

PT ESC Threat Intelligence
Positive Technologies



Практика отслеживания хакерских кампаний и взаимодействия с регистраторами

Аскер Джамирзе, руководитель отдела исследования угроз Positive Technologies

О команде. Цели и задачи

1

Изучение киберугроз

- Анализ ландшафта трендовых и региональных киберугроз
- Изучение инфраструктуры, инструментов и техник атакующих
- Разработка hunt-правил
- Получение упреждающих данных об изменении в арсенале и техниках атакующих

2

Поставка данных в продукт

- Пополнение базы индикаторов компрометации
- Исследование новых инструментов атакующих и написание детектирующих правил

3

Incident Response

- Поддержка команды ИР во время реагирования на инциденты

4

Публичные исследования

- Публикация аналитических материалов

Текущая обстановка

- Количество инцидентов растет
 - Более 60 инцидентов в 2024 году поступило в команду IR PT
 - Около 50 уведомлений о критичных инцидентах по данным киберразведки
- Мотивация атакующих становится вариативной
- Многие организации не имеют бюджета и ресурсов на обеспечение ИБ
- Для эффективной киберразведки взаимодействие с организациями, владеющими данными, становится всё более актуальным

Доменный патруль

Текущее состояние

- Прямое взаимодействие с компетентными организациями

Потенциальное развитие

- Актуализировать список компетентных организаций (вендоры, бигтехи с крупными ИБ-службами и так далее)

Нетоскоп

- Текущие применения
 - Обогащение индикаторов
 - Мониторинг новых индикаторов
 - Принадлежность домена какой-либо компании

Участники проекта



F6

kaspersky



Яндекс

SkyDNS



■ positive technologies

Нетоскоп. Варианты развития

- Расширение схемы
 - Текущая: Дата обнаружения, Категория, Индикатор
 - Новые поля: Дата последнего обнаружения, Источник, Malware Family, Threat Actor
- Реализация фида
- Расширение алгоритма поиска братских доменов

PT TIP ПОИСК ОТПРАВИТЬ ЮС'С

Введите домен, хостнейм, IP, хэш-сумму или загрузите файл на анализ

ri-lil.ru

Критичность:
Высокая

ri-lil.ru

IP 141.8.197.252

Название сети 35278 / Sprinthost.ru LLC

Группировка DarkGaboон

Дата регистрации 2024-08-12

Истекает 2025-08-12

Роль cnc

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS/RDAP СВЯЗАННЫЕ ДОМЕНЫ PDNS (20) DNS (11)

Домен	IP
a4b7c3-f0gl1iz9.ru	185.185.70.246
b8c1d4e9-f2g3.ru	141.8.197.252
b9c1d6-x0yol4.ru	-
be-blo.ru	141.8.197.252
bj-ki.ru	141.8.197.252
bl-xp.ru	141.8.197.252

