Московский экономический журнал 5/2017

УДК 336.71

Бакаева Малика Магомедовна

ассистент, ФГБОУ ВО «Чеченский государственный университет»

Грозный, Россия.

Bakaeva Malika Magomedovna

Assistant, FGBOU VO «Chechen State University»

Grozny, Russia.

КЛОАКИНГ И БЕЗОПАСНОСТЬ БАНКА

CLOAKING AND SECURITY OF THE BANK

Аннотация. В данной статье раскрывается понятие «клоакинг». Рассматриваются возможности его реализации, используя серверные скрипты и программы. Предложено применять для разграничения контента внешней и внутренней сети. Исследованы методы для определения наличия клоакинга. Анализируется, как защищать банки от клоакинга.

Abstract. In this article, the concept of «cloaking» is revealed. The possibilities of its implementation are considered, using server scripts and programs. It is suggested to apply for differentiation of content of external and internal networks. Methods for determining the presence of cloaking were investigated. Analyzed how to protect banks from cloaking.

Ключевые слова: клоакинг, безопасность банка, серверные скрипты, разграничения контента.

Keywords: cloaking, bank security, server scripts, content delimitation.

Что такое клоакинг?

«Клоакинг» («Cloaking») в переводе с английского языка означает «маскировать», «прятать», «скрывать». Хакеры часто используют клоакинг, позволяющий возвращать код посещаемой страницы в зависимости от категории посетителя (простой пользователь, поисковый робот или бот). Незаметно. Для владельца, его ресурс становится линк-фермой, просто «донором». Отображать оптимизированную страницу для робота поисковой системы, тогда как обычный пользователь увидит другую версию страницы по данному адресу – суть и назначение клоакинга [3, с.43].

При этом, посетитель страницы увидит обычную страницу, а поисковый робот – специально видоизмененную страницу, для максимального повышения соответствия страницы определенным запросам. У видоизмененного варианта страницы в большинстве случаев имеется малоудобный для восприятия человеком внешний вид. Например, так в последнее время маскировались мошенники под мобильное приложение «Сбербанк онлайн». Очень опасное явление для банковской деятельности!

Причина применения такого способа заключается в сложности совмещения привлекательности страницы и для «поисковика», и для пользователя одновременно [10, с.72].

Клоакинг можно реализовать, пользуясь серверными скриптами и программами. Выходные данные формируются серверными скриптами в зависимости от модифицированных параметров, например, параметры адреса и самого запроса. Можно установить адресата исходного запроса – является ли он роботом? пользователем? Затем создать для идентифицированного запроса результирующую страницу. Выполнение клоакинга с использованием обычного HTML (JavaScript) невозможно.

Каковы методы клоакинга? Существуют несколько методов для определения наличия клоакинга. К таким методам можно отнести

проверку поля User-agent, проверку IP адресата, а также комбинирование этих методов.

Метод, который основывается на User-agent, является самым простым. При запросе обычно идет передача имени робота, дополнительных данных, проводится сравнение входящих данных. Затем, используя специальный скрипт определяется робот. В итоге, для робота выдается оптимизированная версия страницы, и обычная версия – остальным посетителям страницы. Преимуществом этого метода является простота реализации, а серьезным недостатком – возможность подделки пользователем поля User-agent с целью получения бесплатного доступа. Поэтому, необходимо проводить проверку IP-адреса посетителя.

Как и обычные посетители банка (офлайн, онлайн), все роботы поисковых систем являются владельцами IP-адресов, которые идентифицируют подключение к сети банковского Интранет, причем у каждого – свой фиксированный адрес. Суть метода заключается в определении IP-адреса посетителя, сравнении этого адреса с базой данных, где хранятся IP поисковых роботов. В итоге можно определить, кто (что) является посетителем сайта – человек или робот, а по полученному результату показать соответствующую страницу (роботу – оптимизированную страницу, «остальным» – нормальную). Данный метод является более хитроумным (IP-адреса почти невозможно подделать). Недостатком метода является необходимость в большой базе IP-адресов роботов с периодическим обновлением.

