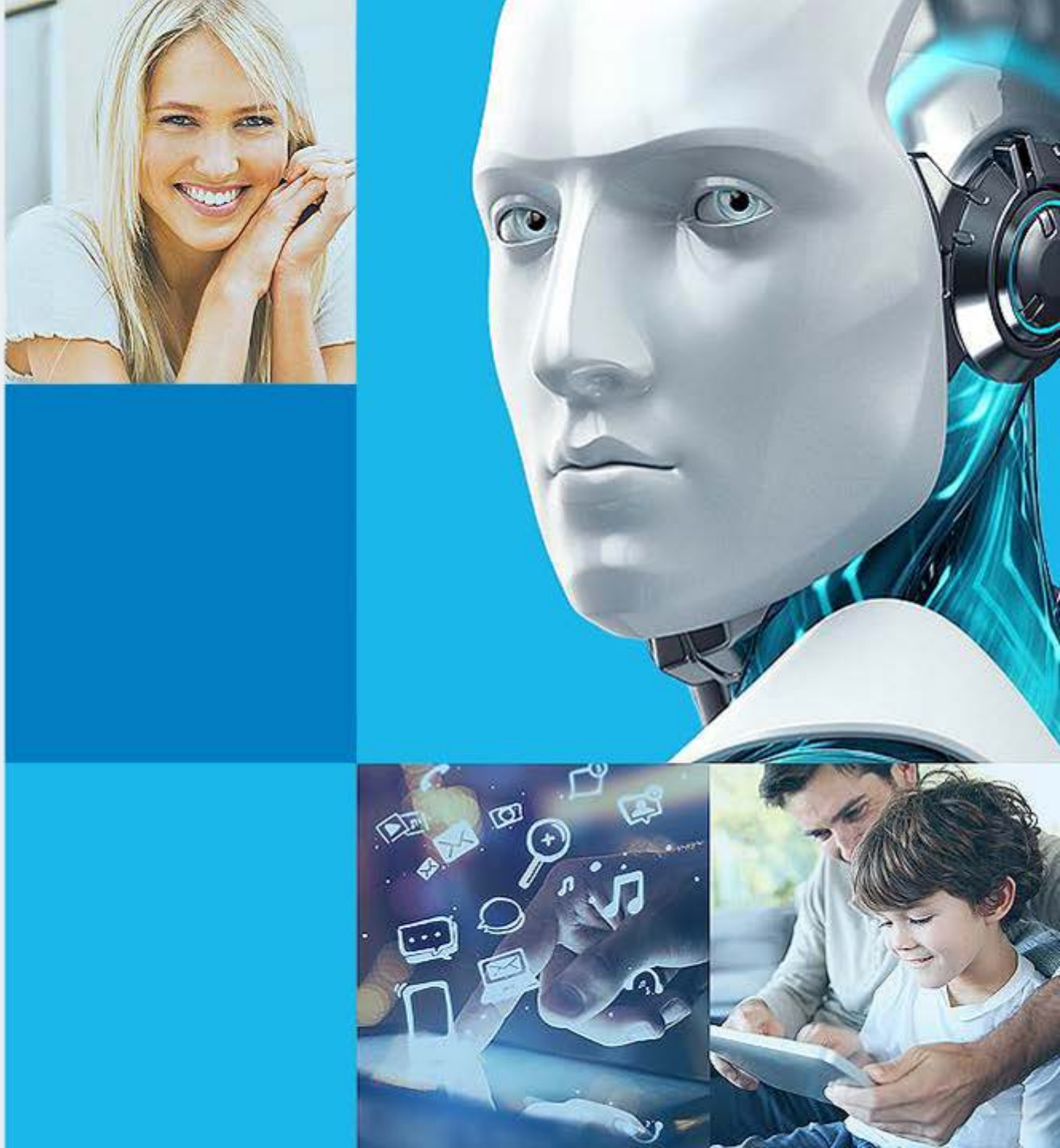
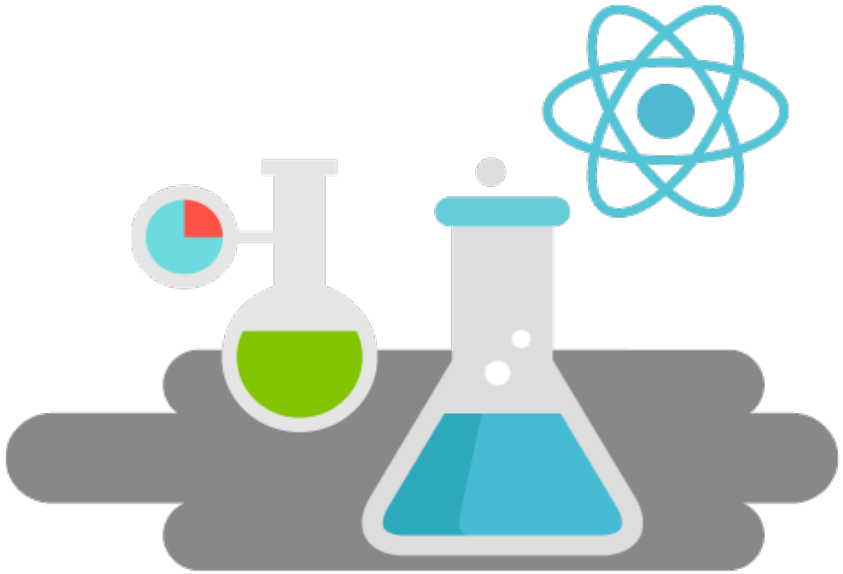
СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ И СПОСОБЫ ЗАЩИТЫ

