PACIFICA
www.pacifica.kz

Управление инцидентами в Казахстане. Цифры и факты

SOC FORUM
ASTANA

Умид Тухтаев
Инженер ИБ, ТОО «Пацифика»

27 апреля 2017 года

О компании

PACIFICA

9 ЛЕТ
На рынке Республики Казахстан

Резиденты - 100%

ПЕРВАЯ в Казахстане

Компания, которая занимается только проектами в области обеспечения информационной безопасности

intella
БИЗНЕС БЕЗОПАСНОСТИ

>20 Мировых вендоров

Лицензия КНБ РК СК №013
на занятие разработкой и реализацией (в том числе иной передачей) средств криптографической защиты информации

- Алматы – Центральный офис
- Астана – Дополнительный офис

bsi.
ASSOCIATE CONSULTANT PROGRAMME
MEMBERSHIP NUMBER 726

Программа ассоциированных консультантов (ACP), созданная мировым лидером в разработке методологии построения систем управления — компанией BSI, объединяет профессионалов в сфере разработки и сертификации систем менеджмента.

Собственный ЦЕНТР по расследованию инцидентов

SERT

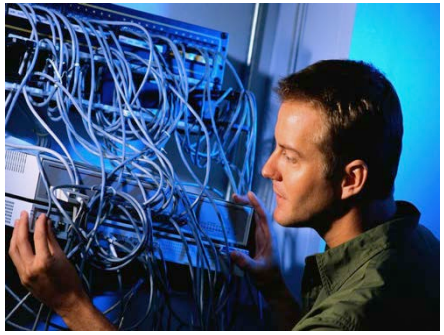
25
сотрудников

Собственный Учебный центр

Структура

PACIFICA

ТОО «ПАЦИФИКА»

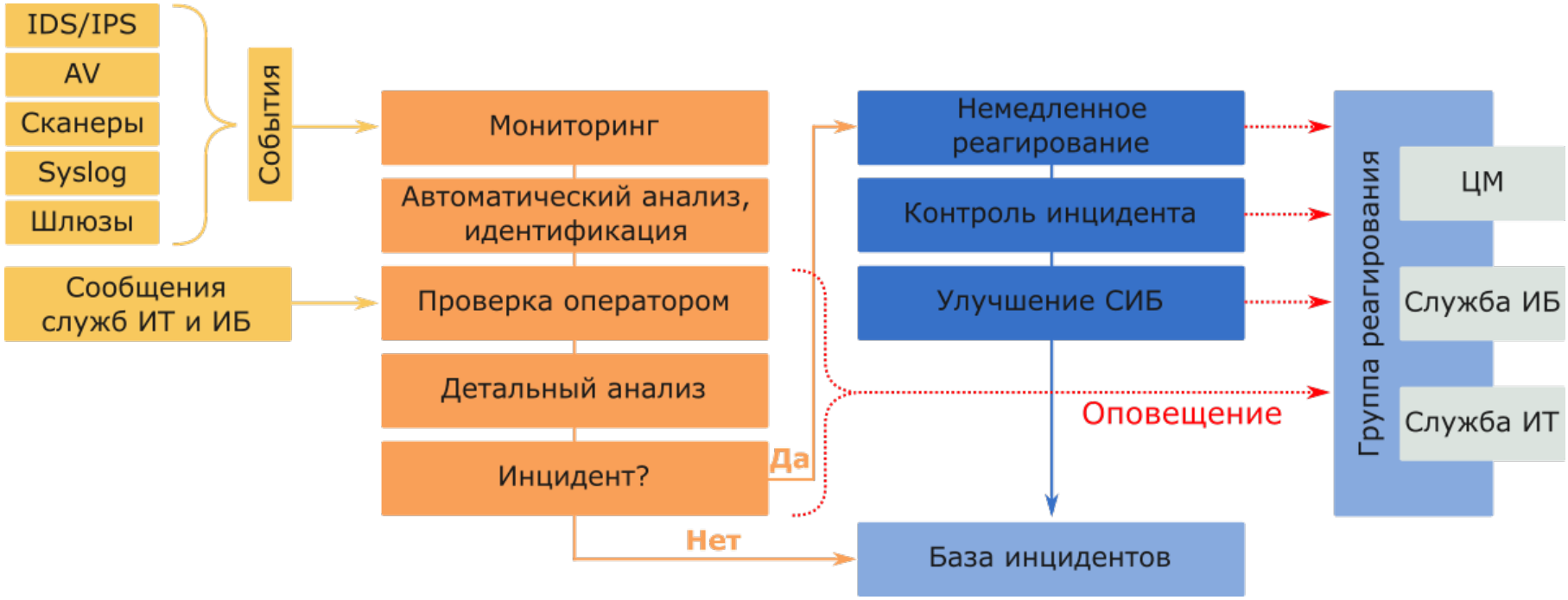
Аудит и консалтинг	Проектирование и внедрение	Техническая поддержка и аутсорсинг	Обучение
			
