Результаты работы исследовательской лаборатории Digital Security Research Group за 5 лет

5

Digital Security

N1 В АУДИТЕ БЕЗОПАСНОСТИ

Результаты работы исследовательской лаборатории Digital Security за 5 лет

С момента официального открытия исследовательской лаборатории компании Digital Security (известной как Digital Security Research Group или DSecRG) прошло более пяти лет, и мы решили подвести промежуточные итоги деятельности подразделения в цифрах, а также отметить ряд наиболее значимых для нас достижений.

В 2013 году руководителем лаборатории стал Дмитрий Евдокимов, зарекомендовавший себя как отличный специалист с глубоким подходом к изучению проблем безопасности, автор большого числа известных на рынке исследований.

Digital Security Research Group в цифрах

1 — 1-й исследовательский центр в России

2 — 2-е место в топ-10 техник web-атак 2012 года

3 — 3 года участия в международных конференциях

4 — 4 выступления на BlackHat в 4 географических точках

5 — 5 лет публичной работы

6 — 6 сотрудников выступали на международных конференциях с собственными докладами

7 — 7 дней в неделю

8 — 8 сотрудников получили благодарности от крупнейших компаний за найденные уязвимости

9 — 9 основных участников

10 — попали в топ-10 докладов BlackHat USA в 2012 году

15 — Участвовали в проведении 15 встреч Defcon Russia

20 — Выступили более чем в 20 странах

30 — Более 30 выступлений на международных технических конференциях

40 — Более 40 исследований

100 — Почти 100 опубликованных уязвимостей в SAP

200 — Почти 200 уязвимостей опубликовано в общем

300 — Более 300 уязвимостей обнаружено

Поиск и обнаружение уязвимостей

С ноября 2007 года лаборатория начала поиск и анализ уязвимостей в программных продуктах. Ключевой особенностью ее деятельности стал принцип Responsible Disclosure: мы сообщаем разработчику об обнаруженной уязвимости, помогаем ее закрыть и после этого публикуем детали. Изначально объектами анализа были простые веб-приложения и CMS-системы, далее фокус сместился на анализ веб-серверов и СУБД, и постепенно мы пришли к бизнес-приложениям и ERP-системам. Необходимо подчеркнуть, что наш исследовательский центр стал уникальным явлением для российского рынка ИБ: ранее поиск уязвимостей осуществлялся бессистемно и нерегулярно, в любительском формате. Открытие лаборатории DSecRG вывело эту деятельность на профессиональный уровень. Со временем некоторые игроки рынка последовали примеру Digital Security, создав свои подразделения по поиску и анализу уязвимостей.

Количество закрытых уязвимостей относительно обнаруженных

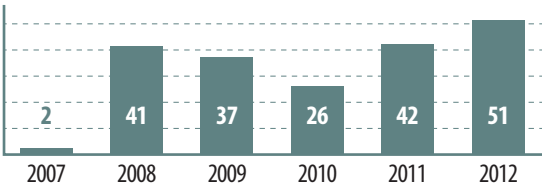
Количество опубликованных уязвимостей по ключевым производителям

За все время специалистами DSecRG было обнаружено 318 уязвимостей, из которых 199 было закрыто производителями, по остальным ведется работа. Сейчас основное направление нашей деятельности – Application Security, в котором мы и будем продолжать работать, стремясь занимать лидирующие позиции не только в России, но и в мире.

Эксперты DSecRG обнаружили около 0,8% от всех уязвимостей, закрытых в мире за 5 лет, что превышает аналогичные показатели всех российских компаний в совокупности.

