Webinar, 28 gennaio 2021

FORENSICNEWS

STOPSECRET editore

OSINT
Open Source Intelligence

Paolo Dal Checco, *Consulente Informatico Forense*
www.dalchecco.it

FORENSIC VIRTUAL SUMMIT

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori su **Crittografia e Sicurezza Informatica**
- Piccole **docenze** a Contratto @UniTO, @UNIMI e @UNIGE
- **Consulente Informatico Forense** (Perizie Informatiche) per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Tra i fondatori dell'Associazione ONIF (www.onif.it)
- Socio IISFA, Tech & Law, Clusit, Lab4Int, AssobIT
- Informatica forense, digital forensics, cryptocurrency forensics, OSINT, perizia fonica, indagini digitali, etc…
- www.dalchecco.it, bitcoinforensics.it, ransomware.it
- paolo@dalchecco.it - @forensico

Definizione di OSINT

Definizione di OSINT

***ATP 2-22.9**

Army Techniques Publication
No. 2-22.9 (FMI 2-22.9)

Headquarters
Department of the Army
Washington, DC, 10 July 2012

Open-Source Intelligence

Contents

		Page
	PREFACE	iv
	INTRODUCTION	v
Chapter 1	OPEN-SOURCE INTELLIGENCE (OSINT) FUNDAMENTALS	1-1
	Definition and Terms	1-1
	Characteristics	1-1
	The Intelligence Warfighting Function	1-2

https://fas.org/irp/doddir/army/atp2-22-9.pdf

Definizione di OSINT

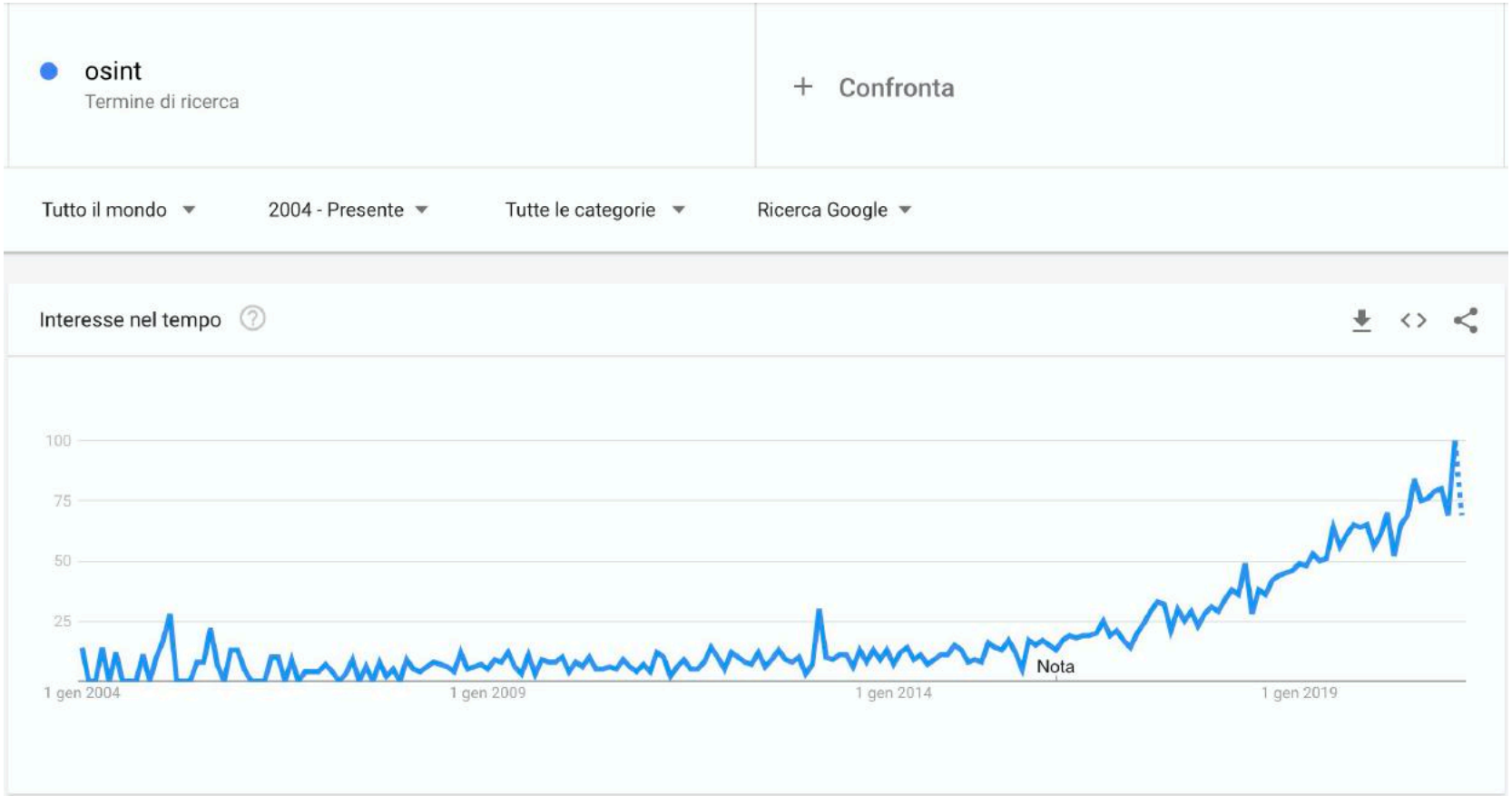
1-1. *Open-source intelligence* is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement (FM 2-0). OSINT also applies to the intelligence produced by that discipline.

