INNOSTAGE

Threat Intelligence - разбираемся в понятиях на практике

Калинин Антон

Руководитель группы аналитиков CyberART

INNOSTAGE

Фиды

TAXII

Threat Intelligence

STIX

OSINT

TLP

киберразведка

YARA

MITRE ATT&CK

Threat hunting

Индикаторы компрометации

Что такое Threat Intelligence?

INNOSTAGE

Threat Intelligence (Кибер-разведка) – Процесс сбора, анализа, систематизации и приоритезации информации об угрозах, получаемой из различных источников – открытых (OSINT), социальных сетей (SOCMINT), оперативных (HUMINT), а также из Даркнета.

- **Тактическая кибер-разведка** – **Индикаторы компрометации (IoC)** прошлых, текущих или будущих атак
- **Операционная** – **в основном TTP – Tactics, Techniques, Procedures** – информация о кампаниях, способах, методах и инструментах, используемых злоумышленником
- **Стратегическая** – **Информация о злоумышленниках, их мотивации, целях**, рекомендации и советы по реагированию, основополагающая информация

Аналитика угроз

- **IOA– Индикаторы атак (Indicators of Attack)**
- описанное поведение (действия злоумышленника) при проведении атак на систему
- **TTP– Тактики, техники и процедуры (Tactics, Techniques and Procedures)**
- Представление способах действия злоумышленников с различным уровнем детализации – от расстановки сил до подробного описания шагов, требуемых для выполнения задач.

- **IOC– Индикаторы компрометации (Indicators of Compromise)**
- **Любая атака содержит следы:**
  - IP, домены, URL, хэши, e-mail и т.д. Это и есть **IOC.**
  - Обладая знаниями об актуальных IOC, вы можете быть в курсе идущих атак, блокировать атаки заранее, искать их у себя и расследовать инциденты
  - IOC можно получать как из коммерческих, так и из бесплатных источников

Отличия IoC от IoA

INNOSTAGE

Фиксируют уже случившийся факт заражения	○	✓ Обнаруживают неизвестные атаки, для которых еще нет индикаторов компрометации
Точечное обнаружение во времени. IoC устаревают	○	✓ Постоянное обнаружение в режиме real-time
Представляют информацию о конкретной угрозе	✓	○ Абстрагированы от конкретных наблюдаемых случаев в отдельных конкретных Инцидентах
Просто детектировать	✓	○ Сложно детектировать

Источники информации об угрозах

INNOSTAGE

Любой источник информации об угрозах,
поступающий в вашу организацию

Источники информации об угрозах

INNOSTAGE

Внешние

- MISP Feeds
- Cisco Talos
- Kaspresky Feeds
- OTX AlienVault
- IBM X-Force
- Twitter
- ФинЦЕРТ
- OpenSource Feeds

Внутренние

- Песочницы
- SIEM
- NGFW

Фиды угроз

INNOSTAGE

Набор сведений из различных источников, обычно одного типа

Листы с IoC

- Индикаторы
- Правила
- Сигнатуры

Структурированные данные

- Индикаторы
- Правила
- Контекст
- Анализ образцов

Комплексные сервисы

- Индикаторы
- Правила
- Контекст
- Аналитика
- Артефакты
- Инструменты
- Оценка угроз

Один источник или много?

INNOSTAGE

- Может отсутствовать информация о массовых атаках
- Может отсутствовать информация о профильных угрозах
- Ошибочная информация (Potential False)

Выбор Фидов

- Тип источника
- Актуальность
- Формат и унифицированность предоставляемых данных (STIX, MAEC, OpenIOC)
- Уникальность
- Частота появления/обновления информации
- Полнота контекста
- Известность
- Автоматизация доставки (Наличие API)
- Релевантность данных

Чем собирать?

INNOSTAGE

- Собственные модули автоматизации (Python, API)
- Threat feed агрегаторы
  - Hippocampe
  - Anomali STAXX
  - Watcher
  - Intel Owl
- Готовые инструменты TI платформ

Детектирование IoA и IoC

INNOSTAGE

SIEM

EDR

Sandbox

UEBA

Anti-APT Platforms

MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

CAPEC™

Средства для поиска угроз на базе IoC

YARA

PowerShell

IoC Finder (FireEye)

THOR (APT Scanner)

LOKI (Windows)

Fenrir (UNIX/Linux)

Что делать с фидами IoC без контекста?

INNOSTAGE

1 Деление на 2 группы

Сетевые

IP

Домены

URL

Почтовые адреса

Хостовые

Файлы

Процессы

Ключи реестра

Хэш-суммы

2 Проверка на релевантность!

