Corso di Sicurezza delle reti e dei Sistemi Software

UNIVERSITÀ DEGLI STUDI DEL SANNIO
Benevento

CYBER THREAT INTELLIGENCE

Prof. Corrado Aaron Visaggio

Ing. Pietro Melillo

```
[~]$ whoami
```

Pietro Melillo

PhD Student @Unisannio
CISO @Wurth Italia
Member @JanaraLab
Head of TI @RedHotCyber

SOC Analyst

YOROI

SOC Analyst\ Team Leader

IBM

Head of TI Services

CISO

EC-Council CEH CERTIFIED

EC-Council ECIH CERTIFIED

EC-Council CTIA CERTIFIED

IBM QRadar SIEM Advanced Topics
IBM
Course Code: BQ203G
Instructor-Led Learning
Advanced

Cybersecurity Threat Intelligence
IBM
IBM Security
Intermediate

IBM QRadar SIEM Foundations
IBM
Course Code: BQ104G
Instructor-Led Learning
Foundational

IBM QRadar SIEM Foundation
IBM
IBM Security
Intermediate

PART 1: INTRO TO CTI

Contents

Cyber Threat Intelligence

What is Cyber Threat Intelligence?

Types of Threat Intelligence

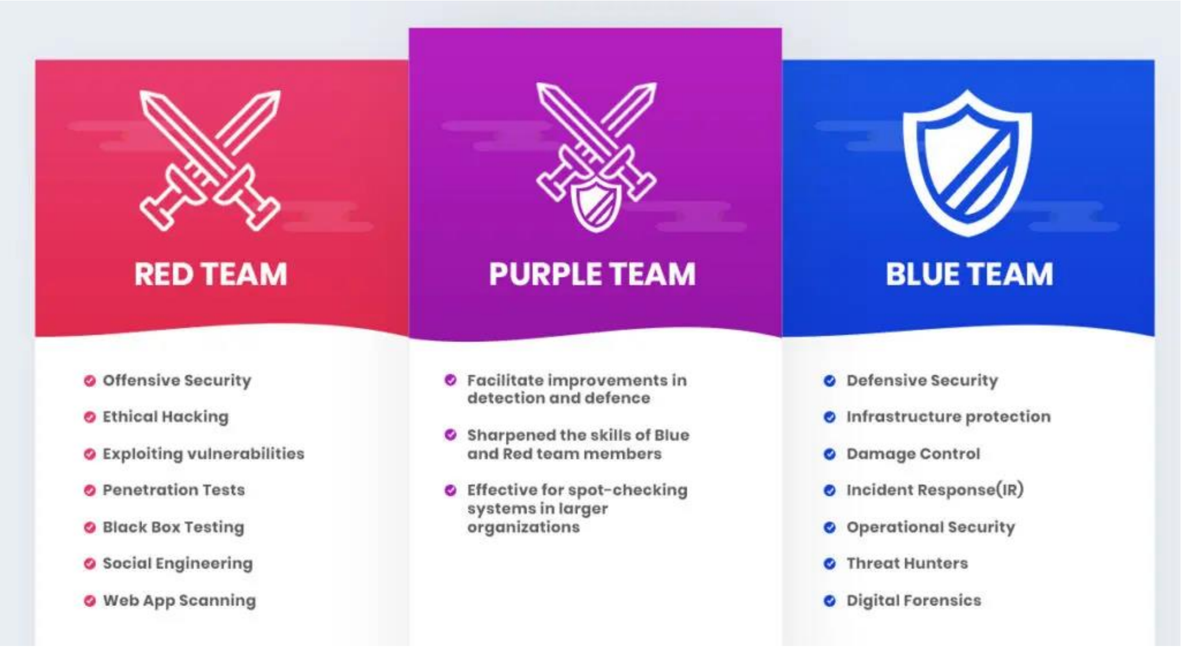
The Threat Intelligence Lifecycle

How Threat Intelligence is performed

Threat Intelligence team center role

Tool to support TI

Prerequisites



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

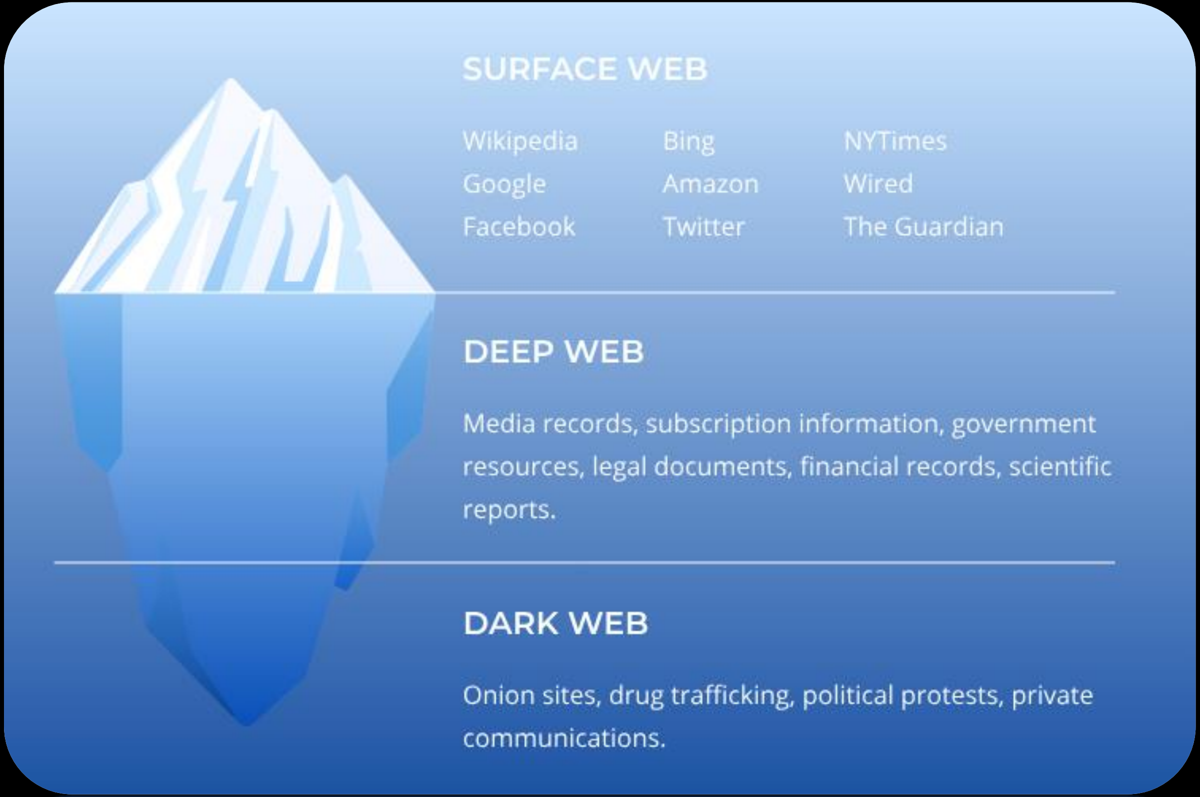
- Blue teams defend an organization from attacks and simulate incident response teams by following company policies and using existing resources

- Red teams simulate or actually conduct pentesting and threat hunting attacks to test the effectiveness of an organization’s security — sometimes including physical security, social engineering, and other non-IT-related methods

- Purple teams blend both roles as a mixed team or as a team that simply facilitates collaboration and communication between the blue and red teams

Surface Web vs Deep Web vs Dark Web

Importance of Understanding the Differences Between Surface Web vs Deep Web vs Dark Web



SURFACE WEB

Wikipedia
Google
Facebook

Bing
Amazon
Twitter

NYTimes
Wired
The Guardian

DEEP WEB

Media records, subscription information, government resources, legal documents, financial records, scientific reports.

DARK WEB

Onion sites, drug trafficking, political protests, private communications.

5%

90%

5%

Data Leak vs Data Breach

Data Leak is when sensitive data is **unknowingly exposed to the public**

Data Breach is an event caused by a cyberattack

Indicators of Compromise (IoCs)

Indicators of compromise (IoCs) are the clues, artifact, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization’s infrastructure.

IoCs are not intelligence, although they do act as a good source of information regarding the threats that serve as data points in the intelligence process.

Security professionals need to perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats.

Categories of indicators of Compromise (IoCs)

Email Indicators

Are used to send malicious data to target organization or individual.

Examples include the sender’s email address, email subject, and attachments or link.

Network Indicators

Are useful for command and control, malware, malware delivery, identifying the operating system, and other task.

Examples include URLs, domain names, and IP addresses.

Host-Based Indicators

Are found by performing an analysis of the infected system within the organizational network.

