ROMAD

Stop chasing. Start eradicating.™

РЕШЕНИЕ ДЛЯ КИБЕРЗАЩИТЫ В ПОСТ - АНТИВИРУСНОМ МИРЕ

Игорь Козаченко, CVO

Ihor.Kozachenko@romad-systems.com

Ihor.Kozachenko@romad.com.ua

www.romad-systems.com

www.romad.com.ua

Обзор рынка

На сегодняшний день в мире используется более 5,7 млрд. устройств

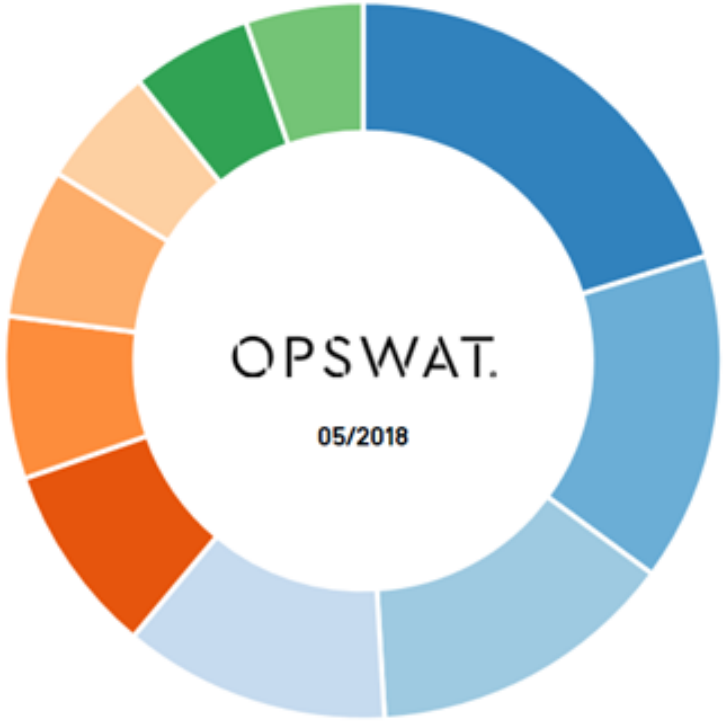
Количество пользователей гаджетов с доступом к Интернету в мире достигло 4,021 млрд. человек

По данным компании Microsoft только 45% всех пользователей (1,8095 млрд.чел) устанавливают защиту от зловредов

Распределение антивирусного рынка

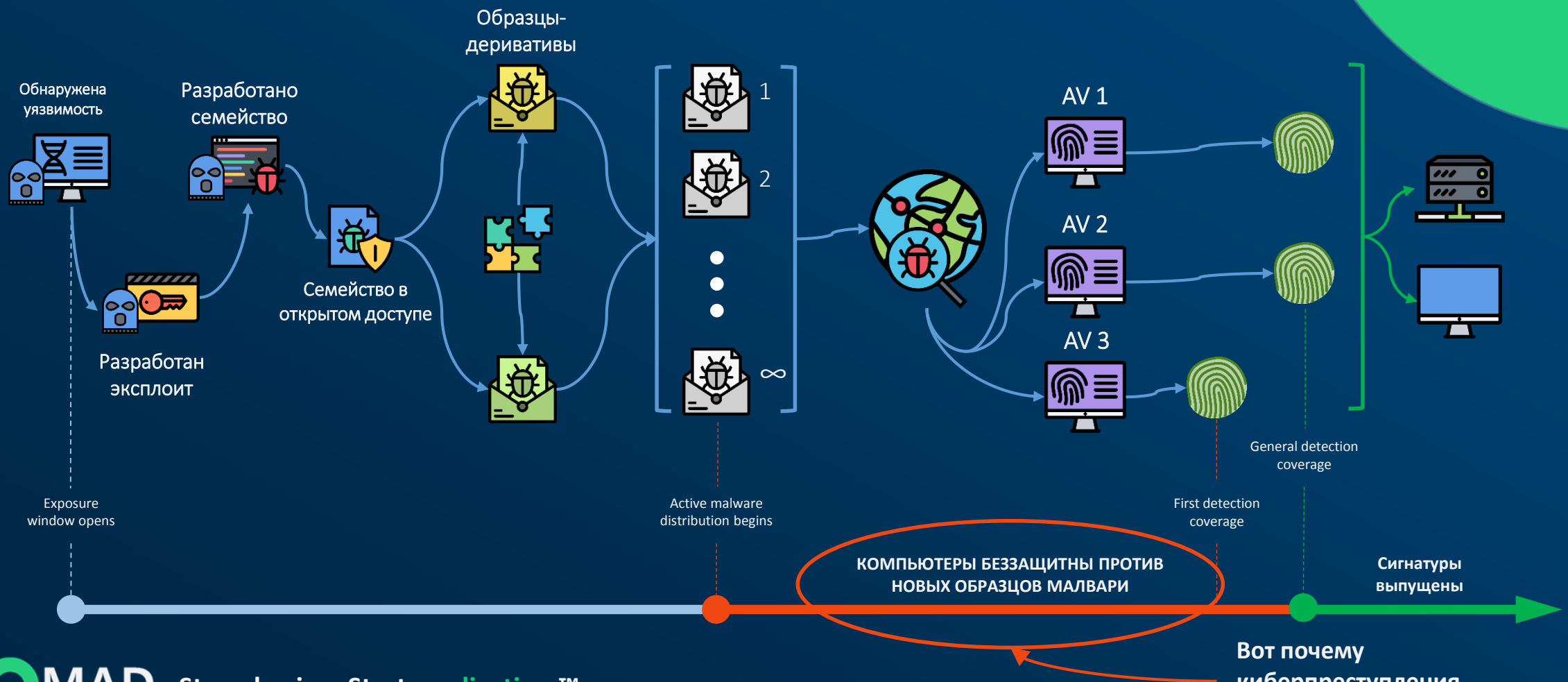
Данные указаны только для MS Windows устройств