Проверка на релевантность

INNOSTAGE

GOSINT – инструмент автоматизации проверок индикаторов на релевантность

Pre-Processing

Indicators that have been scraped by GOSINT are available for processing here.

Notice Cisco Umbrella API key is not defined in the settings and cannot be used for calling on indicators. Enter the API key to utilize Cisco Umbrella API calls.

Show 10 entries Search:

date	indicator	type	source	context	tags	actions	move
Thu 14 Mar 2019 10:10:07	https://ouatmcaalumni.com/yokor/seenewmenews/seenupdatemenows.html	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	
Thu 14 Mar 2019 10:10:07	http://www.daiminhphat.info/1/	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	
Thu 14 Mar 2019 10:10:07	http://lvibrations.com/next/chines/chines/index.php?login=reutv@dor-chem.com	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	
Thu 14 Mar 2019 10:10:07	http://30dayaffiliatechallenge.com/wp-content/plugins/revslider/admin/views/system/.../china/?login=webmaster@mhdz.cn	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	
Thu 14 Mar 2019 10:10:07	http://hathyfan.es/components/com_banners/helpers/boa-user/boa/1addab1a8d6b44257e9e687b37ca341c	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	
Thu 14 Mar 2019 10:10:07	http://hathyfan.es/components/com_banners/helpers/boa-user/boa/1addab1a8d6b44257e9e687b37ca341c/error.php	url	openphish	https://openphish.com/feed.txt		ThreatCrowd VirusTotal Everything	

Что дальше?

В дело вступает Threat Intelligence Platform

Threat Intelligence Platform – платформа, позволяющая агрегировать, коррелировать и анализировать данные Threat Intelligence из различных источников.

Единая база знаний об угрозах

INNOSTAGE

Threat Intelligence Platform (TIP)

01 Получает знания об угрозах из большого количества разнородных источников

02 Агрегирует все данные в одной точке, выстраивает связи между ними

03 Распространяет знания об угрозах на используемые средства защиты информации

04 Позволяет выявлять массовые, целенаправленные и отраслевые атаки

05 Позволяет выстроить в компании процесс Response

60% организаций уже используют TIP, еще 25% собираются внедрять*

78% организаций (из использующих TIP) считают, что это помогло улучшить показатели в области безопасности и реагирования*

*SANS Institute, 2017

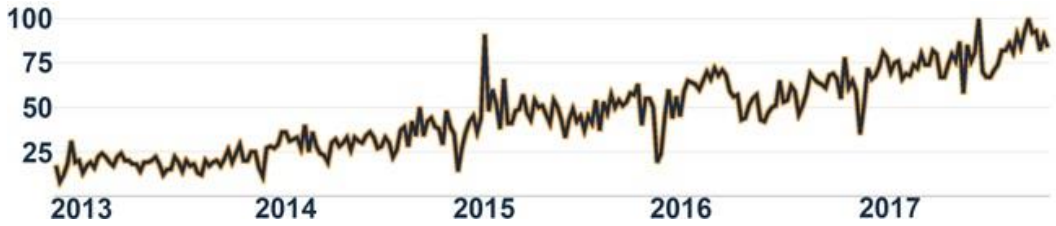


График роста популярности TIP

Платформы для TI

INNOSTAGE

Коммерческая или бесплатная?

