positive technologies

Работа с индикаторами компрометации

Алексей Вишняков
руководитель отдела обнаружения вредоносного ПО
экспертного центра безопасности
Positive Technologies (PT ESC)

ptsecurity.com

О докладчике

- Специалист по анализу APT и отслеживанию киберугроз
- Отвечает за экспертизу в продуктах PT Sandbox, PT CybSI и PT XDR
- Постоянный спикер конференций PHDays, AVAR, Nullcon

Содержание

- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

Содержание

- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

Задачи TI

Threat intelligence (данные о киберугрозах) — это информация об актуальных угрозах и группировках киберпреступников, которая позволяет организациям изучить цели, тактику и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак. Компании могут сами собирать данные о киберугрозах или заказывать информацию у сторонних поставщиков.

Threat Intelligence представляет собой знания об угрозах, полученные в результате анализа и интерпретации данных. Threat Intelligence объединяет три взаимосвязанных элемента: 1) контекст, 2) индикаторы компрометации, 3) взаимосвязи и обогащения. Каждый элемент не несет ценности сам по себе, но в совокупности они образуют как раз эти самые ценные знания.

Что такое кибербразведка (Threat Intelligence)?

Threat Intelligence, или Cyber Threat Intelligence (разведка в области киберугроз), если описать это явление простыми словами, представляет собой строго структурированную информацию и знания, благодаря которым организация имеет чёткое представление о киберугрозах, с которыми она может столкнуться.

Задачи TI

Чего ждём от TI?

- Обнаруживаем угрозы лучше
- Становится яснее суть угрозы
- … разве это не всё?

Задачи TI

Какие индикаторы компрометации нас действительно интересуют?

1. IP-адрес
2. FQDN
3. Веб-ссылка
4. Хеш (MD5, SHA-1, SHA-256)

Какие ещё есть?

- scvhost.exe
- \Default\Policy.1.9.Orcus.Shared
- info@soc-forym.ru
- Global\mukimukix0
- 127.0.0.1:3388
- +74992816994
- fvthbrfycrbte,k.lrb
- …

Содержание

- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

Характеристики IoC

Обогащение файловых индикаторов

1. Формат (MIME-тип)
2. Размер
3. Статус ЦП

Посложнее (топ-n значений или число):

- Имена
- Родительские и дочерние объекты (bundle)
- Детекты облачных анализаторов и песочниц

Характеристики IoC

Обогащение URL

1. Статус TLS-сертификата
2. Статус ответа сервера
3. Размер ответа (body)
4. Метод запроса

Посложнее:

- Список User-Agents
- Число редиректов при обращении
- Характеристики TLS-сертификата (Serial Number, Issuer, Subject…)
- Число параметров запроса

Характеристики IoC

Обогащение доменов

1. WHOIS (время регистрации, инфо о регистранте…)
2. DNS-записи (MX, SOA, CNAME…)
3. Список и число разрешённых IP

Посложнее:

- Признак DGA
- Популярность (Alexa, Tranco)
- Число загружаемых файлов

Характеристики IoC

Обогащение IP

1. ASN
2. Geo
3. Список открытых портов

Посложнее:

- Инфраструктура DDNS
- Синкхол
- Облачный провайдер
- Множество независимых сервисов

Характеристики IoC

Общие критерии обогащения

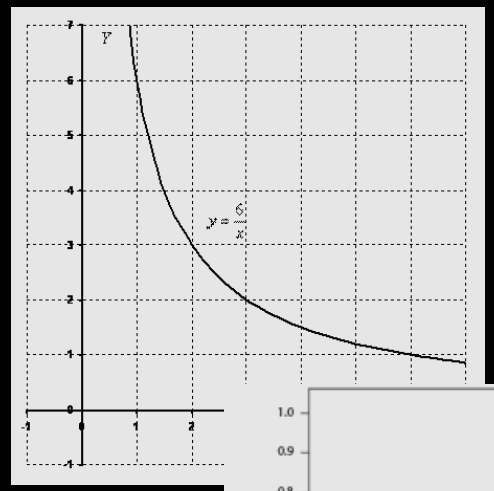
1. Даты первого и последнего появления
2. Число упоминаний
3. Связи с другими индикаторами
4. Ассоциация с семейством ВПО
5. Теги

