ROMAD

Stop chasing. Start eradicating.™

ROMAD TrueProactive™ Threat Defense

Введение в Malware Genetics™ Platform

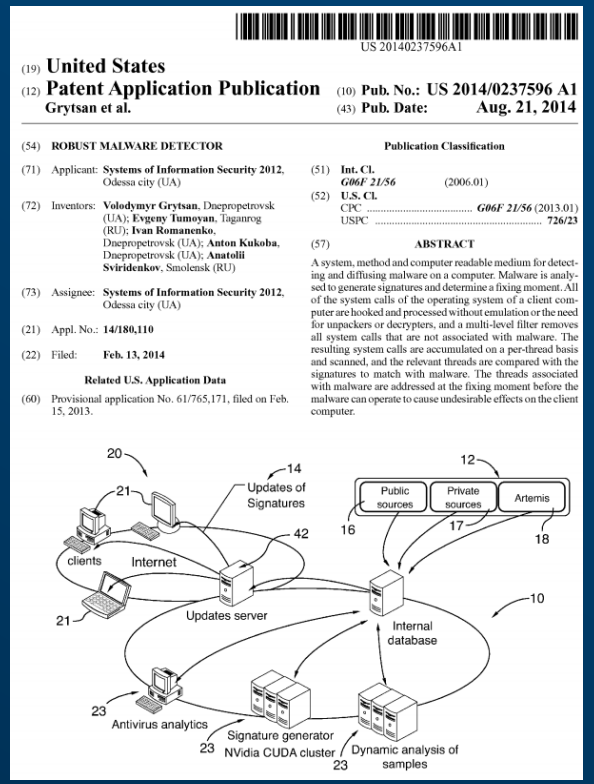
Сентябрь 28, 2017

Vladimir Grytsan, CTO, Co-founder

Масштаб проекта

ROMAD – это **next generation EDR**:

- принцип действия полностью отличается от классического AV: обработка системных вызовов в реальном времени
- решение **enterprise**-уровня
- патент USPTO 9,372,989



US 20140237596A1

(19) **United States**

(12) **Patent Application Publication**
Grytsan et al.

(10) **Pub. No.: US 2014/0237596 A1**

(43) **Pub. Date: Aug. 21, 2014**

(54) **ROBUST MALWARE DETECTOR**

(71) Applicant: **Systems of Information Security 2012**, Odessa city (UA)

(72) Inventors: **Volodymyr Grytsan**, Dnepropetrovsk (UA); **Evgeny Tumoyan**, Taganrog (RU); **Ivan Romanenko**, Dnepropetrovsk (UA); **Anton Kukoba**, Dnepropetrovsk (UA); **Anatolii Sviridenkov**, Smolensk (RU)

(73) Assignee: **Systems of Information Security 2012**, Odessa city (UA)

(21) Appl. No.: **14/180,110**

(22) Filed: **Feb. 13, 2014**

Related U.S. Application Data

(60) Provisional application No. 61/765,171, filed on Feb. 15, 2013.

Publication Classification

(51) **Int. Cl.**
G06F 21/56 (2006.01)