Уязвимости по областям

Количество уязвимостей, опубликованных в разные годы

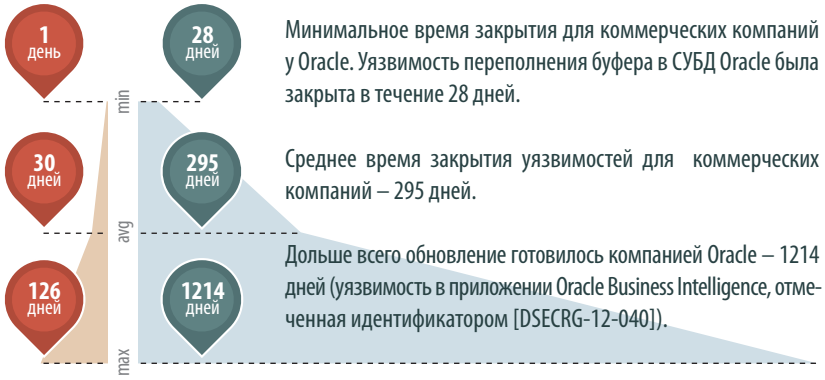


Время закрытия уязвимостей

Минимальное время закрытия для OpenSource у разработчиков Blogcms и 2z. Несколько уязвимостей различного рода были закрыты за один день!

Среднее время закрытия уязвимостей для OpenSource-разработчиков – 30 дней.

Для OpenSource-разработчиков дольше всего готовилось обновление консорциумом Apache – 126 дней (уязвимость в приложении Apache Geronimo, отмеченая идентификатором [DSECRG-09-019]).



Минимальное время закрытия для коммерческих компаний у Oracle. Уязвимость переполнения буфера в СУБД Oracle была закрыта в течение 28 дней.

Среднее время закрытия уязвимостей для коммерческих компаний – 295 дней.

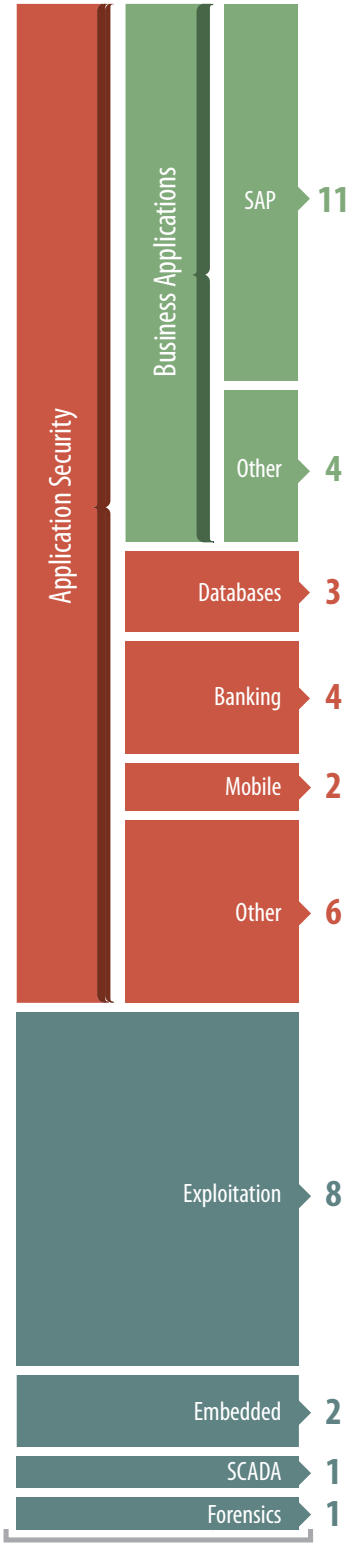
Дольше всего обновление готовилось компанией Oracle – 1214 дней (уязвимость в приложении Oracle Business Intelligence, отмеченная идентификатором [DSECRG-12-040]).

Исследовательские работы

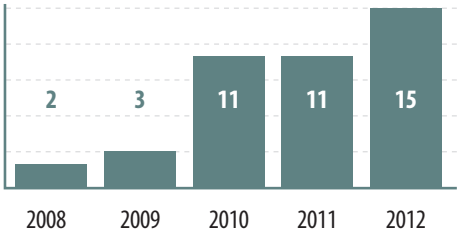
За время работы DSecRG было подготовлено 42 больших исследования, результатами которых стали различные статьи, отчеты и выступления на конференциях.

Исследования по сотрудникам

Исследования по областям



Исследования по годам



Безопасность систем ДБО (2009–2011)

Первое исследование в области безопасности дистанционного банковского обслуживания в России. Раньше на эту тему говорили крайне мало, но проблемы, затронутые специалистами DSecRG, привлекли внимание экспертов из различных организаций отрасли ИБ. Популярность сегмента рынка анализа защищенности выросла в разы.