» Подготовка к аудиту в соответствии с международными стандартами (ISO 27001, PA/PCI DSS) » Консультации по вопросам обеспечения информационной безопасности	» Проектирование и внедрение систем информационной безопасности » Построение центра управления инцидентами, защита центров обработки данных (ЦОД)	» Поддержка и сопровождение систем информационной безопасности (СИБ) » Оптимизация ИБ-инфраструктуры, ИБ-аутсорсинг, облачные ИБ-сервисы	» Проведение тренингов и обучающих семинаров менеджеров и технических специалистов ИБ » Тестирование специалистов ИБ по собственным программам

ПАЦИФИКА предоставляет комплекс решений и услуг, позволяющих нашим клиентам выстраивать систему обеспечения ИБ «с нуля» или оптимизировать существующую.

Центр мониторинга (ЦМ)

PACIFICA

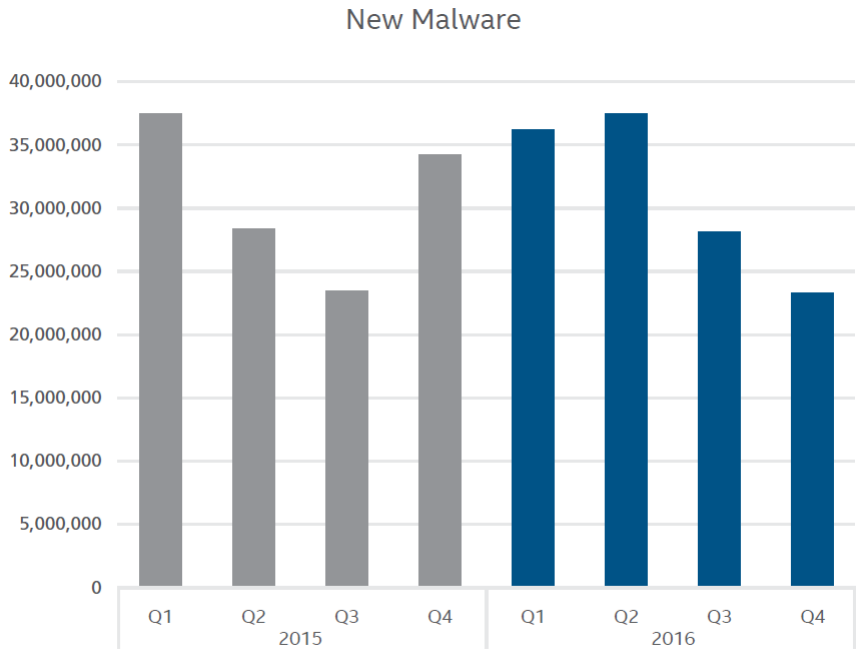
» Сбор данных о событиях и инцидентах информационной безопасности



