УДК 004.056.57

ИССЛЕДОВАНИЕ СООТНОШЕНИЯ ОБНАРУЖИВАЕМЫХ УЯЗВИМОСТЕЙ И ДИНАМИКИ ИХ ОБНАРУЖЕНИЯ В РАЗЛИЧНЫХ ПРОГРАММНЫХ ПРОДУКТАХ

© 2016 Ю.В. Алейнов, М.Е. Бурлаков, Д.А. Голубых

Самарский национальный исследовательский университет имени С.П. Королёва

Статья поступила в редакцию 11.11.2016

В статье приводятся результаты работы комплекса автоматизированного сбора и индексирования информации об уязвимостях в программном обеспечении из открытых и закрытых источников SCAN Project, разработанного в рамках НИОКР «Академия Инфотекс». Проанализирована информация о количестве найденных уязвимостей в программных продуктах различных категорий. Сделан вывод о влиянии популярности продукта на количество найденных уязвимостей. Кроме того, проанализирована динамика количества обнаруженных уязвимостей по конкретным программным продуктам, а также ее связь с изменением популярности этих продуктов согласно мнению экспертного сообщества.

Ключевые слова: обнаружение уязвимостей, сбор и индексация данных, динамика количества обнаруженных уязвимостей, популярность программного продукта.

Работа выполнена в рамках гранта по НИОКР «Академия Инфотекс» - 2016 г.

ВВЕДЕНИЕ

Автоматизация и информатизация все большего спектра сфер деятельности человека является отчетливой тенденцией развития современного общества. С каждым днем появляется все больше различных программных продуктов, призванных решать все более широкие задачи.

Увеличение количества программного кода приводит к увеличению числа ошибок в нем. Некоторые из этих ошибок способны повлечь за собой реализацию различных угроз информационной безопасности. В этом случае говорят об уязвимостях программного обеспечения. Уязвимости потенциально присутствуют в любом программном продукте. Время от времени часть из них обнаруживается и устраняется, однако изменения, вносимые при этом в программный код, могут содержать в себе новые уязвимости. Новые ошибки могут появляться и при обновлении или расширении функционала продукта, и при переносе его на другие платформы. Чем сложнее программное обеспечение, тем чаще в нем обнаруживаются уязвимости.

Одной из актуальных проблем защиты информации в настоящее время является постоянное отслеживание информации о найденных уязвимостях в программном обеспечении и своевременное их устранение.

В условиях современных комплексных инфраструктур, состоящих из большого количества программных компонентов, это сделать бывает очень сложно. Современные приложения создаются, как правило, с использованием нескольких отдельных технологий и облегчающих разработку инструментов (библиотек, «фреймворков»). Кроме того, любое приложение работает в некотором программном окружении (операционная система, серверы приложений, системы управления базами данных), которое также может содержать уязвимости.

Для оперативного отслеживания сообщений о имеющихся во всем стеке компонентов уязвимостях, необходимо постоянно следить за большим количеством разнообразных источников. Кроме официальных источников информации об уязвимостях, существуют и неофициальные. Неофициальные источники включают в себя различные специализированные форумы, блоги, социальные сети. В этих источниках зачастую информация может появляться раньше, чем в официальных или содержать дополнительные сведения, полезные для устранения проблемы. Особый интерес вызывают закрытые источники и источники в «глубоком интернете» (*TOR*, *I2P*).

Таким образом, актуальной является задача агрегации информации об уязвимостях различного программного обеспечения из множества источников, в том числе не предназначенных для автоматической индексации и представления ее в удобном виде.

В 2016 году в рамках НИОКР «Академия Инфотекс» авторами статьи был разработан ин-

Алейнов Юрий Викторович, старший преподаватель кафедры безопасности информационных систем. E-mail: aleinov@gmail.com

Бурлаков Михаил Евгеньевич, лаборант кафедры безопасности информационных систем. E-mail: knownwhat@gmail.com

Голубых Денис Алексеевич, студент механико-математического факультета, специализации «Компьютерная безопасность». E-mail: den1008@bk.ru

струмент *SCAN Project*. Инструмент предназначен для сбора неструктурированной информации об уязвимостях в программном обеспечении из различных источников, в том числе закрытых, и индексации собранных данных при помощи системы полнотекстового поиска *Elasticsearch* [1], основанной на библиотеке *Apache Lucene*.

Выбор *Elasticsearch* был обусловлен быстротой его работы, простотой в настройке, а также возможностью свободного бесплатного использования [2]. В настоящей статье представлен анализ полученной в рамках исследования информации об уязвимостях. Проанализирована динамика атак по различным типам программного обеспечения. А также проиллюстрирована возможность оценки популярности программных продуктов по динамике обнаружения уязвимостей.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПОПУЛЯРНОСТИ ПРОГРАММНОГО ПРОДУКТА НА КОЛИЧЕСТВО ОПУБЛИКОВАННЫХ УГРОЗ

Во время работы системы были проанализированы записи об уязвимостях из источников, представленных в табл. 1.