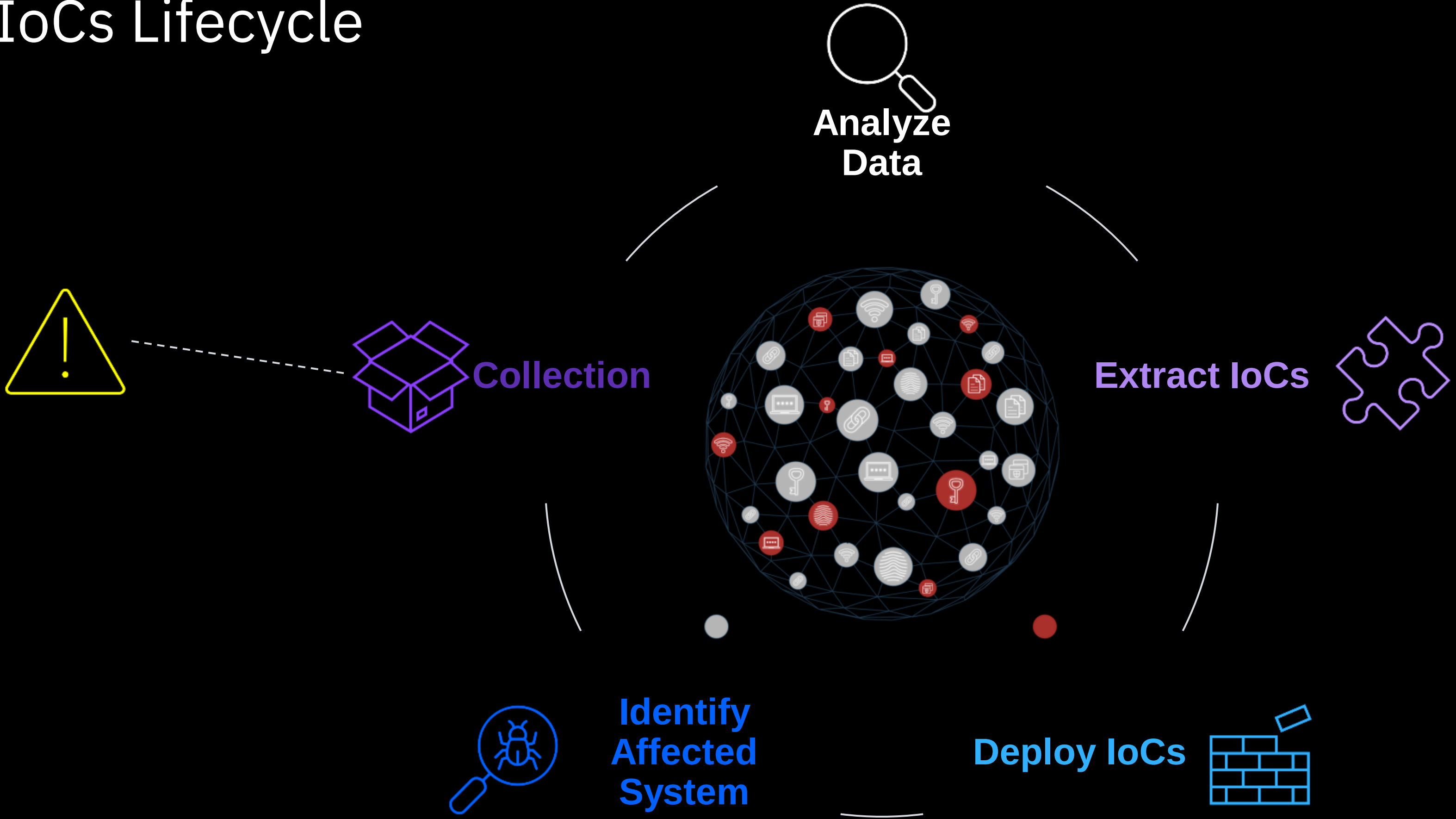
Examples include filenames, file hashes, registry keys, DLLs, and mutex.

Behavioral Indicators

Are used to identify specific behavior related to malicious activities.

Examples of behavioral indicators include document executing PowerShell script, and remote command execution.

IoCs Lifecycle



Analyze Data

Extract IoCs

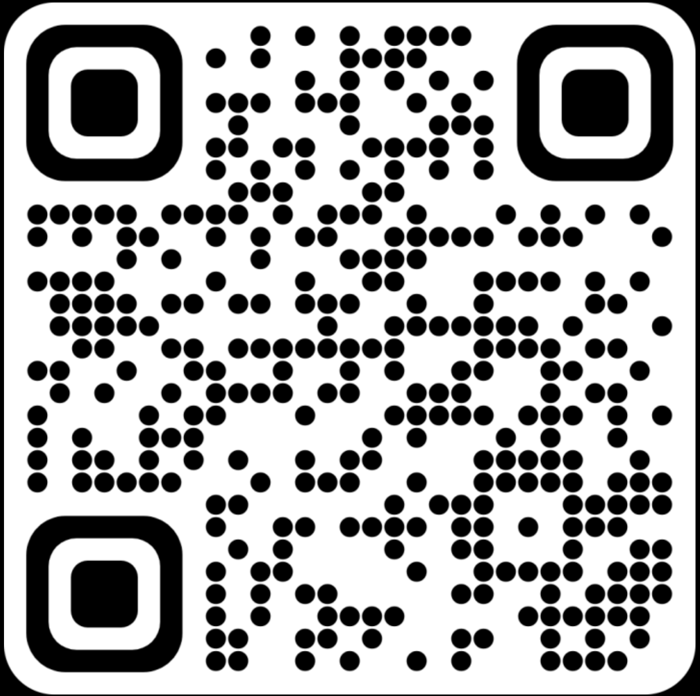
Deploy IoCs

Identify Affected System

Collection

Try It

VIRUSTOTAL



What is cyber threat intelligence?

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject’s response to that menace or hazard.”

Gartner

Information gathering in cyber threat intelligence

One of the main activities of cyber threat intelligence is represented by the **collection** and analysis of data and information, which can typically take place at the OSINT level but also at the CLOSINT level.

- **OSINT**, acronym for Open Source Intelligence, refers to the process of collecting information from open sources and in the public domain, after screening for reliability and reliability;

- **CLOSINT**, an acronym for Close Source Intelligence, refers to the process of gathering information from closed sources, not accessible to the public.

Types of Threat Intelligence Gathering: HUMINT

Human Intelligence (HUMINT) is one of the many disciplines of information-gathering, one of the oldest ones. It relies on people, so it requires almost no technological product. The collection of information can be in the form of questioning people, but also in the form of espionage.

Types of Threat Intelligence Gathering: GEOINT / IMINT

Geospatial Intelligence (GEOINT) and Imagery Intelligence (IMINT), help you keep track of any satellite system’s activity, and check for vulnerabilities as well.

GEOINT is the type of information-gathering discipline that evaluates geospatial information related to activities happening on the earth. Sources like satellites, maps, signals, and even IMINT sources help you get GEOINT information.

Types of Threat Intelligence Gathering: MASINT

Measurement and Signature Intelligence (MASINT) is a discipline more focused on industrial activities. It is information gathered from sensors that record signatures of set targets.

Different electro-optical sources, radars, acoustic sensors, and similar, are examples of how MASINT can be collected. MASINT also leverages data used from IMINT and SIGINT as well.

The collected information using MASINT describes characteristics of events like nuclear explosions. It also finds obscure features of weapon systems. As you can understand, military services are the ones that leverage this type of information-gathering discipline more than other services.

Types of Threat Intelligence Gathering: SOCMINT

Social Media Intelligence (SOCMINT) is information gathered from different social networking sites. This discipline falls under OSINT because it is mainly open-source information.

SOCMINT is very helpful for getting information about a company, its employees, potential partners, and being on track with their activities. Not just that, organizations can also track discussions that threat actors do about them, and be aware in case any of these discussions intends reputational damage.

Possible sources where you can gather SOCMINT information are all social networking sites that most of us use every day.