Адаптация техники JIT-Spray (2010)

Данное исследование улучшило технику атаки на Adobe Flash с целью обхода DEP и ASLR. В результате проведенных работ время атаки было сокращено в 100 раз! Кроме того, исследование показало, что не только JIT-движок Adobe Flash, но и JavaScript-движок браузера Safari подвержен подобной атаке. Результаты этой работы впоследствии использовались многими компаниями в сфере offensive security по всему миру.

Безопасность SAP в цифрах (2007–2012)

Глобальное исследование безопасности SAP с 2007 по 2011 год. Вышло на двух языках и получило награду InfoSecurity Product Guide в номинации Advertising. Исследование затронуло все аспекты безопасности SAP – от статистики уязвимостей и описания топ-5 уязвимостей до анализа SAP-систем, доступных через Интернет в той или иной стране мира, и статистики по наиболее распространенным версиям и патчам.

SSRF и бизнес-приложения (2012–2013)

Исследование было впервые представлено на конференции BlackHat и сделало популярным изучение нового класса атак. В совокупности с другими независимыми работами, посвященными SSRF-атакам, эта публикация заняла 2-е место в списке 10 наиболее интересных техник атак на веб-приложения в 2012 году.

Мобильный банкинг (2012–2013)

Был проведен статический анализ кода клиентской части мобильных платежных приложений под iOS и Android более чем от 30 российских банков. Выяснилось, что все рассмотренные приложения содержат хотя бы одну уязвимость, позволяющую атаковать банк или его клиентов.

Выступления на международных конференциях

В 2009 году лаборатория сделала рывок в развитии, начав выступать с исследованиями на международных технических конференциях. На Западе мы были не первыми (ElcomSoft выступали за рубежом еще 10 лет назад), но Digital Security вывела участие российских исследователей на новый уровень, значительно увеличив присутствие экспертов по ИБ на ключевых конференциях. За три года DSecRG появилась на 36 конференциях в 20 странах Европы, Азии и США, и мы продолжаем работать в этом направлении, завоевывая новые континенты. Отрадно, что инициативу Digital Security поддержали и другие компании и независимые исследователи. К 2013 году наличие у компании докладов на международных конференциях стало нормой, так же как пару лет назад нормой стало наличие благодарностей от производителей.

EUROPE

Poland	5
Germany	3
Netherlands	3
Austria	2
Czech Republic	1
Spain	1
Belgium	1
Portugal	1
Hungary	1
Switzerland	1
Finland	1

ASIA

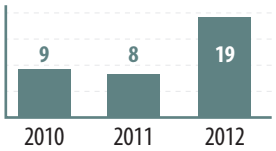
India	3
China	2
Malaysia	2
Korea	1

USA 6

Middle East

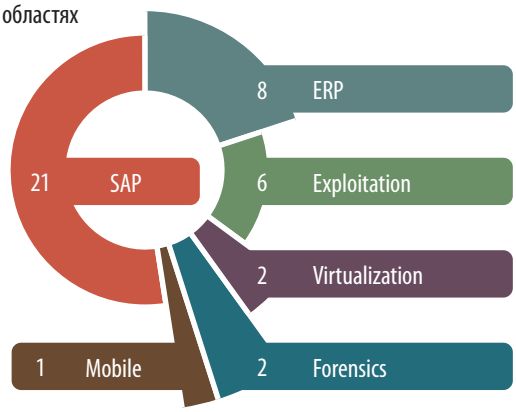
Kuwait	1
UAE	1

Количество выступлений по годам



Количество выступлений по докладчику

Количество выступлений в различных областях



Количество выступлений на разных конференциях

CONFidence	6	Nullcon	1	Source	1
BlackHat	5	HackTivity	1	t2.fi	1
HITB	4	IT-SA	1	BruCON	1
Deepsec	2	Syscan360	1	InfoSecurity Kuwait	1
SecurityByte	2	SAP Security Summit	1	Just4Meeting	1
HackerHalted	2	Hashdays	1	Defcon	1
Troopers	1	PoC	1	RSA	1

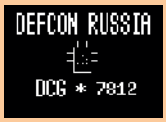
Проекты и общественные инициативы

По мере возможности мы стараемся участвовать в различных проектах и инициативах. Остановимся подробнее на наиболее важных из них.

