

**Kaspersky
Security Day
2021**

Атрибуция кибератак: узнай своего врага

kaspersky

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



WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

SIGN IN

SUBSCRIBE

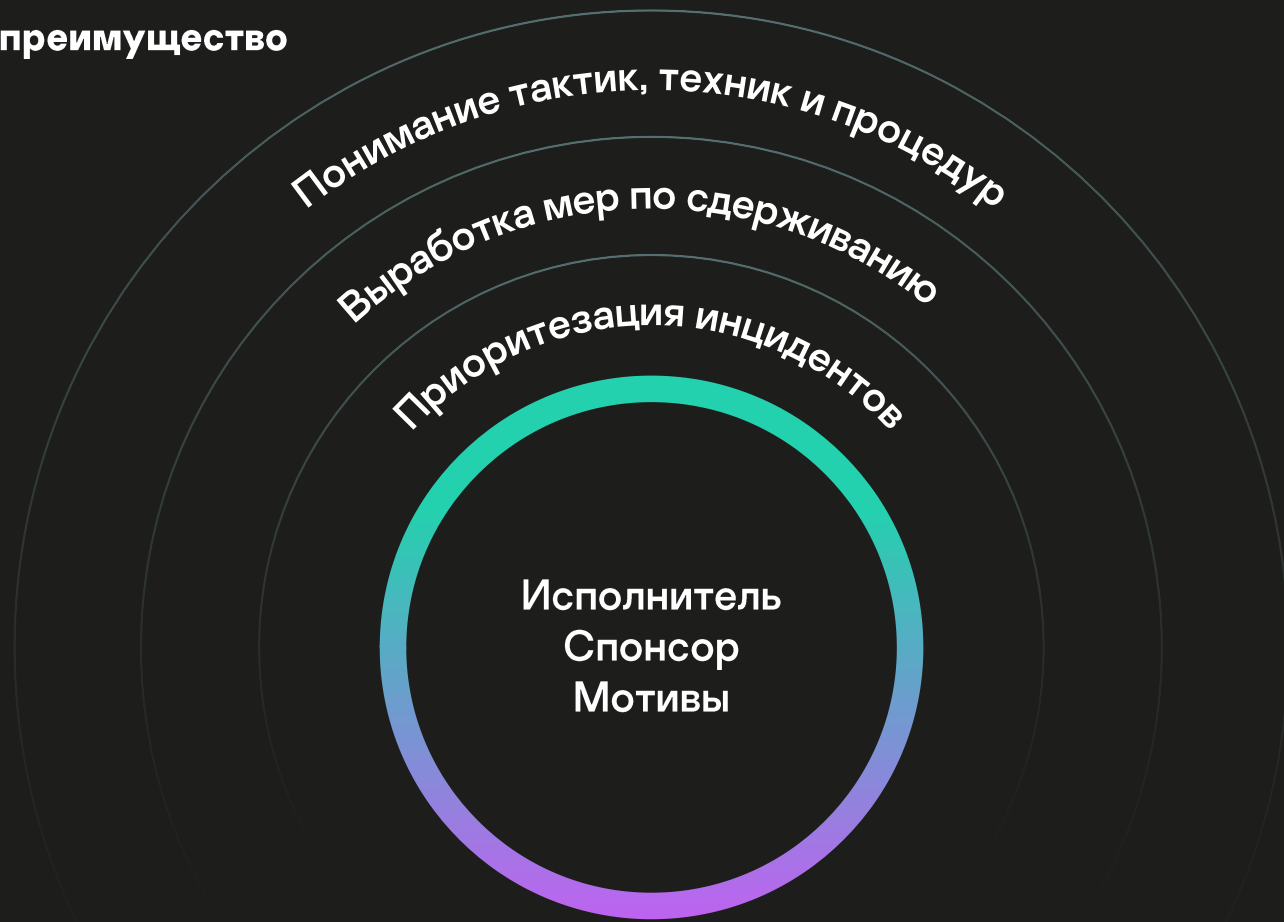
'Olympic Destroyer' Malware Hit Pyeongchang Ahead of Opening Ceremony

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



Стратегическое преимущество

4



Кому прежде всего интересна атрибуция?