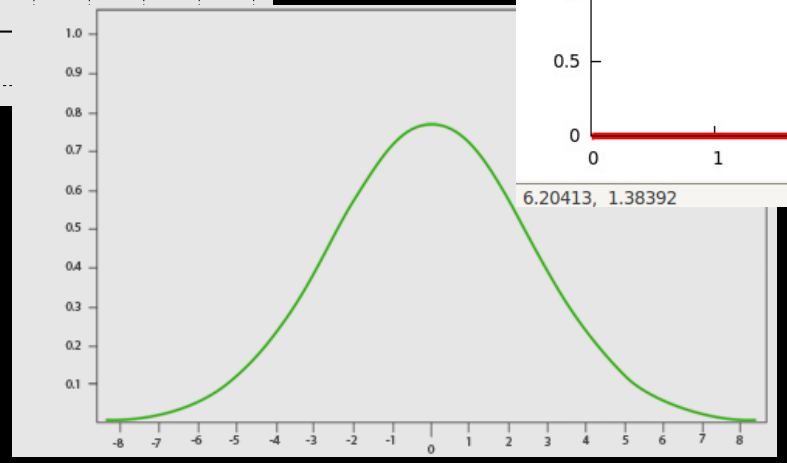
Содержание

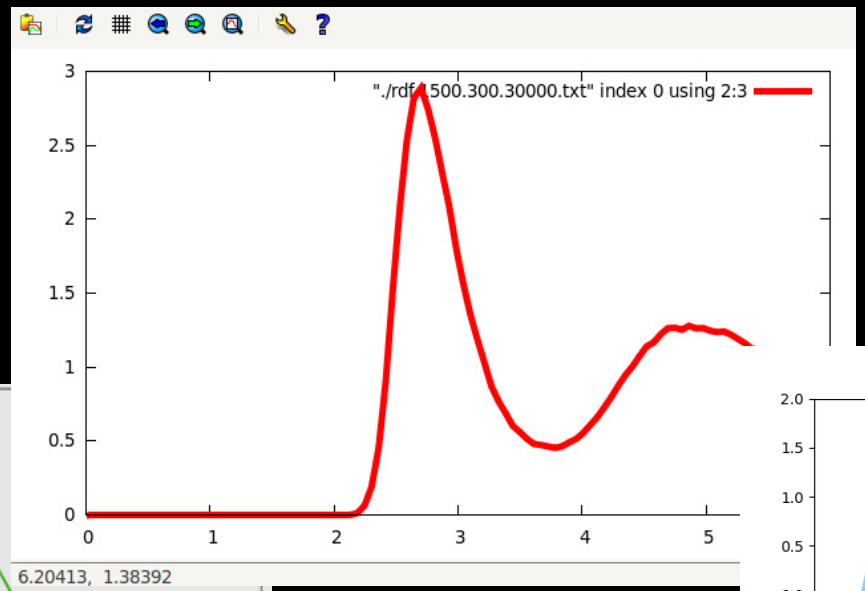
- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

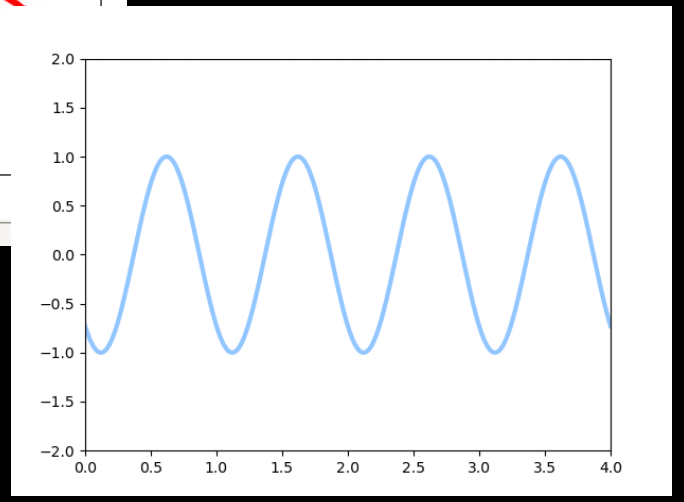
Затухание и вес

Какова скорость протухания мяса?