Жанибек Шутбаев
ESET Kazakhstan

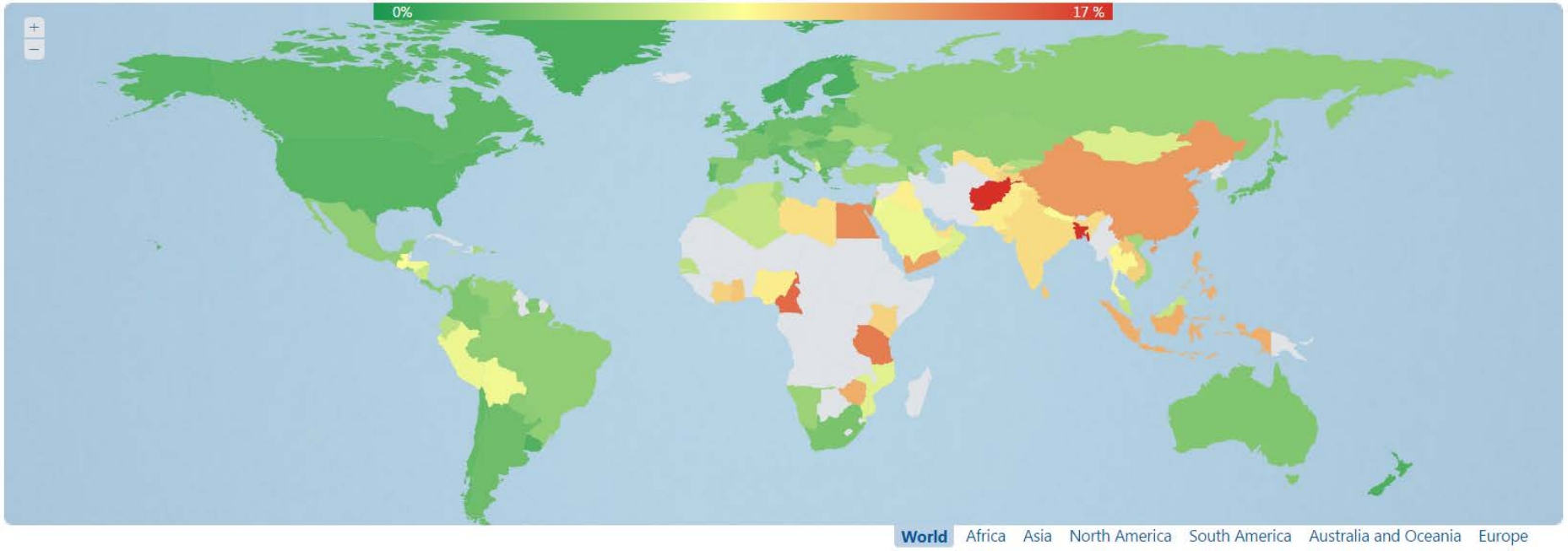


ВИРУСНАЯ ЛАБОРАТОРИЯ ESET

- **500 000** образцов вредоносного ПО каждый день
- **200** образцов мобильных угроз каждый месяц
- В **2014-2015** гг. фиксируется вредоносное ПО для всех устройств: POS-терминалы, банкоматы, роутеры, носимые устройства
- Двухкратный рост числа APT-атак в **2014-2015** гг.
- **ТОП-3** вектора атак: e-mail, 0day, эксплойты