Самым надежным и эффективным является комбинированный метод: совмещение вышеописанных методов, и чтобы избежать проблем – показывать нормальную страницу.

Независимо от того, что клоакинг скоро может стать вполне приемлемым методом, все же не следует применять его для решения всех задач и сразу. Он в большинстве случаев рекомендуется для уже существующих сайтов, где применяется Flash или AJAX.

Клоакинг можно применять для разграничения контента для внешней и внутренней сети [8, с.21].

Как защищать банки от клоакинга?

Можно снизить эффективность воздействие вредоносного влияния в реальном времени, если иметь и реализовывать эффективную интегрированную банковскую политику и систему безопасности, использовать информационно-логическое (финансово-математическое) моделирование угроз. В частности, функциональное представление инфопроцессов, их особенностей, релевантные критерии целостности системы.

Пусть инфопроцесс в системе безопасности банка реализуется n процедурами, причем вероятность v(i) – информационный объем в i-ой подсистеме (транзакции), а V(i) – максимально обрабатываемый системой для i-ой транзакции объем (актуальная при DDoS-атаках).

Показателем полноты обработки служат отношения:

P(V(i) ³V0(i)) = .

Например, v(1) – для процесса «защита от клоакинга», v(2) – для процесса «защита БД» и т.д.

Вероятность реализации вмешательства может оцениваться как время t(i), не более T(i), а своевременность обработки информации:

.

Здесь t(i) – время i-ой транзакции.

Необходимо эффективно:

- тестировать безопасность (контроль доступа);
- совершенствовать инструментарий (программное обеспечение);

- вести тренинг персонала;
- проверять подразделения, координировать их в реальном режиме.

Данная формализация позволит оценивать вероятность достижения цели, например, клоакинга, провести упреждающие защитные мероприятия. Полностью эффективный высокотехнологичный, высокоинтеллектуальный (на мультиагентных и нейросистемах) подход – дело будущего. Сейчас каждому банку нужно (и можно) решить проблему повышения эффективности системы безопасности.

При SQL-инъекциях (доступе к БД пользователей) нужно соблюдать «противоинъекционные» меры, в частности, данные предоставлять лишь через плейсхолдер, использовать идентификаторы (ключевые слова) лишь из «белого» списка. При XSS-атаках, ориентированных на онлайн-пользователей (позволяет украсть «куки», получить к «админке» доступ) многое зависит от их идентификации вовремя, т.е. от моделирования.

Литература

1. Ашманов И., Иванов А. // ВЫВОД САЙТА НА ЭКРАНЫ РАДАРОВ // Интернет-маркетинг. 2002. № 1. С. 2-12.
2. Бексаева Е.А., Чамина О.Г. // ФАКТОРЫ И РЕКОМЕНДАЦИИ SEO-АУДИТА ВЕБ-РЕСУРСОВ ЭЛЕКТРОННОЙ КОММЕРЦИИ // Вестник Ульяновского государственного технического университета. 2015. № 3 (71). С. 39-46.
3. Винокуров П. // ПОИСКОВЫЕ СИСТЕМЫ – ПРАКТИЧЕСКИЕ СОВЕТЫ ОНЛАЙНОВОМУ МАРКЕТОЛОГУ // Интернет-маркетинг. 2002. № 2. С. 39-48.
4. Гранкина Е.С. // ПОИСКОВЫЕ СИСТЕМЫ И ИХ МЕСТО В МАРКЕТИНГОВОЙ СТРАТЕГИИ // Школа университетской науки: парадигма развития. 2012. Т. II. № 6. С. 78-80.
5. Довбенко А.В. // ПРОБЛЕМЫ СОВРЕМЕННОЙ ПОИСКОВОЙ ВЫДАЧИ // Проблемы современной науки и образования. 2016. № 39 (81). С. 19-22.

