Шестая ежегодная международная конференция, посвященная практическим аспектам информационной безопасности

ПРОГРАММА КОНФЕРЕНЦИИ «ZERONIGHTS 2016»

17 ноября (четверг)

	Track 1	Track 2	Workshop 1	Workshop 2
10.00 11.00	Регистрация			
11.00 11.30	Открытие			
11.30 12.20	Добро пожаловать на физический уровень *Михаэль Оссман*			
12.30 13.20	Руткиты в прошивках UEFI: мифы и реальность *Александр Матросов и Евгений Родионов*	Криптография для чайников *Никита Абдуллин*	За пределами OWASP Top 10	Обратная разработка бинарных файлов с использованием Kaitai Struct *Михаил Якшин*
13.30 14.20	Проект Excite: вся правда о символьном исполнении для защиты BIOS *Александр Матросов и Илья Сафонов*	О мышах и клавиатурах: на страже безопасности современных беспроводных устройств ввода *Маттиас Диг и Герхард Клостермайер*		
14.50 16.00	Обед			
16.00 16.50	На страже руткитов: Intel BootGuard *Александр Ермолов*	Hacking ElasticSearch *Иван Новиков*	Современный фаззинг проектов C/C++ *Максим Мороз*	Обратная разработка бинарных файлов с использованием Kaitai Struct *Михаил Якшин*
17.00 17.50	JETPLOW мертв, да здравствует JETPLOW! *Роман Бажин и Максим Малютин*	Hadoop сафари — охота за уязвимостями *Томас Дебиз и Махди Брайк*		**Community**
18.00 19.00	Составляющие шлюза Tesla Motors *Сен Не и Лин Лю*	Advanced Web Application Fuzzing *Михаил Степанкин*		

ПРОГРАММА КОНФЕРЕНЦИИ «ZERONIGHTS 2016»

18 ноября (пятница)

11.00 11.50	Вы больше не на крючке: как ослепить систему безопасности *Джеффри Танг и Алекс Матросов*	Падение системы CICS: в мир транзакций через взлом *Аюб Эль Ассал*	**Defensive Track *** (по 20 минут)	Исследование безопасности АСУ ТП. Тестирование на проникновение и анализ уязвимостей *Борис Савков*
12.00 12.50	Я знаю адрес твоей страницы: дерандомизация адресного пространства ядра последней версии Windows 10 *Энрике Ниссим*	Критический анализ сложных атак с повторным использованием кода с помощью ROPMEMU *Мариано Грациано*		
13.00 13.50	Подход к разработке LPE эксплоитов на Windows 10 с учетом последних обновлений защиты *Дроздов Юрий и Дроздова Людмила*	FIRST: новый взгляд на реверс-инжиниринг *Ангель Вильегас*		
14.00 16.00	Обед			
16.00 16.50	Наносим удар по управлению пином в программируемых логических контроллерах *Али Аббаси и Маджид Хашеми*	Cisco Smart Install. Возможности для пентестера *Александр Евстигнеев и Дмитрий Кузнецов*	**FastTrack **** (по 15 минут)	**Community**
17.00 17.50	Инструмент DPTrace – двойное назначение трассировки для анализа потенциальных уязвимостей *Родриго Рубира Бранко и Рохит Мот*	Как обмануть АЦП, ч.3 или инструментарий для атак на устройства преобразования аналоговых данных в цифровые *Александр Большев*		
18.00 18.50	Разбираемся в режиме восстановления OS и процессе ее локального обновления на компьютерах Mac *Патрик Уордл*	Истории из жизни о взломе low-cost телефонов *Алексей Россовский*		
19.00 19.30	Закрытие			

* DEFENSIVE TRACK

- Сам себе Threat hunter
  Сергей Солдатов и Теймур Хеирхабаров
- Страх и ненависть двухфакторной аутентификации
  Игорь Булатенко
- Управление цифровой подписью приложений в большой компании
  Евгений Сидоров и Эльдар Заитов
- Автоматизация сканирования iOS по методу blackbox
  Михаил Сосонкин
- Мониторинг и анализ почтовых сообщений или инструмент обнаружения кибер-атак на коленке
  Алексей Карябкин и Павел Грачев
- Enterprise Vulnerability Management
  Пухарева Екатерина и Александр Леонов
- 20% вложений и 80% результата. Как реализовать требования ИБ и не потерять внутреннюю свободу
  Куканова Наталья и Гоц Игорь

** FAST TRACK

- HexRaysPyTools
  Игорь Кириллов
- Нейротехнологии в безопасности
  Ксения Гнитько
- Ты какой-то не такой…
  Ковалев Андрей
- Удар ниже пояса. Обход современных WAF/IPS/DLP
  Антон Лопаницын
- Уязвимости конфигурации F5 BIG-IP: поиск и устранение
  Денис Колегов
- Атаки на JAX-RS приложения: неправильный выбор провайдера компонента Entity
  Михаил Егоров
- Reversing golang
  Зайцев Георгий
- Скрытые коридоры вредосного ПО
  Ор Сафран и Омер Яир