Коммерческая

Масштаб
Удобство
Оперативность
Гарантия
Поддержка
Функциональность

Бесплатная

Цена
Энтузиазм

Платформы для TI

INNOSTAGE

Бесплатные платформы

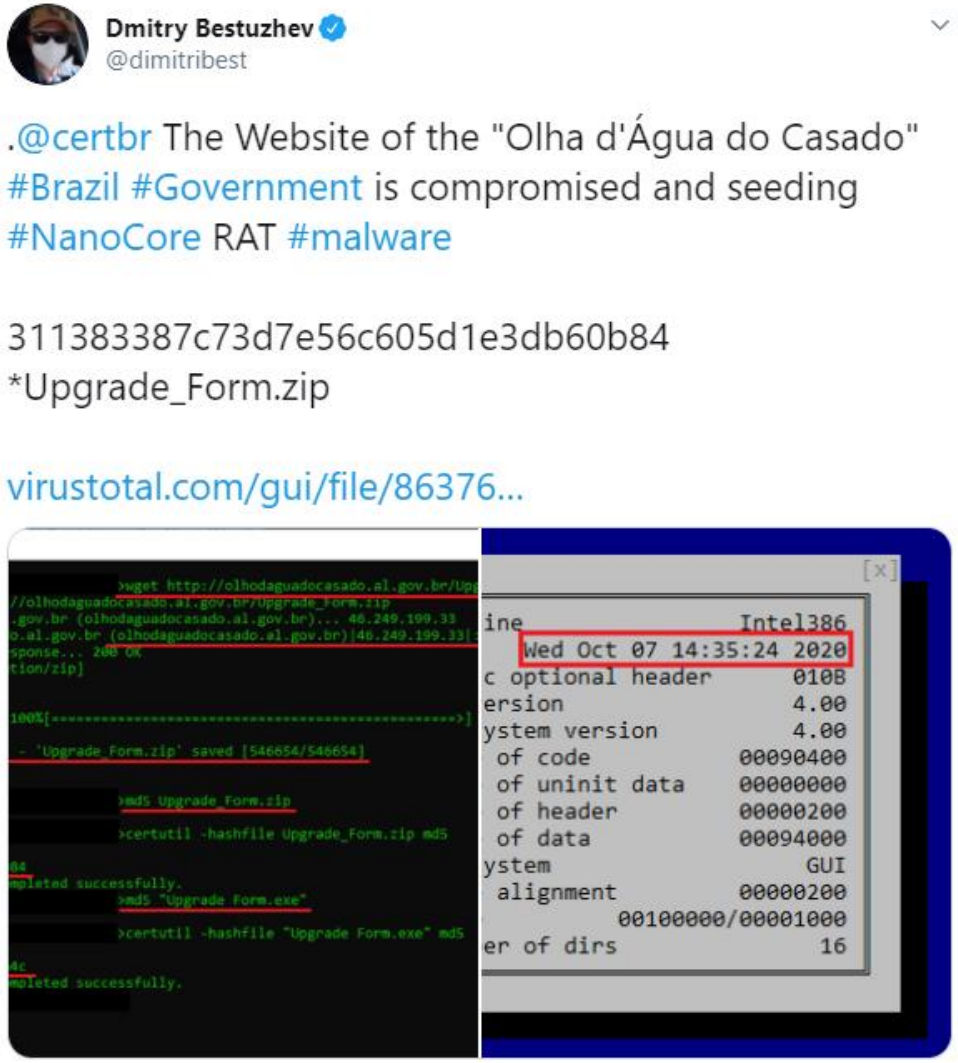
- MISP
- OpenCTI
- YETI
- CRITS

Схема процесса

INNOSTAGE

Скриншоты

INNOSTAGE



Dmitry Bestuzhev
@dimitribest

.@certbr The Website of the "Olha d'Água do Casado" #Brazil #Government is compromised and seeding #NanoCore RAT #malware