- **Open source** is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure. Open-source information can be publicly available but not all publicly available information is open source. Open sources refer to publicly available information medium and are not limited to physical persons.
- **Publicly available information** is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

Utilizzi dell'OSINT

- Innumerevoli contesti e utilizzi:
  - Investigativo
  - Assicurativo
  - Due Diligence
  - Deanonimizzazione/Identificazione
  - VA/PT e Sicurezza Informatica
- Ambito di azione
  - Clear Web
  - Deep Web
  - Dark Web
  - Il resto delle informazioni (mondo reale – es. HUMINT)

Surface/Clear Web



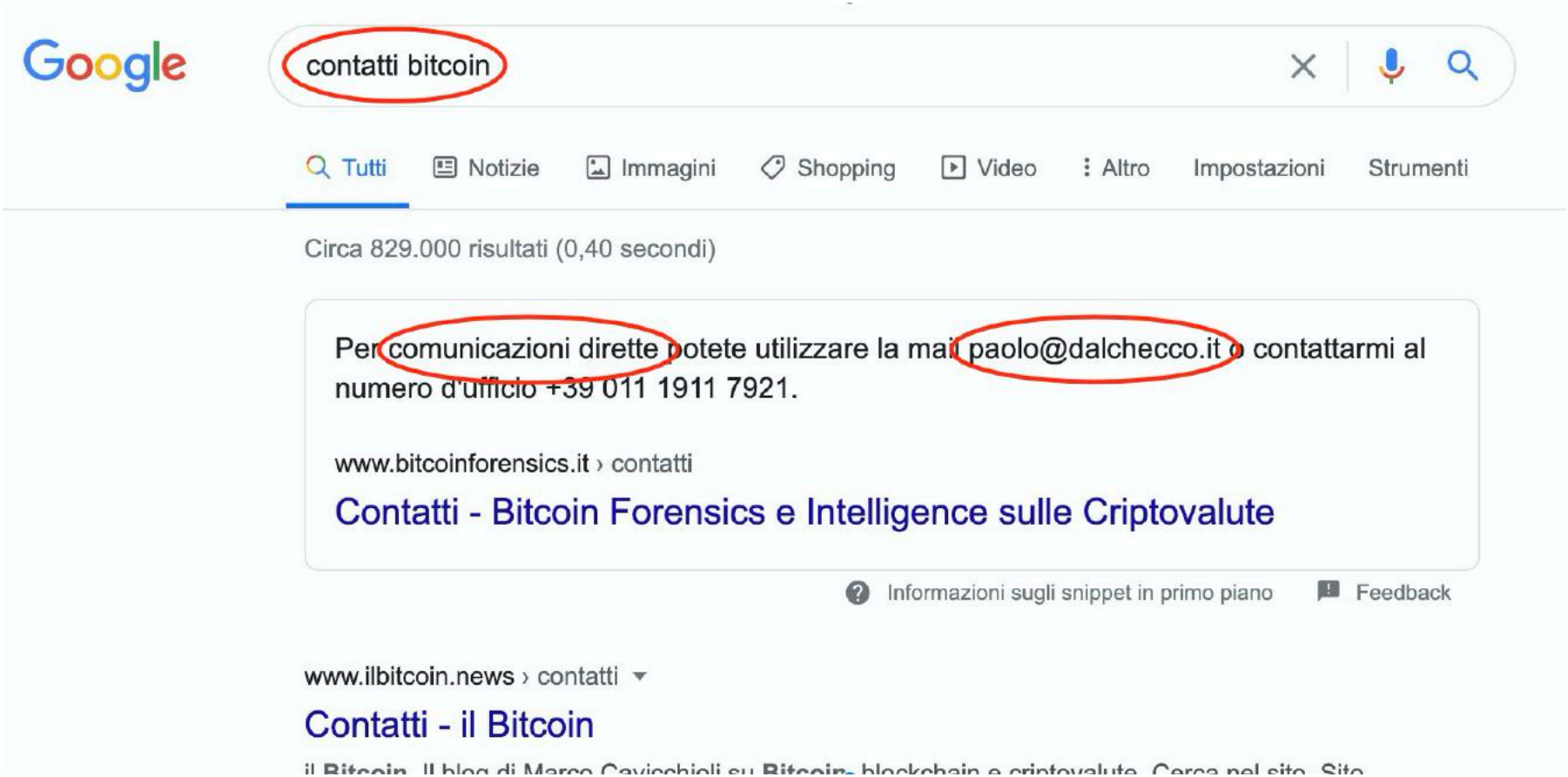
Deep Web

- Contenuto non linkato o indicizzato
- Aree web private (protette da password)
- Contenuto ad accesso limitato (captcha)
- Contenuto generato tramite scripting (javascript)
- Contenuto dinamico (generato tramite query, es. archivo La Stampa)
- Contenuto non in HTML (immagini raster o video)
- Pagine escluse tramite regole robots.txt
- Pagine accessibili tramite software (Tor, i2p, etc…) → **Dark Web**

Dark Web

- Tor (www.torproject.org)
- EEPsites – i2p (geti2p.net)
- Freenet (freenetproject.org)
- AnoNET (www.anonet.org)
- ZeroNET (zeronet.readthedocs.org/en/latest)

Quando l'OSINT porta fuori strada…



Esempi di OSINT

- Identificare chi si cela dietro un profilo di social network
- Identificare di chi è un sito web
- Rintracciare una persona
- Verificare chi è a capo di un'organizzazione
- Individuare il proprietario di una email o numero di telefono
- Datare pagine web
- Ricostruire legami tra persone o società

Information Gathering

Cyber Intelligence

Attiva	Passiva	Semi-passive Info Gathering
Proactive Intelligence (ingegneria sociale, attività sotto copertura, exploit, spyware etc.)	Open Source Intelligence, Intercettazioni, SIGINT, EMINT, ecc.	Modalitá attiva ma sotto la soglia di rilevamento
TRAFFICO ANORMALE	**NESSUN TRAFFICO**	**TRAFFICO NORMALE**

Information Gathering Attiva

- Tracing
- Port scanning
- Scansione delle applicazioni (i.e. robot.txt analisys, ecc.)
- Scansione delle risorse
- Rilevamente di configurazioni errate o predefinite
- Mappatura delle vulnerabilitá (XSS, SQL injection, no patch at all…)
- Ricerca di Exploit utilizzabili

Information Gathering Passiva

- Sniffing di rete
- Motori di ricerca
- Social Network
- Analisi email
- Analisi metadati
- Crawling
- Analisi collegamento tra siti/entità/profili

Alcuni strumenti

- Esistono centinaia di tool/siti/servizi
- Alcuni gratuiti, alcuni commerciali, open source, closed, etc…
- Difficile (o lungo/complicato) ormai fare OSINT senza fonti a pagamento