Types of Threat Intelligence Gathering: COMINT

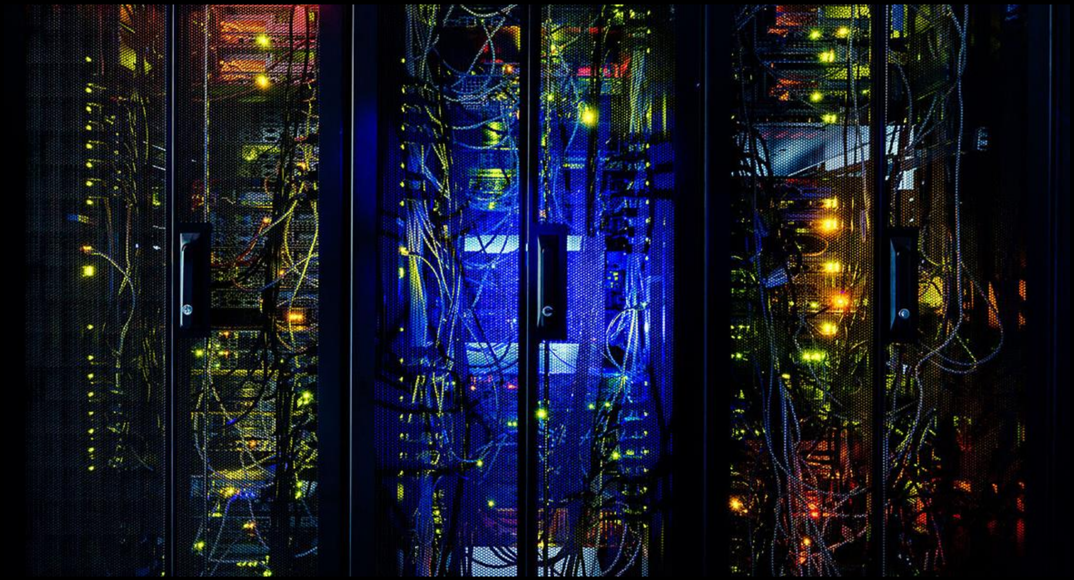
Communication Intelligence (COMINT), is used to obtain information regarding the sender, receiver, location, time, duration, and similar other data from an interception of foreign communication. Airwaves, cable, fiber optics, and other mediums are examples of COMINT sources.

Types of Threat Intelligence Gathering

TECHINT

Technical Intelligence (TECHINT), helps you to obtain better knowledge regarding adversary technical capabilities. It gives you the option to develop technological advantage and effective countermeasures.

Adversary equipment is the main source for gathering TECHINT. And this is why this discipline is highly effective.
Other sources can be satellites, technical research papers, and even human contact. Since the information comes directly from the adversary, it is extremely useful to neutralize the adversary's technological advantages.



Types of Threat Intelligence Gathering

FININT

Financial Intelligence (FININT) helps organizations obtain information about the adversary’s monetary transactions.
Possible sources for gathering this kind of information are, of course, banks, SWIFT, and usually the Financial Intelligence Unit (FIU).
Information gathered from FININT helps your company predict the adversary’s intentions and know its financial sources.

Types of Threat Intelligence

Cyber security threat intelligence is often broken down into four subcategories:

Strategic

Intelligence explains threats for a non-technical audience

Tactical

Intelligence describes threat conditions for technical audience

Technical

Intelligence focuses on specific threat techniques

Operational

Intelligence details hacker information and intent

Types of Threat Intelligence

Strategic

It aims to identify potential cyber attacks and their consequences in order to communicate them to a non-technical public, as in the case of decision makers who do not have in-depth skills in the field of cybersecurity, nor do they actually deal with these tasks in the company but are decisive in allocating the necessary funds so that the security activities are carried out in the best way.

Types of Threat Intelligence

Tactical

The focus of the tactical component lies in detecting the behaviors, techniques and procedures that cybercriminals adopt to shape their deadly threats. The target audience in this case is made up of those who operate at the forefront of IT security, with specific technical skills, to protect systems and data from IT attacks.

Types of Threat Intelligence

Technical

The technical approach of threat intelligence focuses above all on the possible indicators of a cyber attack, with particular attention to what are called social engineering attacks, which aim to exploit the ignorance and carelessness of employees to obtain confidential information and data sensitive, such as login credentials for financial services, as well as proceeding with actual identity theft. A classic example is all the activity that revolves around phishing and all its sub-variants.

Types of Threat Intelligence

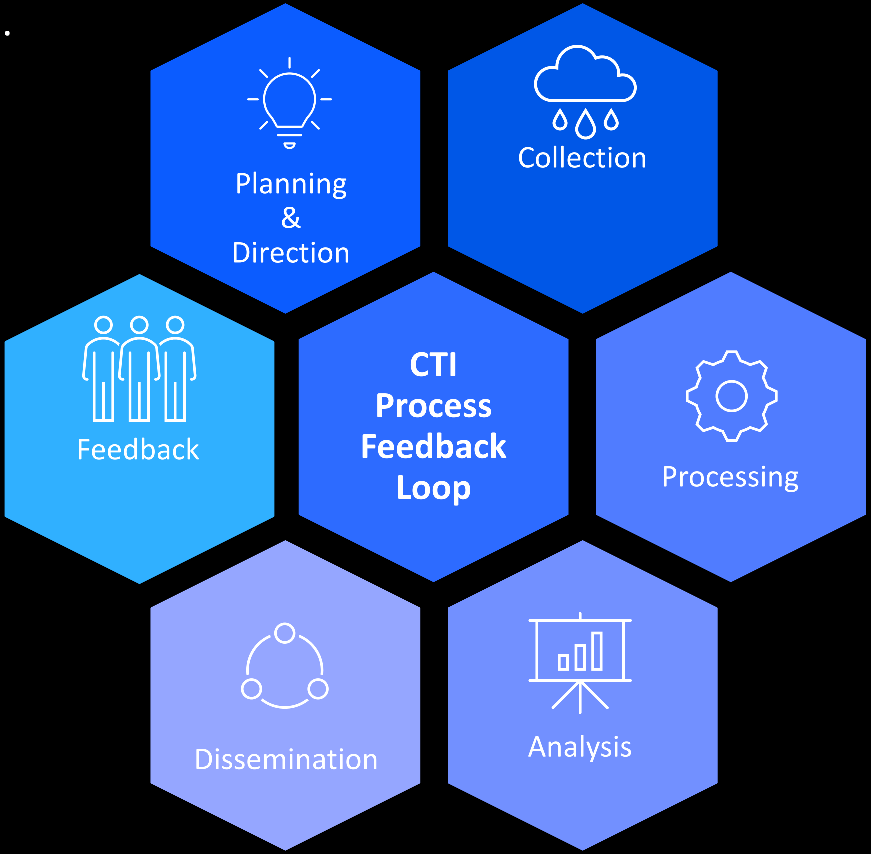
Operational

Another type of threat intelligence derives from a distinctly operational approach, capable of making extensive use of data science. First of all, it is essential to acquire data from a wide variety of sources.

The Threat Intelligence Lifecycle

The importance of threat intelligence in today’s world can hardly be overlooked. The following are the phases of the threat intelligence lifecycle.

1. Planning & Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback



The Threat Intelligence Lifecycle

1. Planning & Direction

This phase focuses on setting goals for the threat intelligence program. This includes:

- Understand which aspects of the organization need to be protected and possibly prioritize them.
- Identify what type of threat intelligence the organization needs to protect its assets and respond to threats.
- Understand the impact of a data breach on your organization.

The Threat Intelligence Lifecycle

2. Collection

This phase concerns the aggregation of data to support the objectives and goals set in Phase 1. Data quantity and quality are both crucial to avoiding not catching serious threatening events or being misled by false positives. At this stage, organizations need to identify their data sources, which includes:

- Metadata from internal networks and security devices
- Threats to data feeds from credible cybersecurity organizations
- Talks with updated stakeholders
- New open source sites and blogs

The Threat Intelligence Lifecycle

3. Processing

All collected data needs to be converted into a format that the organization can use. Different methods of data collection require different processing tools. For example, data from interviews with people may need to be verified and cross-referenced with other data.

The Threat Intelligence Lifecycle

4. Analysis

Once the analysis operations have been completed, the key recommendations and conclusions must be disseminated among the main stakeholders within the company. Within the company, different teams will have different needs. For effective distribution, it is important to understand what kind of intelligence different audiences need, in what format and how often.

The Threat Intelligence Lifecycle

5. Dissemination

Once the analysis operations have been completed, the key recommendations and conclusions must be disseminated among the main stakeholders within the company. Within the company, different teams will have different needs. For effective distribution, it is important to understand what kind of intelligence different audiences need, in what format and how often.

The Threat Intelligence Lifecycle

6. Feedback

Feedback from stakeholders will help improve the threat intelligence program and ensure that it reflects the demands and goals of each group.

The term "life cycle" emphasizes that threat intelligence is not a linear and univocal process. On the contrary, it is a circular and repetitive process that organizations use for constant improvement.

Benefits of Cyber Threat Intelligence

Correctly applied, threat intelligence provides you the chance to proactively allay your most unrelenting threats, instead of just responding to attacks or a stream of incoming alerts. This occurs by comprehending your cyber risk and raising effectiveness and confidence in your security processes.

