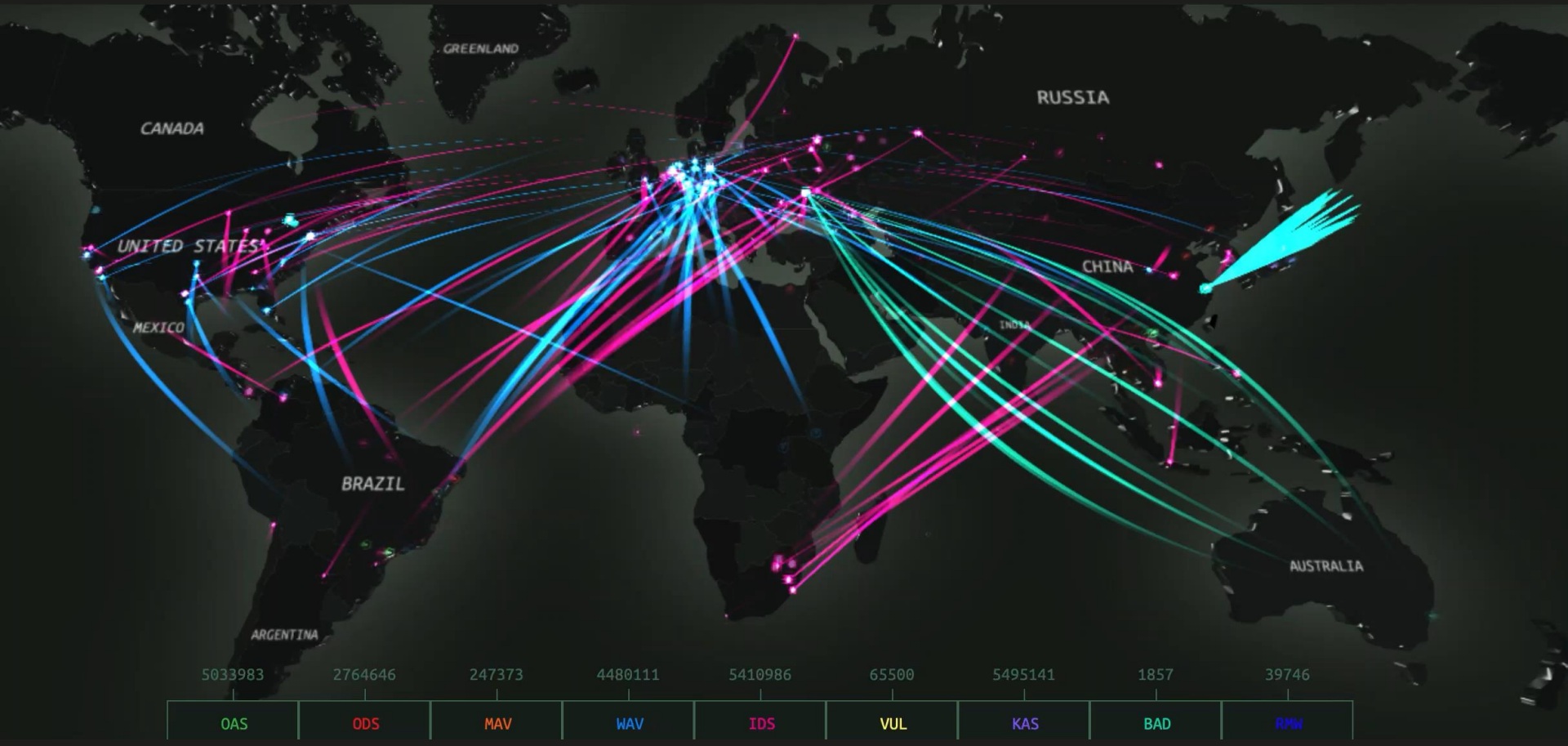
Kaspersky
Security Day
2021

Атрибуция кибератак: узнай своего врага

Дамир Шайхелисламов,
руководитель группы развития решений по защите от сложных угроз

kaspersky

Проблематика



За рамками детектирования угроз

'Olympic Destroyer' Malware Hit Pyeongchang Ahead of Opening Ceremony

Researchers at Cisco Talos detail a new piece of disruptive, highly infectious malware with a clear target: the Pyeongchang Olympics IT infrastructure.

Стратегическое преимущество

Кому прежде всего интересна атрибуция?