5



- 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*

7



Важность профилирования угроз и анализа поведенческих характеристик



Смена собственного поведения (TTP) – трудоемкий и дорогостоящий процесс

MITRE | **ATT&CK[®]**

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

8

**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

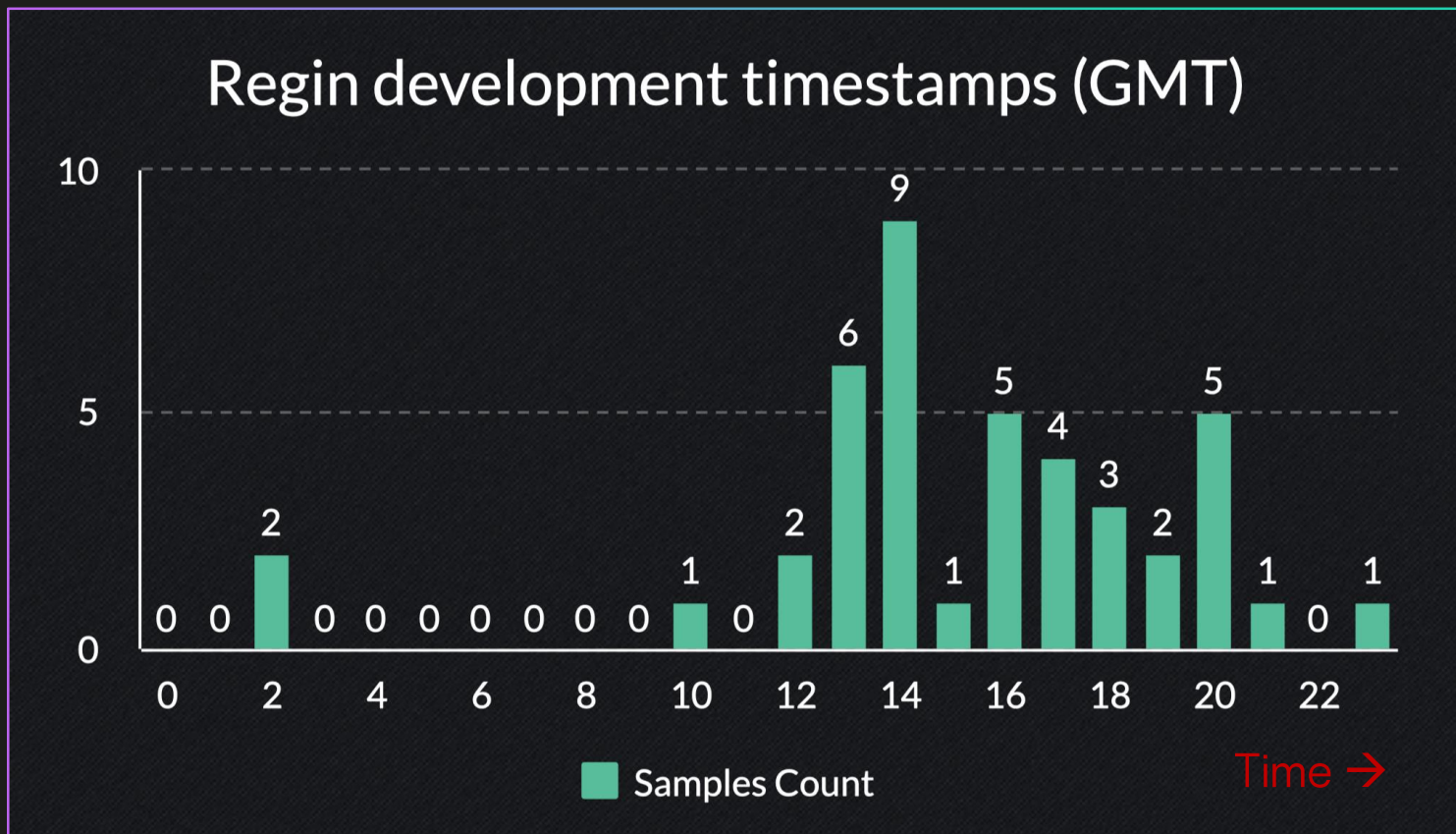
Стиль программирования в
т.ч. обработка исключений
в коде, имена переменных