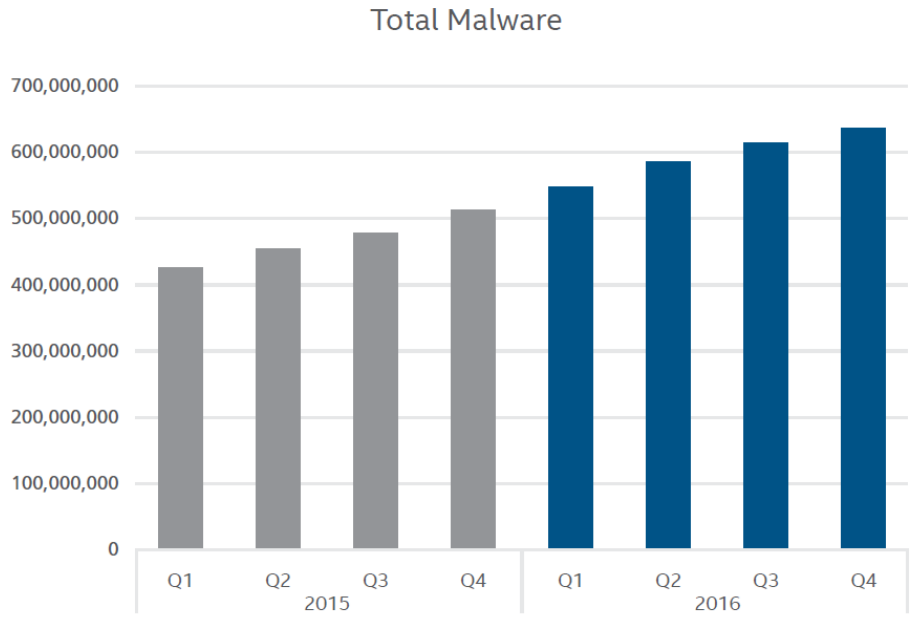
Мировая статистика

PACIFICA

» Количество вредоносного программного обеспечения



Source: McAfee Labs, 2017.

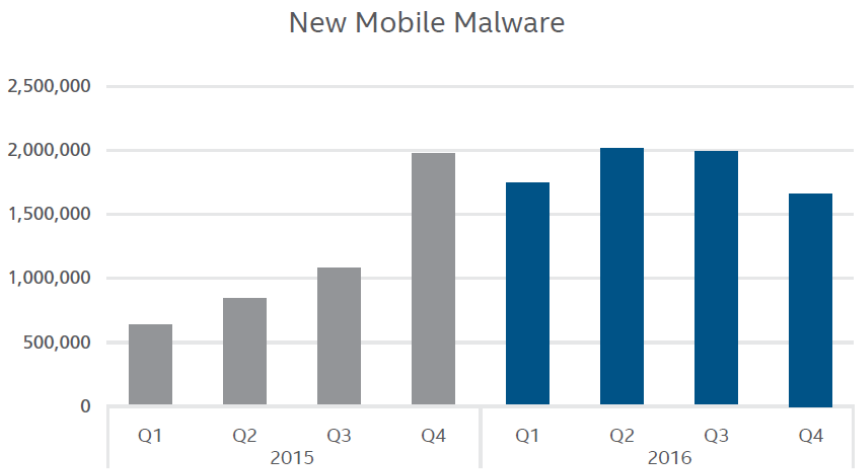


Source: McAfee Labs, 2017.