- Национальные CERT/SOC
- Государственные и правоохранительные органы

- Крупный корпоративный сегмент (SOC)
- Поставщики услуг безопасности

Массовые угрозы сложно атрибутировать

Вероятностный характер

Слабая огласка пострадавшими организациями данных по инцидентам

Тактики, техники и процедуры как modus operandi

- Важность профилирования угроз и анализа поведенческих характеристик

MITRE | ATT&CK®

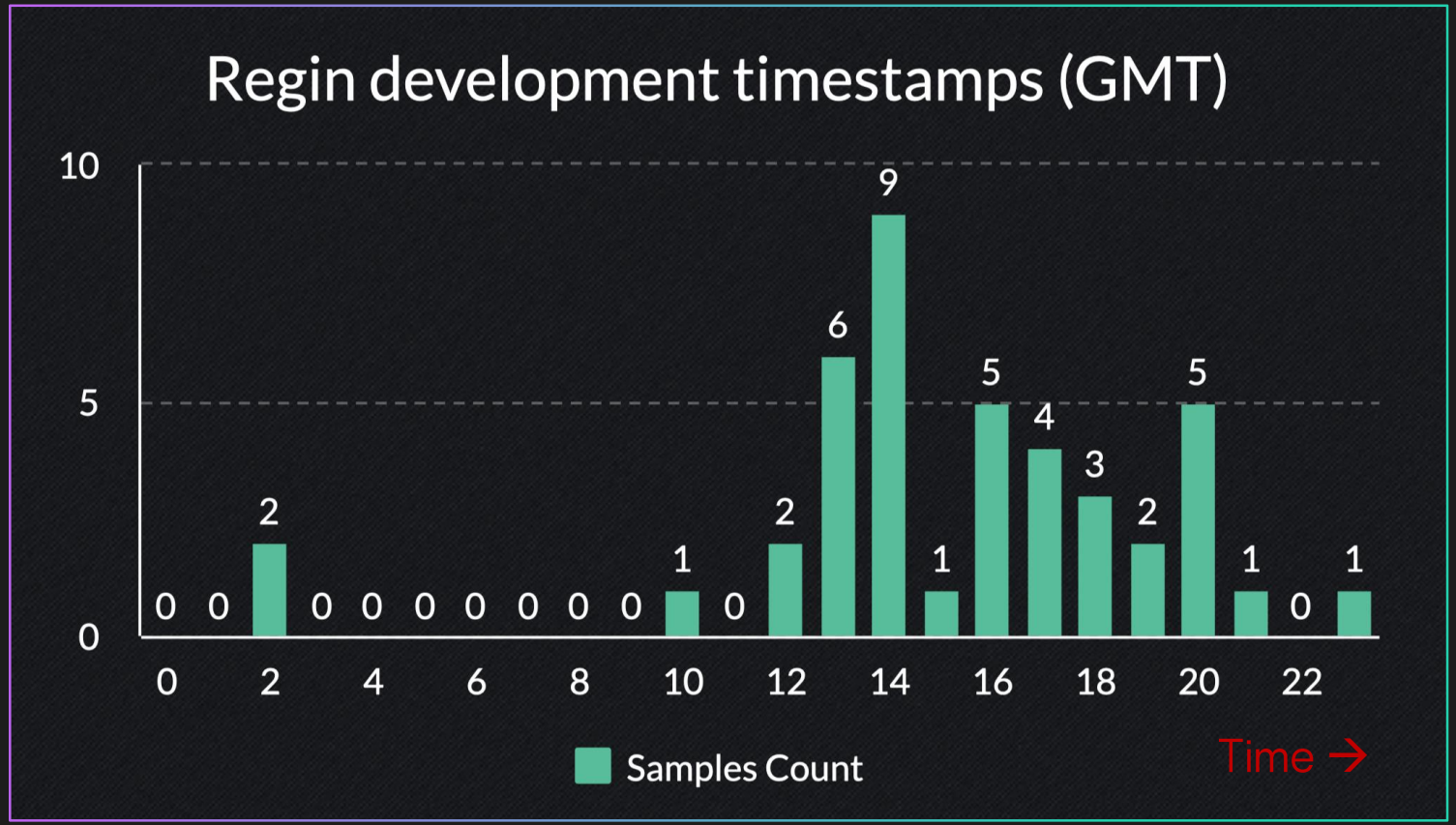
- Смена собственного поведения (TTP) – трудоемкий и дорогостоящий процесс

Ввиду сложности и многоэтапности современных целевых атак, индикаторы, способствующие атрибуции могут быть выявлены на самых разных этапах

Примеры технических признаков и индикаторов, применяемых в атрибуции

Информация о регистрации доменов, владельцах, контактах, ip-адресах	**Временные параметры (часовые пояса/время компиляции)**	**Предопределенные адреса C2 серверов, ключи шифрования, комментарии в коде**
Кастомные версии упаковщиков, инструментов обфускации, алгоритмы шифрования	Стиль программирования в т.ч. обработка исключений в коде, имена переменных	Цифровые подписи и TLS сертификаты
Фейковые личности и псевдонимы отправителей (фишинг)	**Среда разработки, версии компилятора**	**Debug-информация, крипто-кошельки, импорты API функций**