Цифровые подписи и
TLS сертификаты

**Фейковые личности и
псевдонимы отправителей
(фишинг)**

**Среда разработки,
версии компилятора**

**Debug-информация,
крипто-кошельки,
импорты API функций**





Neel Mehta

@neelmehta



9c7c7149387a1c79679a87dd1ba755bc @ 0x402560,
0x40F598

ac21c8ad899727137c4b94458d7aa8d8 @
0x10004ba0, 0x10012AA4

[#WannaCryptAttribution](#)

8:02 PM · May 15, 2017



291



27



Copy link to Tweet



2017 WannaCry



2015 Lazarus Backdoor

WannaCry – Lazarus APT

11

```
.text:10004BA0 push ecx
.text:10004BA1 push ebx
.text:10004BA2 push ebp
.text:10004BA3 mov ebp, [esp+0Ch+arg_0]
.text:10004BA7 push esi
.text:10004BA8 push edi
.text:10004BA9 push 20h ; ''
.text:10004BAB mov eax, [ebp+0]
.text:10004BAE lea esi, [ebp+4]
.text:10004BB1 and al, 1
.text:10004BB3 or al, 1
.text:10004BB5 inc esi
.text:10004BB6 mov [ebp+0], eax
.text:10004BB9 mov byte ptr [esi-1], 3
.text:10004BBD mov byte ptr [esi], 1
.text:10004BC0 inc esi
.text:10004BC1 push esi
.text:10004BC2 call sub_100016B0
.text:10004BC7 add esp, 8
.text:10004BCA push 4
.text:10004BCC push 0
.text:10004BCE call ds:time

.text:10004BD4 add esp, 4
.text:10004BD7 cdq
.text:10004BD8 push edx
.text:10004BD9 push eax
.text:10004BDA call sub_10004CC0
.text:10004BDF mov [esi], eax
.text:10004BE1 add esi, 20h ; ''
.text:10004BE4 add esp, 0Ch
.text:10004BE7 mov byte ptr [esi], 0
.text:10004BEA inc esi
.text:10004BEB call ds:rand
.text:10004BF1 cdq
.text:10004BF2 mov ecx, 5
.text:10004BF7 xor edi, edi
.text:10004BF9 idiv ecx
.text:10004BFB lea eax, [esi+2]
.text:10004BFE add edx, 2
```

```
.text:00402560 push ecx
.text:00402561 push ebx
.text:00402562 push ebp
.text:00402563 mov ebp, [esp+0Ch+arg_0]
.text:00402567 push esi
.text:00402568 push edi
.text:00402569 push 20h ; ''
.text:0040256B mov eax, [ebp+0]
.text:0040256E lea esi, [ebp+4]
.text:00402571 and al, 1
.text:00402573 or al, 1
.text:00402575 inc esi
.text:00402576 mov [ebp+0], eax
.text:00402579 mov byte ptr [esi-1], 3
.text:0040257D mov byte ptr [esi], 1
.text:00402580 inc esi
.text:00402581 push esi
.text:00402582 call sub_408130
.text:00402587 push 0
.text:00402589 call ds:time
.text:0040258F add esp, 0Ch
.text:00402592 push eax

.text:00402593 call ds:htonl
.text:00402599 mov [esi], eax
.text:0040259B add esi, 20h ; ''
.text:0040259E mov byte ptr [esi], 0
.text:004025A1 inc esi
.text:004025A2 call ds:rand
.text:004025A8 cdq
.text:004025A9 mov ecx, 5
.text:004025AE xor edi, edi
.text:004025B0 idiv ecx
.text:004025B2 lea eax, [esi+2]
.text:004025B5 add edx, 2
```

```
.00000001`80090FF1: F2 BD BD 8A-C2 BA CA 30-93 B3 53 A6-A3 B4 24 05 eJ||K_T||L0Y|Sжr|$P
.00000001`80091001: 36 D0 BA 93-06 D7 CD 29-57 DE 54 BF-67 D9 23 2E 6L||yP||=)W|T_lg`#.#
.00000001`80091011: 7A 66 B3 B8-4A 61 C4 02-1B 68 5D 94-2B 6F 2A 37 zf|_Ja-PPh]Φ+o*7
.00000001`80091021: BE 0B B4 A1-8E 0C C3 1B-DF 05 5A 8D-EF 02 2D 20 =P|60P|P-PZHЯP-
.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 6L||yP||=)W|T_lg`#.#
.0071D4D9: 7A 66 B3 B8-4A 61 C4 02-1B 68 5D 94-2B 6F 2A 37 zf|_Ja-PPh]Φ+o*7
.0071D4E9: BE 0B B4 A1-8E 0C C3 1B-DF 05 5A 8D-EF 02 2D 20 =P|60P|P-PZHЯP-
.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 LL@ L
.0071D529: 77 40 00 FF-FF FF FF F8-78 40 00 0C-79 40 00 00 w@ °x@ Py@
```