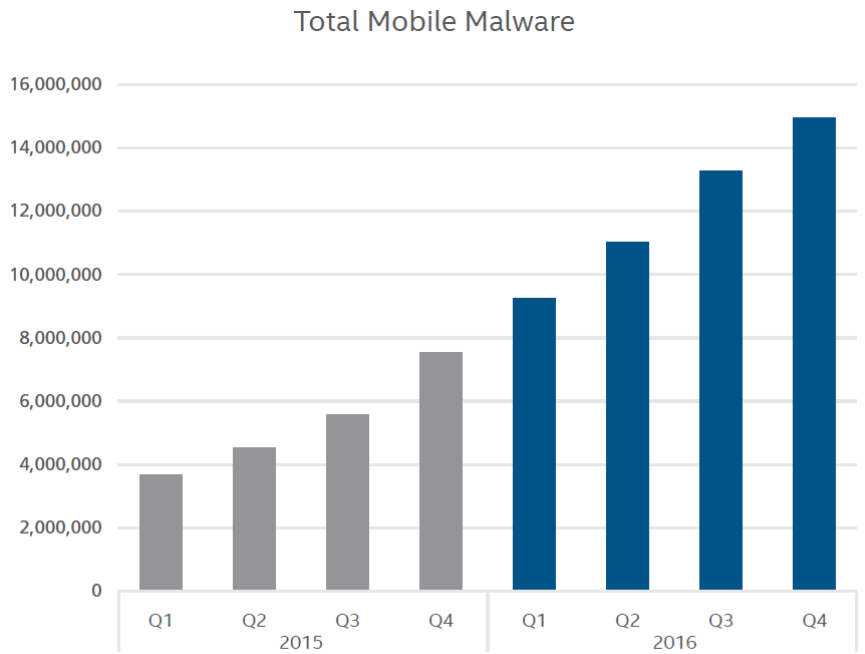
Мировая статистика

PACIFICA

» Количество мобильного вредоносного программного обеспечения



Source: McAfee Labs, 2017.

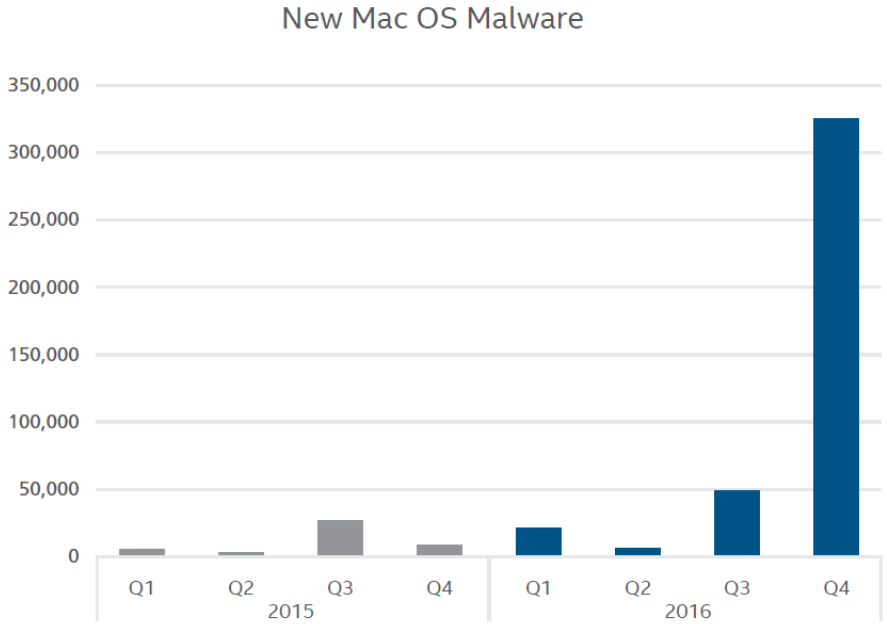


Source: McAfee Labs, 2017.

