КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Threat Intelligence

Как начать пользоваться: от слов к делу

Антон Соловей
Независимый эксперт

./whoami

Антон Соловей

Учился на разработчика. Окончил техникум.

Потом — на защиту информации. Окончил университет.

Прошел школу эникея и админа, технической поддержки и внедренца в вендоре.

Ушел в управление продуктами, так как именно таким образом наношу максимальную пользу. Последние 2,5 года — владелец продукта.

Сейчас — владелец продукта Threat Intelligence platform в R-Vision.

Что такое threat intelligence

?

Что такое threat intelligence?

Индикаторы компрометации?

Контекст?

Что такое threat intelligence?

Контекст

+

Индикаторы компрометации

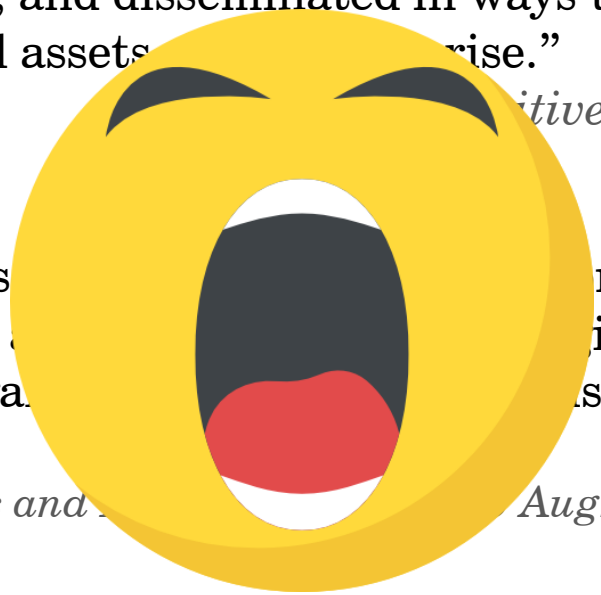
+

Взаимосвязи

Академический подход

“Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analysed, and disseminated in ways that help security and business staff at all levels protect the critical assets rise.”

itive Guide to Cyber Threat Intelligence



“Threat intelligence is evidence bas ntext, mechanisms, indicators, implications and actionable advice, ing menace or hazard to assets that can be used to inform decisions rega se to that menace or hazard.”

Gartner, McMillan (2013)

from Tactics, Techniques and Augment Cyber Threat Intelligence (CTI): A Comprehensive Study

“The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators.”