unzip 0.15 reference in WannaCry (MD5: d724d8cc6420f06e8a48752f0da11c66).



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»

14

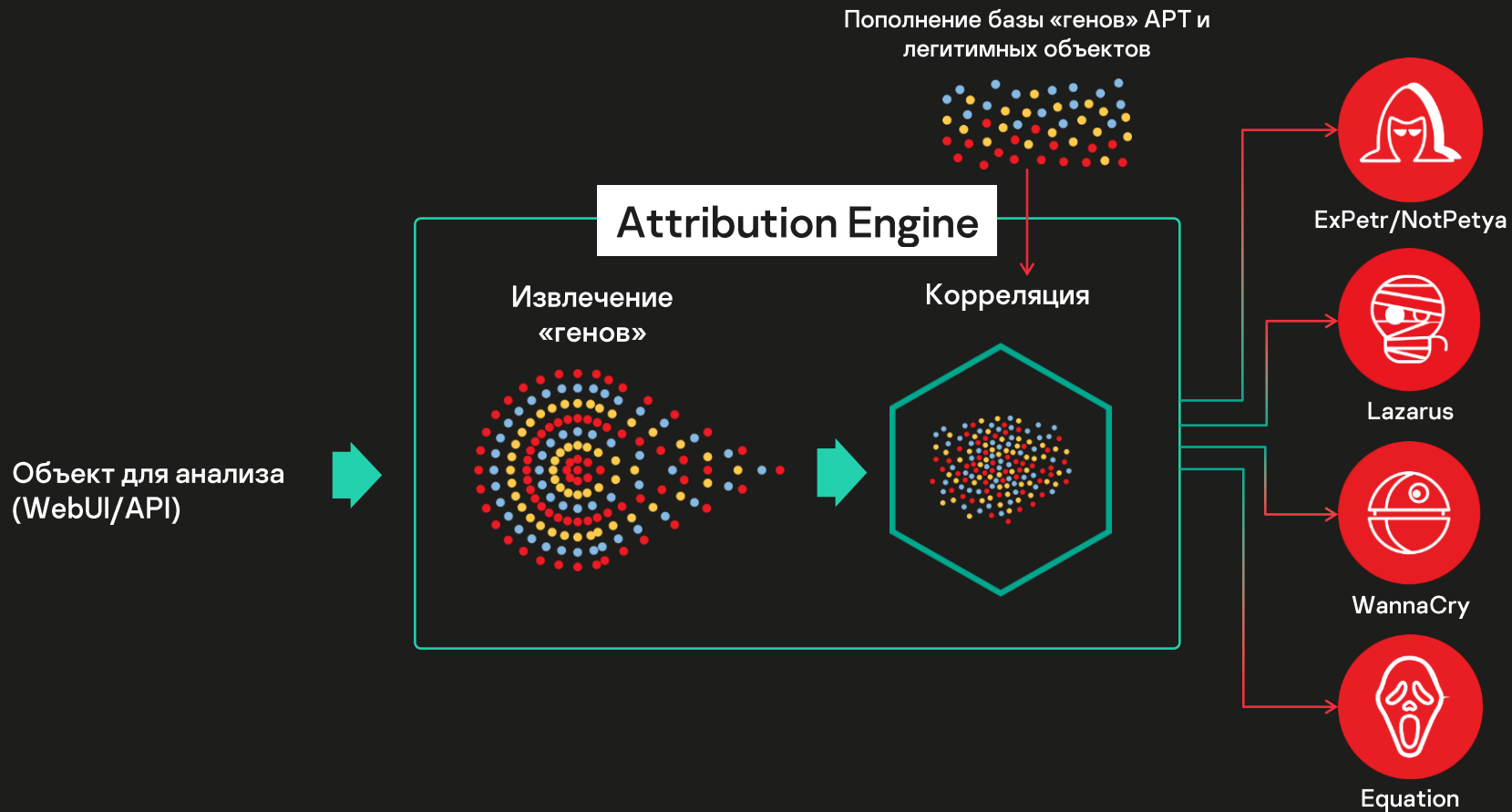
0	9000	3c0d740347b0362331c882c2dee96dbf	
0	4d 5a 90 00 03 00 00 00	04 00 00 00 ff ff 00 00	MZ.....
10	b8 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	@.....
20	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
30	00 00 00 00 00 00 00 00	00 00 00 00 e8 00 00 00	
40	0e 1f ba 0e 00 b4 09 cd	21 b8 01 4c cd 21 54 68	!..L!T
50	69 73 20 70 72 6f 67 72	61 6d 20 63 61 6e 6e 6f	is program cannot
60	74 20 62 65 20 72 75 6e	20 69 6e 20 44 4f 53 20	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 cannot
60	74 20 62 65 20 72 75 6e	20 69 6e 20 44 4f 53 20	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/>