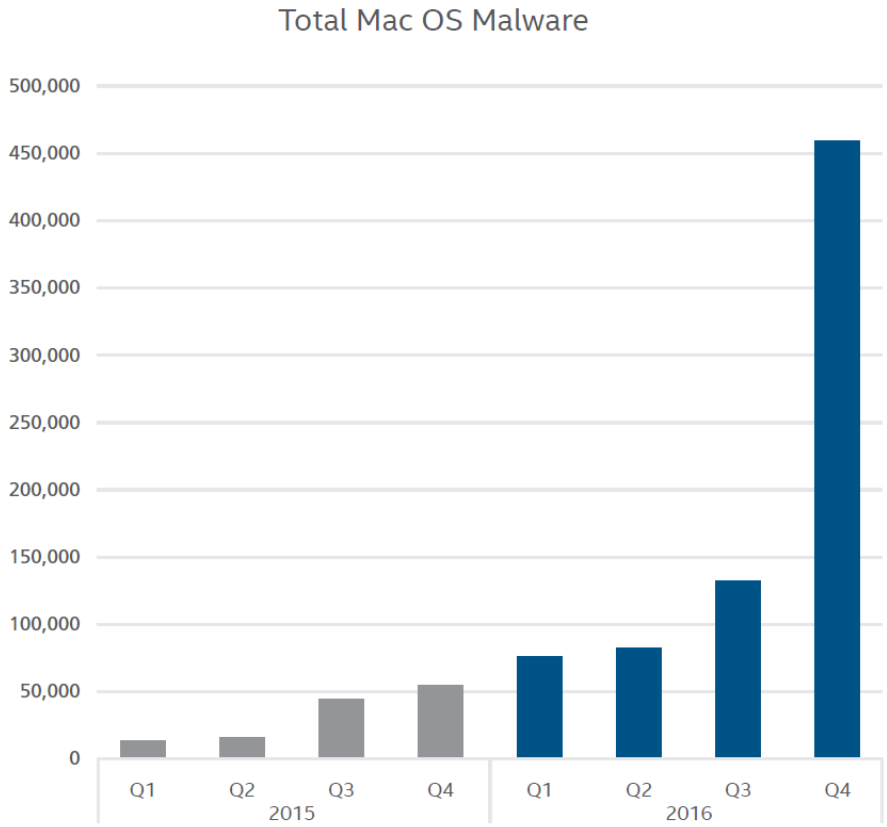
Мировая статистика

PACIFICA

» Количество вредоносного программного обеспечения на ОС Mac



Source: McAfee Labs, 2017.