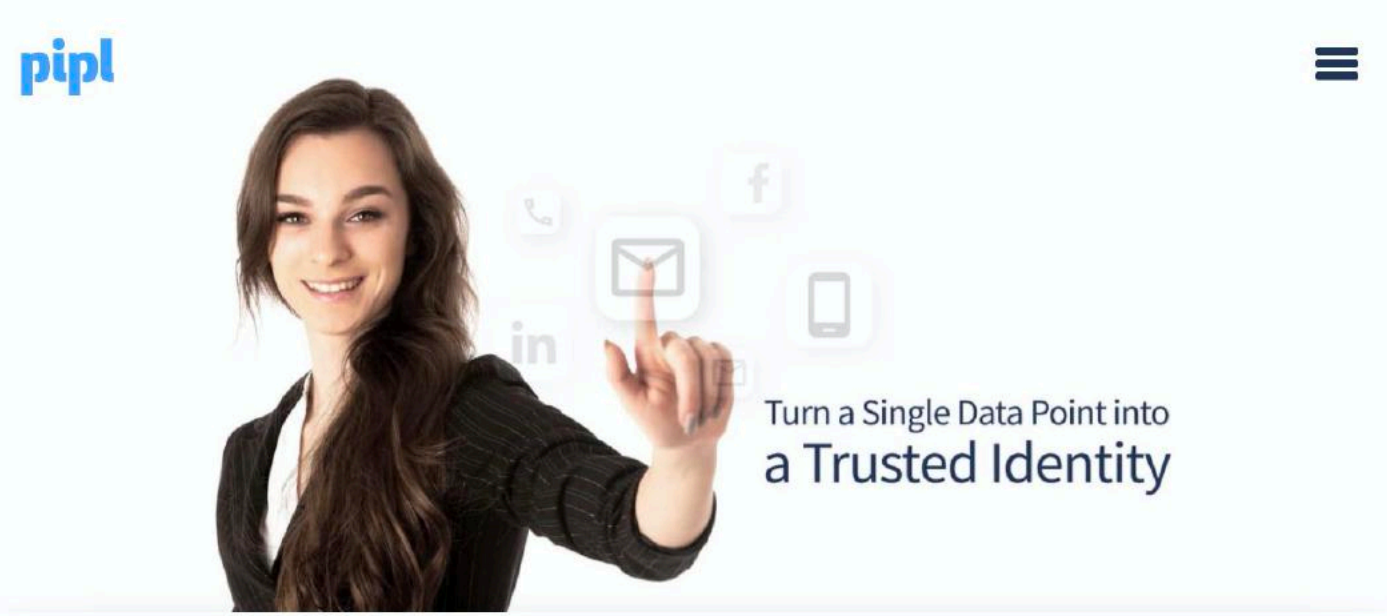
Google

Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

Shodan

https://github.com/JavierOlmedo/shodan-filters

Pipl

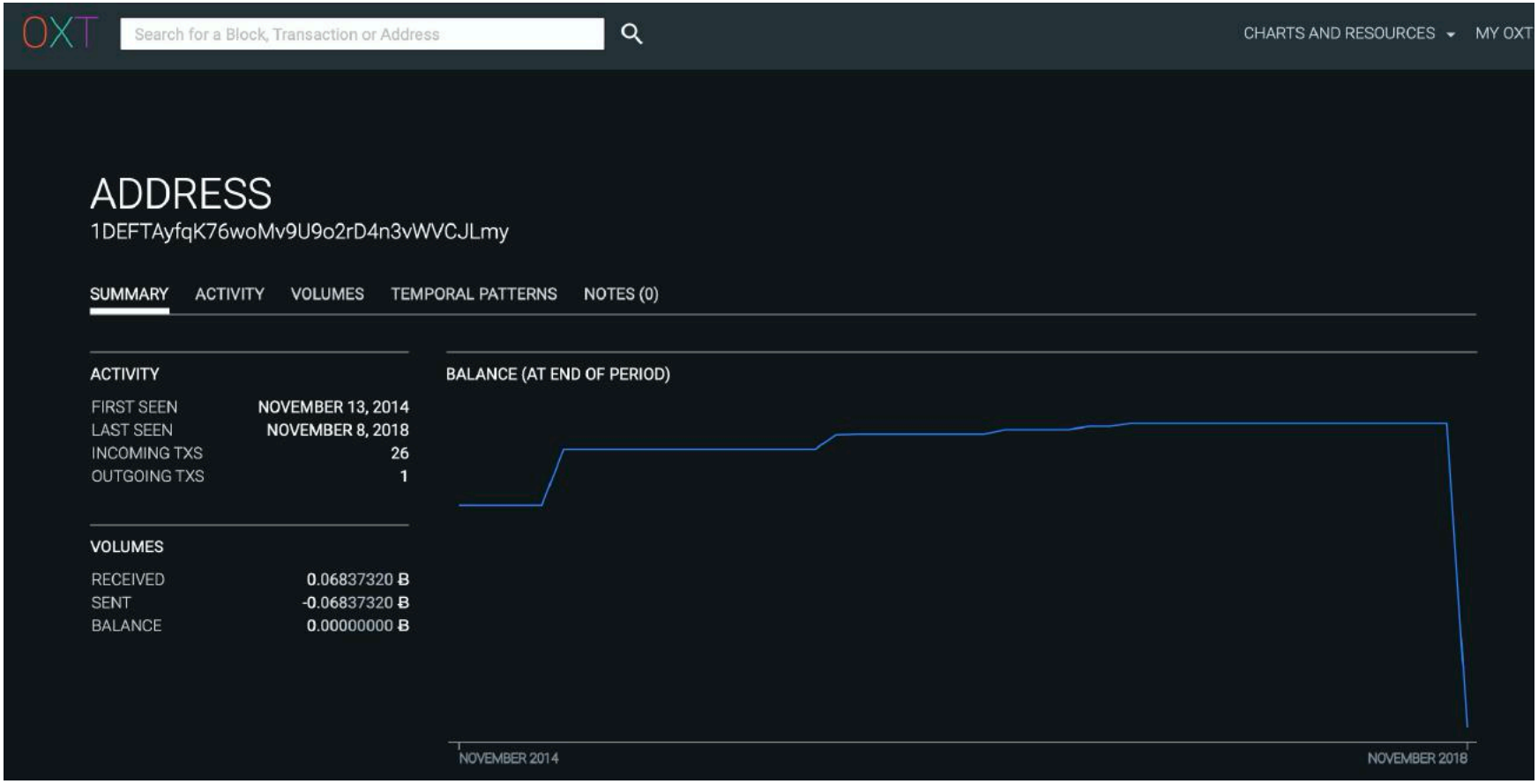

pipl
Turn a Single Data Point into
a Trusted Identity
Speed investigations and fight fraud with the world's leading provider of true identity verification information
Pipl's unique *identity resolution engine* connects the world's personal, professional and social identity data to give analysts and investigators an unmatched global index of over 3 billion trusted identity profiles.

