы — банки и биржи — совершались в целях личного обогащения. При этом в погоне за максимальной выгодой преступники начали вместо клиентских счетов атаковать сами банки.

Рис. 2 Распределение типов атак, применяемых злоумышленниками

Практически в половине (45%) случаев при реализации атак злоумышленники использовали вредоносные программы. При этом в 27% всех атак имело место воздействие на пользователей методами социальной инженерии.

Слабым местом в системе защиты любой организации по-прежнему остается недостаточная осведомленность сотрудников в вопросах информационной безопасности. Злоумышленникам это известно, и потому они активно используют социальную инженерию, как при реализации массовых атак, так и в качестве начального этапа целевой атаки. Среди отличий целевых атак от массовых можно выделить действия атакующего в случае неудачи: если массовые атаки в случае отсутствия реакции со стороны жертвы прекращаются, то целевые продолжаются, но уже с использованием других методов или векторов.

Три четверти компьютерных атак, с которыми сталкивались специалисты Positive Technologies в 2015-2016 годах, оказались целевыми. Однако встречались и такие ситуации, когда к нарушениям работы инфраструктуры хакеры не имели никакого отношения.

Рис. 3 Типы событий ИБ, зафиксированных специалистами Positive Technologies в 2015-2016 годах

Таким образом, согласно выводам экспертов Positive Technologies в последние годы в сфере информационной безопасности сформировались следующие тренды:

- в погоне за максимальной выгодой злоумышленники атакуют финансовые организации: под прицелом оказываются банки и биржи. Преступники мыслят глобально. Украсть денежные средства целого банка выгоднее, чем счет одного клиента.

- в случае атаки на промышленные предприятия под угрозой разглашения оказывается конфиденциальная информация, а иногда и государственная тайна. Такие атаки требуют хорошей подготовки и финансирования, поскольку применяются передовые технологии и программное обеспечение, разработанное с учетом специфики конкретной целевой системы.

- социальная инженерия стала для злоумышленников «отмычкой ко всем дверям». Отраслевая принадлежность пострадавших компаний не имеет значения, поскольку исходным вектором атак является воздействие на сотрудников: их убеждают открыть почтовые вложения, ответить на пару вопросов по телефону, ввести учетные данные на поддельном сайте и т.п.

- процесс управления обновлениями программного обеспечения в компаниях очень длителен и может затянуться на годы. В этой связи в атаках преобладает использование известных уязвимостей [4].

2. Методика определения угроз информационной безопасности

Вопросы обеспечения безопасности информационных систем в настоящее время рассматриваются на государственном уровне, издаются нормативные акты, регламентирующие порядок защиты информации, создаются учреждения, координирующие указанную деятельность и осуществляющие надзор за соблюдением установленных норм. В 2015 году Федеральной службой по техническому и экспортному контролю Российской Федерации в результате проведенных научно-исследовательских работ разработана «Методика определения угроз безопасности информации в информационных системах». Документ устанавливает единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах, защита которых обеспечивается в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17, утверждающим Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [5].

В соответствии с Методикой, описание модели угроз безопасности информации содержит следующие разделы:

1. Общие положения.
2. Описание информационной системы и особенностей ее функционирования.
2.1. Цель и задачи, решаемые информационной системой.
2.2. Описание структурно-функциональных характеристик информационной системы.
2.3. Описание технологии обработки информации.
3. Возможности нарушителей (модель нарушителя).
3.1. Типы и виды нарушителей.
3.2. Возможные цели и потенциал нарушителей.
3.3. Возможные способы реализации угроз безопасности информации.
4. Актуальные угрозы безопасности информации.

Модель угроз безопасности информации создается в целях установления того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе. Кроме того, определяется, приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к на-

ступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора.

Определение угроз безопасности информации предусматривает реализацию непрерывного процесса, в рамках которого определяется область применения процесса определения угроз, идентифицируются источники угроз и угрозы безопасности информации, оценивается возможность реализации угроз и степень возможного ущерба в случае такой реализации, осуществляется мониторинг (периодический пересмотр) и переоценка угроз безопасности информации.