AVAST Software a.s.	18.11%
ESET	13.25%
Malwarebytes	12.45%
McAfee, Inc.	10.74%
Bitdefender	7.69%
Webroot Inc	6.54%
Safer-Networking Ltd.	6.03%
Avira GmbH	4.91%
Kaspersky Lab	4.86%
Sophos Limited	4.74%



Зазор “Время-до-Детекта”

AV полагаются на статические сигнатуры.
Иными словами, по сигнатуре на каждый образец.



Вот почему киберпреступления ВЫГОДНЫ

ROMAD **Stop chasing. Start eradicating.™**

Проигранная битва

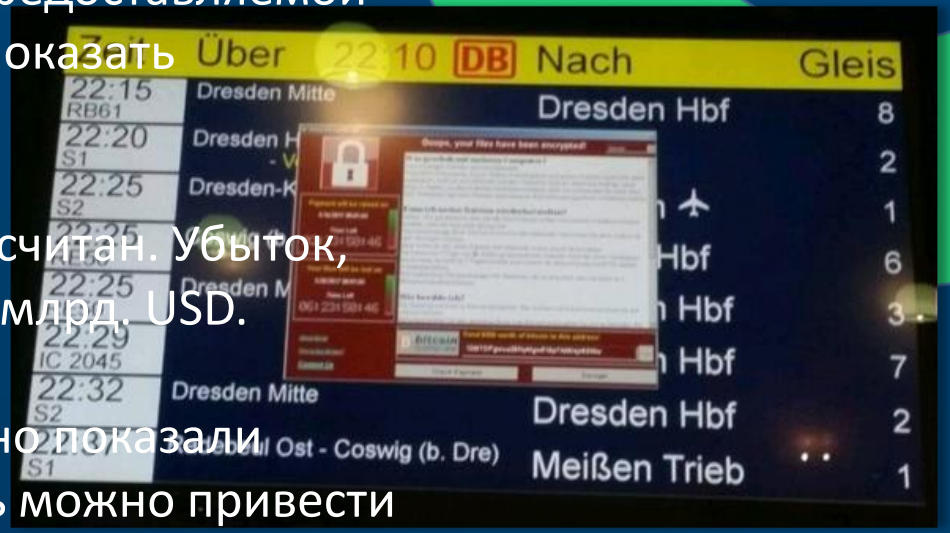
Количество новых штаммов превышает 140 млн. в год

Всего топ **50 семейств** отвечают за **>80% инфицирований**

ROMAD обнаруживает семейства, а не отдельные штаммы

Показательная статистика

В мае 2017 года произошло массовое распространение вируса-шифровальщика WannaCry. Эта атака впервые публично обнажила иллюзорность предоставляемой классической безопасности. Традиционные антивирусы не смогли оказать противодействие новому виду атаки.