Затухание и вес

Почему формулы затухания не работают

Сетевая инфраструктура

Среди расшифрованных строк одного из свежих бэкдоров BACKSPACE можно встретить ряд доменов (newpresses\.com, appsecnic\.com, km153\.com), которые использовались группой более 10 лет назад. Соберем некоторые наиболее интересные WHOIS-данные в таблице ниже:

WHOIS-данные доменов newpresses\.com, appsecnic\.com и km153\.com

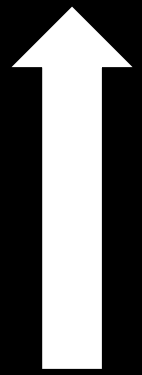
WHOIS-поле	newpresses\.com	appsecnic\.com	km153\.com

https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/orlinyj-glaz-snova-v-igre-apt30/

Затухание и вес

Вес индикатора: метод перекрывающих фактов

1. С IP скачивается > 1000 чистых файлов
3. В IP разрешается чистый домен



2. Бэкдор – инструмент APT
4. IP – это C2 бэкдора

Вывод: IP становится чистым

Затухание и вес

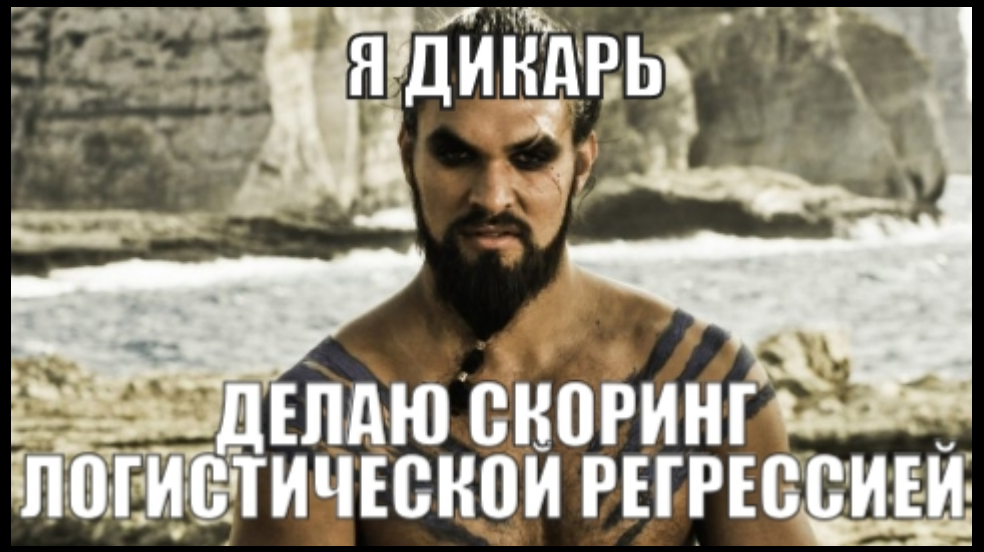
Вес индикатора: метод коэффициентов

$F(x) = a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots$, где

a_i – коэффициент степени важности факта, от $-N$ до $+N$

x_i – наличие факта, 0 или 1

После расчёта всех весов делается нормировка



Затухание и вес

Вес индикатора: вероятностный подход

$P = 1 - (1 - p_1) \cdot (1 - p_2) \cdot (1 - p_3) \ldots$, где

p_i – вероятность того, что индикатор вредоносный

Если факт говорит о легитимности индикатора (90%, что чистый), тогда берётся противоположное значение (10%, что вредоносный)

Содержание

- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

От IOC к TTP

На NGFW сработало обращение к вредоносному домену funding-exchange\.org . Домен – C2 бэкдора Beacon инструмента Cobalt Strike. Бэкдор использовался в атаке на организацию из авиационно-промышленного сектора России в августе 2021 года. Атака ассоциирована с группировкой ChamelGang. В арсенале ChamelGang имеется инструмент для внедрения в IIS веб-сервер в режиме пассивного бэкдора (DoorMe). Проводится аудит веб-серверов на предмет компрометации.

Содержание

- Задачи TI
- Характеристики IoC
- Затухание и вес
- От IoC к TTP
- Выводы

Выводы

- Обогащение не только даёт контекст оператору, но и помогает при ранжировании
- Полезность затухания индикаторов сомнительна
- Сначала результативность, потом объёмность покрытия

Спасибо за внимание!

Алексей Вишняков

avishnyakov@ptsecurity.com

Twitter: @Vishnyak0v