Ну все, приехали!..

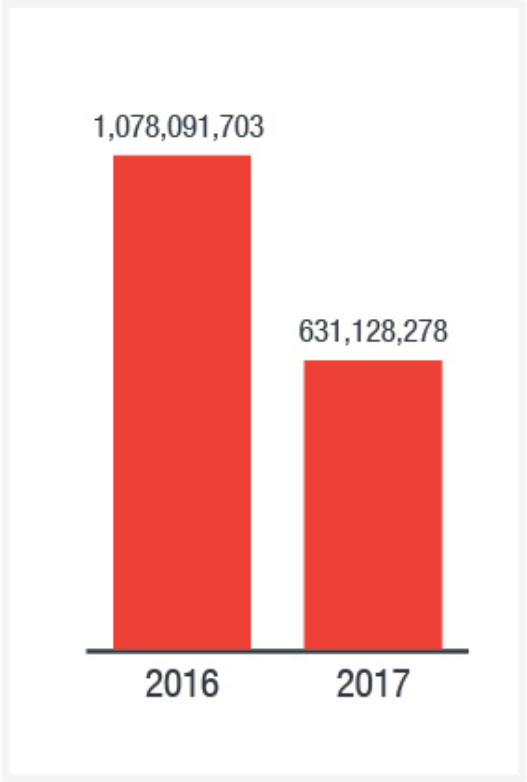
Михаил Кондрашин

Оглавление

- Хорошая новость (спойлер: остальные будут плохими)
- Стремительное изменение ландшафта
- Главная гроза безопасности

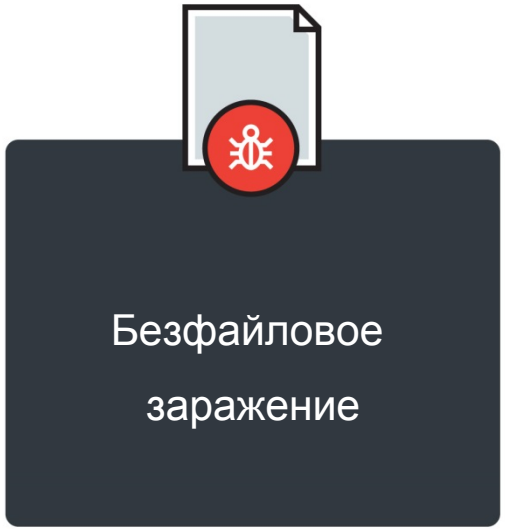
На самом деле:

- Видосики
- Головоломки
- Секс

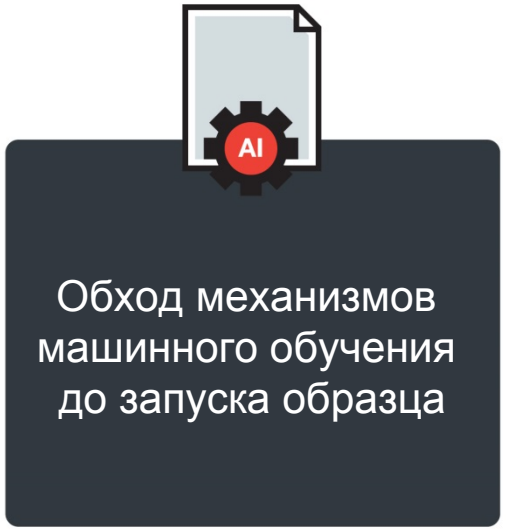


Число угроз, связанных с программами-вымогателями уменьшилось на 41%

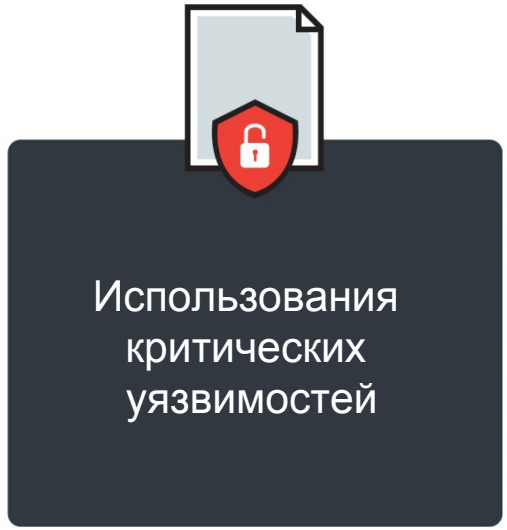
Примечательные особенности программ-вымогателей в 2017