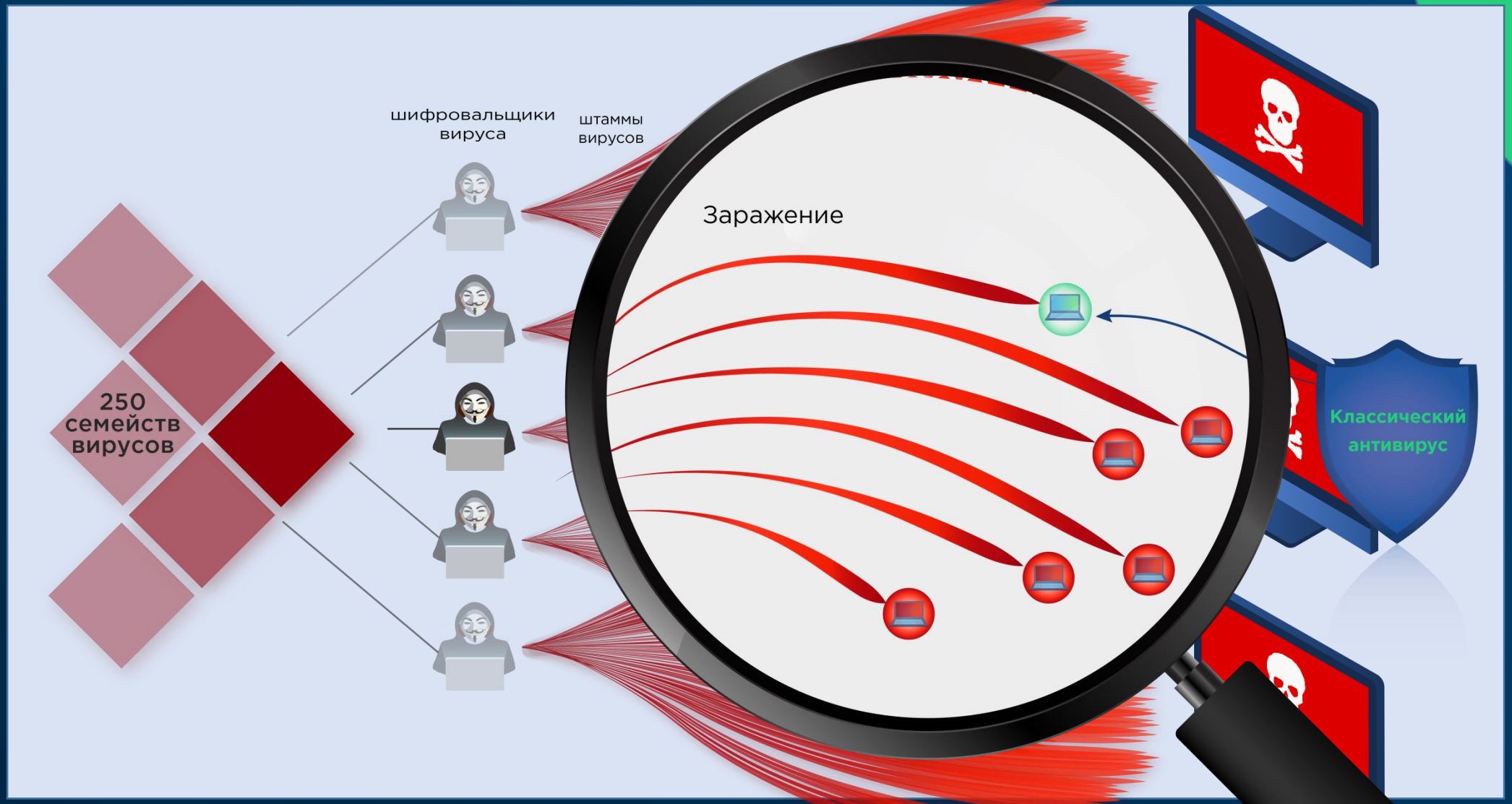


Мировой убыток, причиненный атакой WannaCry, до конца не подсчитан. Убыток, нанесенный только B2B рынку, за первые 4 дня атаки, превысил 1 млрд. USD.

Атаки вирусов-шифровальщиков NotPetya и BadRabbit окончательно показали несостоятельность традиционных антивирусов. Для оценки потерь можно привести в пример компанию Fedex, с убытком, причиненным вирусом NotPetya, в 300 млн. USD. Fedex, конечно же, был защищен одними из самых лучших вариантов классических антивирусов. Тем не менее, защитные меры не дали нужного результата.

Владельцам криптоактивов из-за прямой финансовой привлекательности для злоумышленников, тем более, не стоит считать себя в безопасности. Помимо этого известны и примеры взлома криптобирж с использованием malware

Классический антивирус



Хьюстон, у нас проблема!