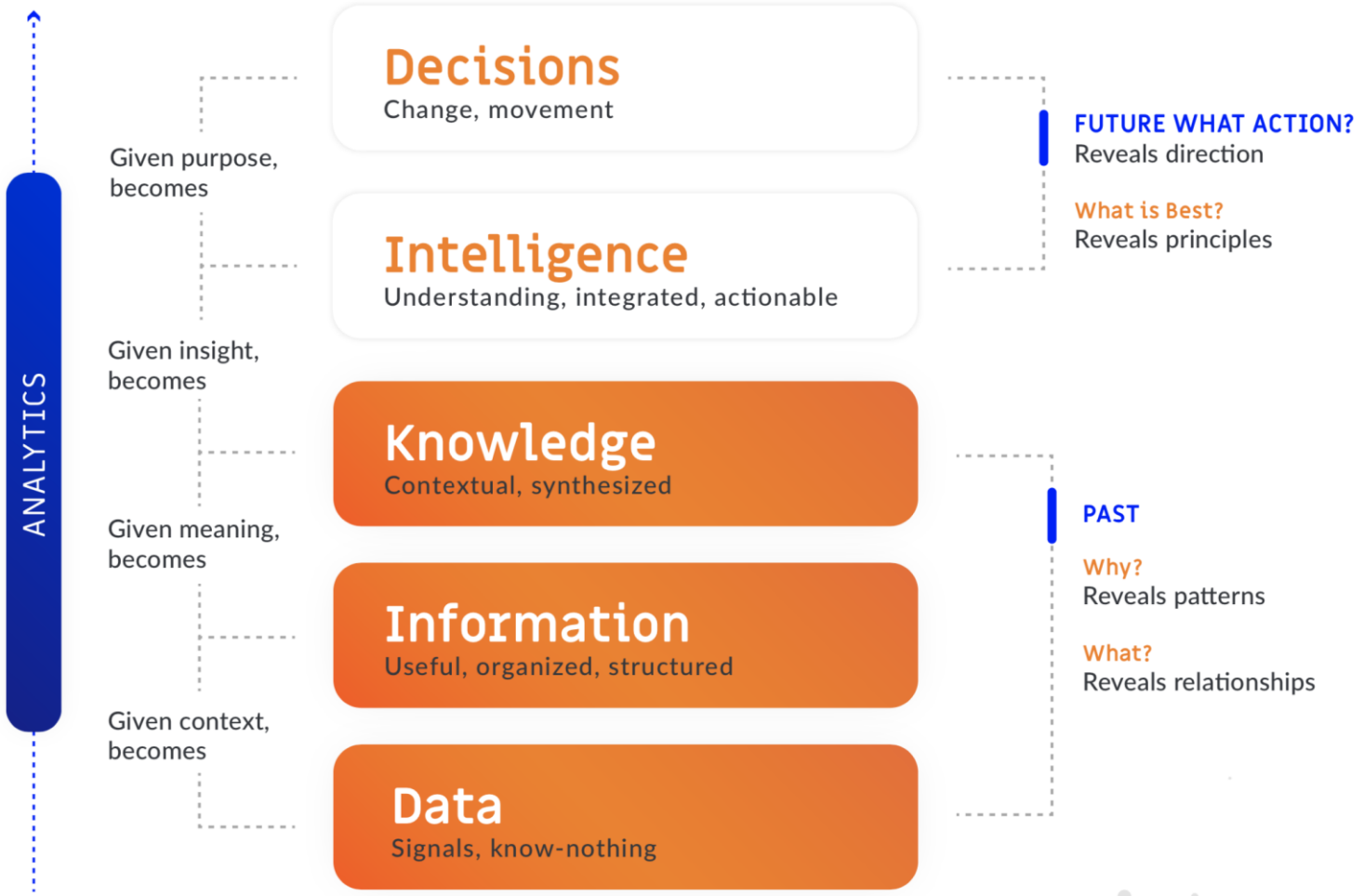
SANS Institute

Threat intelligence — это знания

Которые можно проанализировать и **применить** человеком и **машиной**

#CODEIB

Очень зрело


ANALYTICS
Given purpose, becomes
Given insight, becomes
Given meaning, becomes
Given context, becomes
Decisions
Change, movement
Intelligence
Understanding, integrated, actionable
Knowledge
Contextual, synthesized
Information
Useful, organized, structured
Data
Signals, know-nothing
FUTURE WHAT ACTION?
Reveals direction
What is Best?
Reveals principles
PAST
Why?
Reveals patterns
What?
Reveals relationships

Почему TI мало кто пользуется?

сложно получать

сложно интерпретировать

сложно применять

сложно оценивать пользу от применения TI

Примеры фидов


```
{
    "md5": "8D2A50C4ABE53C48BB85F1D708C4052D",
    "sha1":
    "28E853985367C7FA7B9163DAEE01E63BA47B7421",
    "sha256":
    "B7F638B47D5C44E69C2E63A0AB9F89357784B0658BE
    929D8E1E0216C09FE01F4",
    "link":
    "https://metadefender.opswat.com/results#!/f
    ile/bzE3MDIyMUgxWUZ6MXk5WWxIeTRna3ptVWtuNw/r
    egular?utm_medium=json&utm_source=www&utm_ca
    mpaign=threat_feeds",
    "total_avs": 15,
    "total_detected_avs": 1,
    "threat_name": "Trojan/Heur!vwtunw",
    "file_type_category": "E",
    "file_type_extension": "exe",
    "published": "2019-05-17"
}
```

Примеры фидов


```
{
    "indicator":
    "5bdf483279a4a816ed4f8a235e799d5068d14f
    64",
    "description": "",
    "title": "",
    "content": "",
    "type": "FileHash-SHA1",
    "id": 1055
}
```

Сбор и обработка

```
<cybox:Observable id="ibm:Observable-36987423ad99834bf10eb2abfe88ee82">
<cybox:Title>XFE Observable for 1E3A57CFF7CBA8732364C26F4BBDCBE2
</cybox:Title>
<cybox:Description>XFE Observable for 1E3A57CFF7CBA8732364C26F4BBDCBE2
</cybox:Description>
<cybox:Object id="ibm:Object-54e4b1bf-9bea-6fba-7d96-0f45f4f53ff1">
<cybox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5
</cyboxCommon:Type>
<cyboxCommon:Simple_Hash_Value condition="Equals">1E3A57CFF7CBA8732364C26F4BBDCBE2
</cyboxCommon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</cybox:Object>
</cybox:Observable>
```

Примеры фидов

Malware analysis on Bitter APT campaign (31-08-19)

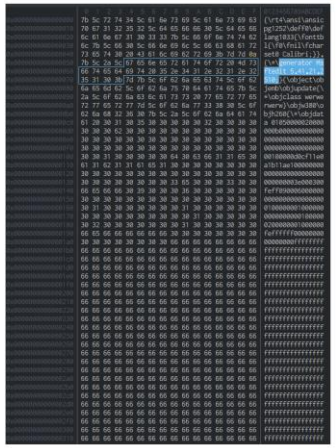
Table of Contents

Malware-analysis

Initial vector

Use a document with a remote template injection as initial vector. This request http[:]//maq.com.pk/ for be redirected on the next URL.