Зачем нам (Global) Passive? DNS

1

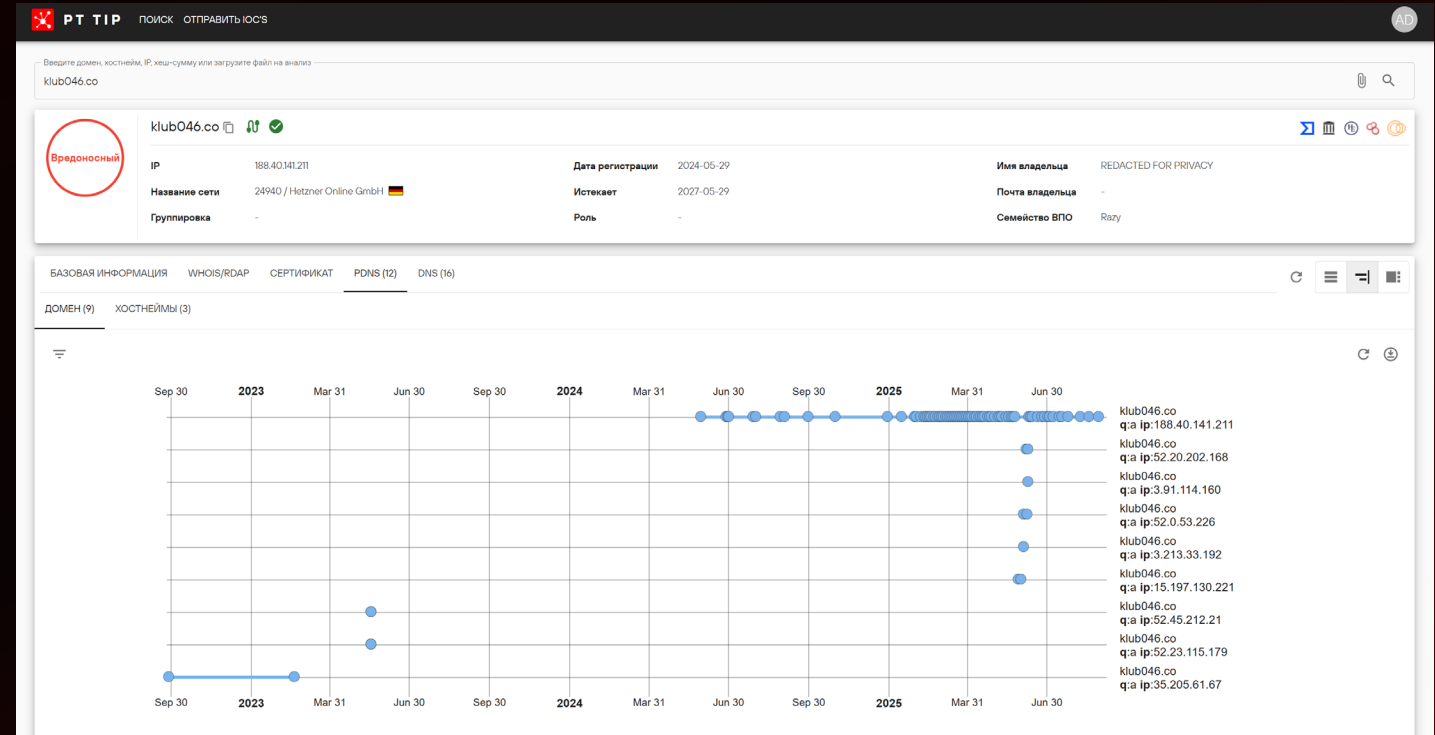
Что такое Passive DNS?

- Сбор DNS-трафика для исторического анализа
- Отслеживание изменений DNS-записей без активного сканирования
- Основа для выявления угроз через накопленные данные

2

Основные ограничения

- Слепые зоны, если недостаточно источников данных
- Пассивный сбор данных
- Вопросы реализации, приватности и так далее



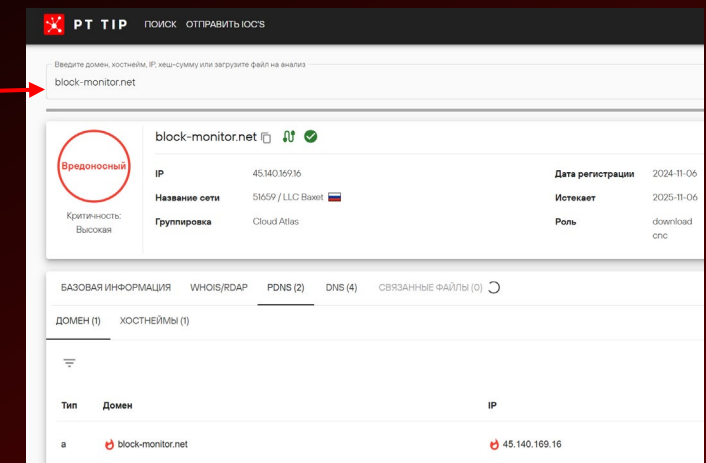
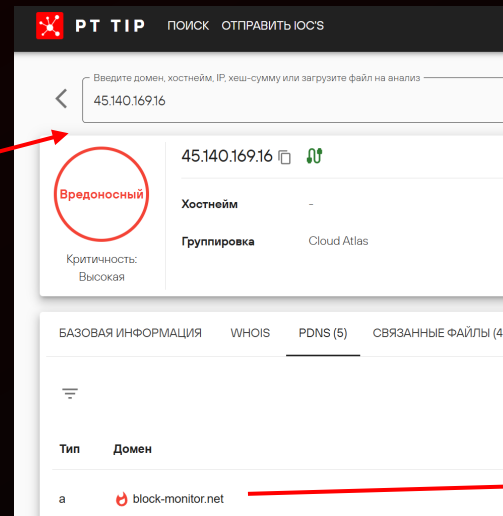
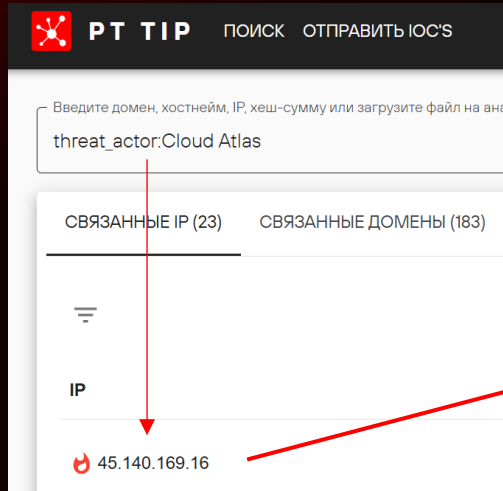
Passive DNS. Возможности