Кроме информации непосредственно о найденных уязвимостях, определенный интерес также представляют сводные сведения о соотношении количества уязвимостей различных продуктов и о динамике изменения количества опубликованных уязвимостей для каждого продукта.

Анализ этих сведений позволяет выявить закономерности развития различных программных продуктов и информационных технологий, а также понять поведение сообщества «*black hat*». Созданная в рамках исследования система в пользовательском интерфейсе автоматически отображает следующую сводную информацию:

- Общее количество найденных уязвимостей за весь период работы.
- Соотношение количества найденных уязвимостей в различных программных продуктах (список интересующих продуктов необходимо задавать вручную).
- Динамика изменения количества найденных уязвимостей по каждому продукту по месяцам в 2-х летней перспективе и по годам в 25-летней.

Разработчиками системы был проведен анализ данной сводной информации, целями которого являлись:

- выявление закономерностей в распределении найденных уязвимостей по типам программного обеспечения;
- выявление закономерностей в распределении количества найденных уязвимостей конкретных продуктов по времени.

Для этой цели был сформирован перечень программных продуктов, предназначенных для различных целей. В данный перечень были включены основные продукты из следующих категорий программного обеспечения:

- операционные системы;
- программные продукты поддержки инфраструктуры (веб-серверы, серверы приложений, почтовые, *DNS*-серверы, программное обеспечение сетевого оборудования, и т.п.);
- офисные продукты;
- системы мгновенного обмена сообщениями;
- системы управления контентом (*CMS*);
- браузеры.

Анализ проводился в два этапа. На первом этапе было рассмотрено соотношение количества найденных уязвимостей в различных программных продуктах. Результат представлен на рис. 1.

Из рисунка хорошо видно, что доля найденных уязвимостей программного обеспечения, используемого для поддержки веб-приложений, а также мобильных платформ, превышает 50% от общего числа всех найденных уязвимостей.

Это можно объяснить стремительным развитием веб-технологий в настоящее время. Веб-приложения в настоящее время набирают свою популярность. Их функциональность растет, все больше традиционных приложений включают в свой функционал веб-компоненты [3, 4]. Отметим, что главным клиентским приложением становится веб-браузер, который присутствует на всех типах платформ, включая мобильные. Популярность мобильных платформ также показывает быстрый рост [4, 5].

Таблица 1. Список источников информации об уязвимостях

Наименование источника	Ссылка	Тип
Security Lab	*http://www.securitylab.ru/*	Открытый
Exploit-DB	*http://www.cvedetails.com/*	Открытый
Malwarebytes.org	*https://ru.malwarebytes.com/trial/*	Закрытый
web.nvd.nist.gov	*https://nvd.nist.gov/*	Закрытый
0 day	*Onion TOR*	Закрытый
Seclists.org	*http://seclists.org/*	Закрытый
Stackoverflow	*http://stackoverflow.com*	Открытый
CVE Detail	*http://www.cvedetails.com/*	Открытый
Htbridge.com	*https://htbridge.com*	Закрытый

Рис. 1. Распределение уязвимостей по программным продуктам

Чем быстрее развивается технология, тем больше создается конкретных программных продуктов в ее рамках. Эти продукты быстрее обновляют свой функционал, и, как следствие, содержат больше уязвимостей, чем те, функционал которых более стабилен. Востребованность программного продукта также означает то, что с ним имеет дело большое число пользователей. Успешная эксплуатация уязвимостей в нем способна затронуть гораздо большее число потенциальных жертв. Это заставляет как злоумышленников, так и специалистов по безопасности обращать более пристальное внимание на обеспечение безопасности в наиболее популярных продуктах. Производители программного обеспечения, заинтересованные в конкурентоспособности своего товара, запускают программы поиска уязвимостей, привлекая большое количество независимых специалистов по безопасности, а также более тщательно исследуют написанный код своими силами. В результате, количество обнаруженных уязвимостей в популярных продуктах значительно превышает количество обнаруженных уязвимостей в другом программном обеспечении.

На втором этапе анализа сводной информации о найденных уязвимостях рассматривались кривые, иллюстрирующие динамику количества обнаруженных уязвимостей по времени для каждого программного продукта в перечне.

Данная информация также позволяет судить об изменении популярности конкретного продукта. Так, при рассмотрении графика обнаруженных уязвимостей платформы *Android* (рис. 2), можно увидеть увеличение количества обнаруженных уязвимостей, что совпадает с данными из других источников, говорящими об увеличении популярности данной платформы [6].