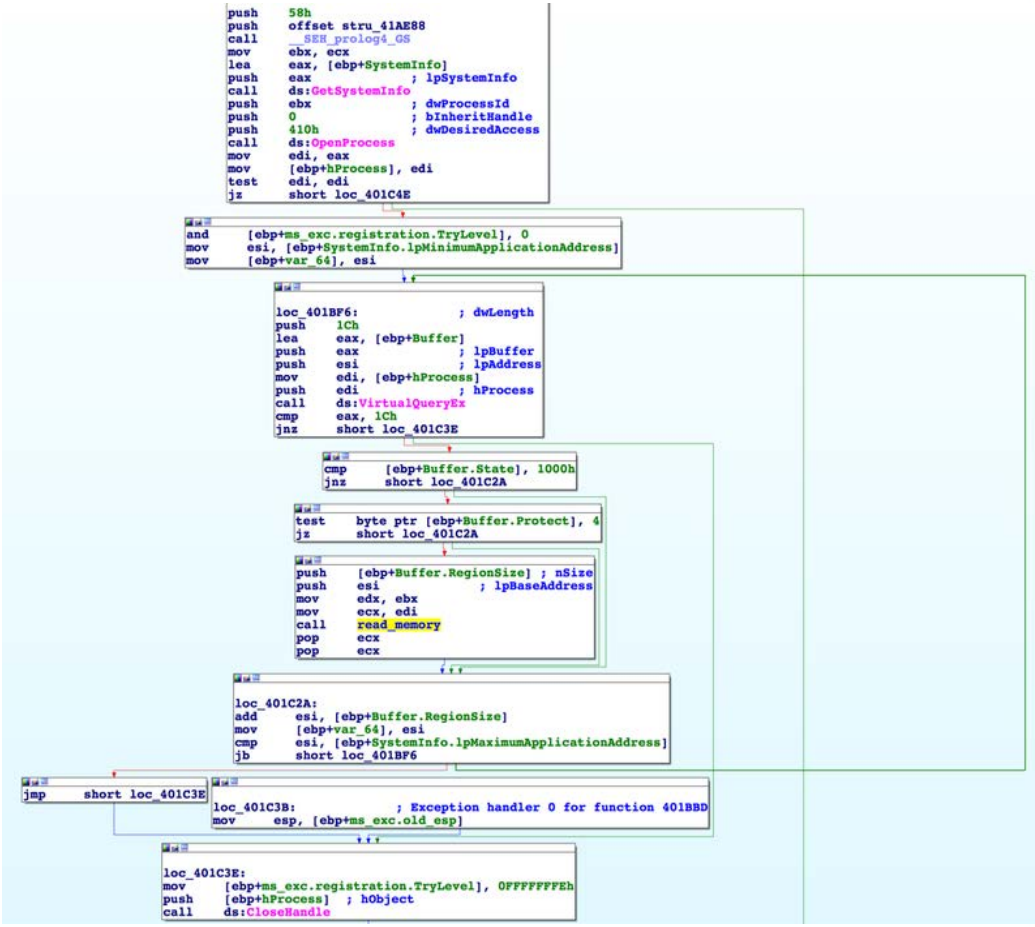
ВИРУСНАЯ ЛАБОРАТОРИЯ ESET



Пример сложного вектора атак

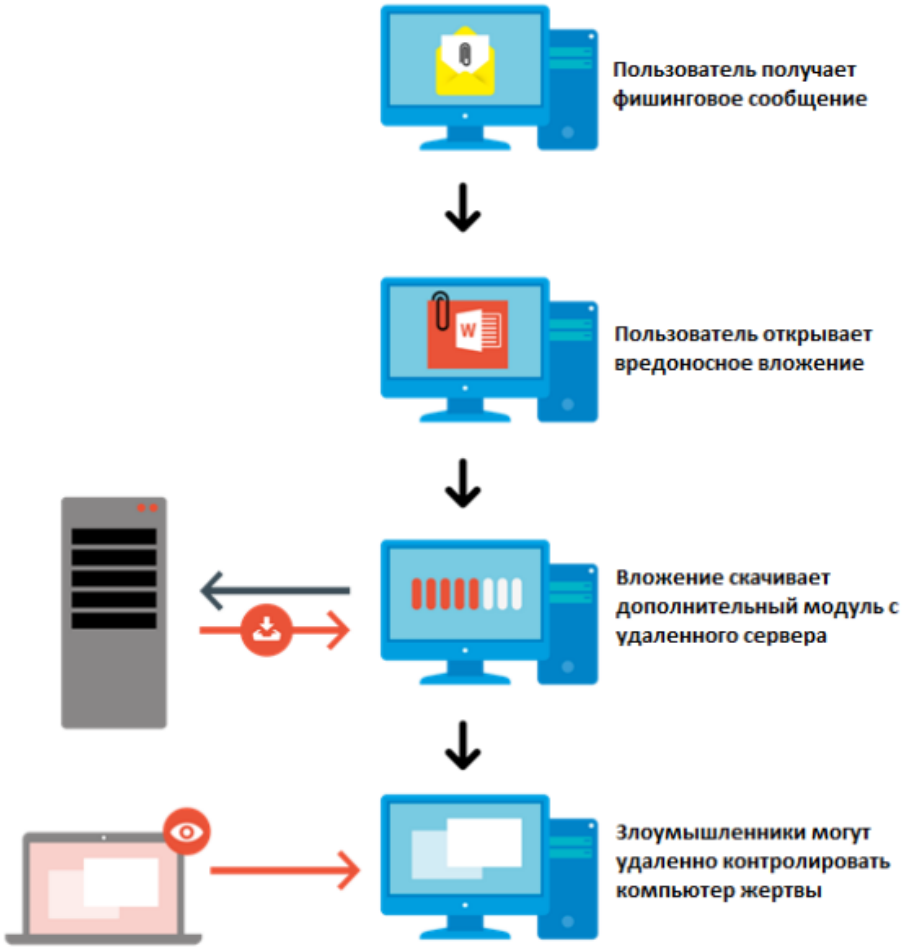
FINDPOS

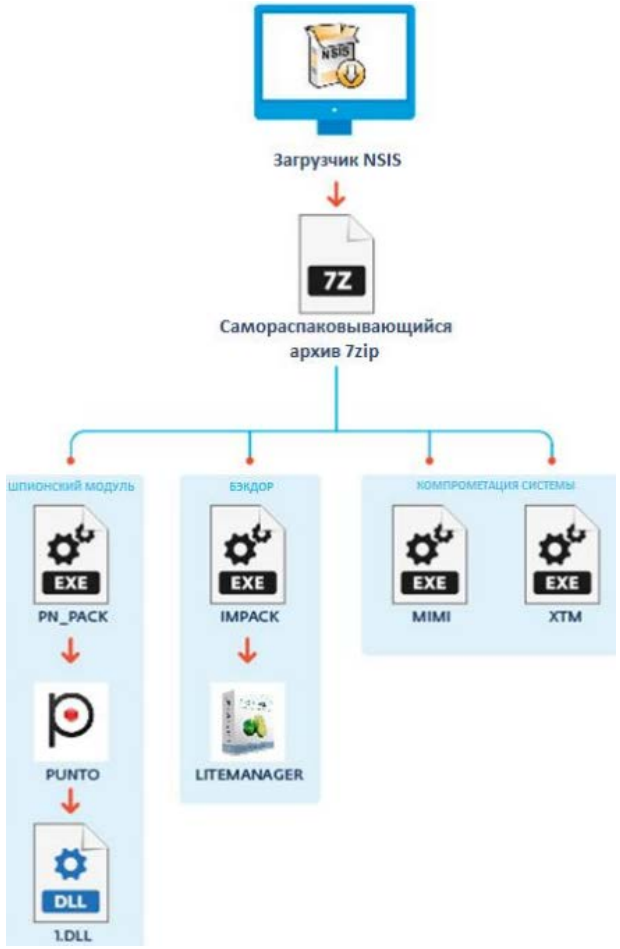
- Внедряет свой код в процесс, отвечающий за получение информации с магнитной ленты банковской карты
- Отправка скопированных из памяти данных на удаленный сервер (exfiltration) выполняется с использованием POST-запроса HTTP-протокола
- Данные перед отправкой переименовываются