ZeroNights

Организация ежегодной международной конференции Zero-Nights в Москве и Санкт Петербурге. Единственная в России бескомпромиссно-техническая конференция, посвященная новейшим методам взлома и защиты, в 2012 году собрала 600 человек и более 50 докладчиков и была отмечена авторитетным изданием SCMagazine как наиболее значимая для посещения в 2013 году, наряду с такими монстрами, как BlackHat, HITB и Infiltrate.

Defcon Russia



Проект создан сотрудниками исследовательской лаборатории. Это своеобразная площадка для обучения молодых специалистов, позволяющая в ходе неформальных встреч получить уникальные знания и навыки и обменяться опытом. Собирает более 50 человек в месяц, является прообразом конференции ZeroNights. На сегодняшний день, успешно проведено 15 встреч.

OWASP

В проекте OWASP мы ведем подпроект OWASP-EAS, посвященный безопасности бизнес-приложений. Первая версия подпроекта была представлена в 2010 году и включала в себя описание основных угроз бизнес-приложениям и методику оценки безопасности бизнес-приложений. После долгого перерыва, обусловленного сбором информации и анализом систем, в 2013 году начата серьезная работа над версией 2.

Project BaseCamp

Участие в проекте, посвященном анализу безопасности АСУ ТП, а именно уязвимостям в программируемых контроллерах. Мы проанализировали PLC фирмы WAGO и систему kingSCADA.

Metasploit

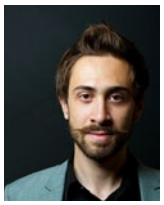
Участие в проекте Metasploit, разработка эксплойтов под СУБД Oracle и других удобных инструментов для помощи в проведении пентестов.

Bounty programs

Участие практически во всех программах поиска уязвимостей. Мы регулярно получаем благодарности и денежные поощрения от Google, Yandex, Nokia, а в будущем планируем поддержать и другие компании, предлагающие подобные программы.

Python Arsenal

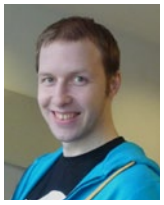
В ходе исследования была собрана и структурирована база из более чем 40 различных инструментов для реверс-инжиниринга и анализа безопасности приложений на языке Python. Результатом масштабной работы стало создание сайта с удобным поиском и обновляемой базой, который ежедневно посещают сотни исследователей со всего мира.



Александр Поляков

@sh2kerr

Основатель исследовательского центра Digital Security Research Group. Автор книги «Безопасность Oracle глазами аудитора: нападение и защита» (2009 г.) и более чем 30 статей, посвященных анализу системы безопасности и приложений в ведущих российских изданиях, включая российскую SAP expertise. Один из наиболее известных специалистов в мире по безопасности SAP и Oracle. Обнаружил более 100 уязвимостей в их программном обеспечении. В свободное время увлекается поиском настандартных векторов атак и специфичных проблем в бизнес-системах.



Алексей Тюрин к.т.н.

@antyurin

Специалист по безопасности веб-приложений и банк-клиентов, имеет большой опыт тестирования на проникновение таких бизнес-систем, как Citrix, VMware и других. С его помощью обнаружено большое количество уязвимостей. Редактор рубрики Easy Hack в журнале Хакер.

Глеб Чербов

@cherboff

Специалист по анализу защищенности сетевых и веб-приложений. Также занимается аспектами безопасности встраиваемых (embedded) систем. Принимает активное участие в исследованиях, проводимых в рамках DSecRG. Соорганизатор и регулярный докладчик на встречах Russian Defcon Group.

Дмитрий Евдокимов

@evdokimovds

Специализируется на безопасности критичных бизнес-систем (SAP) и безопасности мобильных платформ (iOS, Windows Phone, Android). Имеет официальные благодарности от компаний SAP и Oracle за обнаруженные в их продуктах уязвимости. Кроме того, в область интересов входит: reverse engineering, software verification/program analysis (SMT, DBI, IR), поиск уязвимостей и написание эксплойтов, разработка программ для статического и динамического анализа кода на языке Python. В качестве докладчика выступал на таких конференциях, как BlackHat и CONFidence. Ведет рубрики в журнале «Хакер». Является одним из организаторов конференций Russian Defcon Group (DCG#7812) и ZeroNights.