(52) **U.S. Cl.**
CPC *G06F 21/56* (2013.01)
USPC **726/23**

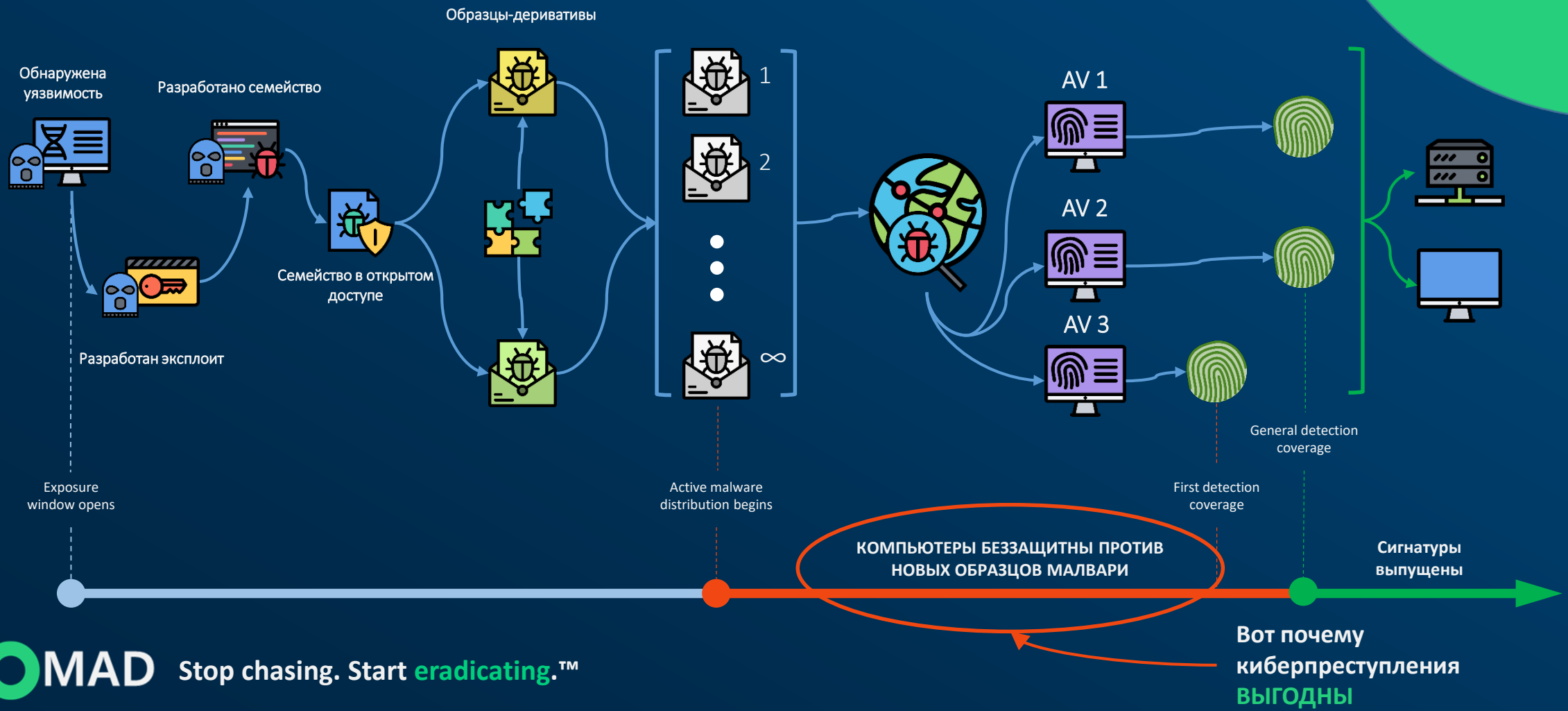
(57) **ABSTRACT**

A system, method and computer readable medium for detecting and diffusing malware on a computer. Malware is analysed to generate signatures and determine a fixing moment. All of the system calls of the operating system of a client computer are hooked and processed without emulation or the need for unpackers or decrypters, and a multi-level filter removes all system calls that are not associated with malware. The resulting system calls are accumulated on a per-thread basis and scanned, and the relevant threads are compared with the signatures to match with malware. The threads associated with malware are addressed at the fixing moment before the malware can operate to cause undesirable effects on the client computer.

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

Зазор “Время-до-Детекта”