- Обогащение и расширение списка индикаторов (SOC, DFIR, TI)
- Обнаружение фишинговых/typosquatting доменов (TI, Brand Protection)
- Идентификация и мониторинг сетевого профиля угрозы (TI)

Сетевой профиль:

- WHOIS (почта, улица и т.п.)
- Ключевые слова и шаблоны доменов
- Поля в TLS-сертификатах
- Используемые хостинги, ASN
- Конфигурация серверов (открытые порты, сервисы)
- Другие признаки

Passive DNS. Связи Domain-IP



- Расширение множества индикаторов
- Обогащение алертов SOC
- Мониторинг появления новых связей

Связь доменов группы Tolik через WHOIS

PT TIP ПОИСК ОТПРАВИТЬ IOC'S

Введите домен, хостнейм, IP, хеш-сумму или загрузите файл на анализ
teiehram.org

Вредоносный

teiehram.org  

IP	-	Дата регистрации	2024-11-13
Название сети	-	Истекает	2025-11-13
Группировка	Tolik	Роль	-

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS/RDAP СЕРТИФИКАТ PDNS (14) DNS (3)

WHOIS ИСТОРИЧЕСКИЙ WHOIS ИСТОРИЧЕСКИЙ RDAP

Домен teiehram.org

Зарегистрирован 2024-11-13

Срок действия истекает 2025-11-13

Контакты	Наименование	Организация	Адрес электронной почты
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com	-	abuse-contact@publicdomainregistry.com
Registrant	Anatolij Orlov	REDACTED FOR PRIVACY	tolya.orlov.080@gmail.com
Admin	Anatolij Orlov	-	tolya.orlov.080@gmail.com
Abuse	-	-	-
Tech	Anatolij Orlov	-	tolya.orlov.080@gmail.com

PT TIP ПОИСК ОТПРАВИТЬ IOC'S

Введите домен, хостнейм, IP, хеш-сумму или загрузите файл на анализ
whois_email:tolya.orlov.080@gmail.com

WHOIS EMAILS (8)

Домен

- vm-tiktok.org
- teiehram.org
- petition-change.org

Ключевые слова в доменах группы DarkGaboон

PT TIP ПОИСК ОТПРАВИТЬ IOC'S

Введите домен, хостнейм, IP, хеш-сумму или загрузите файл на анализ

31.13.224.86

Вредоносный

Критичность: Высокая

31.13.224.86

Хостнейм: - ASN: 401116

Группировка: DarkGaboон Роль: спс

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS PDNS (5)

Тип	Домен	Хостнейм
a	run.place	www.kilimanjaro.run.place
a	run.place	kilimanjaro.run.place
a	crabdance.com	kilimanjaro.crabdance.com
a	kilimanjaro.theworkpc.com	kilimanjaro.theworkpc.com
a	rampage.myvnc.com	rampage.myvnc.com