Безфайловое заражение



Обход механизмов машинного обучения до запуска образца



Использования критических уязвимостей

Программы-вымогатели в 2017

94% электронная почта

5% URL

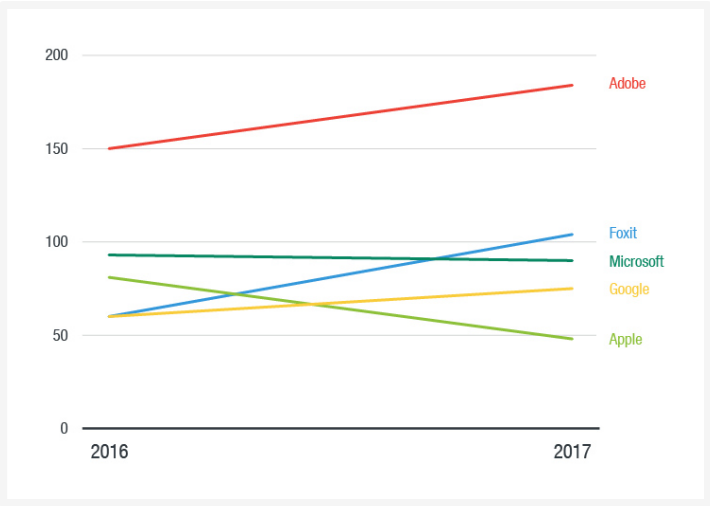
1% файл

Кейс: угрозы в документах

- Угрозы в исполняемых файлах, документы безвредны
- Макровирусы только в .DOC, давайте пользоваться RTF
- Редактируемые форматы опасны, пришлите в PDF
- Adobe Acrobat — это дыра на дыре, нужно пользоваться альтернативными приложениями…

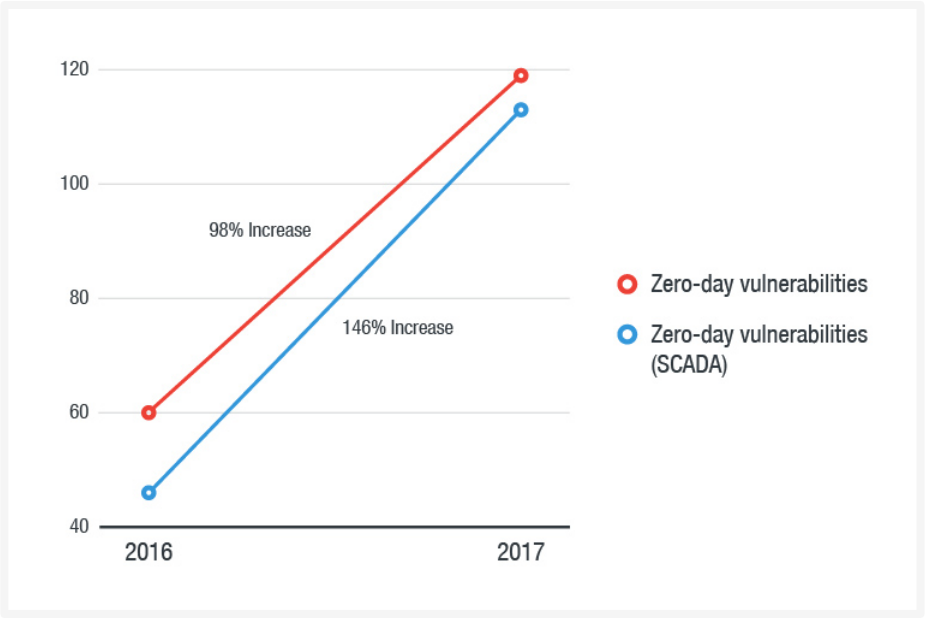
Еще больше уязвимостей найдено в продуктах Adobe, Google и Foxit

	2016	2017	
Adobe	150	184	↑
Google	60	75	↑
Apple	81	48	↓
Microsoft	93	90	↓
Foxit	60	104	↑



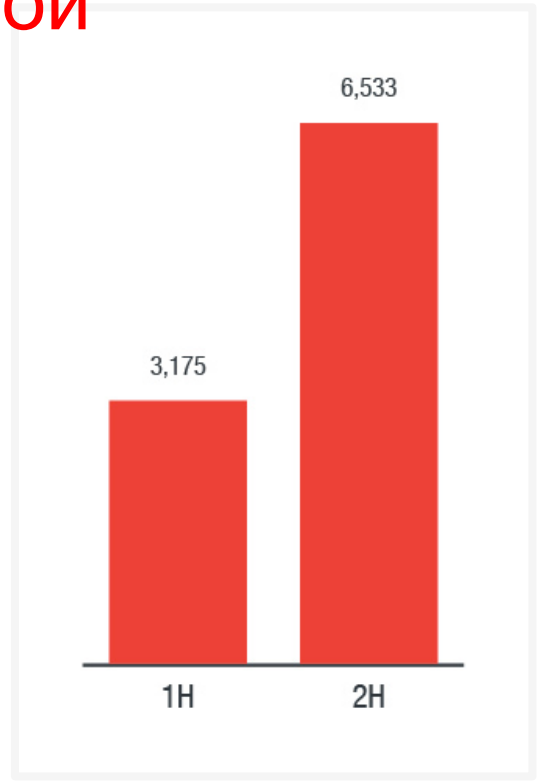
Рост уязвимостей нулевого дня, выявленных в системах АСУ ТП

	2016	2017
Уязвимости нулевого дня	60	119
Уязвимости нулевого дня в АСУ ТП	46	113



Значительный рост попыток BEC «компрометация деловой корреспонденции»

	1H	2H
Попыток BEC в 2017	3,175	6,533



Криптовалютные угрозы

- Приложения со скрытыми функциями майнинга
- Распространение майнинговых ботов через социальные сети
- Взлом криптовалютных кошельков
- Аферы с приемами социальной инженерии
- Вебсайты с манинговыми скриптами
- Инструментарии для взлома внедряющие майнинговый код на компьютер жертвы
- Рекламные сети распространяющие майнинговые сценарии

Защита от изощренных угроз

обозначения
«хорошие» файлы
«плохие» файлы
«неизвестные» файлы