В обобщенном виде угрозы безопасности информации характеризуются:

- источниками угроз;
- факторами, обуславливающими возможность реализации угроз;
- способами реализации угроз;
- последствиями от реализации угроз безопасности информации.

В ходе эксплуатации информационной системы регулярно проводится анализ изменения угроз безопасности информации, а актуальные угрозы безопасности информации подлежат периодической переоценке. Случаи пересмотра (переоценки) угроз безопасности информации , как минимум, осуществляется в случаях, указанных в табл. 1.

Таблица 1. Критерии необходимости переоценки угроз безопасности информации

Переоценка угроз безопасности информации необходима в случае	изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации
	изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало возникновение новых угроз безопасности информации
	выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих
	появления сведений и фактов о новых возможностях нарушителей

Для определения угроз безопасности информации могут использоваться опубликованные в общедоступных источниках данные об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, а также результаты специально проведенных исследований по выявлению угроз безопасности информации. Автоматизация процесса выявления и анализа указанных сведений является составляющим компонентом системы мер по защиты информации в информационной системе.

3. Форумы хакерской направленности

В глобальной сети Интернет в настоящее время существует значительное количество дискуссионных информационных ресурсов (далее - форумов), посвященных вопросам

информационной безопасности и механизмам получения несанкционированного доступа к компьютерной информации. В части из них преобладают участники, заинтересованные в обмене сведениями о защите информации, в других – интересующиеся способами совершения компьютерных атак. Указанные форумы могут рассматриваться в качестве общедоступных источников данных об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, на основании анализа сообщений которых может приниматься решение о необходимости пересмотра модели информационной безопасности, а также формироваться прогноз о возникновении новых угроз информационной безопасности.

Наиболее популярными темами, обсуждаемыми в настоящее время на хакерских форумах являются:

- программирование, направленное на реализацию угроз информационной безопасности;
- программное обеспечение, которое используется при организации компьютерных атак;
- социальная инженерия с использованием информационных технологий;
- противоправные действия в финансовой сфере;
- созданием вредоносных компьютерных программ;
- защита информации;
- вопросы обеспечения анонимности при совершении противоправных действий с использованием информационных технологий.

Перечисленные темы соответствуют категориям актуальных в настоящее время угроз информационной безопасности.

При организации форумов, как правило, используются наиболее популярные программные платформы:

- Invision Power Board (IPB)
- vBulletin
- PunBB
- Simple Machines Forum (SMF)
- Vanilla
- XenForo
- phpBB

Задача по сбору сообщений пользователей форумов является алгоритмически разрешимой, существуют компьютерные программы, обладающие указанными функциональными возможностями.

Заключение

Тематические интернет-форумы имеют высокую популярность среди пользователей, интересующихся определенными предметными областями. Как правило, события, происходящие в определенной предметной области, находят свое отражение на посвященных им дискуссионных интернет-площадках. Указанный фактор позволяет прогнози-

ровать возникновение новых событий интересующей предметной области на основе анализа потока текстовых сообщений тематических интернет-форумов.

Результаты анализа создаваемых на хакерских форумах сообщений, могут быть использованы в качестве критериев при прогнозировании возникновения новых угрозах информационной безопасности.

Получая прогноз о возникновении новой угрозы информационной безопасности, специалист по защите информации имеет возможность оценить степень угрозы для защищаемых им информационных ресурсов, пересмотреть модель угроз информационной безопасности и предпринять меры по нейтрализации возможных уязвимостей.

Список литературы

1. http://www.securelist.com/ (дата обращения 18.09.2017).
2. http://scm.symantec.com/ (дата обращения 18.09.2017).
3. http://www.trustwave.com/ (дата обращения 18.09.2017).
4. http://anti-malware.ru/ (дата обращения 18.09.2017).
5. http://fstec.ru/ (дата обращения 18.09.2017).