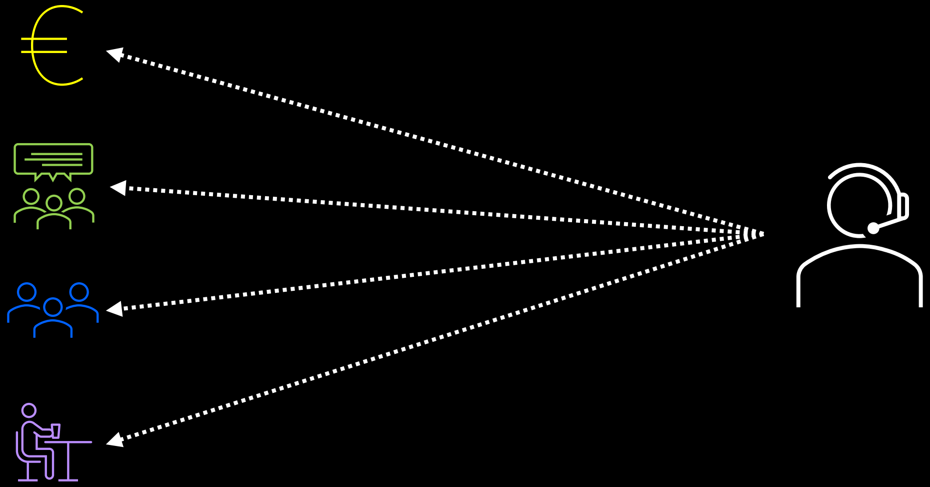
Here are some key benefits of threat intelligence:

1. Comprehending Your Cyber Risk
2. Performing Efficient Security Operations
3. Other Important Benefits:

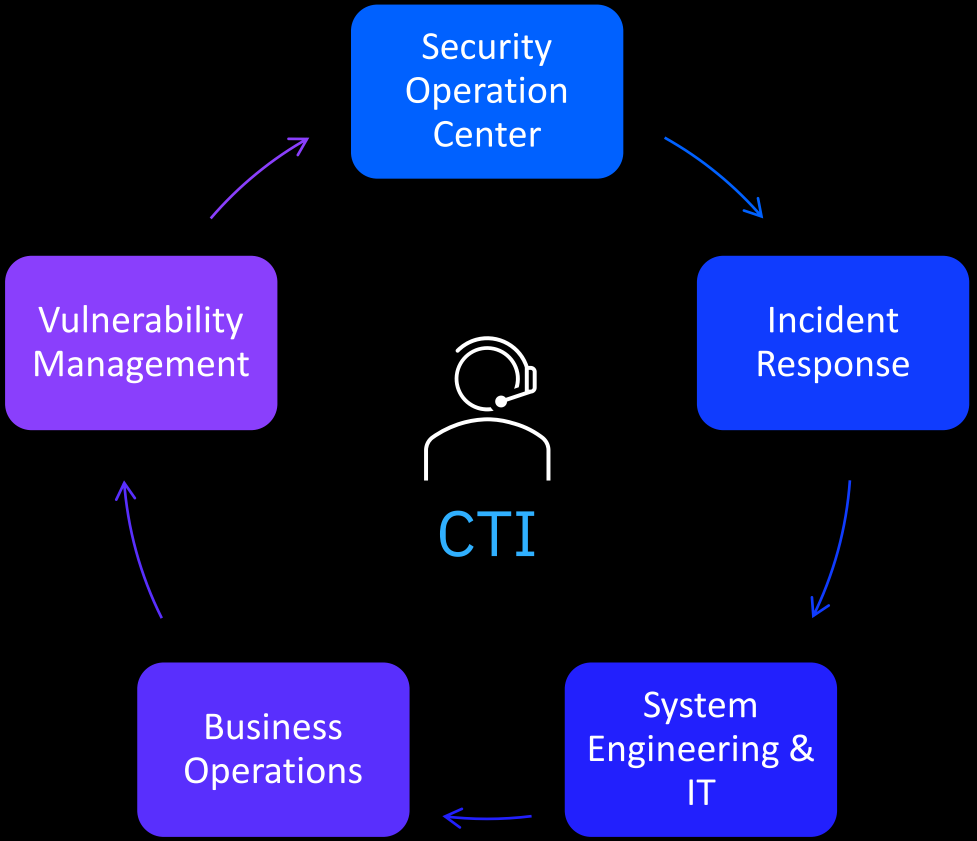
- Identify leaked credentials.
- Prioritize vulnerability remediation.
- Monitor for mentions of your brand online.
- Uncover emerging threats.
- Track hacktivist activity in your industry.
- Study threat actor tactics, techniques, and procedures (TTPs).

How TI is performed

- Commercial Tools
- Open-Source Tools
- Community Platforms
- Human Analysis



CTI team center role



Security Operation Center

Incident Response

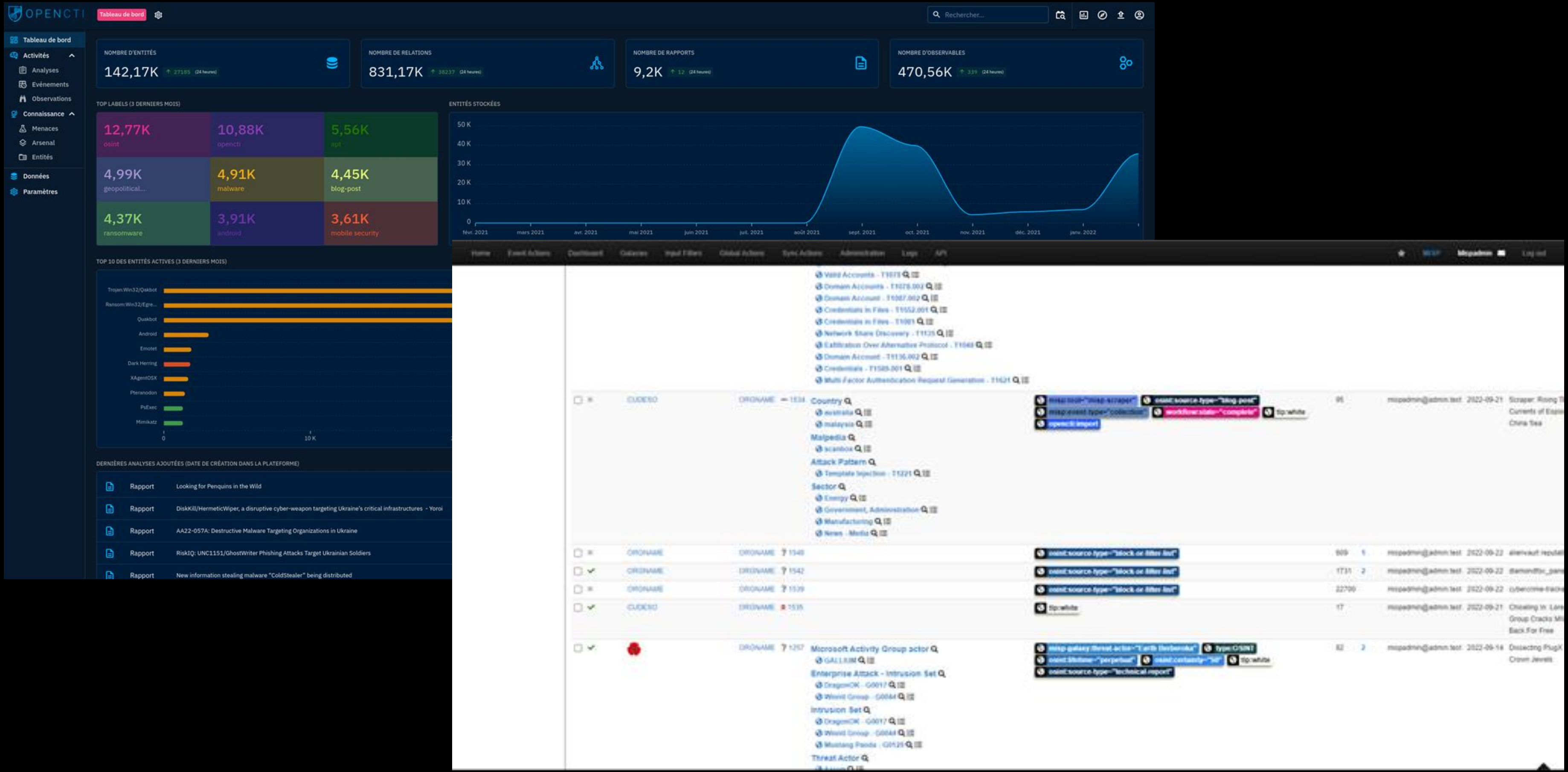
System Engineering & IT

Business Operations

Vulnerability Management

CTI

Tool to support Threat Intelligence - TIP



NOMBRE D'ENTITÉS 142,17K ↑ 27185 (24 heures)