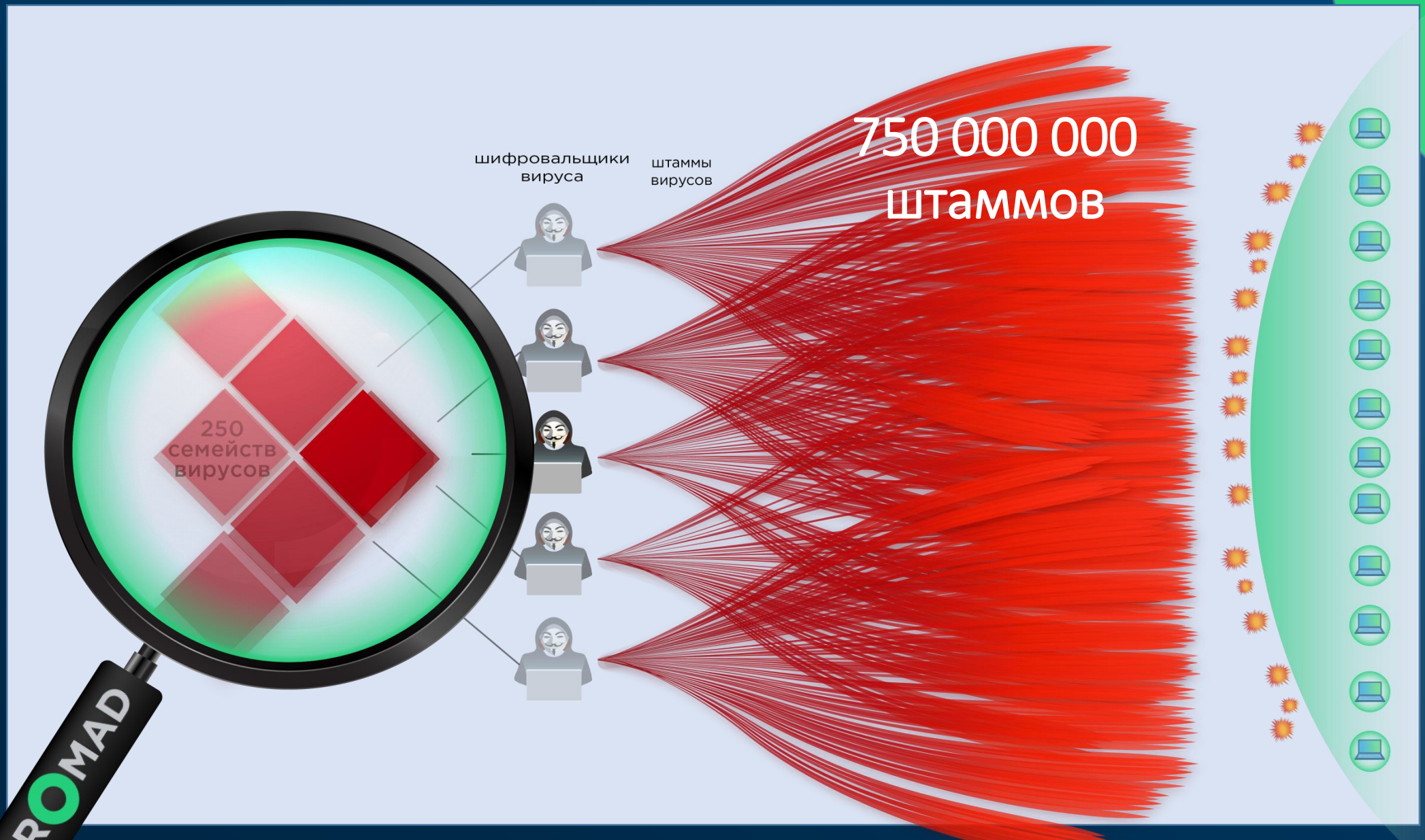
Ответ индустрии киберзащиты

Решения Следующего Поколения (Next Generation)

Gartner классифицирует решения:

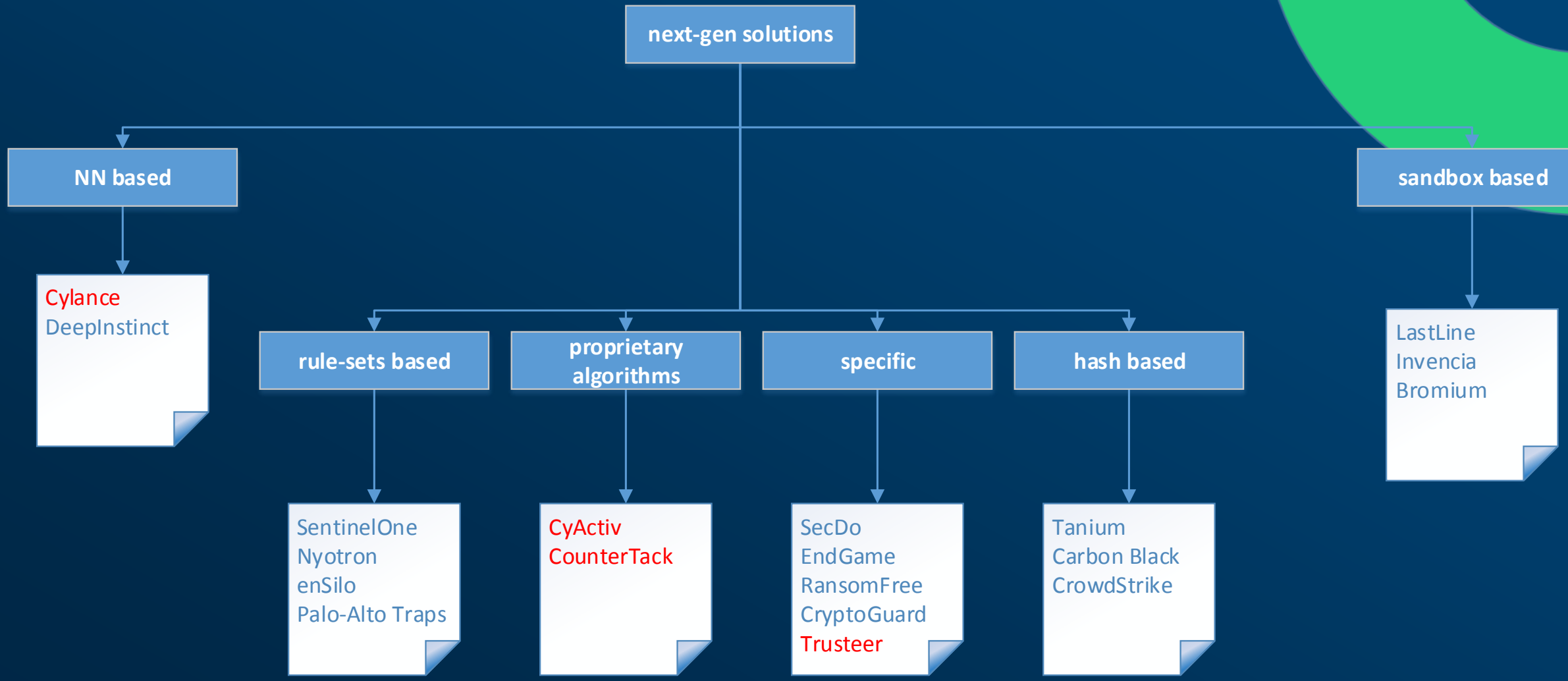
- EPP (Endpoint Protection Platform)
- EDR (Endpoint Detection and Response)