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



ROMAD Stop chasing. Start eradicating.™

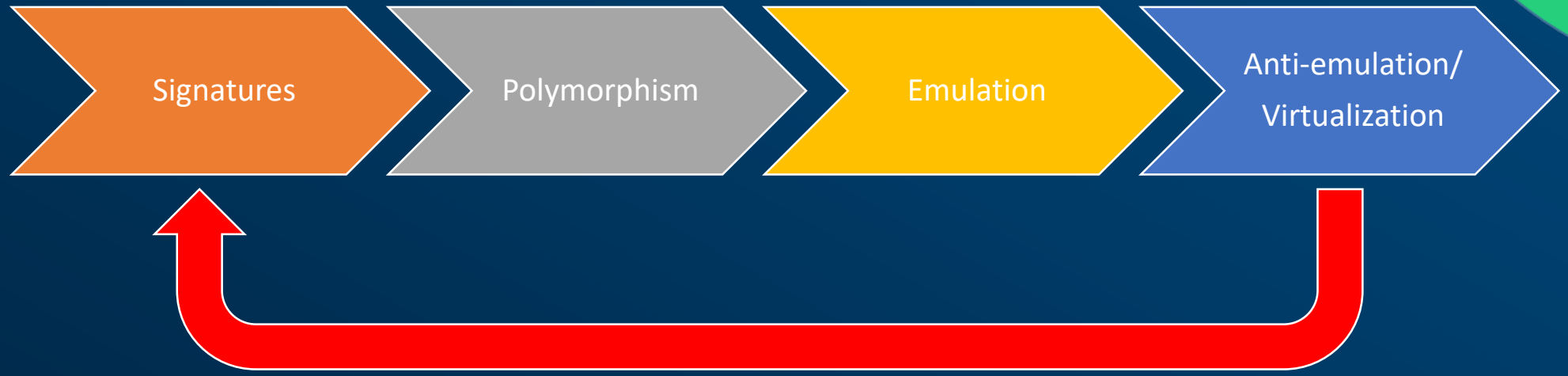
Вот почему киберпреступления ВЫГОДНЫ

Проигранная битва

Количество новых штаммов превышает 140 млн в год

ROMAD обнаруживает семейства, а не отдельные штаммы

Обфускация и упаковка



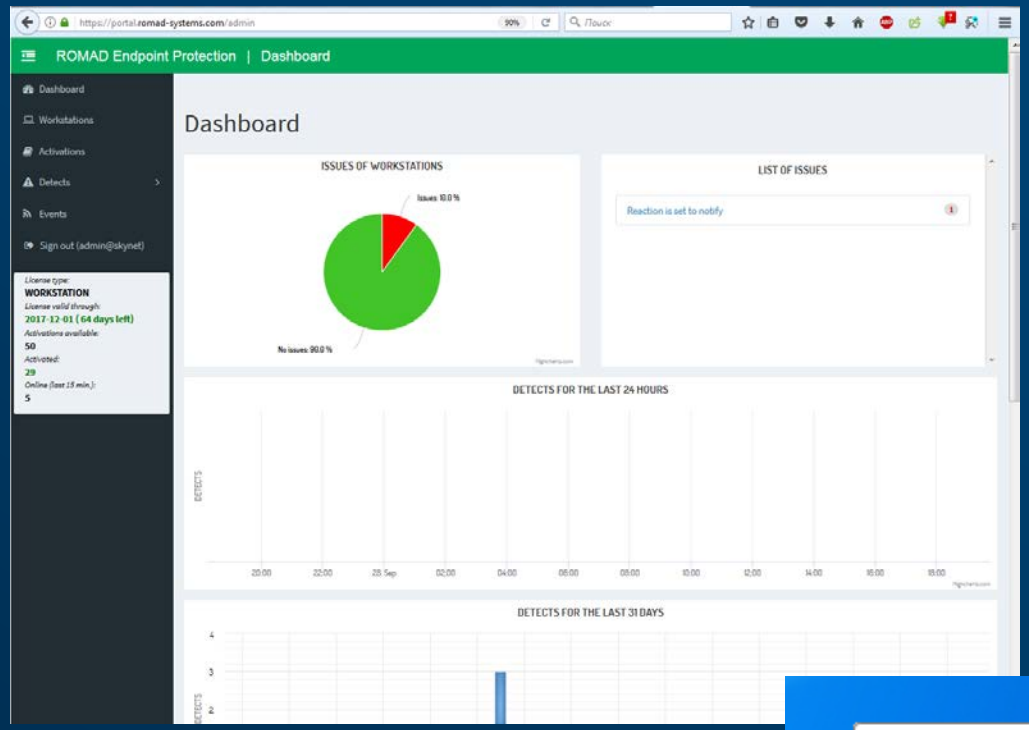
- Назад к регуляркам?

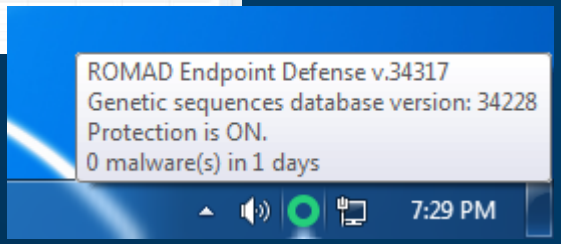
Хьюстон, у нас проблема!