NOMBRE DE RELATIONS 831,17K ↑ 38237 (24 heures)

NOMBRE DE RAPPORTS 9,2K ↑ 12 (24 heures)

NOMBRE D'OBSERVABLES 470,56K ↑ 339 (24 heures)

TOP LABELS (3 DERNIERS MOIS)

12,77K osint	10,88K opencti	5,56K apt
4,99K geopolitical...	4,91K malware	4,45K blog-post
4,37K ransomware	3,91K android	3,61K mobile security

ENTITÉS STOCKÉES

TOP 10 DES ENTITÉS ACTIVES (3 DERNIERS MOIS)

DERNIÈRES ANALYSES AJOUTÉES (DATE DE CRÉATION DANS LA PLATEFORME)

Rapport	Looking for Penquins in the Wild
Rapport	DiskKill/HermeticWiper, a disruptive cyber-weapon targeting Ukraine's critical infrastructures - Yoroi
Rapport	AA22-057A: Destructive Malware Targeting Organizations in Ukraine
Rapport	RiskIQ: UNC1151/GhostWriter Phishing Attacks Target Ukrainian Soldiers
Rapport	New information stealing malware "ColdStealer" being distributed

Valid Accounts - T1078
Domain Accounts - T1078.002
Domain Account - T1087.002
Credentials in Files - T1552.001
Credentials in Files - T1081
Network Share Discovery - T1135
Exfiltration Over Alternative Protocol - T1048
Domain Account - T1136.002
Credentials - T1589.001
Multi-Factor Authentication Request Generation - T1621

Country
australia
malaysia
Malpedia
scanbox
Attack Pattern
Template Injection - T1221
Sector
Energy
Government, Administration
Manufacturing
News - Media

misp:tool="misp-scraper" osint:source-type="blog-post" misp:event-type="collection" workflow:state="complete" tlp:white opencti:import

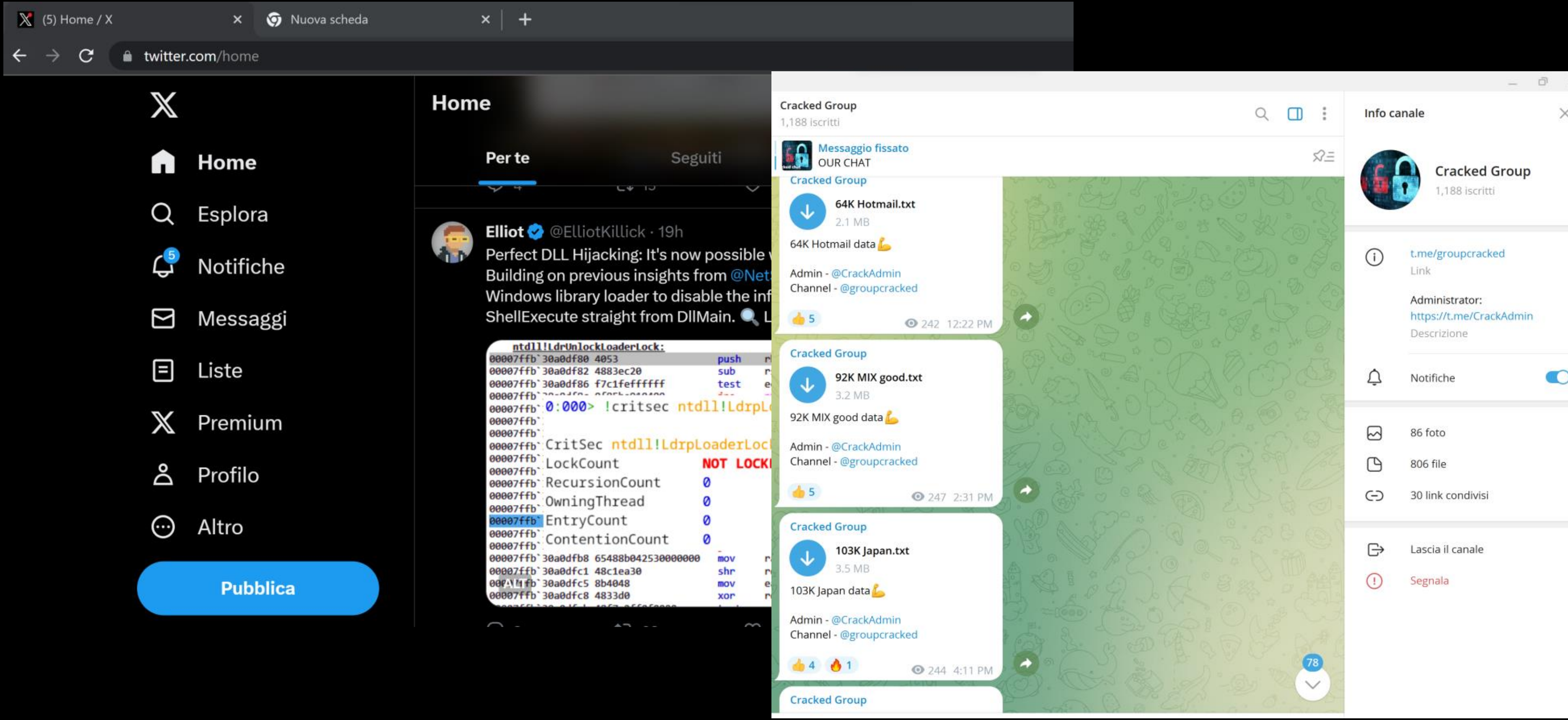
osint:source-type="block-or-filter-list"

tlp:white

Microsoft Activity Group actor
Enterprise Attack - Intrusion Set
Intrusion Set
Threat Actor

osint:lifetime="perpetual" osint:source-type="technical-report" tlp:white

Tool to support Threat Intelligence - SOCMINT



Elliot @ElliotKillick · 19h

Perfect DLL Hijacking: It's now possible
Building on previous insights from @Net
Windows library loader to disable the inf
ShellExecute straight from DllMain. 🔍 L

```
    ntdll!LdrUnlockLoaderLock:
00007ffb`30a0df80 4053                  push    r
00007ffb`30a0df82 4883ec20              sub     r
00007ffb`30a0df86 f7c1feffffff          test    e
00007ffb` 0:000> !critsec ntdll!LdrpL
00007ffb`
00007ffb`
00007ffb` CritSec ntdll!LdrpLoaderLoc
00007ffb` LockCount          NOT LOCK
00007ffb`
00007ffb` RecursionCount     0
00007ffb` OwningThread       0
00007ffb`
00007ffb` EntryCount         0
00007ffb` ContentionCount    0
00007ffb`
00007ffb`30a0dfb8 65488b042530000000    mov     r
00007ffb`30a0dfc1 48c1ea30              shr     r
00007ffb`30a0dfc5 8b4048                mov     e
00007ffb`30a0dfc8 4833d0                xor     r
```