Несколько семантически схожих доменов на одном C2 сервере

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS/RDAP PDNS (4) СВЯЗАННЫЕ ФАЙЛЫ (7)				
СВЯЗАННЫЕ ФАЙЛЫ (7)				
Имя	Тип	Размер файла	Группировка	Семейство
TCPVCS.EXE	pe	6.26 MB	-	Revenge Rat
oxdio0.exe	pe	6.16 MB	DarkGaboон	Revenge Rat
Акт сверки взаимных расчетов предприятия № 136 от 19 августа 2025 года.exe	pe	6.16 MB	DarkGaboон	Revenge Rat
file.exe	pe	6.15 MB	-	Revenge Rat
Акт сверки взаимных расчетов предприятия № 142 от 19 августа 2025 года.exe	pe	6.14 MB	-	Revenge Rat
031a89dcd2128d3d7536e514e2d9efbe48d8c3cdfc15812cc99b757d06cbd50.exe	pe	6.15 MB	DarkGaboон	Revenge Rat
backup-message-10.48.112.41_9045-5167261.eml	eml	212.07 KB	-	-

Более 200 семплов Revenge RAT с финансовым неймингом

SSL-сертификаты стиллера Rhadamanthys

SERVER	DOMAIN	EMAIL	HOSTNAME	GET SERVER SSL INFO	GET DOMAIN SSL INFO	GET NS RECORDS	GET MX RECORDS	GET COUNTRY	GET CITY	GET PROVIDER
104.37.175.249	104.37.175.249:8888	-	-	3e:51:a2:c0:c5:35:a4:75:df:ee:21:2e:73:a8:f7:d7:f1:1a:13:b4 36:83:CC:4F:72:38:F8:6D:63:93:DA:DC:59:87:FA:5F:CE:81:26:60:9F:EB:73:0A:A6:58:B7:AD:3A:70:BC:AA Rhadamanthys rhadamanthys.local Rhadamanthys rhadamanthys.local	-			United States	Carrollton	Majestic Hosting Solutions, LLC

SERVER	DOMAIN	EMAIL	HOSTNAME	GET SERVER SSL INFO	GET DOMAIN SSL INFO	GET NS RECORDS	GET MX RECORDS	GET COUNTRY	GET CITY	GET PROVIDER
192.30.242.216	192.30.242.216:443	-	-	13:e7:29:7b:64:46:14:50:90:bc:73:12:68:43:9a:96:94:e3:62:ae 73:04:CF:3F:CF:4A:ED:EB:A9:4C:97:41:68:AB:33:58:83:32:07:18:CB:84:5A:C7:55:87:5C:44:96:2B:8E:33 Rhadamanthys rhadamanthys.local Rhadamanthys rhadamanthys.local	-			United States	Carrollton	Majestic Hosting Solutions, LLC