311383387c73d7e56c605d1e3db60b84
*Upgrade_Form.zip

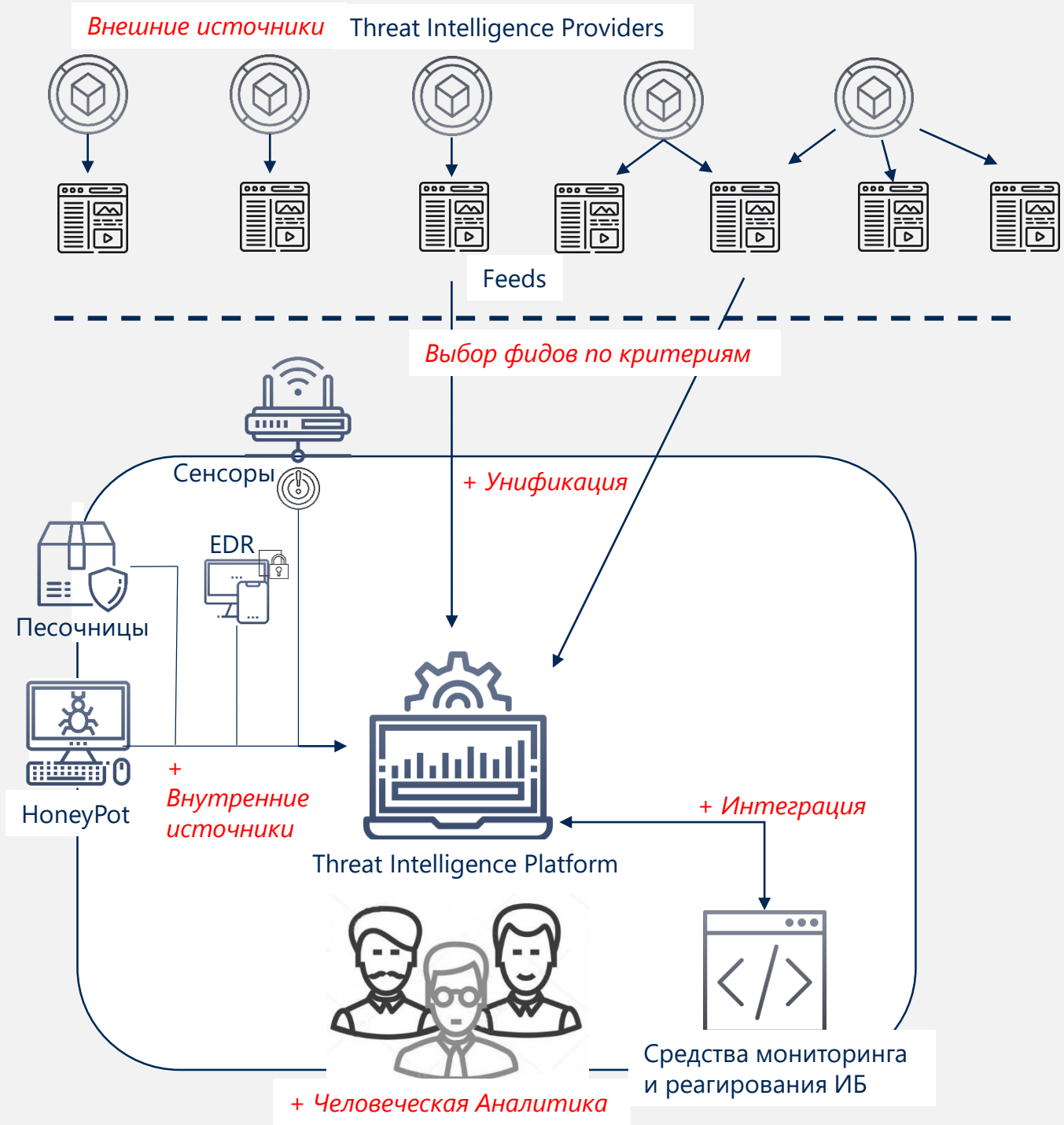
virustotal.com/gui/file/86376...

Date	Org	Category	Type	Value	Tags
2020-10-20		Other	comment	The Website of the "Olha d'Água do Casado" #Brazil #Government is compromised and seeding #NanoCore RAT	
2020-10-20		Network activity	ip-dst	79.134.225.82	C&C IPs x
2020-10-20		Payload delivery	filename	Upgrade Form.exe	veris:action:hackin
2020-10-20		Payload delivery	filename	Upgrade_Form.zip	
2020-10-20		External analysis	link	https://www.virustotal.com/gui/file/86376655aa7fc015020c6ed1f3a2487c109a73e893c0eec44aff6697a619fd2f/detection	
2020-10-14		Payload delivery	md5	311383387c73d7e56c605d1e3db60b84	
2020-10-14		Payload delivery	sha256	86376655aa7fc015020c6ed1f3a2487c109a73e893c0eec44aff6697a619fd2f	
2020-10-14		Other	comment	https://twitter.com/dimitribest/status/1315746871768383488	
2020-10-14		Other	comment	#Government	
2020-10-14		Other	comment	#NanoCore	
2020-10-14		Other	comment	#malware	

Скриншоты

INNOSTAGE

✗	SOC_TI	SOC_TI	12313		Twitter TA551 shathak IcedID
✗	SOC_TI	SOC_TI	12311		Twitter
✗	SOC_TI	SOC_TI	12309		Twitter agenttesla
✗	SOC_TI	SOC_TI	12310		Twitter agenttesla
✗	SOC_TI	SOC_TI	12308	Banker Trickbot	AEGIS tlp:amber Threat-Report misp:tool="misp2stix2" trickbot
✗	SOC_TI	SOC_TI	12307	Botnet Mirai	tlp:green AEGIS Threat-Report Mirai misp:tool="misp2stix2"
✓	SOC_TI	SOC_TI	12306	Tool Emotet	misp:tool="misp2stix2" Threat-Report AEGIS tlp:amber Emotet
✓	SOC_TI	SOC_TI	11765		urlhouse
✓	SOC_TI	SOC_TI	12305		Malshare
✓	SOC_TI	SOC_TI	10558		osint:source-type="block-or-filter-list"



Threat Intelligence – это процесс, и терминология TI вытекает одна из другой, проводя взаимосвязь всех этапов процесса.

Главная задача TI— дать специалистам по информационной безопасности актуальные данные и контекст для приоритезации своих действий и принятия решений.

INNOSTAGE

Спасибо за внимание!