This seconds URL (http[:]//maq.com.pk/wehsd) send an RTF exploit.



Executive Summary

Since at least 2015, a suspected South Asian threat grouping known as BITTER has been targeting Pakistan and Chinese organizations using variants of a previously unreported downloader. We have named this malware family ArtraDownloader based on a PDB string discovered within the samples. We've observed three variants of this downloader with the earliest timestamp of February 2015. This downloader has frequently been observed downloading the Remote Access Trojan (RAT) BitterRAT which is associated with BITTER threat operations.

Starting in September 2018 and continuing through the beginning of 2019, BITTER launched a wave of attacks targeting Pakistan and Saudi Arabia. This is the first reported instance of BITTER targeting Saudi Arabia. Details surrounding these attacks and the three ArtraDownloader variants observed are described below.

Activities

Between mid-September 2018 and January 2019, Unit 42 observed the ArtraDownloader used in the targeting of Pakistan and Saudi Arabian organizations. Several malicious documents have been identified, all communicating with likely compromised, legitimate Pakistan websites to retrieve the payload. These websites include those associated with the Pakistan government and other Pakistan organizations.

Beginning on Sep 12, 2018, we observed files with the following names hosted on the URL https://wforc[.]pk/js/.

- Internet Data Traffic Report – August 2018.docx
- PAF Webmail Security Report.doc.exe

The presumed spear phish targeted an employee of an organization in Saudi Arabia. The malicious file communicated with the C2 nethosttalk[.]com.

Around the same timeframe, two additional files (listed below) were observed being hosted on another Pakistan website. These executables, which had the following names, were hosted on the URL khurram.com[.]pk/js/drvn and communicated with the domain nethosttalk[.]com for C2.

- Handling of Logistics.pdf[.]com
- Cyber security work shop.pdf[.]com

Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксирован факт массового распространения вредоносного программного обеспечения семейства «Buhtrap». Указанное ВПО используется в атаках на организации кредитно-финансовой сфере и их клиентов – юридических лиц.

2. Основные индикаторы компрометации

1	URL-адреса и IP-адреса, к которым производятся обращения	puntoyandex[.]in 85.217.170[.]37 139.60.163[.]158
2	Адреса и домены отправителей писем	**подменные:** kashcheev@arenda-volgograd[.]ru komplekt1@kmsd[.]ru mainsister@surgutgp5[.]ru ar@soctrade[.]com **реальные:** 23.106.223[.]12

Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусными средствами различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей организации антивирусного средства.

Обращаем внимание на то, что использование авторами рассылки ВПО иных имён файлов, кроме указанных в настоящем бюллетене, **не исключено**.

1) «akt_kass.doc»

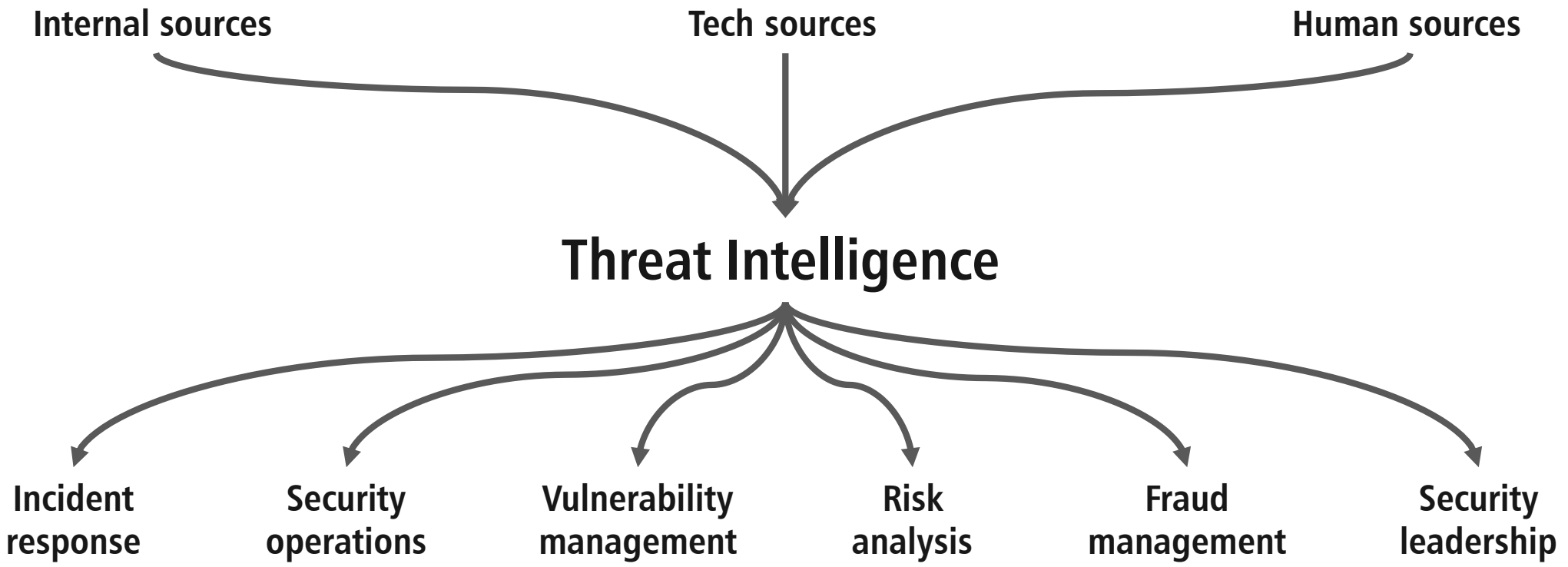
MD5	664E95FBD9C4439C9800CC93F0474D1B
SHA1	A472995CB37965F3F938152D965EF6CDB4CFE327
SHA256	7CEF4B46501F605030427C3F0C6DB5E190AF8EA757D75533F900AADA952DA0A0
Размер файла (байт)	179200