CASES BY SSL CERT	SHA256	ISSUER ORG	ISSUER CN	SUBJECT ORG	SUBJECT CN
3e:51:a2:c0:c5:35:a4:75:df:ee:21:2e:73:a8:f7:d7:f1:1a:13:b4	36:83:CC:4F:72:38:F8:6D:63:93:DA:DC:59:87:FA:5F:CE:81:26:60:9F:EB:73:0A:A6:58:B7:AD:3A:70:BC:AA	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
2b:d3:58:5e:42:9b:b6:21:e5:65:81:71:22:3b:52:49:51:c7:d8:c8	A0:12:5D:16:4A:50:8A:8F:F6:F4:1:8B:DE:78:5D:AB:4B:01:10:35:1F:92:D3:82:E4:D9:80:CEFC:86:5E:97	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
18:cebcb:2a:d6:a3:7c:04:75:c8:11:c8:72:91:26:99:07:at:c3:2f	4D:C5:49:79:1F:07:85:ED:D5:BF:8B:7E:53:21:FD:2A:2F:6C:22:8B:EB:00:40:0D:CE:AE:04:C8:82:A7:10:A5	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
31:89:3b:42:af:6b:66:e5:11:46:0c:9d:cd:84:91:96:59:87:AB:90	0B:DA:35:52:8D:1E:A9:83:11:6CA:59:68:0B:1B:27:45:9E:8B:5C:12:F8:9C:0B:1C:BA:C1:45:54:31:23:6F	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
4bf3:f3:75:1fb:66:1d:5b:83:c4:59:0f:18:9e:43:18:3c:46:26	8E:80:D2:89:0D:8D:74:BB:A5:EE:29:94:C7:A9:8CA:73:AA:4C:D0:07:80:A7:C9:65:73:77:94:15:EF:AF:0F:C0	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
07:37:0d:87:db:d4:95:88:61:cf:cf:4a:48:9b:49:4a:3b:62:e2:8d	9F:79:86:86:52:51:83:F2:E6:98:34:F2:16:83:3B:A8:C1:68:AB:89:8A:E7:49:FE:65:23:D1:05:12:B1:D1:F6	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
27:b4:92:31:53:53:84:8e:de:96:59:8a:79:66:b8:c6:db:d9:9f:0e	EA:3D:3EDC:3F:67:6F:D3:D9:83:05:68:1B:94:3EA:68:00:1:32:82:FA:1E:02:82:58:D3:32:43:81:02:20:8A	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
76:62:45:d3:d8:83:c3:d2:2d:d5:3c:77:c9:fb:a4:a7:1d:7b:02:86	3B:22:86:8B:C2:87:E2:18:E0:68:A3:D6:71:13:DC:3D:50:BC:98:40:18:42:6E:2F:1A:1CFE:7E:A8:1D:D1:07	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
4a:c5:3a:68:7e:03:23:df:eb:4b:df:a8:42:d3:b4:b1:9f:75:02:12	67:CA:3C:2B:C7:69:85:71:0F:AC:BC:55:9A:C9:AB:D0:25:5C:78:ED:F4:4A:16:93:D3:08:A4:5C:DC:A3:44:A8	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
1f:58:a8:27:47:c7:22:fb:37:2d:6d:28:e3:5b:4b:be:94:et:45:33	20:CD:55:CE:D4:11:89:1A:A6:32:13:7B:50:4F:57:71:44:1C:FF:D5:E9:83:6E:60:19:78:2CA:68:FC:07:9B	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
41:40:6a:39:6a:9e:ab:07:40:fd:aa:8a:eb:66:46:91:78:c2:27:d4	FC:85:3E:F2:84:E8:03:07:61:CA:45:B9:12:34:BF:5D:9A:19:7F:87:01:D9:BF:AB:EA:3D:5B:BE:4A:3B:6F:ED	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
07:1a:74:f5:4ee:5:00:18:15:03:cb:30:3fb:5:4cee:04:01:fd	FB:94:11:4D:DA:8E:90:31:CC:01:5C:06:6C:0B:82:6A:60:FA:AS:D0:DC:F5:2B:F0:C9:FA:EF:6E:EA:7CEB:DC	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
1b:d3:d0:19:87:79:35:49:d3:c5:3a:29:a5:a3:49:cd:2e:2b:4a:0	72:2D:1ECE:8C:D6:80:7F:31:DA:CA:07:4C:51:4D:C4:AD:E1:1C:85:B6:27:65:7C:22:8E:96:E8:D5:A4:E1:AE	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
03:67:80:5e:7fa:ea:eb:db:59:d2:d5:4f:37:4d:53:32:35:c3:60	5D:37:D3:81:F:D1:B1:71:54:5A:CF:7:FF:E8:4E:63:77:F3:C7:B0:C0:94:59:2C:F0:66:62:D1:FA:F6:F9:82	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