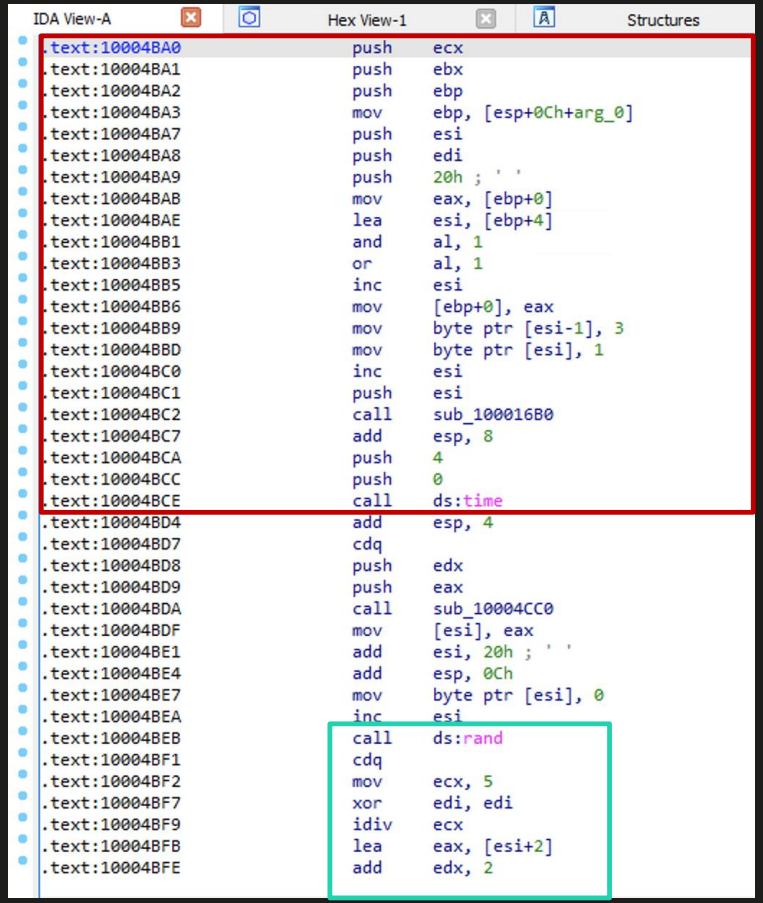
Примеры технических признаков и индикаторов