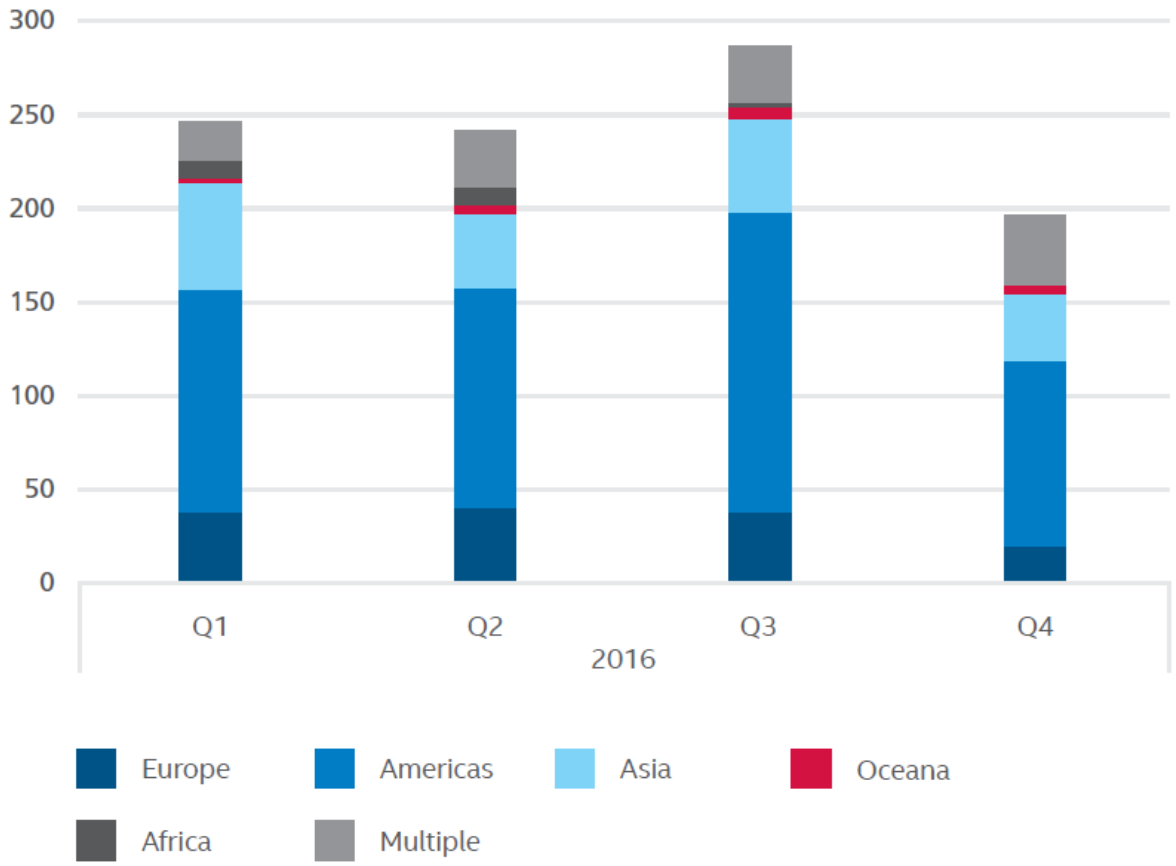


Source: McAfee Labs, 2017.

Мировая статистика

PACIFICA

» Публично-раскрытые инциденты в 2016 году

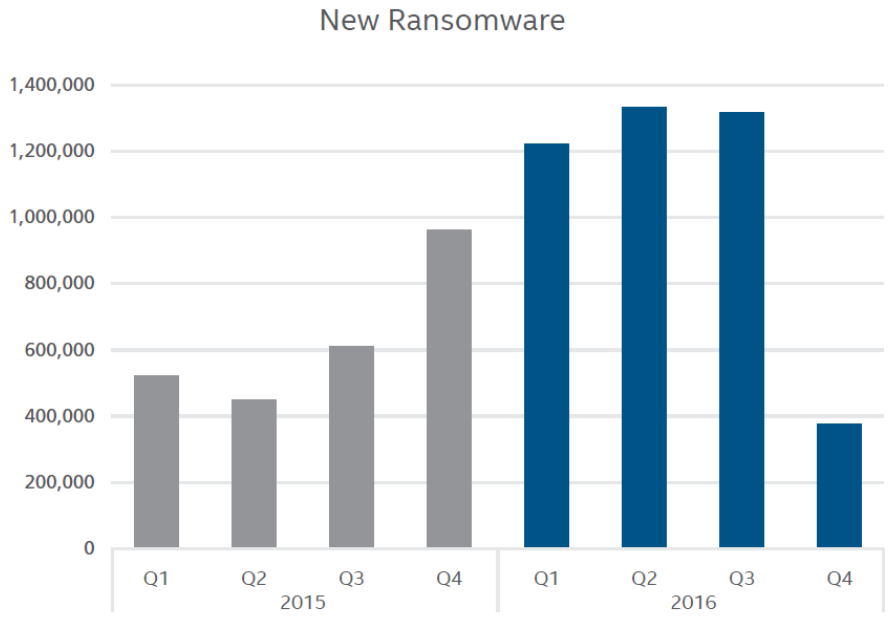


Source: McAfee Labs, 2017.