Skopenow

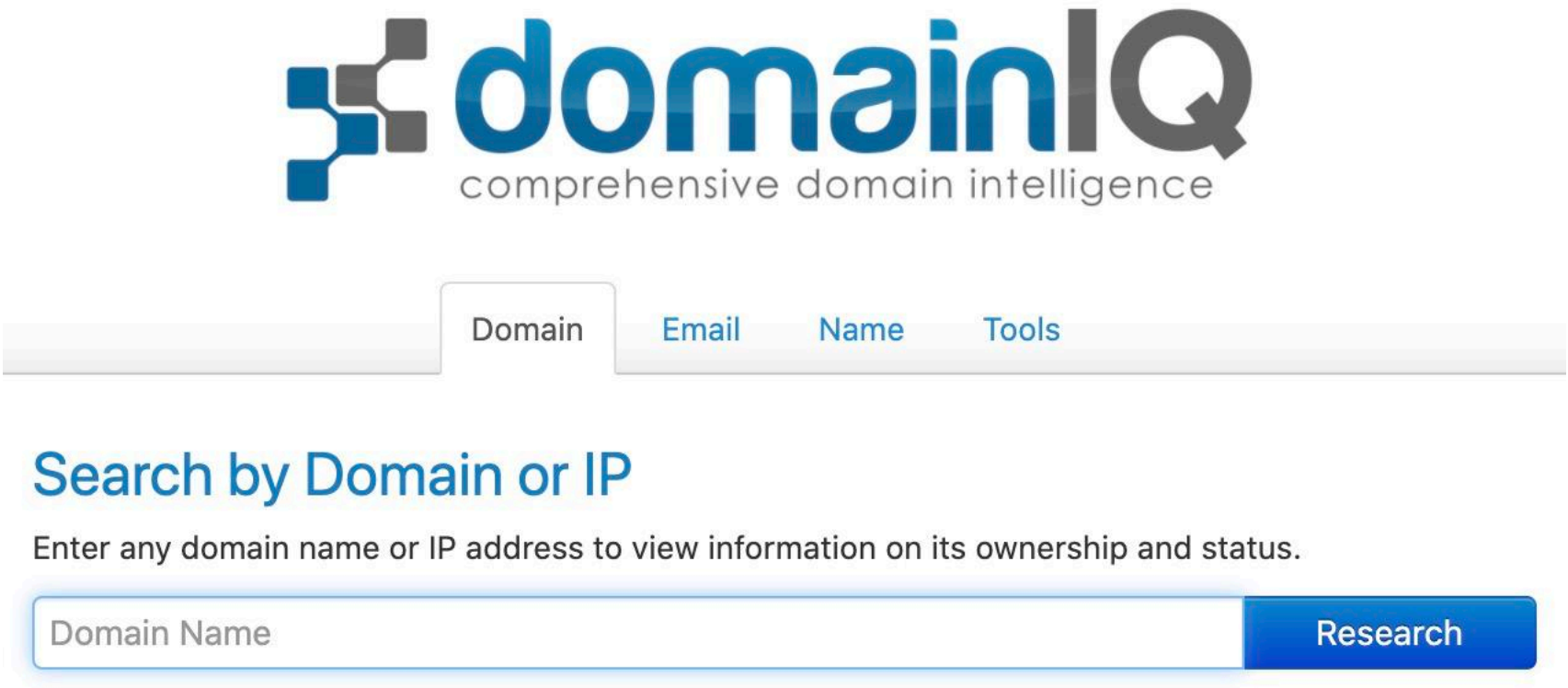

SKOPENOW
AUTOMATED SOCIAL MEDIA INVESTIGATIONS
from enhanced open source intelligence.
Book a Demo
Start a Trial