2) «kassovy_akt.doc»

MD5	35BE4860A6EA917A9F680F5D2FAAA2E2

Email: fincert@cbr.ru

Внутренние потребители TI



Но не все так страшно на самом деле

Классы задач при работе с TI

1. **Сбор**
   из разных источников
2. **Обработка**
   нормализация, агрегация
3. **Обогащение**
   если данных недостаточно
4. **Обнаружение**
   индикаторов компрометации внутри инфраструктуры
5. **Распространение**
   на средства защиты для мониторинга и блокировки
6. **Автоматизация**
   сценариев использования индикаторов

КАК НАЧАТЬ РАБОТАТЬ С TI ?

Определить, нужно ли это вам в принципе
Ответьте себе на вопрос: какие задачи вы планируете решать с помощью TI?

Использовать платформу для сбора TI
Руками — сложно и неэффективно!

Регулярно оценивать качество источников TI
Фолсящие и бесполезные — выкидывать

Автоматизировать рутинные операции
Обогащение, мониторинг, блокирование

Бонус: годные материалы про TI. Софт.

MISP — продакшн-реди решение

OpenCTI— молодой проект, подающий надежды, заложены правильные идеи

Бонус: годные материалы про TI. Софт.

1. CRITS
2. CIF
3. GOSINT
4. GRR
5. OSQUERY
6. Awesome threat intelligence

Бонус: годные материалы про TI. Софт.

Отдельный респект: **Politraf**

https://github.com/ainich/politraf

Бонус: годные материалы про TI. Фиды.

ФинЦЕРТ — доступен всем

180+ свободно-распространяемых фидов в моей подборке:
https://github.com/like-a-freedom/Intelligent-harvester/blob/master/config/settings.yaml

IBM X-Force Exchange

AT&T Cybersecurity
(ex Alien Vault OTX)

Подытожим

1. **TI обычно нужен там, где есть реагирование на инциденты**
   Без процесса IR ценность TI неочевидна

2. **Кибербразведка похожа на обычную разведку**, как с точки зрения данных, так и с точки зрения процесса

3. **Качество TI прямо влияет на качество реагирования на инциденты ИБ**: чем лучше выше будет качество TI, тем ниже время реагирования и разрешения инцидента в общем случае

4. **Это осведомленность специалистов по ИБ**, что позволяет понимать ландшафт угроз, планировать, внедрять и реализовывать адекватные защитные меры

Что было, что будет, на чем сердце успокоится?

1 **Унификация и стандартизация**
Не изобретение и принятие новых стандартов, а повсеместное принятие и использование, типовые решения под отрасли и классы задач

2 **End-to-end автоматизация процесса**
Закрытие полного цикла сценариев работы с threat intelligence

3 **Развитие культуры обмена данными TI**
Отраслевые центра обмена данными кибербразведки: государственные и коммерческие

4 **Появление большего количества локальных источников TI**
Просто потому, что сейчас их мало — а это практически отсутствие конкуренции и монополизация ниши

Бонус: годные материалы про TI. Почитать.

Definitive guide to threat intelligence

The Threat Intelligence handbook by Recorded future

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

solovey.anton@gmail.com
+7 906 075-53-63
facebook.com/solovey.anton


КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