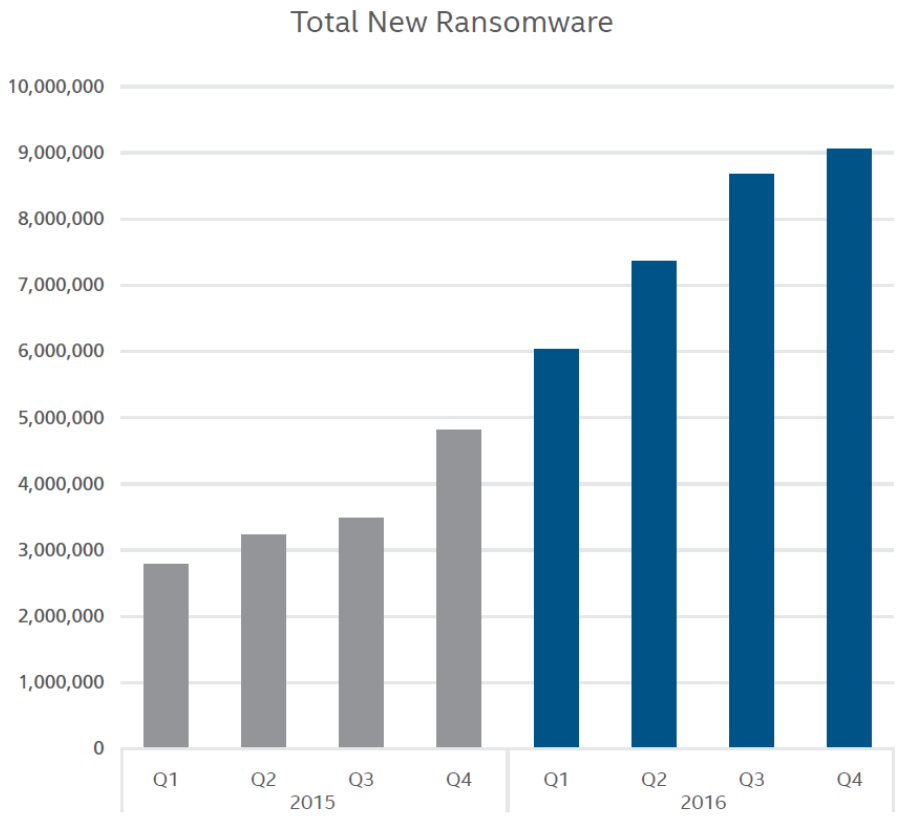
Мировая статистика

PACIFICA

» Количество программ-вымогателей



Source: McAfee Labs, 2017.



Source: McAfee Labs, 2017.

На сегодняшний день вымогатель *Locky* распространился по **114** странам мира, в том числе и в Казахстане

Наиболее распространенные семейства программ-вымогателей

PACIFICA

	Название	Вердикты*	Доля пользователей**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32%
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07%
3	TeslaCrypt (был активен до мая 2016 г.)	Trojan-Ransom.Win32.Bitman	6,54%
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85%
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79%
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36%
7	Shade	Trojan-Ransom.Win32.Shade	1,73%
8	(Generic-вердикт)	Trojan-Ransom.Win32.Snocry	1,26%
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15%
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90%

* Детектирующие вердикты продуктов «Лаборатории Касперского». Информация получена от пользователей продуктов «Лаборатории Касперского», давших свое согласие на передачу статистических данных.

** Процент пользователей, атакованных данным семейством шифровальщиков-вымогателей, от числа всех пользователей, атакованных шифровальщиками-вымогателями.

Проект «No More Ransom»

PACIFICA

NO MORE RANSOM!

» Проект «No More Ransom» был запущен в июле 2016 года совместными усилиями:

EUROPOL EC3 European Cybercrime Centre | POLITIE | KASPERSKY lab | intel Security

Powered by: powered by amazon web services | Barracuda

Троянец-вымогатель – это вредоносное ПО, которое, попав в компьютер или мобильное устройство, блокирует или зашифровывает файлы. Вы не сможете получить доступ к своим данным, не заплатив выкуп. Однако ни каких гарантий нет, и платить ни в коем случае не следует!

https://www.nomoreransom.org/

PACIFICA

ТОО «ПАЦИФИКА»

Офис в г. Алматы: ул. Тимирязева 42, Бизнес-центр «Экспо-сити», Павильон 15/7

Тел.: +7 (727) 334-15-74; +7 (727) 334-15-67

Офис в г. Астана: ул. Кунаева 29/1, ГК «Дипломат», офис 1906, 19 этаж

Тел.: +7 (717) 255-01-42

info@pacifica.kz | www.pacifica.kz

www.facebook.com/Pacifica

Контактное лицо: Исполнительный директор – Павел Гениевский (+7-777-212-0089)