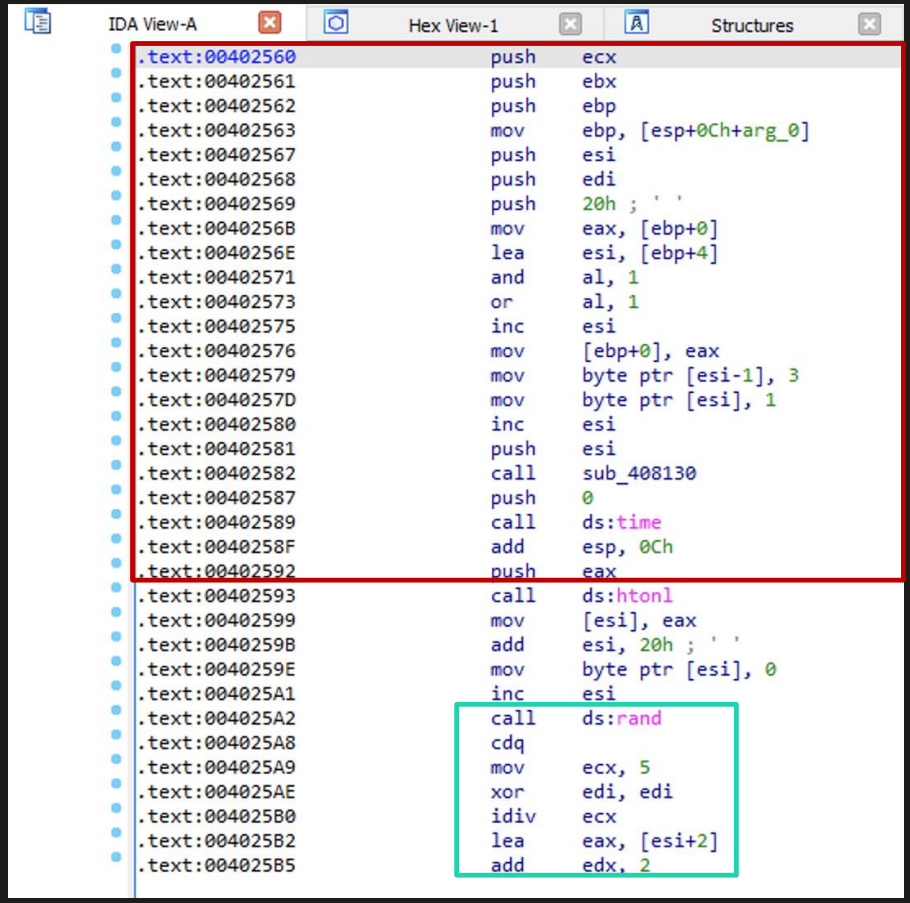


WannaCry – Lazarus APT

- 2017 WannaCry
- 2015 Lazarus Backdoor

WannaCry – Lazarus APT





WannaCry – Lazarus APT


```
.00000001`80090FF1:  F2 BD BD 8A-C2 BA CA 30-93 B3 53 A6-A3 B4 24 05  ...........0..S.....$.
.00000001`80091001:  36 D0 BA 93-06 D7 CD 29-57 DE 54 BF-67 D9 23 2E  6.......)W.T.g.#.
.00000001`80091011:  7A 66 B3 B8-4A 61 C4 02-1B 68 5D 94-2B 6F 2A 37  zf..Ja...h].+o*7
.00000001`80091021:  BE 0B B4 A1-8E 0C C3 1B-DF 05 5A 8D-EF 02 2D 20  ..........Z...-
.00000001`80091031:  75 6E 7A 69-70 20 30 2E-31 35 20 43-6F 70 79 72  unzip 0.15 Copyr
.00000001`80091041:  69 67 68 74-20 31 39 39-38 20 47 69-6C 6C 65 73  ight 1998 Gilles
.00000001`80091051:  20 56 6F 6C-6C 61 6E 74-20 00 00 00-00 00 00 69   Vollant       i
.00000001`80091061:  6E 76 61 6C-69 64 20 6C-69 74 65 72-61 6C 2F 6C  nvalid literal/l
.00000001`80091071:  65 6E 67 74-68 20 63 6F-64 65 00 00-00 00 00 69  ength code     i
.00000001`80091081:  6E 76 61 6C-69 64 20 64-69 73 74 61-6E 63 65 20  nvalid distance
```

unzip 0.15 reference in Lazarus backdoor (MD5: 17bc6f5b672b7e128cd5df51cdf10d37).

```
.0071D4C9:  36 D0 BA 93-06 D7 CD 29-57 DE 54 BF-67 D9 23 2E  6.......)W.T.g.#.
.0071D4D9:  7A 66 B3 B8-4A 61 C4 02-1B 68 5D 94-2B 6F 2A 37  zf..Ja...h].+o*7
.0071D4E9:  BE 0B B4 A1-8E 0C C3 1B-DF 05 5A 8D-EF 02 2D 20  ..........Z...-
.0071D4F9:  75 6E 7A 69-70 20 30 2E-31 35 20 43-6F 70 79 72  unzip 0.15 Copyr
.0071D509:  69 67 68 74-20 31 39 39-38 20 47 69-6C 6C 65 73  ight 1998 Gilles
.0071D519:  20 56 6F 6C-6C 61 6E 74-20 00 00 C8-D4 40 00 4C   Vollant      @ L
.0071D529:  77 40 00 FF-FF FF FF F8-78 40 00 0C-79 40 00 00  w@      x@  y@
```

unzip 0.15 reference in WannaCry (MD5: d724d8cc6420f06e8a48752f0da11c66).

Сложность задачи

Нехватка инструментов - традиционные решения по безопасности неспособны справиться с задачей

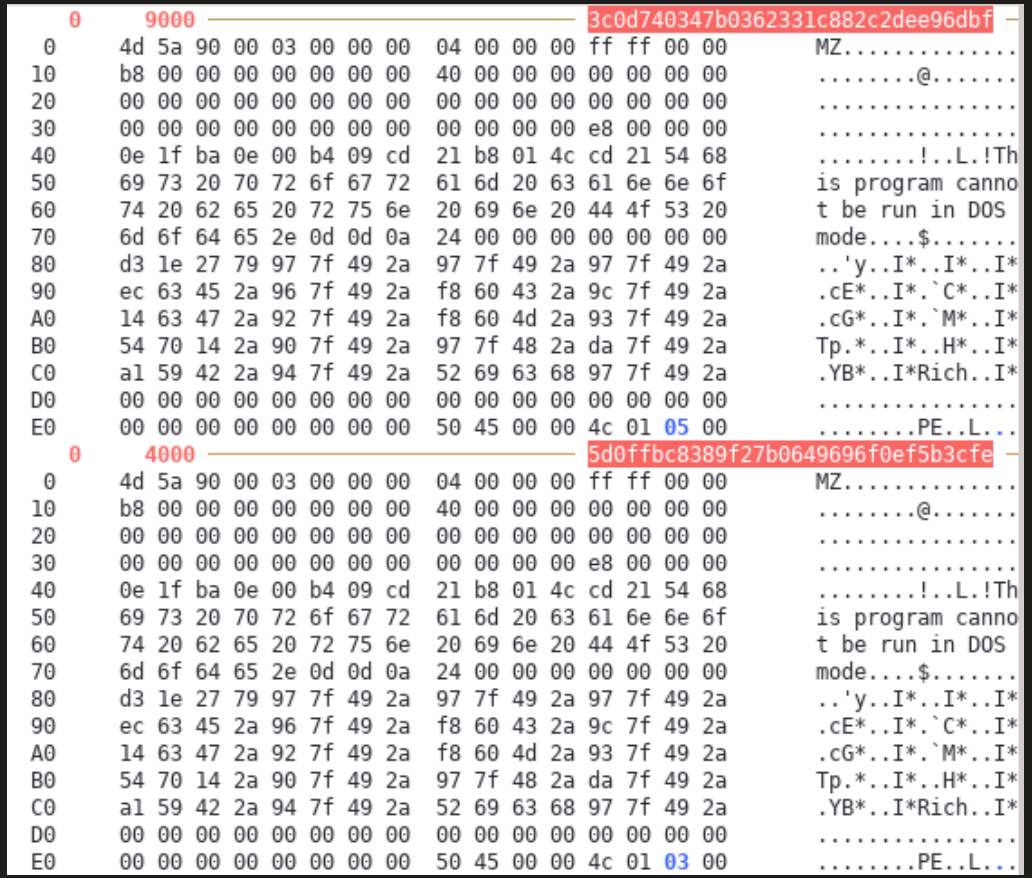
Переиспользование кода/инфраструктуры для организации атак