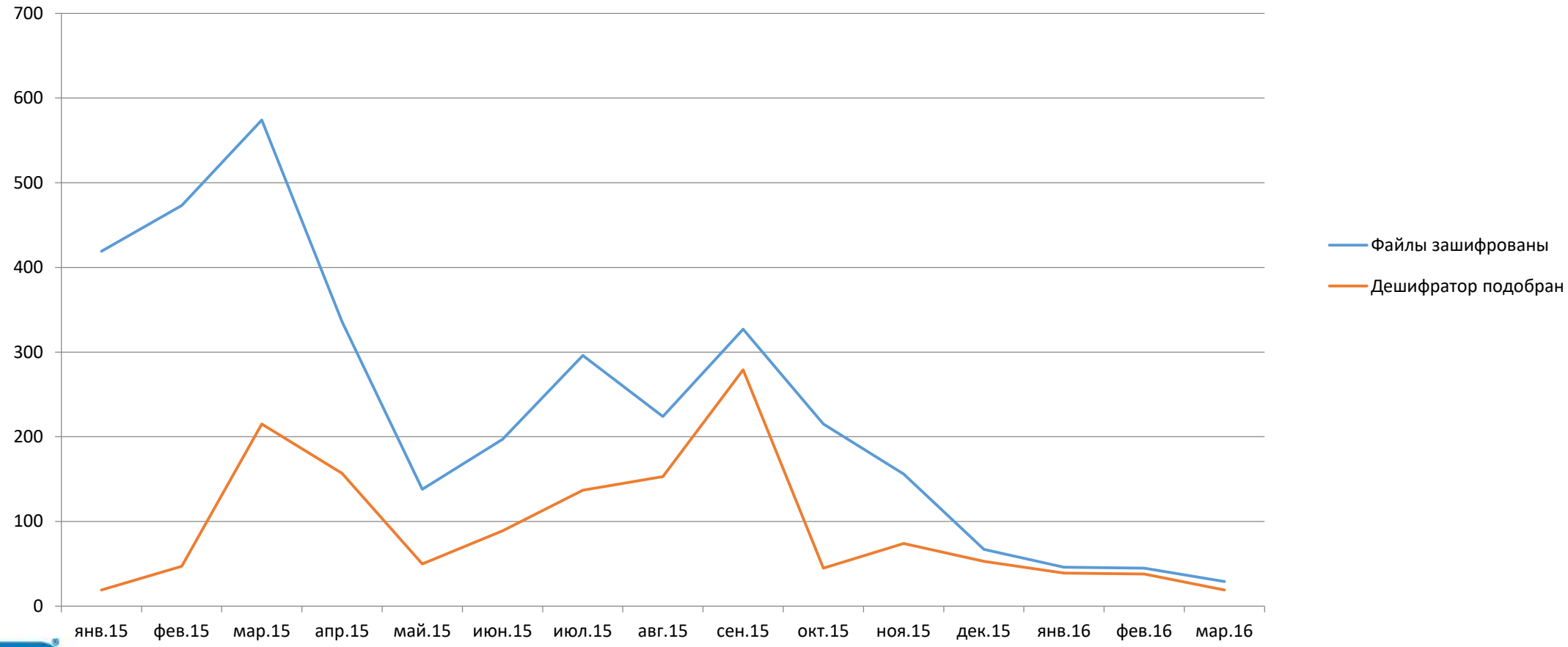
ШИФРАТОРЫ

СЦЕНАРИЙ ЗАРАЖЕНИЯ



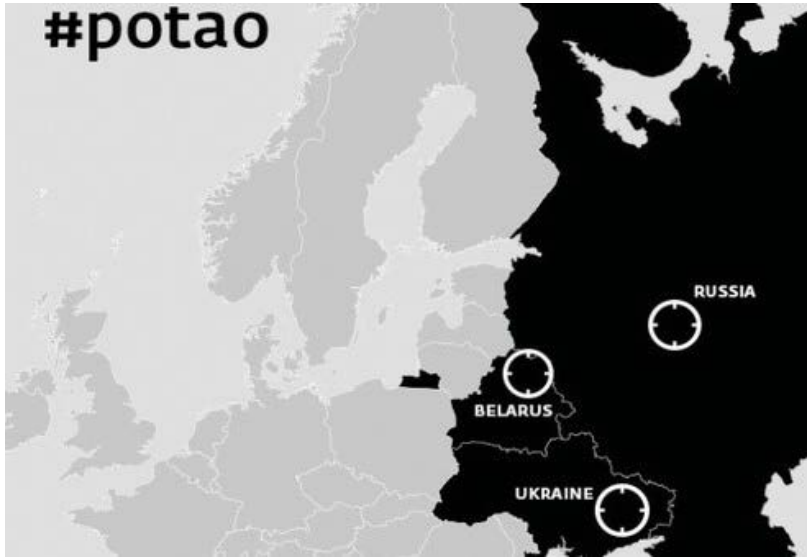


ШИФРАТОРЫ


700
600
500
400
300
200
100
0
янв.15
фев.15
мар.15
апр.15
май.15
июн.15
июл.15
авг.15
сен.15
окт.15
ноя.15
дек.15
янв.16
фев.16
мар.16
Файлы зашифрованы
Дешифратор подобран