Александр Миноженко

@al3xmin

Ведущий исследователь ИБ. Имеет большой опыт тестирования на проникновение таких бизнес-систем, как SAP, VMware и других. Выступал на конференциях CONFidence и Defcon.

Николай Мещерин

@Ab7orbent

Отвечает за аналитику и тестирование ERPScan Security Monitoring Suite for SAP, а также активно участвует в поиске и анализе уязвимостей SAP-систем. Имеет официальные благодарности от SAP AG за уязвимости, обнаруженные в продуктах корпорации.

Дмитрий Частухин

@_chipik

Является одним из ведущих специалистов по безопасности SAP и веб-приложений. Большой фанат Bug-Bounty. Имеет официальные благодарности от Yandex, Google, Nokia и SAP. Выступал на BlackHat USA, HackInTheBox и BruCON, ZeroNights. Активно участвует в деятельности Russian Defcon Group.

Евгений Неелов

@neyolov

Ключевые интересы — безопасность бизнес-приложений, анализ киберпреступлений, методы форензики и ее обхода, безопасность электронной коммерции, системы антифрода. Выступал на SyScan360 и других конференциях, где рассказывал о методах обхода антифрод-систем. Один из организаторов ZeroNights и Russian Defcon Group. Имеет благодарности за обнаруженные уязвимости от Microsoft, SAP и других компаний.

Александр Большев, к.т.н.

@dark_k3y

Имеет кандидатскую степень по специальностям «математическое обеспечение вычислительных машин» и «защита информации», ведет научную работу в СПбГЭТУ «ЛЭТИ», участвует в исследованиях лаборатории Digital Security, в том числе как консультант по проблемам прикладной математики. Автор исследования «SSRF DoS Relaying» (2013 г.).

А еще в нашей команде есть исследователи из различных городов России, а также Швейцарии, Индии и Казахстана. Если ты хочешь быть частью нашей команды, пиши на research@dsec.ru с информацией о себе, и, надеемся, мы найдем общие интересы.

Digital Security

N1 В АУДИТЕ БЕЗОПАСНОСТИ

Digital Security — одна из ведущих российских консалтинговых компаний в области информационной безопасности. Digital Security предоставляет широкий спектр услуг в области оценки защищенности, включая комплексный аудит ИБ, тестирование на проникновение, аудит защищенности бизнес-приложений (SAP, Oracle, веб-приложения, системы ДБО), аудит защищенности АСУ ТП и SCADA. Digital Security имеет статус PCI QSA и PA QSA. Финансовым организациям компания оказывает полный комплекс услуг по достижению соответствия Стандарту безопасности данных индустрии платежных карт (PCI DSS). С 2002 года клиентами Digital Security стали более 500 компаний на всей территории России, стран СНГ и Балтии, а также в Восточной Европе, Германии и ЮАР. Со многими из них за это время сложились долгосрочные партнерские отношения.

Digital Security является официальным сервис-партнером SAP AG, международным лидером по поиску и анализу уязвимостей в продуктах SAP, а также разработчиком ERPScan Security Monitoring Suite – инновационного продукта по комплексной оценке защищенности и проверке соответствия стандартам для платформы SAP.

Контактная информация:

ООО «Диджитал Секьюрити»

Штаб-квартира:
Россия, 115054, Москва
Ул.Дубининская, д.57, стр.6
тел/факс: +7 (495) 223-07-86

R & D Центр:
Россия, 197183, Санкт-Петербург
Ул.Сабировская, д.37
тел/факс: +7 (812) 703-1547, 430-9130

Электронная почта:

- По общим вопросам: info@dsec.ru
- Отдел продаж: sales@dsec.ru
- Отдел технической поддержки: support@dsec.ru
- Работа сайта: support@dsec.ru

Адрес в Интернет: www.dsec.ru