

ФАКТЫ О RAUNCH И ЕГО ДЕЯТЕЛЬНОСТИ

Создатель наборов эксплоитов «Blackhole» и «Cool Exploit Kit», а также сервиса анонимных антивирусных проверок «Crypt.am»



40%
заражений
в мире

происходило с использованием инструментов Raunch



Минимальный доход Raunch
50 000\$ в месяц

Raunch платил **100 000–200 000\$**



за приватные эксплойты

Цена аренды связки эксплоитов «Blackhole» на сервере продавца составляла **500\$** в месяц



А цена аренды самого ПО для установки на собственном сервере **700\$** за три месяца

ХОД РАССЛЕДОВАНИЯ

Идентификация участников 1-й группы Carberg



2010

Идентификация участников 2-й группы Carberg



2011

Изучение процесса «заражения» банковским трояном обратившихся клиентов




2011

Отслеживание действий Carberg и их круга общения



2011

 Carberg — технологический банковский троян, созданный в 2008 году

Попадание в поле зрения Raunch, отслеживание его активности в сети

2011



ИДЕНТИФИКАЦИЯ RAUNCH И ЕГО ПАРТНЕРОВ

2012
Передача материалов в МВД и возбуждение уголовного дела

 Участие Group-IB в качестве специалистов и экспертов

2012–2013



Аресты клиентов Raunch

2013



Проверка предоставленной информации от Group-IB и формирование доказательственной базы преступной деятельности Raunch

2013




Задержание Raunch и партнеров

2013



Сотрудниками полиции были предъявлены обвинения еще 12 членам межрегиональной преступной группы

 Показания подельников

 Телефонные переговоры

 Оплаты услуг

 Фиксация доступа к определенным ресурсам

и т.д.