Платформа ROMAD

- ROBUST
- MALWARE
- DETECTOR

  - » Unique
  - » Resilient
  - » Reliable
  - » Sustainable
  - » Patented





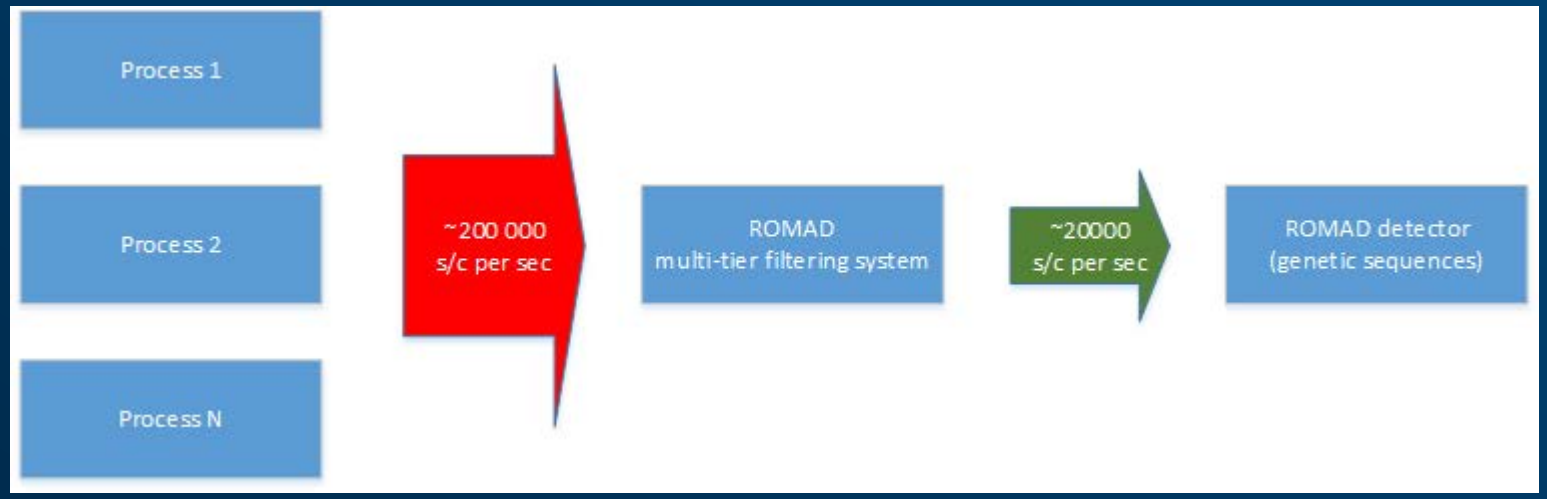
ROMAD Stop chasing. Start eradicating.™

Надежный детект

- ~10 секвенций для описания целого семейства – **устраняем семейства**, а не штаммы
- **Malware Genetic Sequence™** всегда на шаг впереди малвари, все традиционные методы обхода классических AV не действуют
- Мультиуровневая модель доверия обеспечивает **высокий уровень производительности**
- Участие человеческого фактора сведено к минимуму