Bitcoin/Blockchain Intelligence

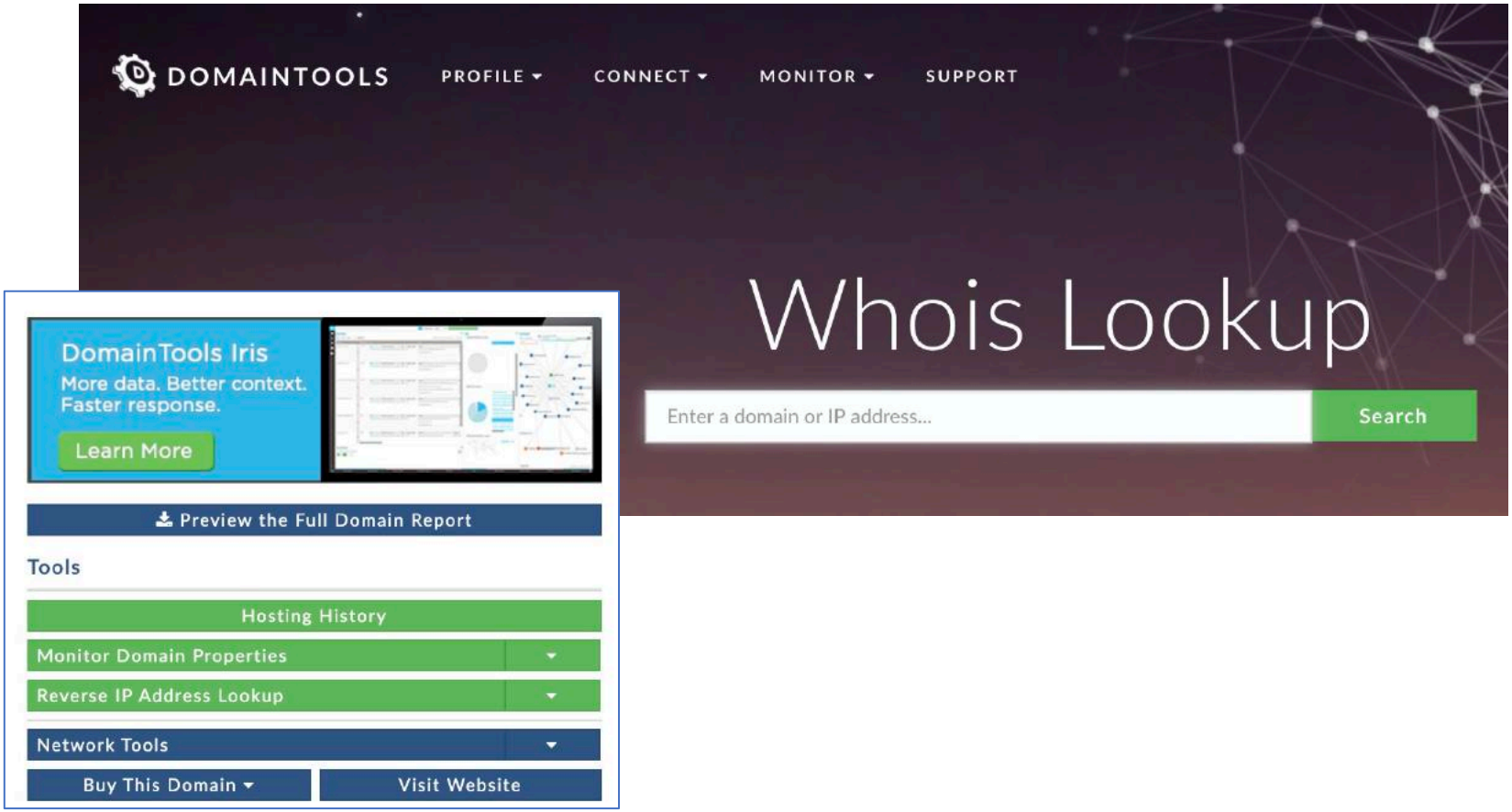
Bitcoin/Blockchain Intelligence



DomainIQ

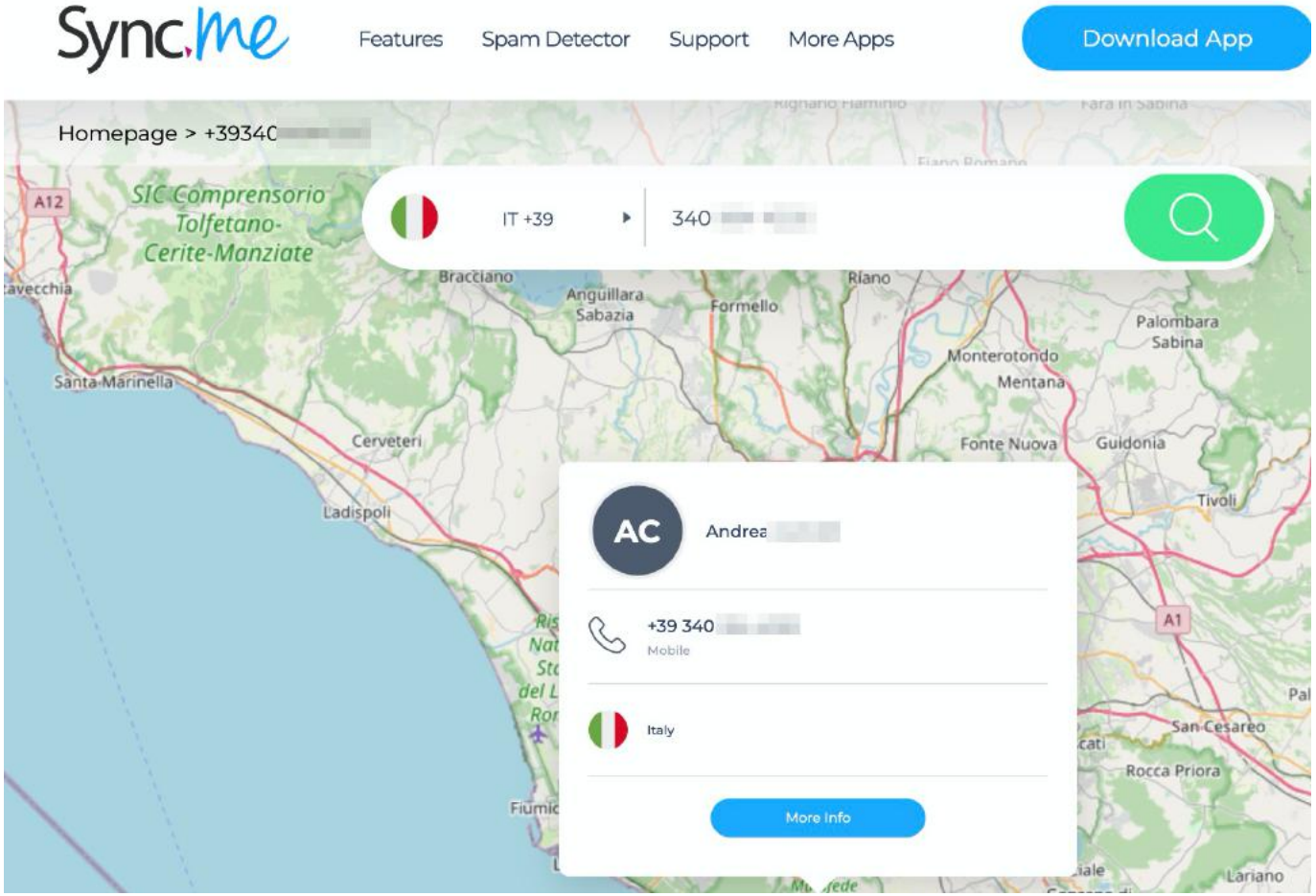

domainIQ
comprehensive domain intelligence
Domain
Email
Name
Tools
Search by Domain or IP
Enter any domain name or IP address to view information on its ownership and status.
Domain Name
Research