6. Ермакова Л.М. // МЕТОДЫ КЛАССИФИКАЦИИ ТЕКСТОВ И ОПРЕДЕЛЕНИЯ КАЧЕСТВА КОНТЕНТА // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2011. № 3. С. 47-53.
7. Ершов Е.А., Лобачев В.В. // МЕТОДЫ ПРОДВИЖЕНИЯ САЙТОВ В ИНТЕРНЕТЕ // Системный анализ в науке и образовании. 2011. № 4 (14). С. 44-48.
8. Лебедянцева Л. // НАВИГАЦИОННЫЕ И ПОИСКОВЫЕ СИСТЕМЫ В ИНТЕРНЕТЕ И ИХ ОПТИМИЗАЦИЯ // Интернет-маркетинг. 2005. № 6. С. 18-24.
9. Луцук А.И., Быта С.В., Самохвалов С.М. // SEO – ТЕХНОЛОГИИ ДЛЯ ОПТИМИЗАЦИИ WEB-ПОИСКА // Россия молодая: передовые технологии – в промышленность!. 2011. № 1. С. 279-282.
10. Михеев М.Ю., Сомин Н.В., Галина И.В., Золотарев О.В., Козеренко Е.Б., Морозова Ю.И., Шарнин М.М. // ФАЛЬШТЕКСТЫ: КЛАССИФИКАЦИЯ И МЕТОДЫ ОПОЗНАНИЯ ТЕКСТОВЫХ ИМИТАЦИЙ И ДОКУМЕНТОВ С ПОДМЕНОЙ АВТОРСТВА // Информатика и ее применения. 2014. Т. 8. № 4. С. 70-77.
11. Пахомова Т.В., Смагина И.В. // К ВОПРОСУ ОБ ОПТИМИЗАЦИИ САЙТА // Научные записки ОрелГИЭТ. 2014. № 2 (10). С. 315-318.
12. Пирко И.Ф. // К ВОПРОСУ ИЗУЧЕНИЯ МЕТОДОВ И ЭТАПОВ ПОИСКОВОЙ ОПТИМИЗАЦИИ ПРИ ПРОДВИЖЕНИИ WEB-САЙТОВ КАК ИНСТРУМЕНТА МАРКЕТИНГОВОЙ ПОЛИТИКИ // Экономика и предпринимательство. 2015. № 10-2 (63-2). С. 938-941.
13. Прохорова А.М. // SEO-ОПТИМИЗАЦИЯ // Евразийский союз ученых. 2016. № 30-4. С. 79-82.
14. Сироткин И. // ПОИСКОВЫЕ СИСТЕМЫ И ИХ МЕСТО В МАРКЕТИНГОВОЙ СТРАТЕГИИ // Интернет-маркетинг. 2005. № 5. С. 33-39.
15. Султанов И.И. // ПОИСКОВЫЕ СТРАТЕГИИ САЙТОВ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОПТИМИЗАЦИИ // Вестник Казанского государственного университета культуры и искусств. 2007. № специальный. С. 290-296.
16. Тоичкина И.В. // ПОИСКОВАЯ ОПТИМИЗАЦИЯ САЙТА В СИСТЕМЕ ЭЛЕКТРОННОГО БИЗНЕСА // Экономика и социум. 2016. № 4-2

(23). С. 349-353.
17. Чамина О.Г., Бексаева Е.А. // SEO-АНАЛИТИКА ВЕБ-РЕСУРСОВ ЭЛЕКТРОННОЙ КОММЕРЦИИ // Модели, системы, сети в экономике, технике, природе и обществе. 2015. № 3 (15). С. 180-188.
18. Юлов А. // МАРКЕТИНГОВЫЕ ИССЛЕДОВАНИЯ КОНКУРЕНТНОГО ОКРУЖЕНИЯ В СЕТИ ИНТЕРНЕТ // Интернет-маркетинг. 2004. № 3. С. 21-29.