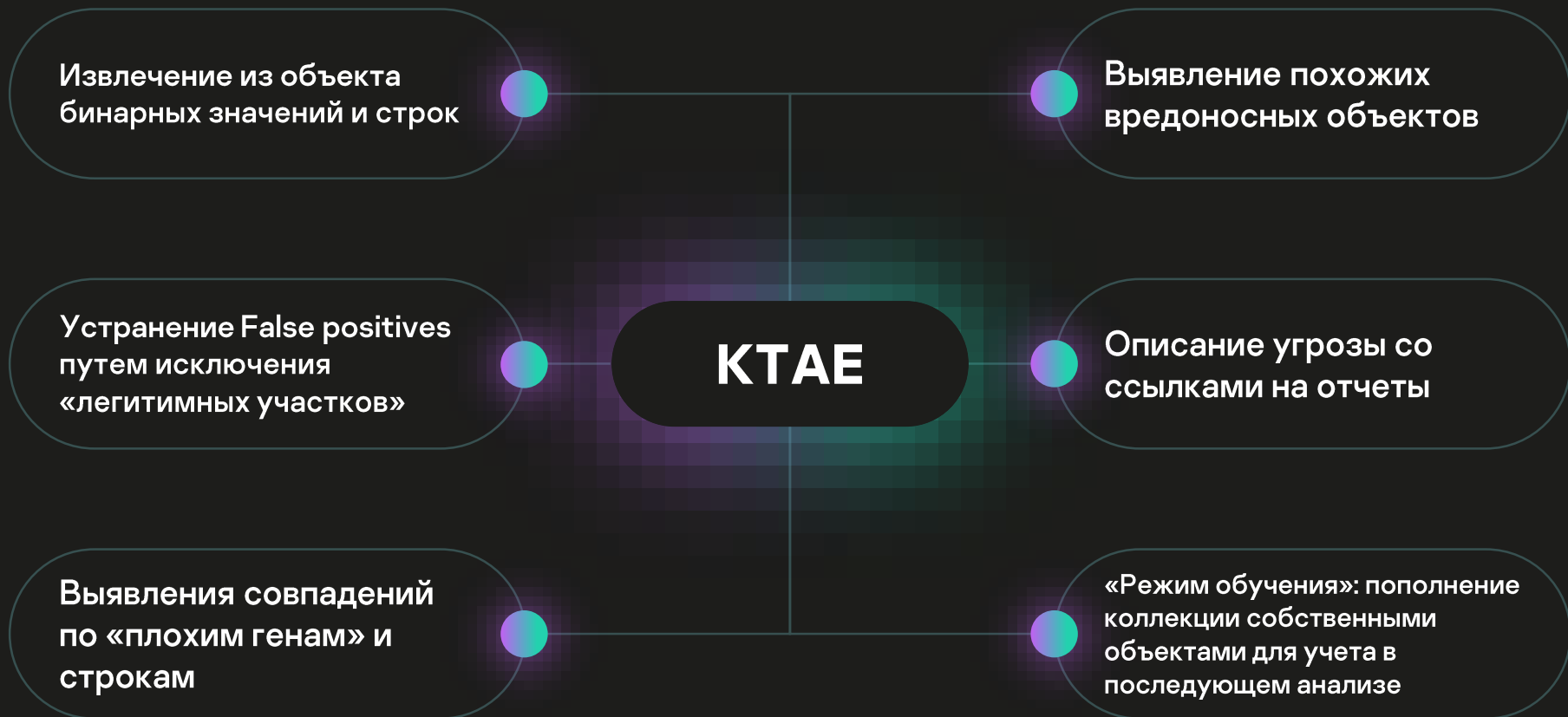
Kaspersky Threat Attribution Engine

15



Как это работает?

16





kaspersky

Threat Attribution Engine

+ New analysis

History

Analysis

Attribution entities

Settings

Analysis / Sample a539d27f33ef16e52430d3d2e92e9d5c

Sample a539d27f33ef16e52430d3d2e92e9d5c

Size: 100864
Extracted path: /8_equ.zip/a539d27f33ef16e52430d3d2e92e9d5c
Matched attribution entities: [ShadowBrokers](#) (100%), [Regin](#) (25%)

Attribution Entity Samples

Previously Analyzed Samples

Similar samples (250)

Search

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity	Aliases
07cc65907642abdc8...	125440	1 / 1296	591 / 594	99%	ShadowBrokers	
ee2d6e1d976a3a92fb...	106496	5 / 2412	459 / 473	97%	ShadowBrokers	
2adfb571bf176b80a51...	16256	80 / 326	0 / 4	25%	Regin	Prax.Qwertv

< Previous 1 2 3 4 5 6 ... 125 Next >

Matched genotypes (572)

Search

Genotype	Matched	Bad rat...	Used by
74053b450c760d395d0c750533c040eb	143	144	Regin (143)
75036a05588946108b451489460c891e	143	144	Regin (143)

Matched strings (591)

Search

String	Matched	Bad rat...	Used by
CNEMem_cleanNClearNDestroyPointer	8	22	ShadowBrokers
CNE_allocateCleanMemoryFunc	8	22	ShadowBrokers

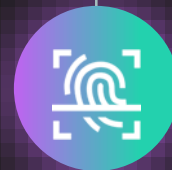
Отсутствие привязки к версиям ОС



Любые форматы файлов
(исполняемые, офисные и др)



Поддержка
архивов/упаковщиков



Дампы
памяти



Инфраструктура заказчика



Частное облако (Amazon AWS)



Интеграция с Threat Intelligence
Portal

Скоро

Threat Intelligence Portal

20



Kaspersky

Threat Intelligence Portal

Help

Support

Damir Shaykhelislamov

APT Reporting

Financial Reporting

ICS Reporting

Threat Lookup

Cloud Sandbox

Digital Footprint 1

Data Feeds

Actor profiles

View mode



Lazarus

Hiddencobra Apt38 G0032

Industry

Bitcoin, Defense, Educational, Energy, FinTech, Financi...