NG EDR – новое решение киберзащиты

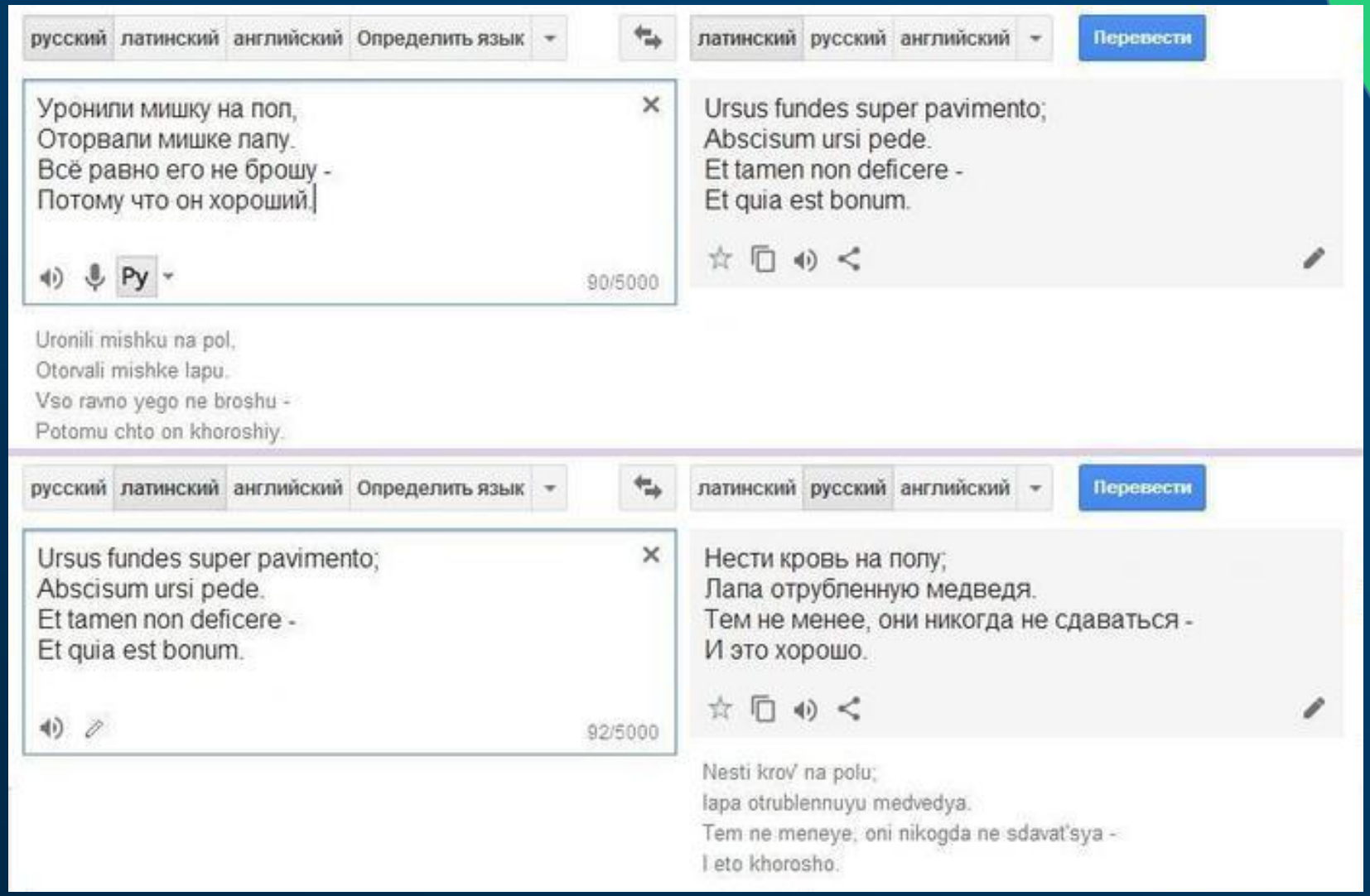


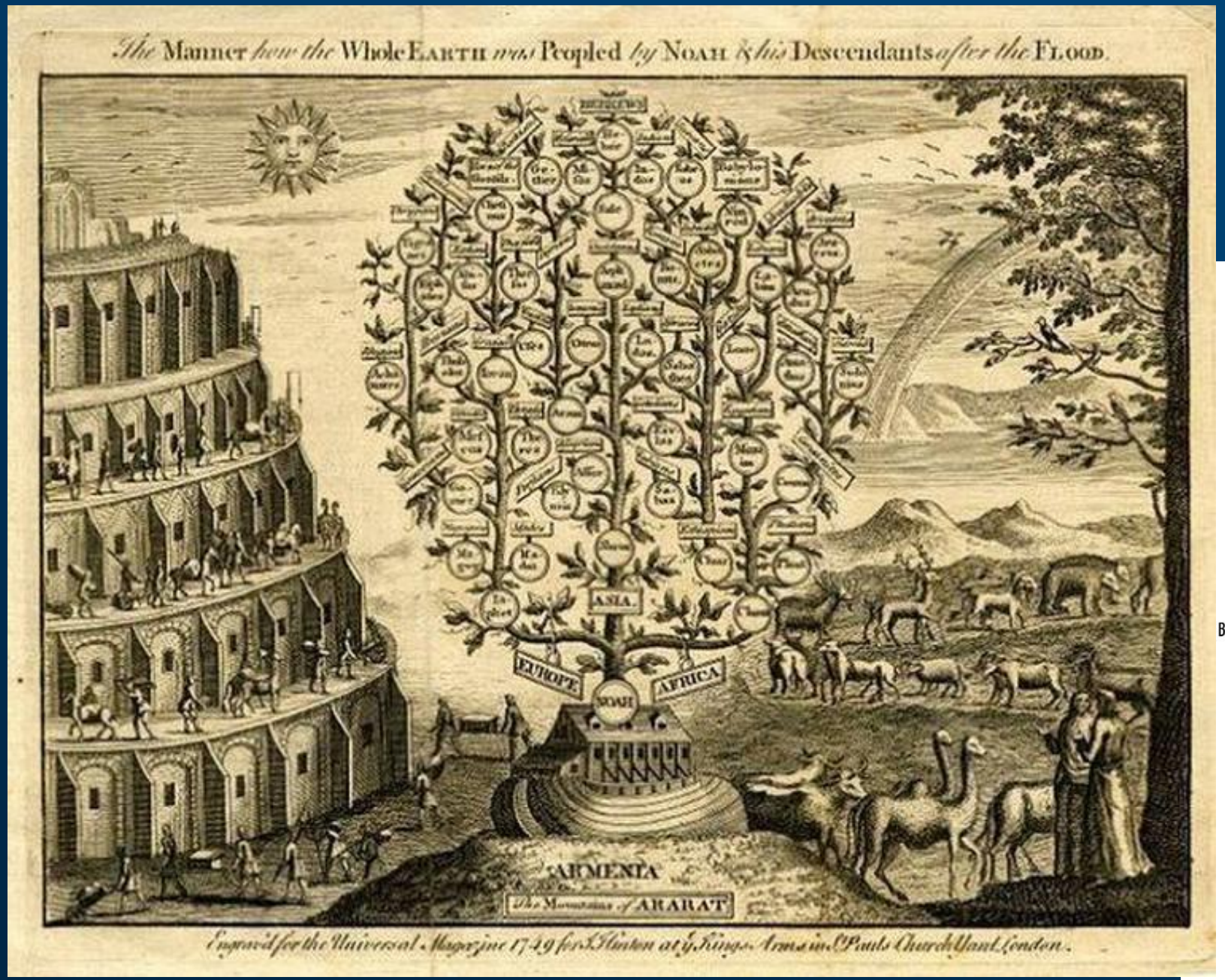
ROMAD

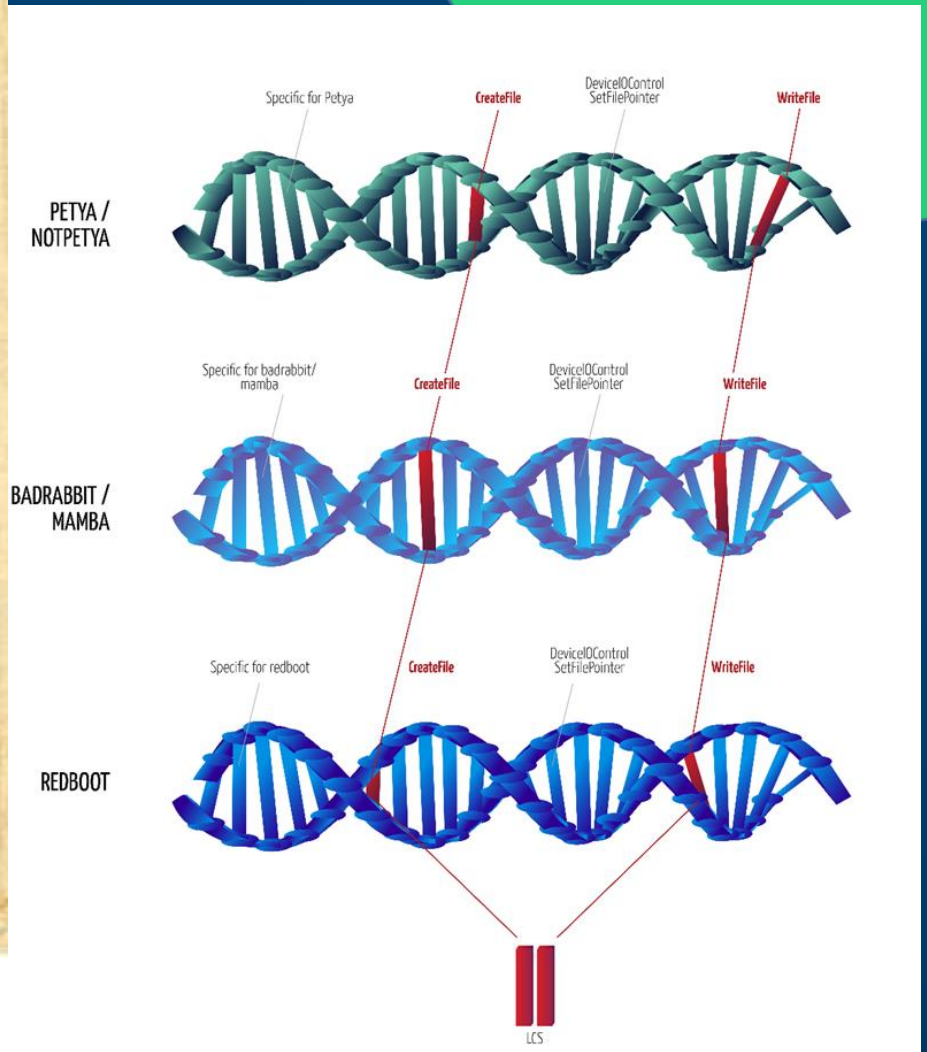
Рынок NG EDR


next-gen solutions
NN based
sandbox based
Cylance
DeepInstinct
rule-sets based
proprietary algorithms
specific
hash based
LastLine
Invencia
Bromium
SentinelOne
Nyotron
enSilo
Palo-Alto Traps
CyActiv
CounterTack
SecDo
EndGame
RansomFree
CryptoGuard
Trusteer
Tanium
Carbon Black
CrowdStrike