"Мимикрия" и ложный след, использование распространенных компонент (CodeProject, Github, etc.)

Ресурсоемкий процесс

Наличие исследовательской экспертизы, исторических данных в т.ч. вредоносных объектов, тесное взаимодействие с представителями индустрии

Ложные знаки и «мимикрия»

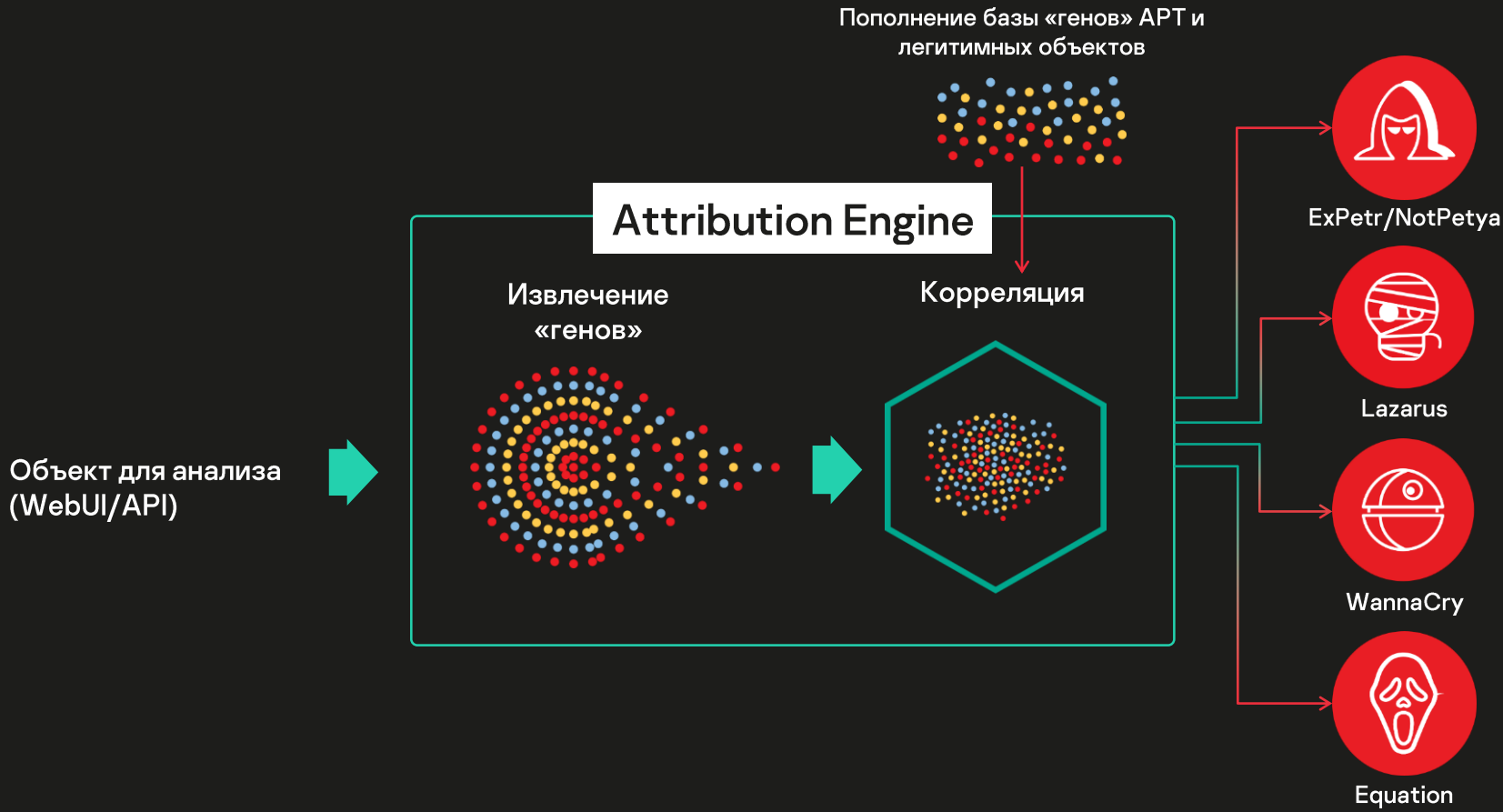


```
    0     9000 ──────────────────────────────────────  3c0d740347b0362331c882c2dee96dbf ─
 0      4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00       MZ..............
10      b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00       ........@.......
20      00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00       ................
30      00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00       ................
40      0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68       ........!..L.!Th
50      69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f       is program canno
60      74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20       t be run in DOS
70      6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00       mode....$.......
80      d3 1e 27 79 97 7f 49 2a  97 7f 49 2a 97 7f 49 2a       ..'y..I*..I*..I*
90      ec 63 45 2a 96 7f 49 2a  f8 60 43 2a 9c 7f 49 2a       .cE*..I*.`C*..I*
A0      14 63 47 2a 92 7f 49 2a  f8 60 4d 2a 93 7f 49 2a       .cG*..I*.`M*..I*
B0      54 70 14 2a 90 7f 49 2a  97 7f 48 2a da 7f 49 2a       Tp.*..I*..H*..I*
C0      a1 59 42 2a 94 7f 49 2a  52 69 63 68 97 7f 49 2a       .YB*..I*Rich..I*
D0      00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00       ................
E0      00 00 00 00 00 00 00 00  50 45 00 00 4c 01 05 00       ........PE..L...
    0     4000 ──────────────────────────────────────  5d0ffbc8389f27b0649696f0ef5b3cfe ─
 0      4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00       MZ..............
10      b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00       ........@.......
20      00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00       ................
30      00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00       ................
40      0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68       ........!..L.!Th
50      69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f       is program canno
60      74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20       t be run in DOS
70      6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00       mode....$.......
80      d3 1e 27 79 97 7f 49 2a  97 7f 49 2a 97 7f 49 2a       ..'y..I*..I*..I*
90      ec 63 45 2a 96 7f 49 2a  f8 60 43 2a 9c 7f 49 2a       .cE*..I*.`C*..I*
A0      14 63 47 2a 92 7f 49 2a  f8 60 4d 2a 93 7f 49 2a       .cG*..I*.`M*..I*
B0      54 70 14 2a 90 7f 49 2a  97 7f 48 2a da 7f 49 2a       Tp.*..I*..H*..I*
C0      a1 59 42 2a 94 7f 49 2a  52 69 63 68 97 7f 49 2a       .YB*..I*Rich..I*
D0      00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00       ................
E0      00 00 00 00 00 00 00 00  50 45 00 00 4c 01 03 00       ........PE..L...
```