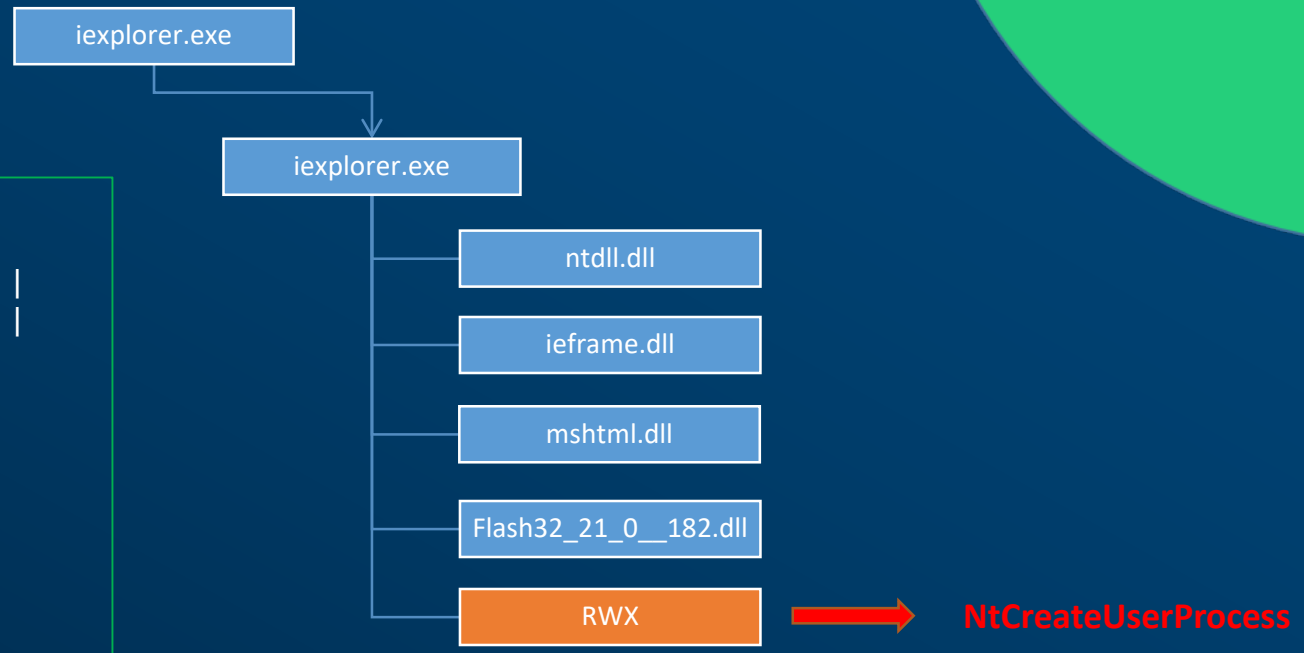
Принцип действия

- USPTO 9,372,989 – выпущен в июне 21, 2016
- EPO EP 14 155 268.7

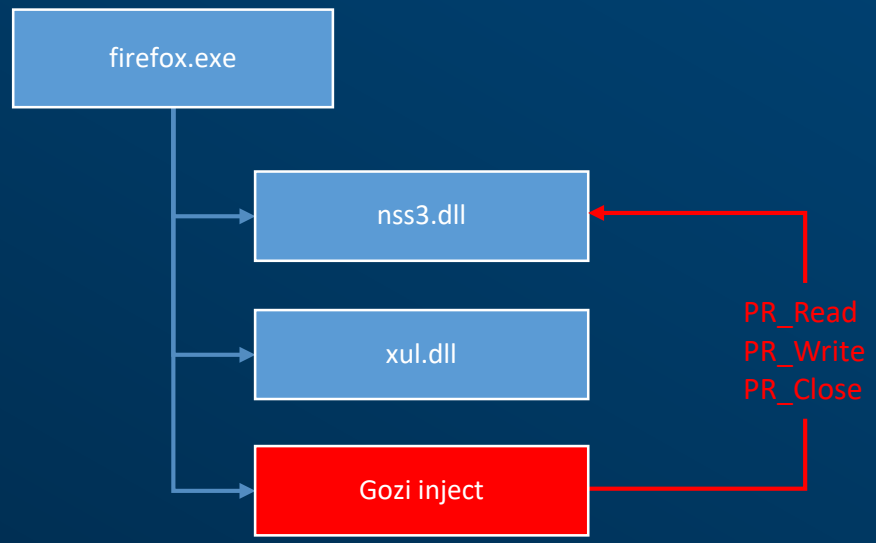


Пример: отлов шеллкода эксплоита

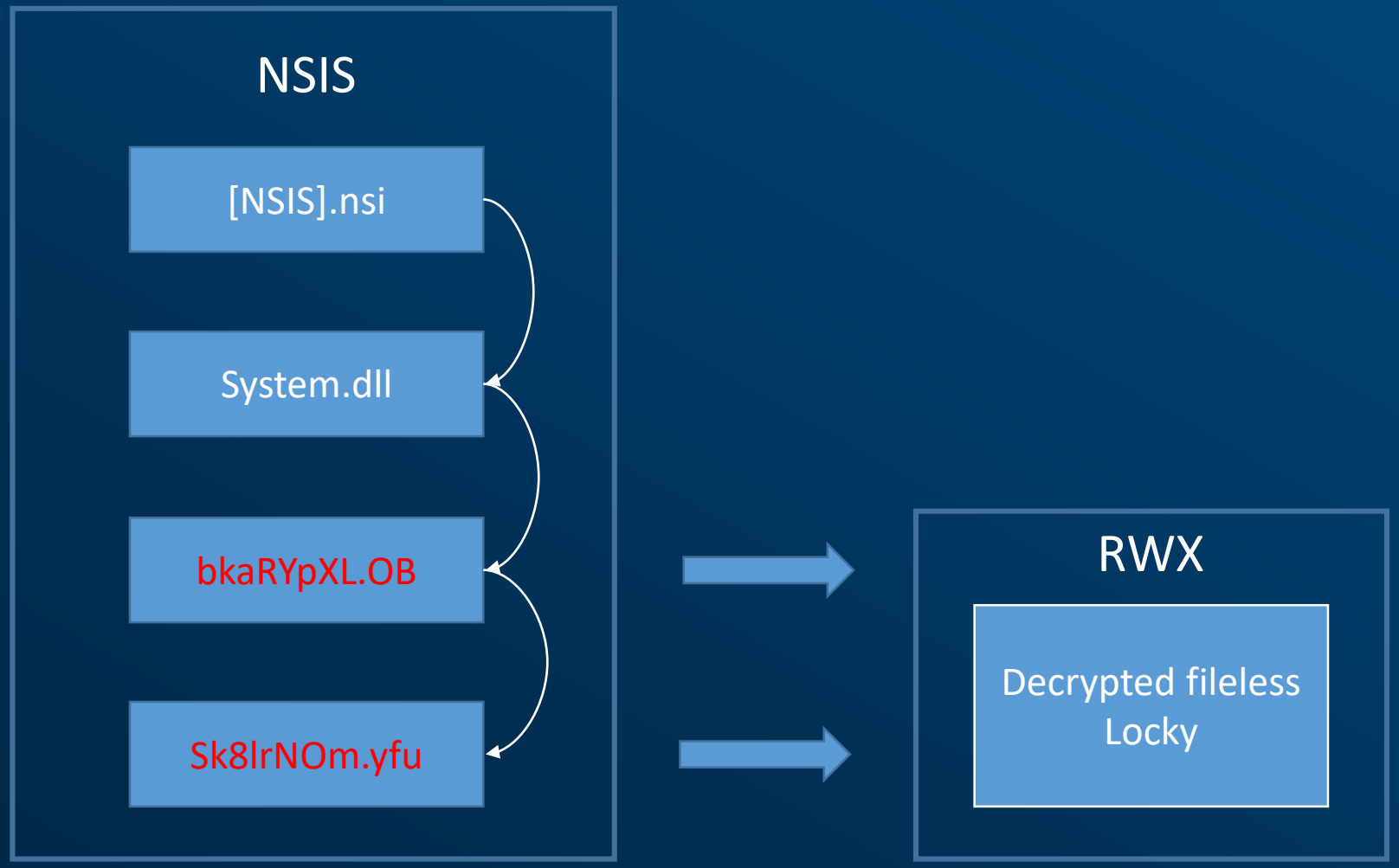
```
NtCreateUserProcess |
NtCreateUserProcess(0x77F05784) *ntdll* |
CreateProcessInternalW(0x77E30F4F) *kernel32* |
CreateProcessInternalA(0x77E3CA2F) *kernel32* |
CreateProcessA(0x77DE20AE) *kernel32* |
0x695E0A6 |
0x59327D1 *Flash32_21_0_0_182* |
0x593331B *Flash32_21_0_0_182* |
0x596310F *Flash32_21_0_0_182* |
0x59334C5 *Flash32_21_0_0_182* |
0x5940199 *Flash32_21_0_0_182*
|+++user+++|
```