Aliases	Industry	Countries	TTP's	Reports
3	18	32	311	35



TA542

Emotet

Aliases	Industry	Countries	TTP's	Reports
1	0	0	0	0



Carbanak

Anunak Cobalt goblin Fin7

Industry

Financial institutions, Telecommunications

Aliases	Industry	Countries	TTP's	Reports
4	2	13	87	6



Sofacy

Apt28 Fancy bear

Industry

Civil aviation, Defense, Diplomatic, Educational, Energy...

Aliases	Industry	Countries	TTP's	Reports
7	17	82	207	34



Leviathan

APT40 TEMP.Periscope

Industry

Diplomatic, Government, Military

Aliases	Industry	Countries	TTP's	Reports
4	3	1	22	2



IAmTheKing

PowerPool SLOTHFULMEDIA

Industry

Aerospace, Defense, Educational, Electrical/electronics...

Aliases	Industry	Countries	TTP's	Reports
3	8	10	63	4



DeathStalker



MuddyWater



CactusPete

Поиск следов угроз в
инфраструктуре



Kaspersky
Threat Attribution
Engine



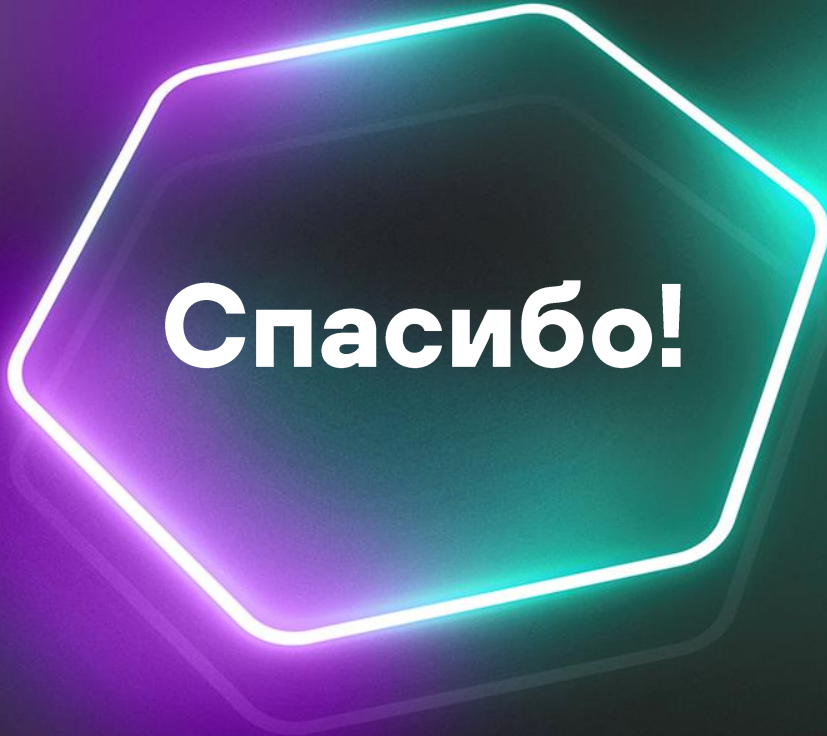
Kaspersky
Endpoint Detection
and Response

Атрибуция завтра?

Больше «ложных»
следов

Дальнейшая автоматизация
процесса

Интеграция технологий
атрибуции с решениями
операционной
безопасности



Спасибо!

kaspersky