

ZERO NIGHTS

2015 25-26 november

25 ноября

	Track 1	Track 2	Workshop 1	Workshop 2
10.00	Регистрация			
11.00	Открытие			
11.30 12.20	"Ода хакерам", Родриго Рубира Бранко (BSDaemon)			
12.30 13.20	"Взлом виртуальных устройств", Джереми Браун	"Ломай, как кинозвезда: пошаговое руководство к созданию боевой нагрузки под SCADA для физических атак с катастрофическими последствиями", Марина Кротофил	"Практический объектно-ориентированный реверс-инжиниринг", Александр Матросов, Евгений Родионов	"Enlarge your Burp, или Как перестать бояться Javadocs", Часть первая Иван Елкин, Игорь Булатенко
13.30 14.20	"При вскрытии гарантия аннулируется, или атаки на MPLS-сети", Георги Гешев	"Модификация прошивок промышленных свитчей" Александр Ермолов		
14.50	Обед			
16.00 16.50	"Большие проблемы с "большими данными": безопасность интерфейсов Nadoor", Якуб Калужный	"Максимальная отдача от CSP: глубокое погружение", Сергей Шемян	"Практический объектно-ориентированный реверс-инжиниринг", Александр Матросов, Евгений Родионов	"Enlarge your Burp, или Как перестать бояться Javadocs", Часть вторая Иван Елкин, Игорь Булатенко
17.00 17.50	"Математическая модель уязвимостей и атак на ошибки проверки пользовательского ввода" Иван Новиков	"illuSoryTLS: Никто, кроме нас. Имитация, модификация и эксплуатация", Альфонсо де Грегорио		
18.00 19.00	"Cisco IOS shellcode - all-in-one", Георгий Носенко	"Browser Fuzzing with a Twist (and a Shake)", Джереми Браун	Обзор RuCTFE 2015	

	Track 1	Track 2	Workshop 1	Workshop 2
11.00 11.50	“Знакомьтесь, Choronzon – концепция интеллектуального эволюционного фаззинга”, <i>Николаос Назиридис, Зисис Сиалверас</i>	“Как построить свою систему Эшелон. Атаки на 3G модемы”, <i>Тимур Юнусов</i>	Defensive Track (20 минут) “Корреляция событий безопасности с помощью Esper”, <i>Николай Клендар</i> “Анализируй это: собираем современную SIEM на основе Open Source компонентов для анализа логов в большом масштабе”, <i>Даниил Светлов</i>	“Практическая эксплуатация устройств на базе МК AVR”, Часть первая <i>Александр Большев, Борис Рютин</i>
12.00 12.50	“SmartTV: как собрать небезопасное устройство в современном мире”, <i>Сергей Белов</i>	“ESIL - универсальный IL (Intermediate Language) для radare2”, <i>Антон Кочкин</i>	“Борьба с 0-day в flash: охота на модифицированный вектор”, <i>Андрей Ковалев, Константин Отрашкевич, Евгений Сидоров</i> “Банковские трояны: взгляд с другой стороны”, <i>Алексей Левин</i>	
13.00 13.50	“А ты получил свой токен?”, <i>Цзинь Лонг и Йанг Циетао</i>	“S[с]runt повсюду. Или как прервать непрерывную интеграцию”, <i>Андрей Пластунов</i>	“Автоматизация сканирования веб-приложений – опыт Яндекса”, <i>Эльдар Заитов</i> “Банковский SDL своими руками”, <i>Шабалин Юрий</i> “Сыграем в игру: еще один способ тестирования на проникновение”, <i>Кирилл Ермаков</i>	
14.00	Lunch			
16.00 16.50	“Почини сам: закрываем уязвимости в UEFI своими руками”, <i>Николай Шлей</i>	“Безопасность в KNX, или как украсть небоскроб”, <i>Егор Литвинов</i>	FastTrack (15 min) “Уязвимости программного обеспечения телекоммуникационного оборудования Yota”, <i>Михаил Фирстов</i> “Разбор реконструкции промежуточного представления для анализа сложного вредоносного ПО”, <i>Александр Матросов, Евгений Родионов</i> “Сеть контролируемых браузеров на основе BeEF и Google Drive”, <i>Денис Колегов</i>	“Практическая эксплуатация устройств на базе МК AVR”, Часть вторая <i>Александр Большев, Борис Рютин</i>
17.00 17.50	“Атаки на гипервизоры с использованием прошивок и железа”, <i>Александр Матросов</i>	“Вырываем большой (синий) зуб”, <i>Маттео Беккаро, Маттео Коллура</i>	“Что нужно знать хакеру о протоколе WebDav? Обзор уязвимостей в реализации WebDav”, <i>Андрей Ефимюк, Михаил Егоров</i> “ORM2Pwn: эксплуатируем инъекции в Hibernate”, <i>Михаил Егоров, Сергей Солдатов</i> “Увеличиваем производительность сканеров, используя Data Mining”, <i>Сергей Игнатов, Омар Ганиев</i> “Обфускация интерпретируемых языков программирования на практике”, <i>Александр Курилин</i>	“На пути в (не)правильную анонимность. Базовые приемы цифровой контрацепции и гигиены приватных данных”, <i>Влад Воронков</i>
18.00 18.50	“Direct X – прямой путь к ядру Microsoft Windows”, <i>Никита Тараканов</i>	“[Реальное] Состояние безопасности BGP”, <i>Александр Асимов, Артем Гавриченко</i>	Обзор RuCTFE 2015	
19.00 19.30	Закрытие			