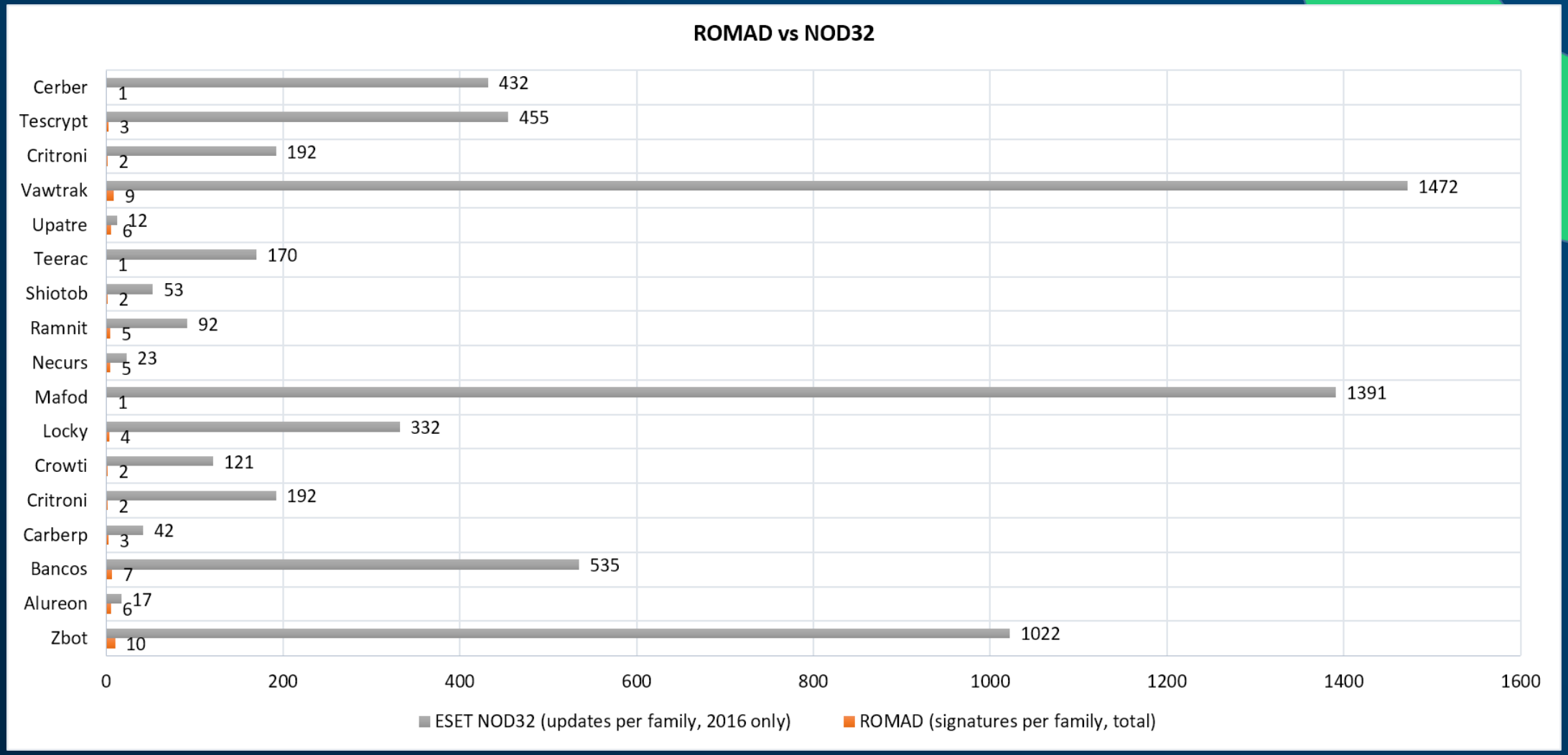
Пример: Gozi внутри FireFox



Пример: безфайловый Locky

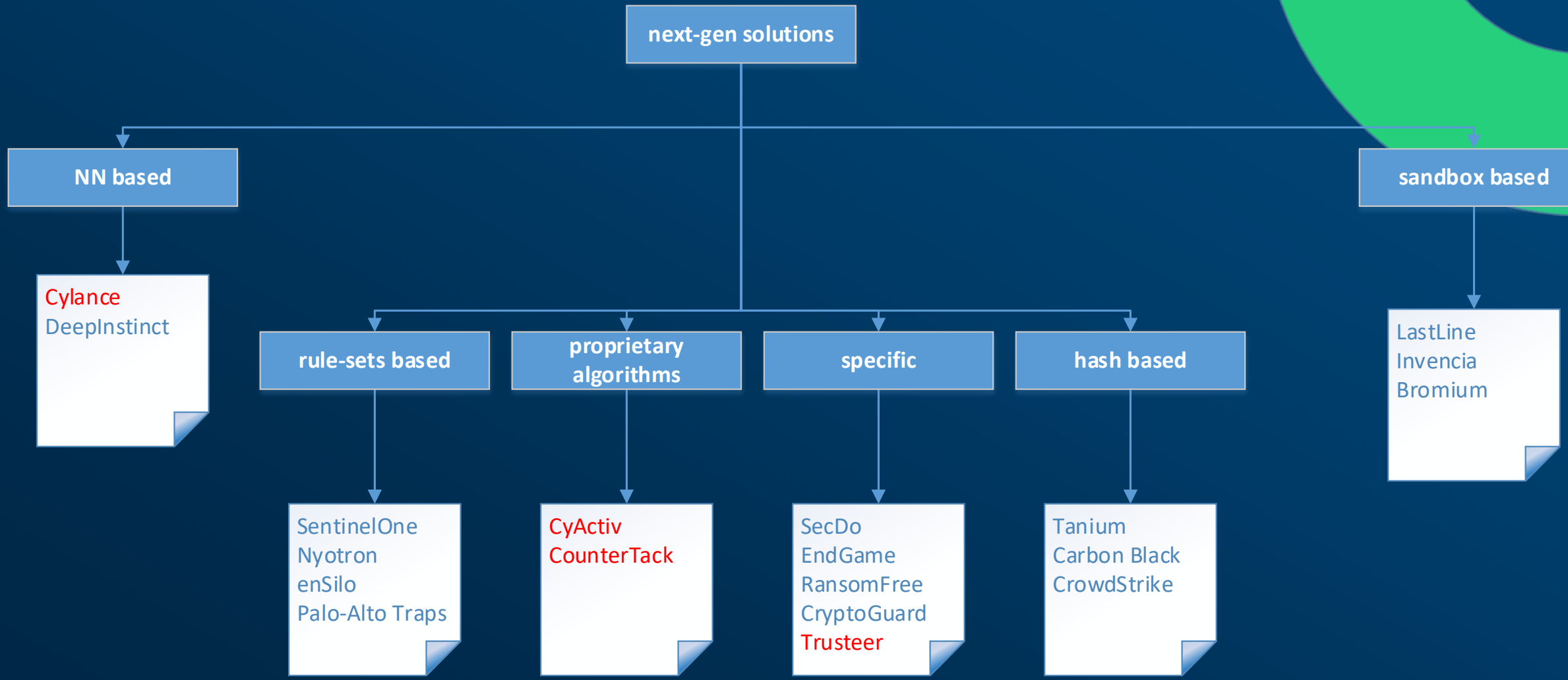


Сравнительная эффективность

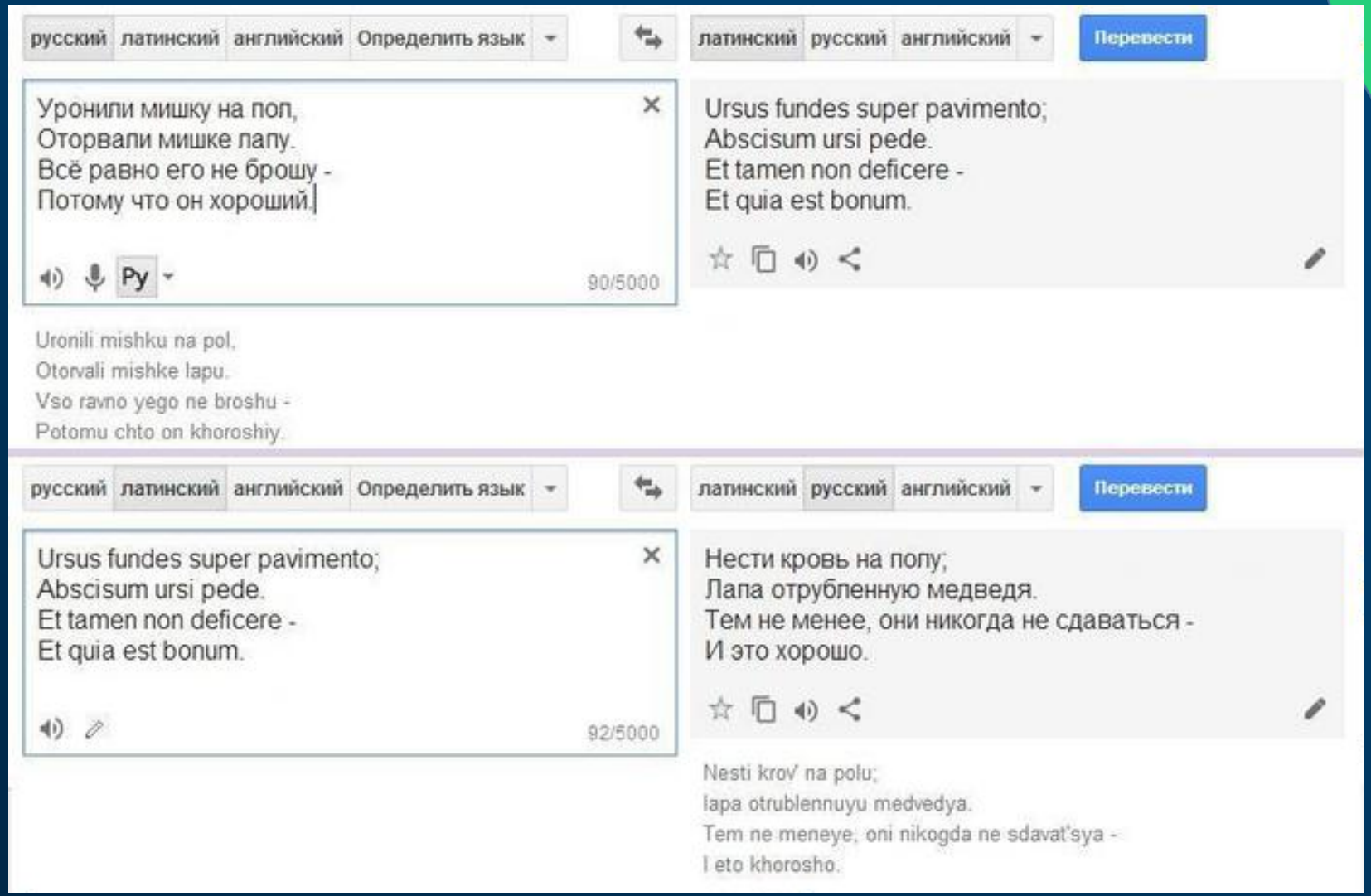


* http://virusradar.com/en/update/info/2016/0

Рынок NGEP


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

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.

ROMAD

Stop chasing. Start eradicating.™

Спасибо!

www.romadcyber.com