Пики на представленном графике соответствуют периоду с сентября по ноябрь 2014 года. Они объясняются тем, что в этот период актуальными были версии *Android* 4.1 / 4.2 / 4.3 «*Jelly Bean*» [7]. В этих версиях было обнаружено большое количество уязвимостей в функционале работы с пользовательскими данными и в реализации протоколов. Так, например, устройства с установленной *Android* 4.1.1 подвержены уязвимости реализации протокола *SSL* «*Heartbleed*» [8].

Напротив, график найденных уязвимостей для *CMS Joomla!* (рис. 3, 4) демонстрирует нисходящий тренд, что совпадает с данными *Google Trends* [9]:

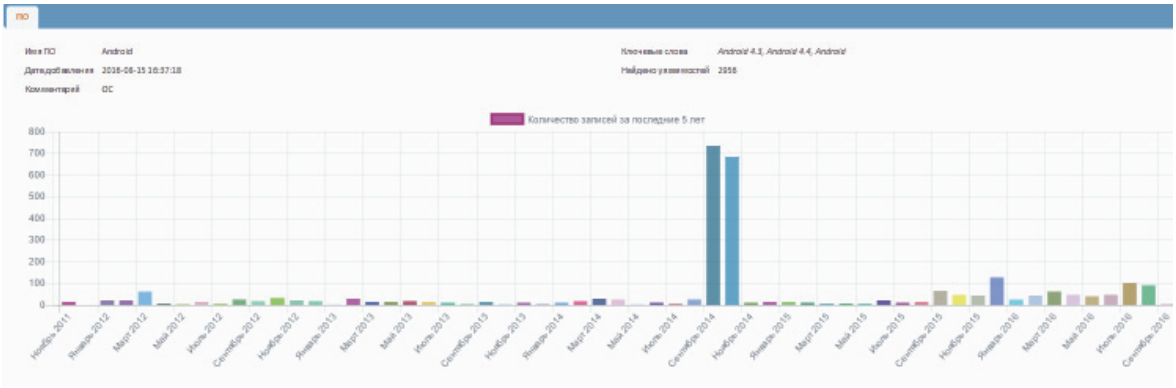

Рис. 2. Динамика количества обнаруженных уязвимостей в ОС Android

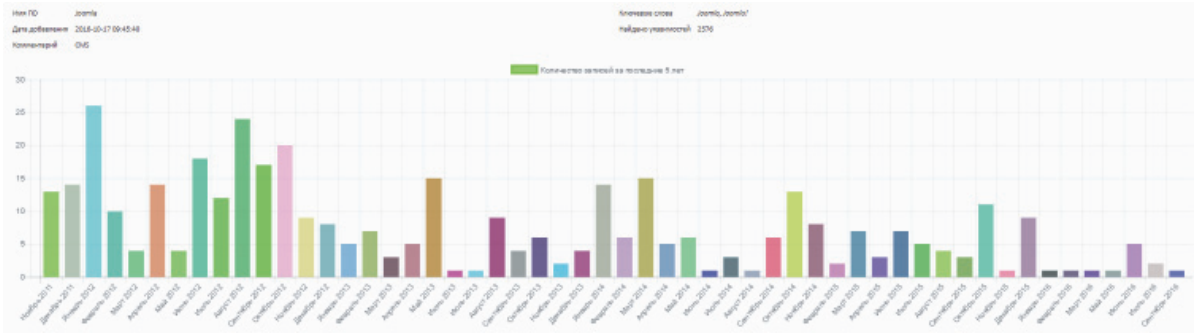

Рис. 3. Динамика количества обнаруженных уязвимостей в CMS Joomla!

