

Программы-вымогатели: реальное положение вещей

Враг у ворот, он силен и не стоит на месте!



Утрата важных и конфиденциальных данных



Нарушение работы



Финансовые потери



Репутационные потери

Вредоносное ПО с нештучным ценником



Осознать растущую угрозу



НОМЕР 3 в списке "Hot Topics for 2015" ФБР США¹

Более 2400 обращений в ФБР, общая сумма средств, выплаченных вымогателям, составила

24 млн долл. США²

Пресечена кампания на основе эксплойтов Angler, которая могла принести преступникам до

60 млн долл. США³

2015

Процесс набирает темп



2016

Год вымогательского ПО

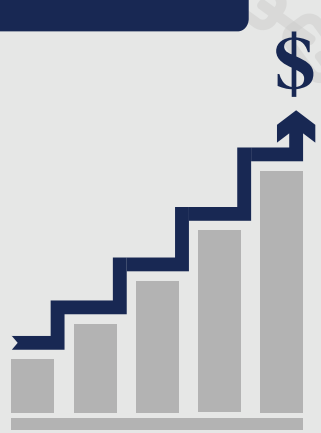
Общая сумма выкупа, выплаченная за первые 3 месяца, составила

209 млн долл. США⁴

В 2016 г. доход киберпреступников ожидается на уровне

1 млрд долл. США⁵

Шестикратное увеличение количества жертв среди корпоративных пользователей⁶



Понимать векторы атак

Наборы эксплойтов – это специализированные инструменты, при помощи которых хакеры распространяют вредоносное ПО. Эксплойт-киты доставляются в систему следующими способами.

Электронная почта: фишинговые письма и спам с вредоносными вложениями и ссылками

Веб-серверы: точки входа для доступа к сети

Веб-приложения: файлы распространяются в зашифрованном виде через социальные сети и системы мгновенного обмена сообщениями

Вредоносная реклама: Drive-By-загрузки с зараженного веб-сайта

Вектор заражения



Управление и контроль



Шифрование файлов



Требование выкупа



Часто применяются веб-сайты и электронная почта

Контроль над целевыми системами

Утрата доступа к файлам

Владелец/компания выплачивает выкуп (биткойны) за разблокирование системы

Подход к предотвращению атак, основанный на архитектуре сети



Защита, охватывающая уровень DNS, оконечные устройства, электронную почту, веб и сеть



Защита устройств внутри сети и за ее пределами



Готовность в кратчайшие сроки обнаружить и изолировать активность вредоносного ПО

Обнаружение и нейтрализация программ-вымогателей

Группа Cisco Talos нейтрализует атаку, которая могла ежегодно приносить преступникам **60 млн долл.** США⁷



При помощи одного из самых объемных и мощных эксплойт-китов были организованы целевые кампании с применением вредоносной рекламы



Пресечена ежедневная эксплуатация **90 000 жертв**, приносящая **30-миллионный** годовой доход; злоумышленники применяли около **150 прокси-серверов**

Узнайте больше уже сегодня

На странице cisco.com/go/ransomware описан простой, открытый, автоматизированный и эффективный подход Cisco к проблеме безопасности.



¹ 2015 Internet Crime Report (Отчет об интернет-преступности за 2015 г.), Министерство юстиции США, Федеральное бюро расследований, https://pdf.ic3.gov/2015_IC3Report.pdf
² Ransomware: Latest Cyber Extortion Tool (Вымогательское ПО: новейший метод кибервымогательства), Федеральное бюро расследований, апрель 2016 г., <https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool>
³ Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60m Annually from Ransomware Alone (В центре внимания: группа Cisco Talos пресекает доступ к объемному международному комплексу эксплойтов, приносящему годовой доход в 60 млн долл. США за счет одних лишь программ-вымогателей), Talos, октябрь 2015 г., <http://www.talosintelligence.com/angler-exposed/>
⁴ Cyber-Extortion Losses Skyrocket, Says FBI (По данным ФБР, ущерб от кибервымогательства стремительно растет), Дэвид Фитцпатрик (David Fitzpatrick) и Дрю Гриффин (Drew Griffin), CNN Money, апрель 2016 г., <http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/>
⁵ Ibid.
⁶ History and Statistics of Ransomware (История и статистика программ-вымогателей), Кевин Таунсенд (Kevin Townsend), Security Week, июнь 2016 г., <http://www.securityweek.com/history-and-statistics-ransomware>
⁷ Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating \$60m Annually from Ransomware Alone (В центре внимания: группа Cisco Talos пресекает доступ к объемному международному комплексу эксплойтов, приносящему годовой доход в 60 млн долл. США за счет одних лишь программ-вымогателей), Cisco Talos, октябрь 2015 г., <http://www.talosintelligence.com/angler-exposed/>