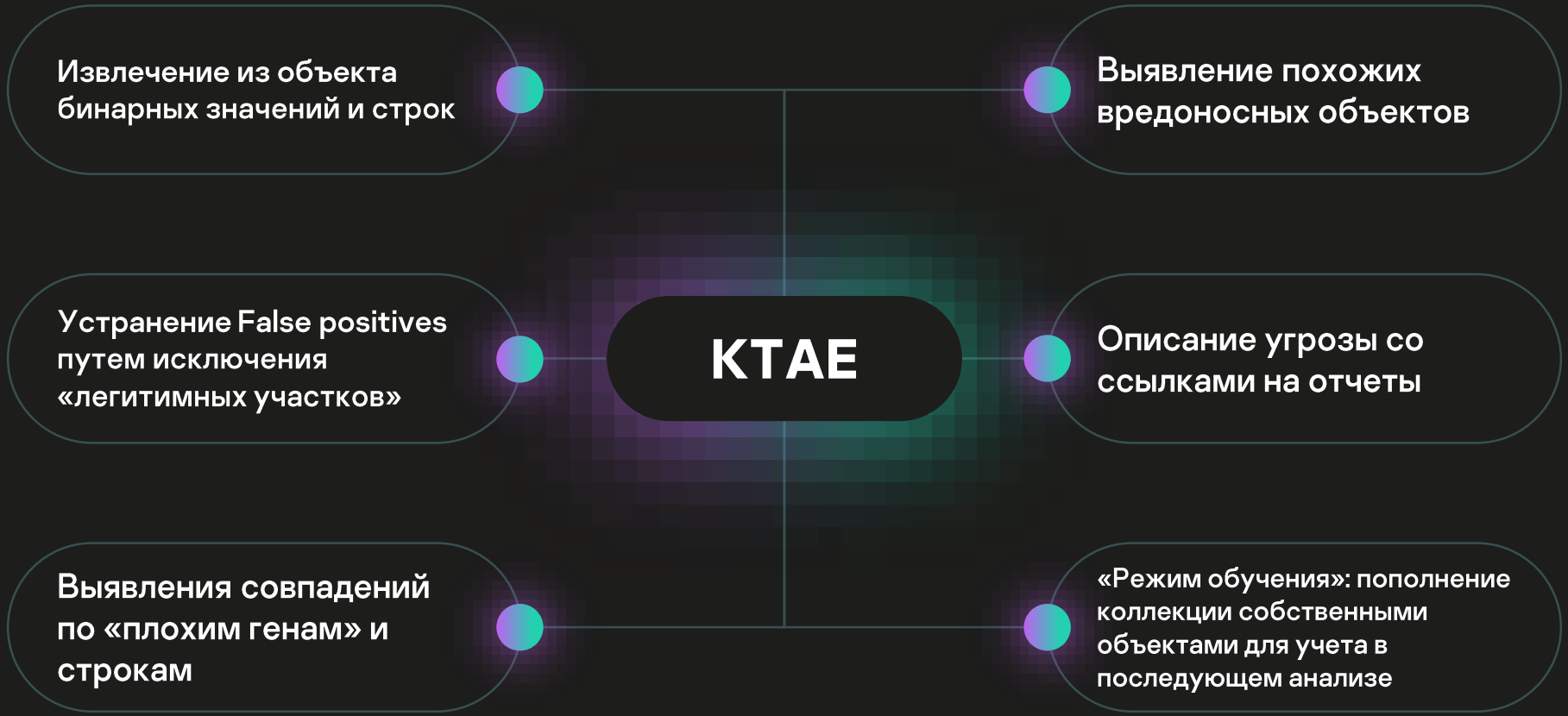
Совпадающие фрагменты Rich заголовков образцов Olympic Destroyer и Bluenoroff (Lazarus)