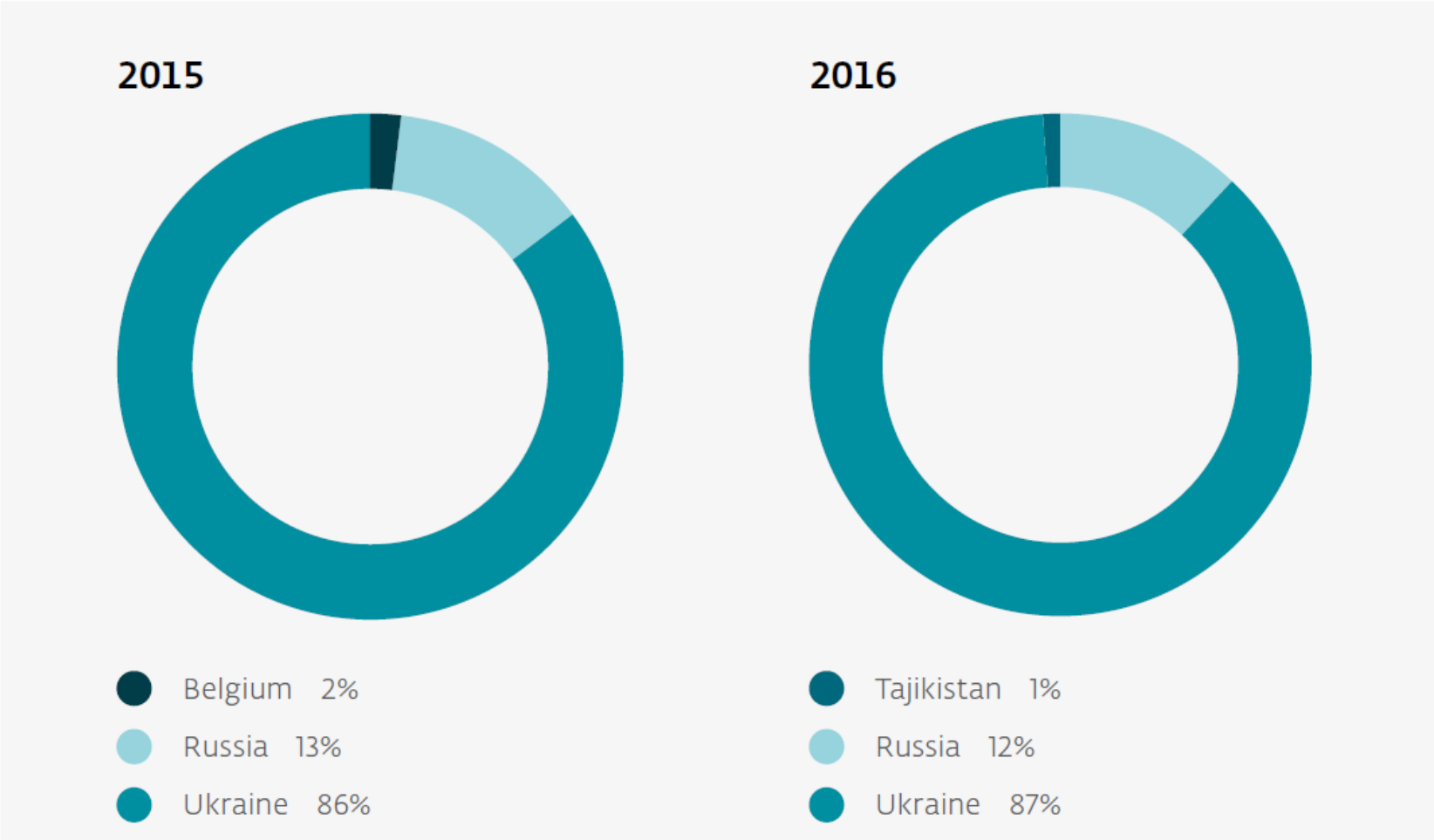
КИБЕРАТАКИ

ВОСТОЧНАЯ ЕВРОПА – В ЦЕНТРЕ КИБЕРАТАК



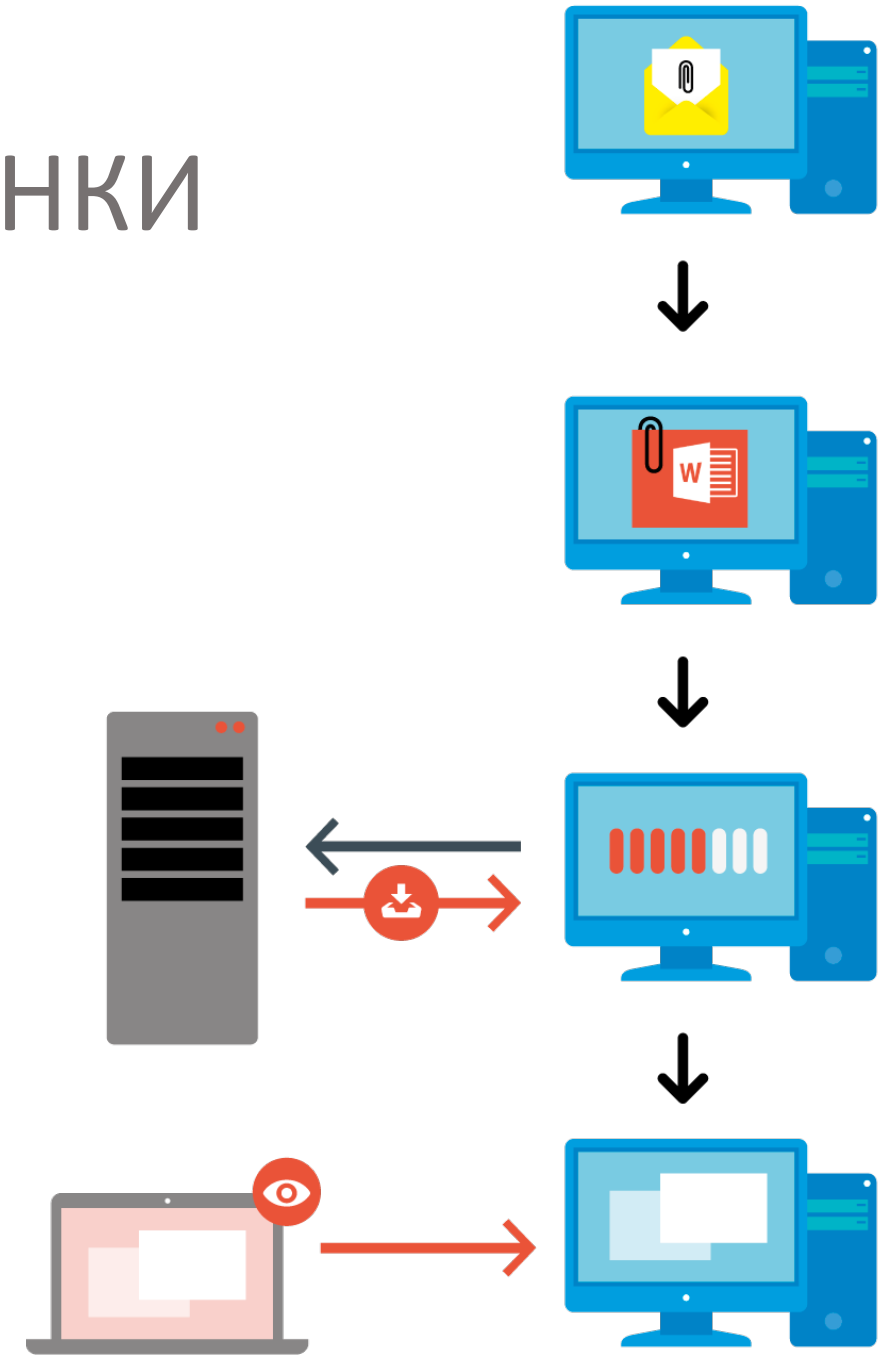
АТАКИ НА ГОССЕКТОР и КИБЕРШПИОНАЖ

Операция «Прикормка»



АТАКИ НА БАНКИ

«Ловушка для бухгалтера»



Пользователь получил спам

Открывает зараженный word-файл

Файл скачивает допмодуль

За жертвой можно следить

АТАКИ НА ЭНЕРГЕТИКУ

- Более **60%** сотрудников открыли зараженные файлы.
- **38%** выслали личную и конфиденциальную информацию.
- Сотрудники ИТ и ИБ также попали в первые два пункта.

ПРОДУКТЫ ESET

	РАБОЧИЕ СТАНЦИИ	МОБИЛЬНЫЕ УСТРОЙСТВА	ФАЙЛОВЫЕ СЕРВЕРЫ	ПОЧТОВЫЕ СЕРВЕРЫ	ШЛЮЗЫ	ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ
ESET NOD32 SECURE ENTERPRISE	■	■	■	■	■	■
ESET NOD32 SMART SECURITY BUSINESS EDITION	■	■	■			■
ESET NOD32 BUSINESS EDITION	■	■	■			■
ESET NOD32 MAIL SECURITY FOR MICROSOFT EXCHANGE				■		■
ESET NOD32 MAIL SECURITY FOR LINUX/BSD/SOLARIS				■		■
ESET NOD32 ANTIVIRUS FOR LOTUS DOMINO				■		■
ESET NOD32 FOR KERIO CONNECT				■		■
ESET NOD32 GATEWAY SECURITY FOR LINUX/BSD/ SOLARIS					■	■
ESET NOD32 FOR KERIO CONTROL					■	■