References

1. Ashmanov I., Ivanov A. // CONCLUSION OF THE SITE TO THE RADAR SCREEN // Internet Marketing. 2002. № 1. P. 2-12.
2. Beksaeva EA, Chamina O.G. // FACTORS AND RECOMMENDATIONS OF SEO-AUDIT OF WEB-RESOURCES OF ELECTRONIC COMMERCE // Bulletin of Ulyanovsk State Technical University. 2015. No. 3 (71). Pp. 39-46.
3. Vinokurov P. // SEARCH SYSTEMS – PRACTICAL ADVICE ONLINE MARKETOLOGY // Internet Marketing. 2002. № 2. P. 39-48.
4. Grankina E.S. // SEARCH SYSTEMS AND THEIR PLACE IN THE MARKETING STRATEGY // School of University Science: Development Paradigm. 2012. T. II. № 6. P. 78-80.
5. Dovbenko A.V. // PROBLEMS OF MODERN SEARCH SEARCH »// Problems of modern science and education. 2016. No. 39 (81). Pp. 19-22.
6. Ermakova L.M. // METHODS OF CLASSIFICATION OF TEXTS AND DETERMINATION OF QUALITY OF CONTENT // Bulletin of Perm University. Series: Mathematics. Mechanics. Computer science. 2011. № 3. P. 47-53.
7. Ershov EA, Lobachev VV // METHODS OF PROMOTING SITES IN THE INTERNET // System analysis in science and education. 2011. № 4 (14). Pp. 44-48.
8. Lebedyantseva L. // NAVIGATION AND SEARCH SYSTEMS IN THE INTERNET AND THEIR OPTIMIZATION // Internet Marketing.

2005. № 6. With. 18-24.
9. Lutsuk AI, Byta S.V., Samokhvalov S.M. // SEO – TECHNOLOGIES FOR OPTIMIZATION OF WEB-SEARCH // Russia is young: advanced technologies – in industry !. 2011. № 1. P. 279-282.
10. Mikheev M.Yu., Somin N.V., Galina IV, Zolotarev OV, Kozerenko EB, Morozova Yu.I., Sharnin M.M. // FALSE TEXTS: CLASSIFICATION AND METHODS OF IDENTIFICATION OF TEXT IMITATIONS AND DOCUMENTS WITH SUBSCRIPTION OF AUTHORITY // Informatics and its applications. 2014. T. 8. № 4. S. 70-77.
11. Pakhomova TV, Smagina IV // TO THE QUESTION OF OPTIMIZATION OF THE SITE // Scientific notes OrelGiET. 2014. No. 2 (10). Pp. 315-318.
12. Pirko I.F. // TO THE QUESTION OF STUDYING METHODS AND STAGES OF SEARCH OPTIMIZATION AT PROMOTING WEB-SITES AS A TOOL OF MARKETING POLICY // Economics and Entrepreneurship. 2015. No. 10-2 (63-2). Pp. 938-941.
13. Prokhorov A.M. // SEO-OPTIMIZATION // Eurasian Union of Scientists. 2016. No. 30-4. Pp. 79-82.
14. Sirotkin I. // SEARCH SYSTEMS AND THEIR PLACE IN THE MARKETING STRATEGY // Internet Marketing. 2005. № 5. P. 33-39.
15. Sultanov II // SEARCH STRATEGIES OF SITES: CONTEMPORARY PROBLEMS OF OPTIMIZATION // Bulletin of the Kazan State University of Culture and Arts. 2007. No. special. Pp. 290-296.
16. Toychkina I.V. // Search optimization of the site in the system of electronic business // Economics and society. 2016. No. 4-2 (23). Pp. 349-353.
17. Chamina OG, Beksaeva EA // SEO-ANALYSIS OF WEB-RESOURCES OF ELECTRONIC COMMERCE // Models, systems, networks in economics, technology, nature and society. № 3 (15). Pp. 180-188.
18. Yulov A. // MARKETING RESEARCH OF COMPETITIVE ENVIRONMENT IN THE NETWORK INTERNET // Internet marketing. № 3. P. 21-29.