Cracked Group
1,188 iscritti

Messaggio fissato
OUR CHAT

Cracked Group
64K Hotmail.txt
2.1 MB
64K Hotmail data💪

Admin - @CrackAdmin
Channel - @groupcracked

👍 5 242 12:22 PM

Cracked Group
92K MIX good.txt
3.2 MB
92K MIX good data💪

Admin - @CrackAdmin
Channel - @groupcracked

👍 5 247 2:31 PM

Cracked Group
103K Japan.txt
3.5 MB
103K Japan data💪

Admin - @CrackAdmin
Channel - @groupcracked

👍 4 🔥 1 244 4:11 PM

Cracked Group

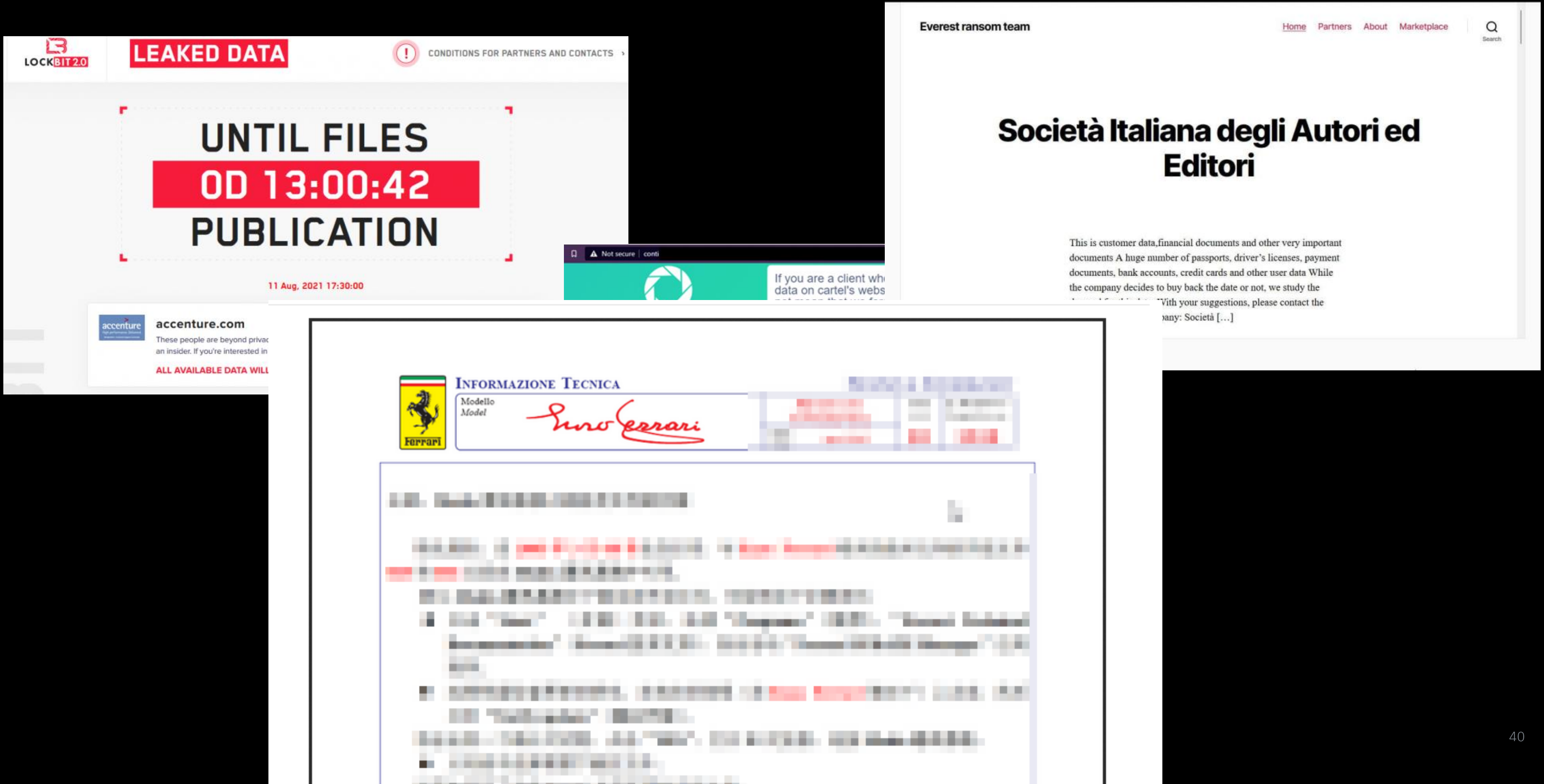
Info canale

Cracked Group
1,188 iscritti

t.me/groupcracked
Link

Administrator:
https://t.me/CrackAdmin
Descrizione

Tool to support Threat Intelligence – Ransomware Monitor



UNTIL FILES
0D 13:00:42
PUBLICATION

11 Aug, 2021 17:30:00

accenture.com

These people are beyond privac
an insider. If you're interested in

ALL AVAILABLE DATA WILL

If you are a client wh
data on cartel's webs

Società Italiana degli Autori ed Editori

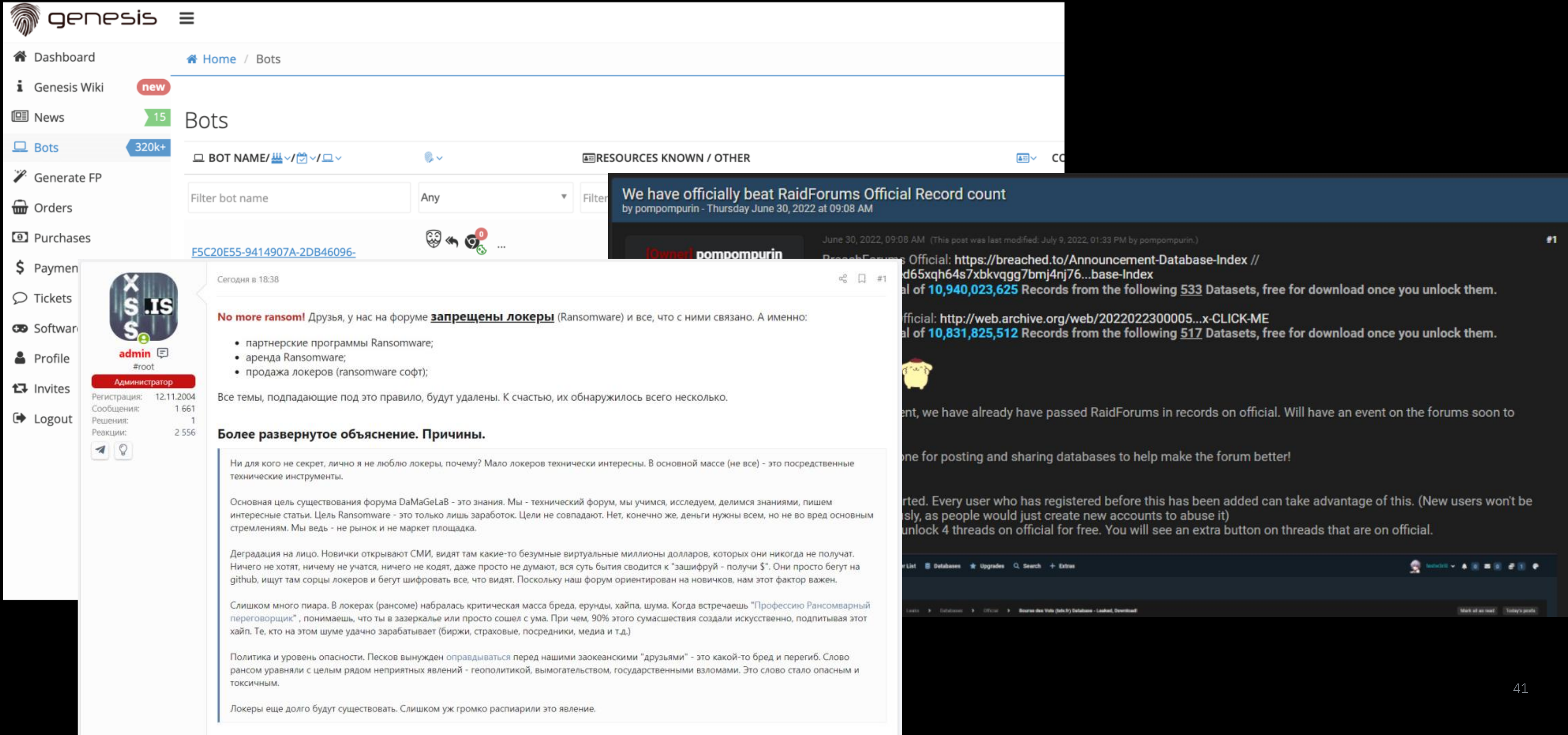
This is customer data,financial documents and other very important documents A huge number of passports, driver's licenses, payment documents, bank accounts, credit cards and other user data While the company decides to buy back the date or not, we study the
…With your suggestions, please contact the
…pany: Società […]

INFORMAZIONE TECNICA

Modello
Model

Enzo Ferrari

Tool to support Threat Intelligence – Dark Market



admin
#root
Администратор

Регистрация:	12.11.2004
Сообщения:	1 661
Решения:	1
Реакции:	2 556

Сегодня в 18:38 #1

No more ransom! Друзья, у нас на форуме **запрещены локеры** (Ransomware) и все, что с ними связано. А именно:

- партнерские программы Ransomware;
- аренда Ransomware;
- продажа локеров (ransomware софт);

Все темы, подпадающие под это правило, будут удалены. К счастью, их обнаружилось всего несколько.

Более развернутое объяснение. Причины.

