УДК 004.492.3

М. А. Ляшков[*]

МОДЕЛЬ СИСТЕМЫ МОНИТОРИНГА УТЕЧЕК ИНФОРМАЦИИ И НЕБЕЗОПАСНЫХ КОНФИГУРАЦИЙ

Предлагаемая система базируетя на *OSINT*-методологии. *OSINT* (англ. *Open source intelligence*) – разведка на основе открытых источников. Под термином «конкурентная разведка» в этой работе следует понимать сбор и обработку данных из разных источников для выработки управленческих решений с целью повышения конкурентоспособности коммерческой организации, проводимые в рамках закона и с соблюдением этических норм. Дорками называют специальные запросы в поисковые системы для облегчения нахождения того или иного контента в Интернете. Так же при разработке используется *Shodan* [1]. *Shodan* – поисковый движок, собирающий метаинформацию о службах, запущенных на портах 21 (*FTP*), 22 (*SSH*), 23 (*Telnet*), 25 (*SMTP*), 53 (*DNS*), 80 (*HTTP*), 81 (*HTTP*), 110 (*POP3*), 37 (*NetBIOS*), 143 (*IMAP*), 161 (*SNMP*), 443 (*HTTPS*), 445 (*SMB*), 993 (*IMAP + SSL*), 995 (*POP3 + SSL*), 1023 (*Telnet*), 1434 (*MS-SQL*), 2323 (*Telnet*), 3306 (*MySQL*), 3389 (*RDP*), 5432 (*PostgreSQL*), 5560 (*Oracle*), 5900 (*VNC*), 6379 (*Redis*), 8080 (*HTTP*), 8443 (*HTTPS*) и др. Полный список таких портов содержит

[*] Работа представлена в отборочном туре программы У.М.Н.И.К. 2015 г. в рамках Десятой межвузовской научной студенческой конференции ассоциации «Объединенный университет им. В. И. Вернадского» «Проблемы техногенной безопасности и устойчивого развития» и выполнена под руководством канд. техн. наук, доцента В. А. Гриднева.

40 наименований. Для более детального анализа конфигурации веб-сервера используется *GHDB* [2] (*GoogleHackingDatabase*). *GHDB* – это открытая база, содержащая дорки, помогающие найти заведомо уязвимые веб-серверы или проверить веб-сервер на наличие известных уязвимостей. Так же составляется база дорков, позволяющая отслеживать утечки конфиденциальной служебной информации и персональных данных (ПДн). Сбор информации бывает пассивным (без прямого контакта с исследуемым объектом) и активным (подразумевающим прямой контакт с исследуемым объектом).

С точки зрения пользователя, предлагаемая система выглядит следующим образом. После регистрации и оплаты выбранного тарифа пользователь задает адреса ресурсов, заказывая их мониторинг. Не все тарифы обязывают пользователя доказывать владение ресурсом, мониторинг которого он заказал. Кроме того, создается список адресов, которые система не мониторит в независимости от тарифа (это, например, ресурсы спецслужб и государственных органов власти). Периодичность мониторинга того или иного ресурса зависит от тарифа. По результатам мониторинга системой составляется отчет и отправляется на почту пользователя. Предполагается бесплатный тариф с сильно урезанными возможностями и несколько платных тарифов.

Бизнес-модели продажи и использования – программное обеспечение, как услуга (*SaaS*). Выбор этой бизнес-модели обусловлен необходимостью поддержки базы знаний (*GHDB* + база дорков для поиска конфиденциальной, служебной информации и ПДн), необходимостью периодического мониторинга и существенным упрощением сопровождения программной реализации. К целевой аудитории данного проекта можно отнести системных администраторов, веб-мастеров, специалистов по информационной безопасности. Основные виды услуг: мониторинг заведомо слабых конфигураций; мониторинг утечек в открытый доступ конфиденциальной служебной информации и ПДн; услуги конкурентной разведки.