https://securelist.com/the-devils-in-the-rich-header/84348/

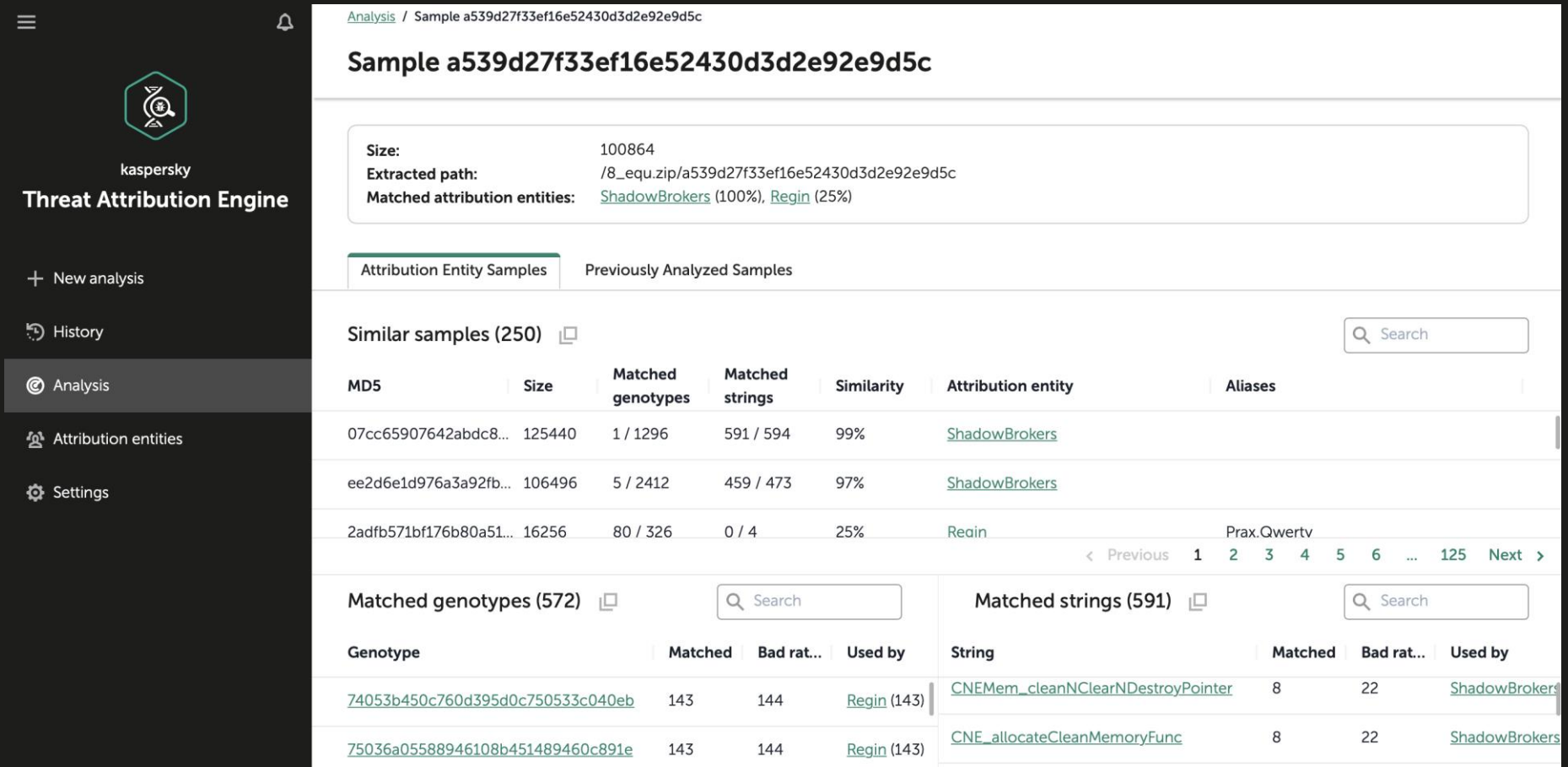
Kaspersky Threat Attribution Engine



Как это работает?