34:cb:a8:8e:d6:32:1e:cd:3a:70:27:5e:90:aeb:14:feb:7b:27:b0	D7:69:60:61:ED:90:D7:29:62:A5:0B:F8:20:27:5D:99:46:83:A3:86:8F:D5:7E:A7:78:74:01:29:D1:F7:D6:04	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
76:19:85:0e:3b:0a:9f:3c:63:17:0a:8d:21:de:f7:e5:8b:7f:75:f1	ED:19:8F:3C:7D:2E:4D:F5:68:40:4C:35:27:EB:D6:1A:1C:10:F9:8B:D6:9A:20:4E:F5:ED:85:27:40:46:24:7D	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
02:4a:56:ac:23:73:76:e5:0c:1e:4d:dc:52:37:93:30:36:a7:13:9d	FC:57:9E:C8:5A:33:A6:D2:8C:5C:61:A8:76:43:64:D2:2F:80:95:05:F0:8A:CA:29:3B:8E:09:3A:F8:0E:8D:98	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
4da:01:96:1b:52:18:eb:4d:10:9c:bd:14:b1:21:41:0c:62:d3:76	B5:84:8F:0C:62:7D:07:55:62:B5:65:8B:AC:E1:68:4D:71:08:64:D7:72:8C:06:F7:36:97:9E:5F:98:5E:9E:1	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
13:e7:29:7b:64:46:14:50:90:bc:73:12:68:43:9a:96:94:e3:62:ae	73:04:CF:3F:CF:4A:ED:EB:A9:4C:97:41:68:AB:33:58:83:32:07:18:CB:84:5A:C7:55:87:5C:44:96:2B:8E:33	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
0b:d0:c2:31:d2:42:3c:0a:dc:cb:eb:50:9b:3b:6a:8c:36:76:89:32	93:8F:B7:3E:DF:11:E8:81:52:87:FF:59:A1:08:93:ED:5B:58:93:C8:39:04:F8:3C:FA:6C:DB:90:3B:09:FD:E8	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
6b:bd:04:c5:3e:89:b4:0f:10:66:26:5f:6e:85:14:09:98:1f	F9:31:E8:82:95:FB:C6:64:47:90:D0:A3:77:D0:0E:F6:BE:15:EC:73:D1:7D:72:E9:60:09:67:45:DF:97:EB:10	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
6d:35:b3:90:1c:d4:f1:79:d7:49:99:3a:0c:8f:8c:b9:f1:41:dd	3F:EA:9E:73:05:EF:C4:72:71:79:56:80:9F:C2:2B:10:5D:24:3F:9D:0A:E5:40:40:27:ET:EC:60:31:86:AC:4A	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
73:8b:0b:60:de:7a:5d:0c:35:24:67:78:5b:eb:89:db:0d:89:45	AA:5E:17:38:80:2E:D8:D7:A8:5E:88:13:01:49:4d:1F:11:8D:03:04:28:66:58:6F:4F:D1:88:CB:73:36:7CFE	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
47:36:ab:3f:93:5c:91:fc:0b:11:99:56:7e:61:18:96:17:9e:56:14	2A:EB:1E:21:EB:14:4F:90:89:94:9F:20:7B:D0:C5:BC:8D:64:E6:21:24:C7:4A:8E:1E:99:04:CD:41:DD:1C:90	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
27:1fa:eb:db:50:4f:6c:c5:94:b5:b3:2f:7c:94:34:ee:3cb:9f:d6:7e	4d:58:84:EF:8A:FA:09:4CC:6:F7:3B:39:04:64:08:C2:A1:D3:EB:FC:D8:05:4F:54:03:12:62:57:8E:64:C1:71	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local
15:ba:82:a3:38:be:45:44:1b:fe:87:2f:53:fb:85:66:8d:87:98	41:CD:2E:20:D0:41:71:75:08:A2:4B:4C:2:C9:12:AC:5B:1E:C4:C5:95:96:73:4B:C6:88:EB:8A:26:64:68:98	Rhadamanthys	rhadamanthys.local	Rhadamanthys	rhadamanthys.local



Паттерн – «Rhadamanthys» в TLS-сертификатах

Passive DNS. Варианты развития

- Взаимодействие по созданию общей БД для DNS
 - Полнота данных
- Использование журналов публичных DNS для детектирования угроз
 - Полнота данных
 - Детектирование атак и взломов в организациях без службы ИБ и внешних SOC
- Добавление данных активного сканирования (аналоги Shodan, FOFA и так далее)
 - Расширенный сетевой профиль

Спасибо