eset

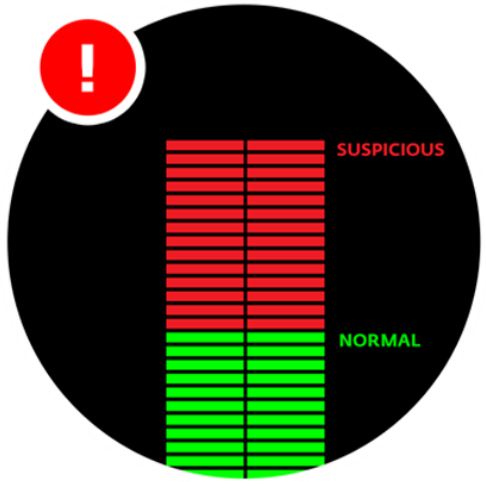
MITSUBISHI
MOTORS

ТЕХНОЛОГИИ ESET

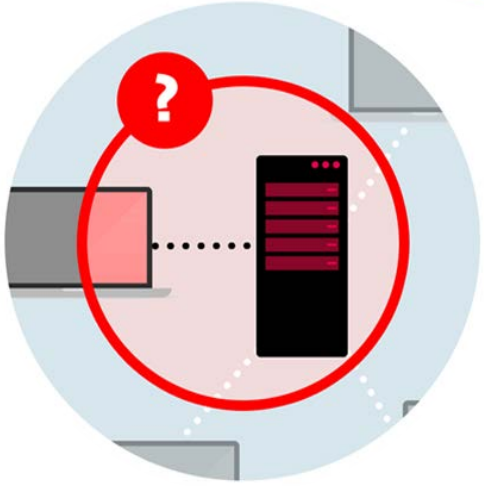
Антифишинг

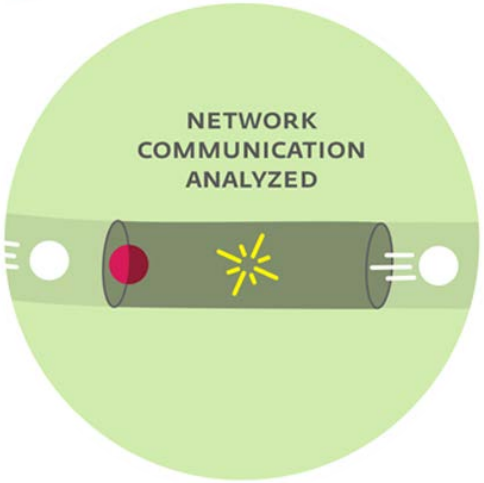
Защита от эксплойтов

Расширенное сканирование памяти



Защита от ботнетов





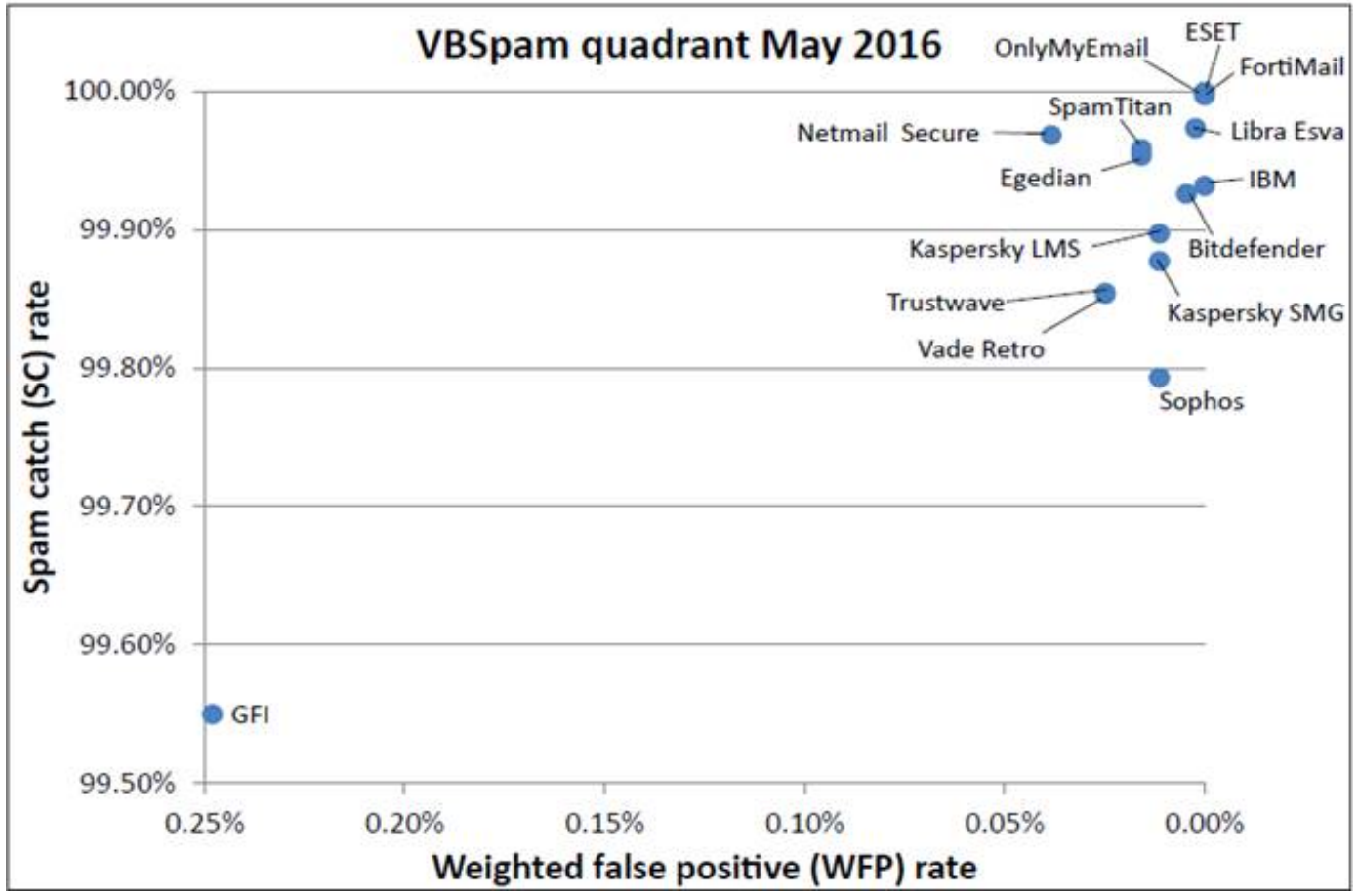
Щит уязвимости


BURGER
KING
TM

ЗАЩИТА ПОЧТЫ – отражение 90% атак

ESET Mail Security for Exchange

- Антивирусная защита
- Антиспам
- Централизованное управление



СПАСИБО ЗА ВНИМАНИЕ