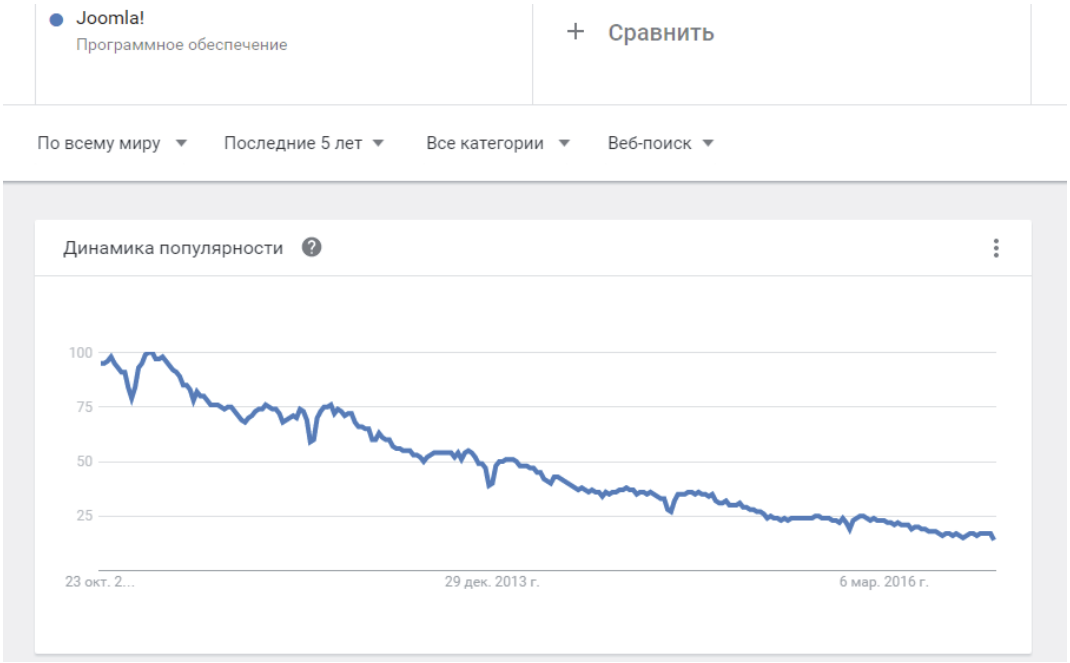

Рис. 4. Динамика изменения популярности CMS Joomla! по данным Google Trends

ЗАКЛЮЧЕНИЕ

В результате работы системы была собрана и проиндексирована информация об уязвимостях различных программных продуктов из 4 открытых и 5 закрытых источников. На основе анализа данной информации авторами исследования был сделан вывод о влиянии популярности конкретного продукта на количество обнаруженных в нем уязвимостей.

Наибольшее число уязвимостей было обнаружено в наиболее популярных продуктах, таких как программное обеспечение для поддержки веб-приложений, веб-браузеры, а также в мобильных приложениях. Анализ данных о динамике публикаций информации об уязвимостях по отдельным программным продуктам показал, что количество найденных уязвимостей за некоторый промежуток времени также зависит от популярности продукта и изменяется вместе с ним. Таким образом, разработанная система позволяет отслеживать тенденции изменения популярности отдельных продуктов со временем, что имеет отдельное прикладное значение в области исследования рынка программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Официальная страница проекта Elasticsearch URL: https://www.elastic.co/products/elasticsearch (дата обращения 30.10.2016).
2. *Akdogan H.* Elasticsearch Indexing. – Packt Publishing Ltd, 2015.
3. Netcraft Site Report URL: http://toolbar.netcraft.com/site_report (дата обращения 30.10.2016).
4. Исследование компании Яндекс. Развитие интернета в регионах России. URL: https://yandex.ru/company/researches/2016/ya_internet_regions_2016 (дата обращения 30.10.2016).
5. Обзор. Эволюция мобильных технологий: Чего ждать в 2016? URL: https://rusability.ru/internet-marketing/evolyutsiya-mobilnyih-tehnologiy-chego-zhdat-v-2016/ (дата обращения: 30.10.2016)
6. Smartphone OS Market Share, 2016. URL: http://www.idc.com/prodserv/smartphone-os-market-share.jsp (дата обращения 01.11.2016).
7. История версий Android // Википедия. URL: https://

ru.wikipedia.org/wiki/история_версий_Android (дата обращения: 28.10.2016).
8. Google Report. Android Security 2014 Year in Review. URL: https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2014_Report_Final.pdf (дата обращения 10.11.2016).
9. Google Trends. Анализ. URL: https://www.google.ru/trends/explore?q=%2Fm%2F07qb81 (дата обращения 23.10.2016).

RESEARCH OF THE RATIO OF DETECTED VULNERABILITIES IN DIFFERENT SOFTWARE PRODUCTS AND DETECTION DYNAMICS

© 2016 Y.V. Aleinov, M.E. Burlakov, D.A. Golubyh

Samara National Research University named after Academician S.P. Korolev

The article describes the results obtained with automated tool for gathering and indexing information about vulnerabilities in software products. The tool named SCAN Project was developed within the scope of «Infotecs Academy» research and collects data from both open and private sources. The collected information about amount of vulnerabilities in various software products was analyzed and the conclusion about correlation of this amount and product popularity was made. Also the article contains an analysis of correlation between dynamics of vulnerability finding and product›s popularity variations according to expert community opinion.
Keywords: vulnerabilities detection, data gathering and indexing, vulnerability detection dynamics, popularity of software.

Yury Aleinov, Senior Lecturer at the Information Security Systems Department. E-mail: aleinov@gmail.com
Mikhail Burlakov, Labour at the Information Security Systems Department. E-mail: knownwhat@gmail.com
Denis Golubyh, Student of Faculty of Mechanics and Maths, Specialization "Computer Security". E-mail: den1008@bk.ru