> Ни для кого не секрет, лично я не люблю локеры, почему? Мало локеров технически интересны. В основной массе (не все) - это посредственные технические инструменты.
>
> Основная цель существования форума DaMaGeLaB - это знания. Мы - технический форум, мы учимся, исследуем, делимся знаниями, пишем интересные статьи. Цель Ransomware - это только лишь заработок. Цели не совпадают. Нет, конечно же, деньги нужны всем, но не во вред основным стремлениям. Мы ведь - не рынок и не маркет площадка.
>
> Деградация на лицо. Новички открывают СМИ, видят там какие-то безумные виртуальные миллионы долларов, которых они никогда не получат. Ничего не хотят, ничему не учатся, ничего не кодят, даже просто не думают, вся суть бытия сводится к "зашифруй - получи $". Они просто бегут на github, ищут там сорцы локеров и бегут шифровать все, что видят. Поскольку наш форум ориентирован на новичков, нам этот фактор важен.
>
> Слишком много пиара. В локерах (рансоме) набралась критическая масса бреда, ерунды, хайпа, шума. Когда встречаешь "Профессию Рансомварный переговорщик" , понимаешь, что ты в зазеркалье или просто сошел с ума. При чем, 90% этого сумасшествия создали искусственно, подпитывая этот хайп. Те, кто на этом шуме удачно зарабатывает (биржи, страховые, посредники, медиа и т.д.)
>
> Политика и уровень опасности. Песков вынужден оправдываться перед нашими заокеанскими "друзьями" - это какой-то бред и перегиб. Слово рансом уравняли с целым рядом неприятных явлений - геополитикой, вымогательством, государственными взломами. Это слово стало опасным и токсичным.
>
> Локеры еще долго будут существовать. Слишком уж громко распиарили это явление.

We have officially beat RaidForums Official Record count
by pompompurin - Thursday June 30, 2022 at 09:08 AM

[Owner] pompompurin

June 30, 2022, 09:08 AM (This post was last modified: July 9, 2022, 01:33 PM by pompompurin.) #1

BreachForums Official: https://breached.to/Announcement-Database-Index //
d65xqh64s7xbkvqgg7bmj4nj76...base-Index
al of 10,940,023,625 Records from the following 533 Datasets, free for download once you unlock them.

fficial: http://web.archive.org/web/2022022300005...x-CLICK-ME
al of 10,831,825,512 Records from the following 517 Datasets, free for download once you unlock them.

ent, we have already have passed RaidForums in records on official. Will have an event on the forums soon to

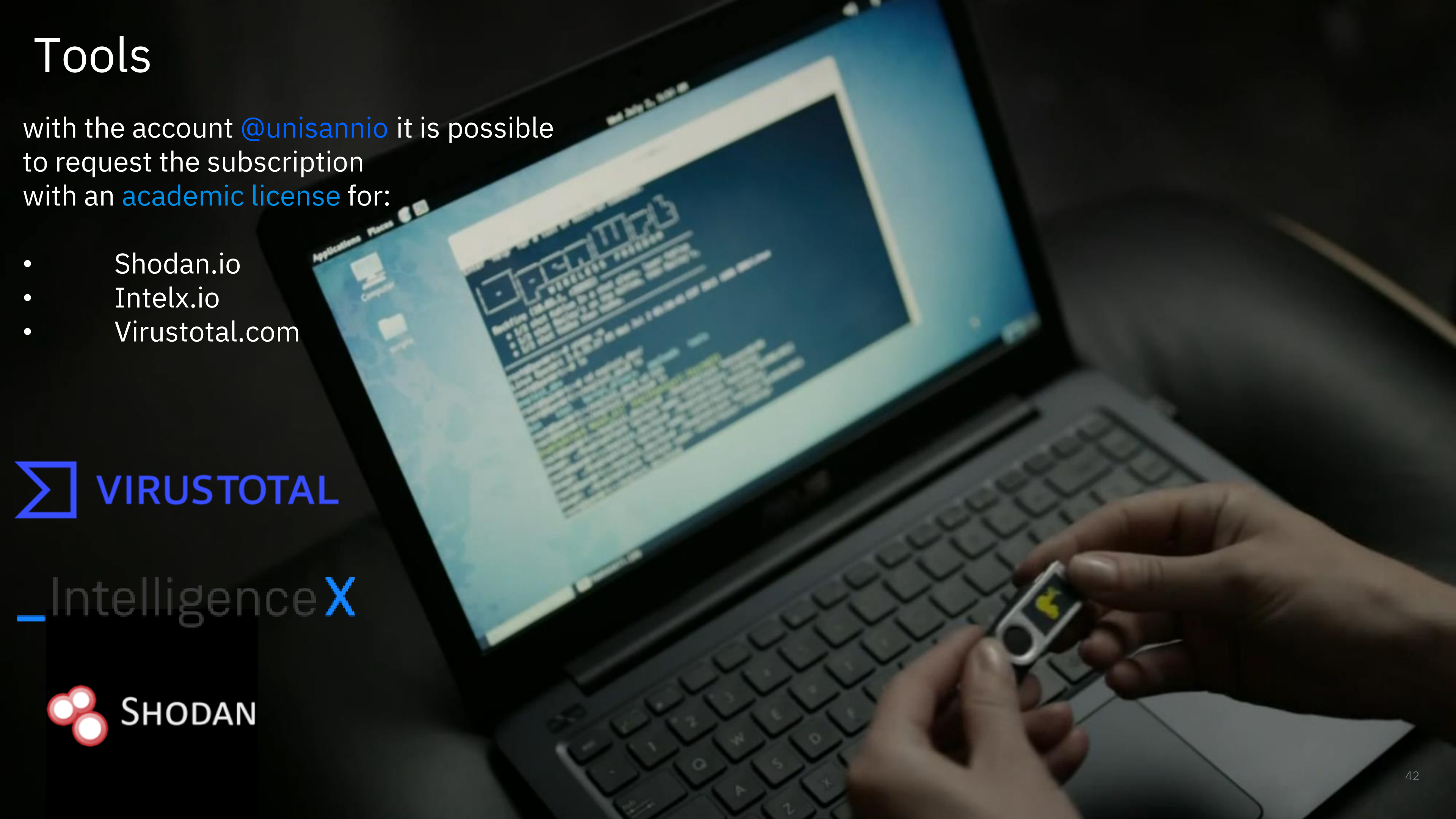
one for posting and sharing databases to help make the forum better!

rted. Every user who has registered before this has been added can take advantage of this. (New users won't be
sly, as people would just create new accounts to abuse it)
unlock 4 threads on official for free. You will see an extra button on threads that are on official.

Tools

with the account @unisannio it is possible to request the subscription with an academic license for:

- Shodan.io
- Intelx.io
- Virustotal.com



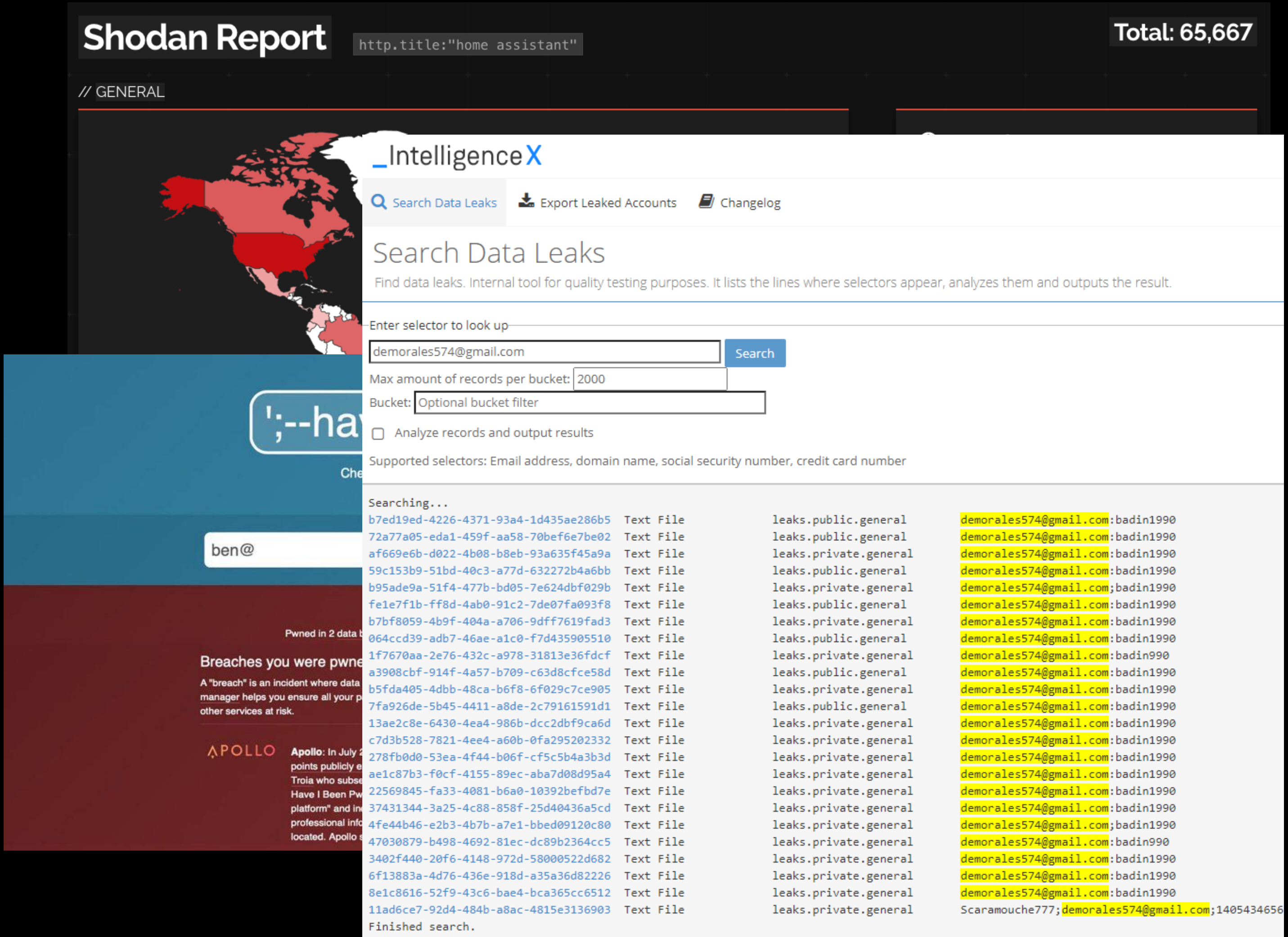
VIRUSTOTAL

_IntelligenceX

SHODAN

Try It

- Shodan
- Haveibeenpwned
- IntelX



_IntelligenceX

Search Data Leaks · Export Leaked Accounts · Changelog

Search Data Leaks

Find data leaks. Internal tool for quality testing purposes. It lists the lines where selectors appear, analyzes them and outputs the result.

Enter selector to look up: demorales574@gmail.com [Search]

Max amount of records per bucket: 2000

Bucket: Optional bucket filter

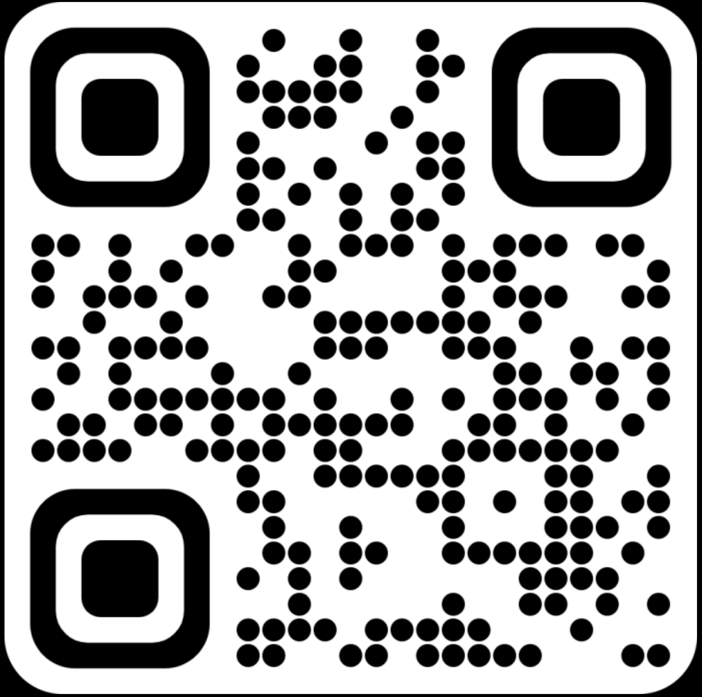
☐ Analyze records and output results

Supported selectors: Email address, domain name, social security number, credit card number

```
Searching...
b7ed19ed-4226-4371-93a4-1d435ae286b5  Text File         leaks.public.general      demorales574@gmail.com:badin1990
72a77a05-eda1-459f-aa58-70bef6e7be02  Text File         leaks.public.general      demorales574@gmail.com:badin1990
af669e6b-d022-4b08-b8eb-93a635f45a9a  Text File         leaks.private.general     demorales574@gmail.com:badin1990
59c153b9-51bd-40c3-a77d-632272b4a6bb  Text File         leaks.public.general      demorales574@gmail.com:badin1990
b95ade9a-51f4-477b-bd05-7e624dbf029b  Text File         leaks.private.general     demorales574@gmail.com;badin1990
fe1e7f1b-ff8d-4ab0-91c2-7de07fa093f8  Text File         leaks.public.general      demorales574@gmail.com:badin1990
b7bf8059-4b9f-404a-a706-9dff7619fad3  Text File         leaks.private.general     demorales574@gmail.com:badin1990
064ccd39-adb7-46ae-a1c0-f7d435905510  Text File         leaks.public.general      demorales574@gmail.com:badin1990
1f7670aa-2e76-432c-a978-31813e36fdcf  Text File         leaks.private.general     demorales574@gmail.com:badin990
a3908cbf-914f-4a57-b709-c63d8cfce58d  Text File         leaks.public.general      demorales574@gmail.com:badin1990
b5fda405-4dbb-48ca-b6f8-6f029c7ce905  Text File         leaks.private.general     demorales574@gmail.com:badin1990
7fa926de-5b45-4411-a8de-2c79161591d1  Text File         leaks.public.general      demorales574@gmail.com:badin1990
13ae2c8e-6430-4ea4-986b-dcc2dbf9ca6d  Text File         leaks.private.general     demorales574@gmail.com:badin1990
c7d3b528-7821-4ee4-a60b-0fa295202332  Text File         leaks.private.general     demorales574@gmail.com:badin1990
278fb0d0-53ea-4f44-b06f-cf5c5b4a3b3d  Text File         leaks.private.general     demorales574@gmail.com:badin1990
ae1c87b3-f0cf-4155-89ec-aba7d08d95a4  Text File         leaks.private.general     demorales574@gmail.com:badin1990
22569845-fa33-4081-b6a0-10392befbd7e  Text File         leaks.private.general     demorales574@gmail.com:badin1990
37431344-3a25-4c88-858f-25d40436a5cd  Text File         leaks.private.general     demorales574@gmail.com:badin1990
4fe44b46-e2b3-4b7b-a7e1-bbed09120c80  Text File         leaks.private.general     demorales574@gmail.com;badin1990
47030879-b498-4692-81ec-dc89b2364cc5  Text File         leaks.private.general     demorales574@gmail.com:badin990
3402f440-20f6-4148-972d-58000522d682  Text File         leaks.private.general     demorales574@gmail.com:badin1990
6f13883a-4d76-436e-918d-a35a36d82226  Text File         leaks.private.general     demorales574@gmail.com:badin1990
8e1c8616-52f9-43c6-bae4-bca365cc6512  Text File         leaks.private.general     demorales574@gmail.com:badin1990
11ad6ce7-92d4-484b-a8ac-4815e3136903  Text File         leaks.private.general     Scaramouche777;demorales574@gmail.com;1405434656
Finished search.
```

Try It

';--have i been pwned?

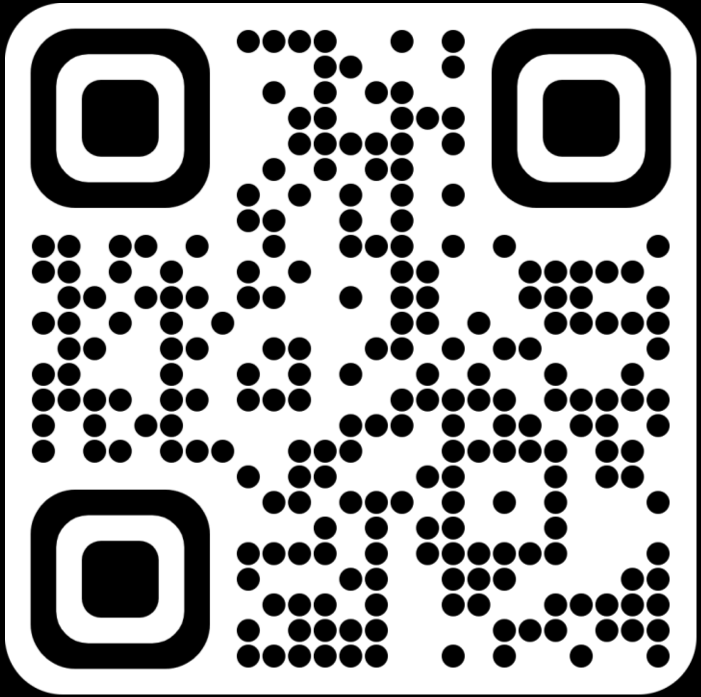


Try It

SHODAN

Try It

_IntelligenceX



Question and Answer

Thank You

UNIVERSITÀ DEGLI STUDI DEL SANNIO
Benevento

pimelillo@unisannio.it
pietro.melillo@redhotcyber.com
melillopietro@gmail.com

https://melillopietro.github.io/
https://janaralab.github.io/
https://www.linkedin.com/in/melillopietro/