Kaspersky Threat Attribution Engine



Анализируемые объекты

Отсутствие привязки к версиям ОС

Любые форматы файлов (исполняемые, офисные и др)

Поддержка архивов/упаковщиков

Дампы памяти

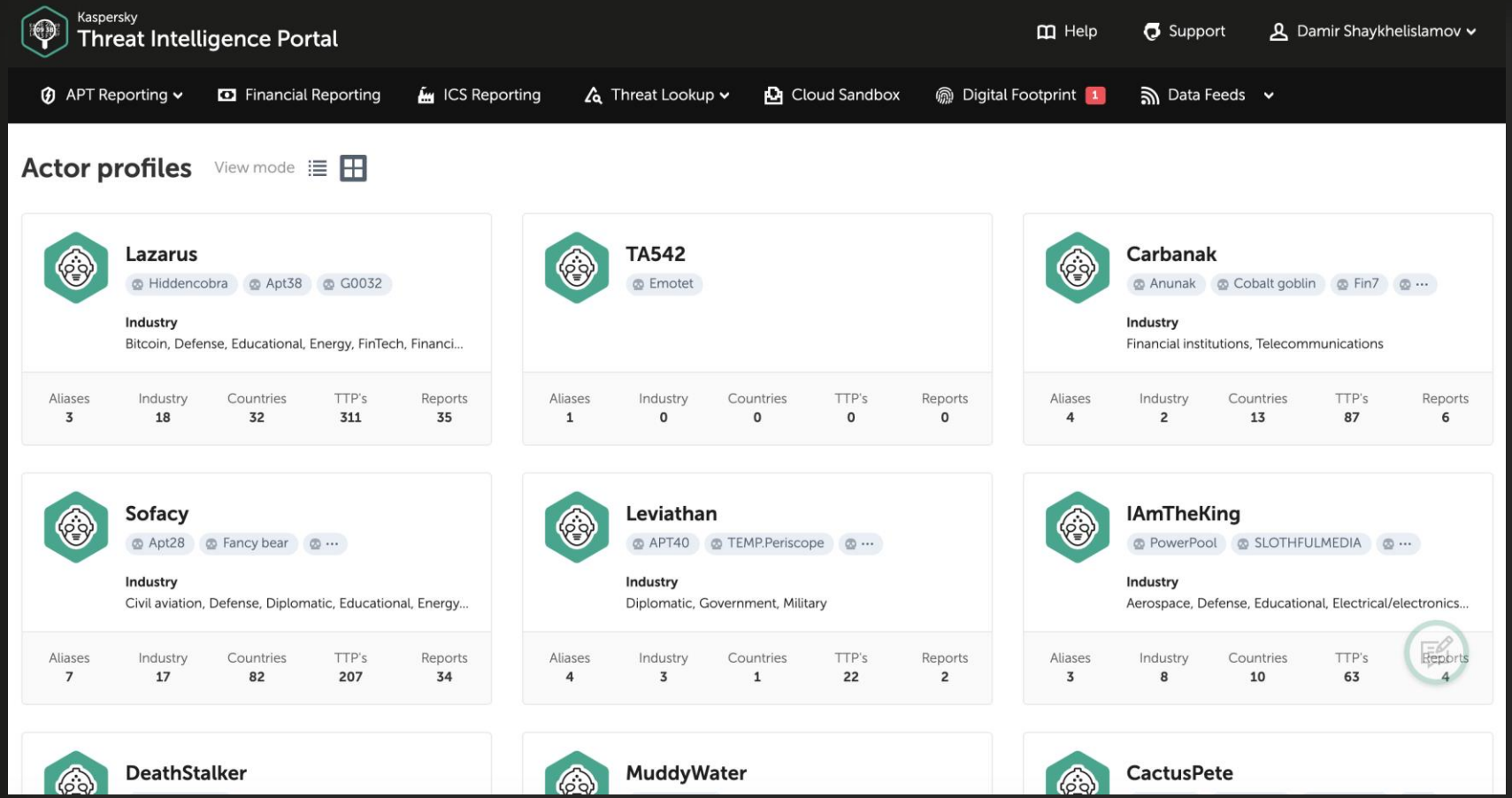
Варианты разворачивания

Инфраструктура заказчика

Частное облако (Amazon AWS)

Интеграция с Threat Intelligence Portal Скоро

Threat Intelligence Portal



Применение результатов анализа

Kaspersky
Threat Attribution
Engine

Поиск следов угроз в
инфраструктуре

Kaspersky
Endpoint Detection
and Response

Атрибуция завтра?

Больше «ложных» следов

Дальнейшая автоматизация процесса

Интеграция технологий атрибуции с решениями операционной безопасности

Спасибо!

kaspersky