Актуальность проекта обусловлена выводами статистических исследований. Например, по данным Аналитического Центра компании *InfoWatch* [3] статистика по утечкам информации за I-е полугодие 2015 г. такова:

– в I полугодии 2015 г. в мире обнародовано 723 случая утечки конфиденциальной информации, что на 10% превышает количество утечек, зарегистрированных за аналогичный период 2014 г.;

– 90% утечек связано с компрометацией персональных данных (за исследуемый период скомпрометированы более 262 млн записей, в том числе платежная информация);

– Россия заняла второе место по числу утечек, ставших достоянием общественности (в исследуемый период зарегистрировано 59 случаев утечки конфиденциальной информации из российских компаний и государственных организаций; число «российских» утечек по сравнению с аналогичным периодом 2014 г. сократилось на 39%);

– транспортные компании, наряду с интернет-сервисами и медицинскими учреждениями, являются основным источником утечек ПДн;

– внешние атаки стали причиной 32% утечек данных (доля таких утечек выросла на 9% по сравнению с показателем I полугодия 2014 г.).

Распределение утечек по вектору воздействия и распределение утечек по источнику представлено на рис. 1 и 2.

Предлагаемая система занимается пассивным сбором информации, комбинируя поисковую выдачу (при запросе с использованием дорков) и метаинформацию о состоянии портов и службах, запущенных на них. Под заведомо уязвимыми конфигурациями понимаются либо службы, имеющие версию ниже оговоренной, с уже опубликованными в открытом доступе эксплоитами, либо отсутствие парольной аутентификации, либо иные варианты (например, определение по отпечаткам заведомо слабых ключей *SSH*). В зависимости от условий конкретного тарифа, система должна будет периодически собирать информацию и

Рис. 1. Распределение утечек по вектору воздействия

Рис. 2. Распределение утечек по источнику

высылать автоматически сгенерированный отчет на почту, высылать отчет после первой проверки, а следующий только при изменении результатов мониторинга.

Приток новых клиентов обеспечивается по технологии «холодных продаж». Система также собирает информацию о ресурсах сети Интернета, на которые не заказывали услуги мониторинга. При обнаружении ресурсов с небезопасной конфигурацией в автоматическом режиме отправляется отчет, содержащий краткий перечень найденных уязвимостей и установленных утечек (без советов по устранению и пояснений технической сути уязвимостей) и предложение к сотрудничеству с перечнем предлагаемых услуг.

Научная составляющая проекта обусловлена объединением существующих баз знаний, комбинированием различных существующих методик (с последующей оценкой их эффективности как по отдельности, так и в совокупности), доработкой базы дорков путем добавления дорков, позволяющих обнаружить утечки информации, сбором и анализом статистики в обезличенном виде в контексте пассивного сбора информации в Интернете.

Коммерческая эффективность проекта определяется наличием ниши в рынке услуг пассивного сбора информации с целью обнаружения утечек в поисковые выдачи и наличием небезопасных конфигураций. Проект ориентирован на малый и средний бизнес, в отличие от существующих решений, ориентированных преимущественно на крупный бизнес. Большинство работ в настоящий момент проводится вручную, что приводит к высокой стоимости услуг. Удешевление в предлагаемом решении происходит за счет автоматизации. При этом ожидается несущественное снижение качества отчетов и объема проводимых исследований. При запросах малого и среднего бизнеса и учета среднестатистических объемов выделяемых бюджетов, предлагаемый вариант является наиболее приемлемым для небольших фирм.

Список литературы

1. *Shodan*. Поисковый движок [Электронный ресурс]. – URL : https://www.shodan.io/ (дата обращения: 30.09.2015).

2. *GHDB* (GoogleHackingDatabase) [Электронный ресурс]. – URL : https://www.exploit-db.com/google-hacking-database/ (дата обращения: 30.09.2015).

3. *Статистика* по утечкам информаци за I полугодие 2015 года Аналитического Центра компании InfoWatch [Электронный ресурс]. – URL : http://www.infowatch.ru/analytics/reports/16340/ (дата обращения: 30.09.2015).

Кафедра «Информационные системы и защита информации»
ФГБОУ ВПО «ТГТУ»