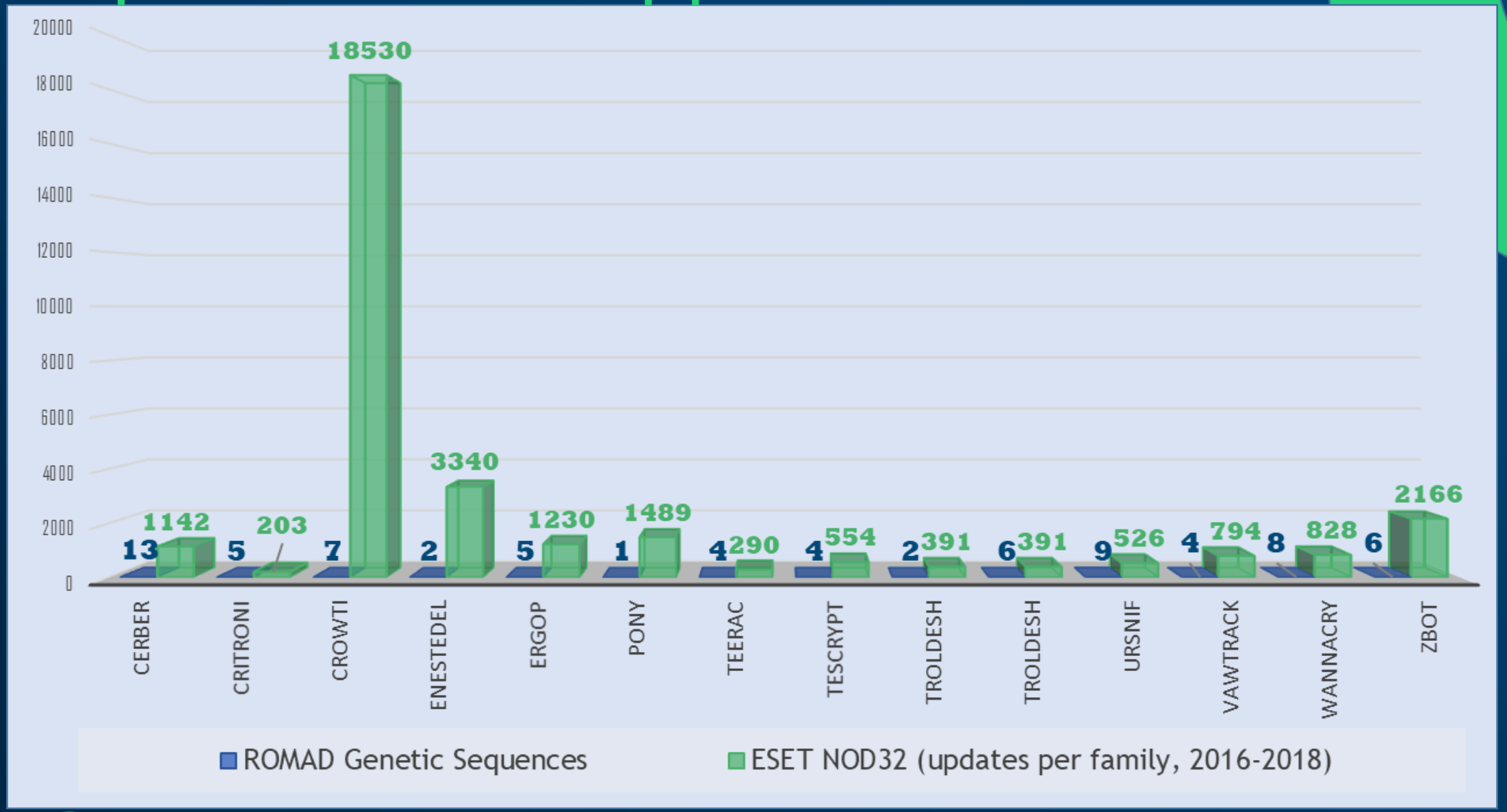
И это хорошо


русский латинский английский Определить язык
латинский русский английский
Перевести
Уронили мишку на пол,
Оторвали мишке лапу.
Всё равно его не брошу -
Потому что он хороший.
Ру
90/5000
Ursus fundes super pavimento;
Abscisum ursi pede.
Et tamen non deficere -
Et quia est bonum.
Uronili mishku na pol,
Otorvali mishke lapu.
Vso ravno yego ne broshu -
Potomu chto on khoroshiy.
русский латинский английский Определить язык
латинский русский английский
Перевести
Ursus fundes super pavimento;
Abscisum ursi pede.
Et tamen non deficere -
Et quia est bonum.
92/5000
Нести кровь на полу;
Лапа отрубленную медведя.
Тем не менее, они никогда не сдаваться -
И это хорошо.
Nesti krov' na polu;
lapa otrublennuyu medvedya.
Tem ne meneye, oni nikogda ne sdavat'sya -
I eto khorosho.


The Manner how the Whole Earth was Peopled by Noah & his Descendants after the Flood.
ASIA
EUROPE
AFRICA
NOAH
ARMENIA
The Mountains of ARARAT
Engraved for the Universal Magazine 1749 for S. Hinton at ye Kings Arms in St Pauls Church Yard London.


PETYA / NOTPETYA
Specific for Petya
CreateFile
DeviceIOControl SetFilePointer
WriteFile
BADRABBIT / MAMBA
Specific for badrabbit/ mamba
CreateFile
DeviceIOControl SetFilePointer
WriteFile
REDBOOT
Specific for redboot
CreateFile
DeviceIOControl SetFilePointer
WriteFile
LCS

Сравнительная эффективность



ROMAD™. Позиционирование

- ROBUST
- MALWARE
- DETECTOR

» Проактивный
» Инновационный
» Надежный
» Устойчивый
» Экспертиза Госспецсвязи

Решение Next Gen класса EDR

Next Generation Endpoint Detection and Response,

согласно классификации Gartner

Обнаружение и Реагирование на угрозы для Конечных точек Следующего Поколения

2009 R&D project launched

2011 Malware Genetics™ POC Completed

2012 Patent application for Robust Malware Detection filled

2013 Unsolicited acquisition offer rejected

2014 Endpoint beta shipped. 100k downloads.

2015 Industrial (ICS/SCADA) manufacturer testing completed. Reseller agreement offered.

2016 US Patent 9,372,989 issued. US presence established. First US pilot customer.

Q4 ROMAD TrueProactive™ Threat Defense for Endpoint

ROMAD Stop chasing. Start eradicating.™

ROMAD™ - NG EDR

Миссия:

Искоренить вредоносное программное обеспечение, каким мы его знаем, **в глобальном масштабе**

Основная цель:

Эффективно и постоянно **защищать** данные и информационные системы Конечного Пользователя от вредоносного программного обеспечения

ROMAD защищает Ваши данные так же и в те периоды времени, **пока не работает защита от традиционных антивирусов**

ROMAD

Stop chasing. Start eradicating.™

БЛАГОДАРЮ ЗА ВНИМАНИЕ

www.romad.com.ua
www.romad-systems.com
Ihor.kozachenko@romad-systems.com