DomainTools

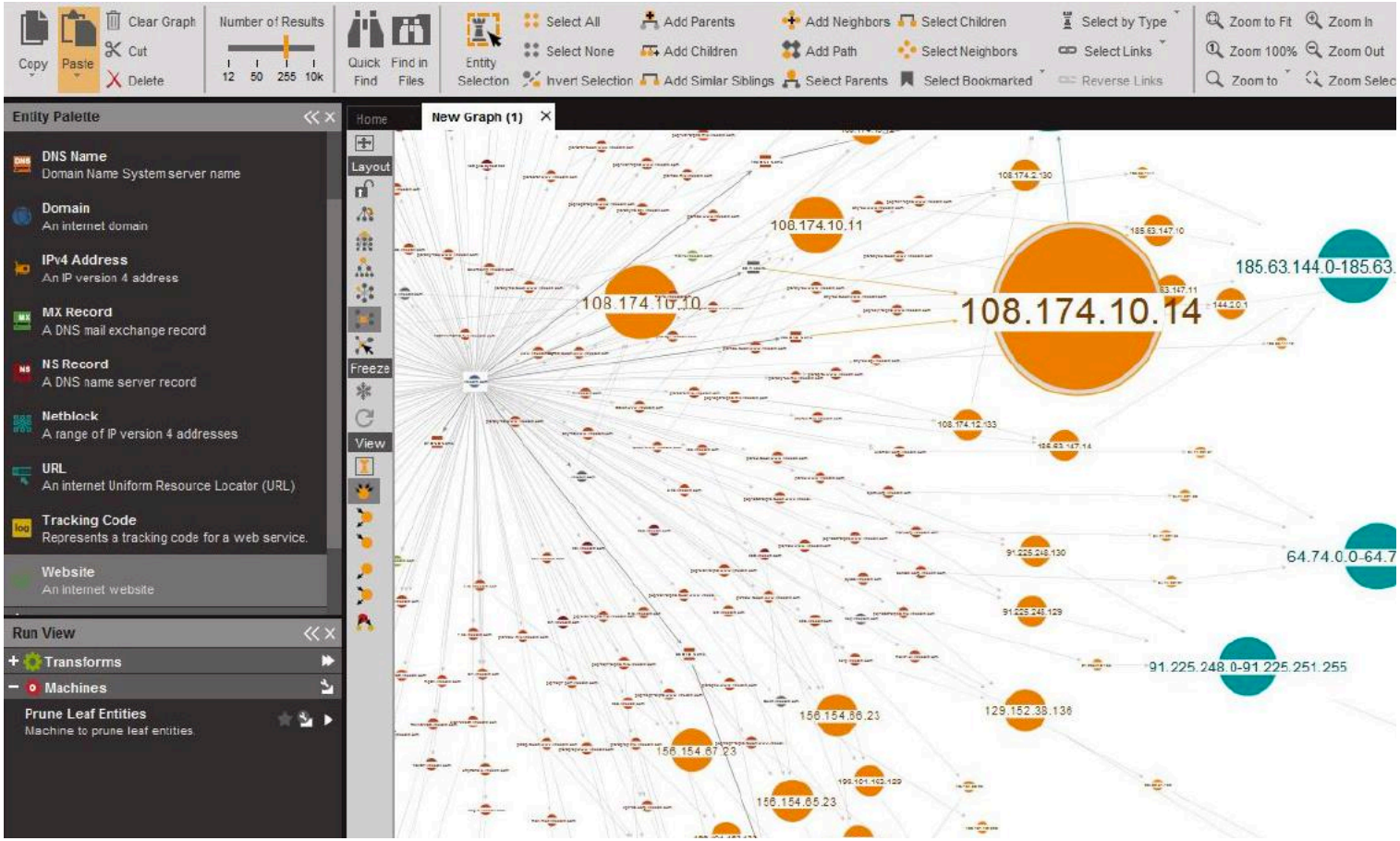


Wayback Machine

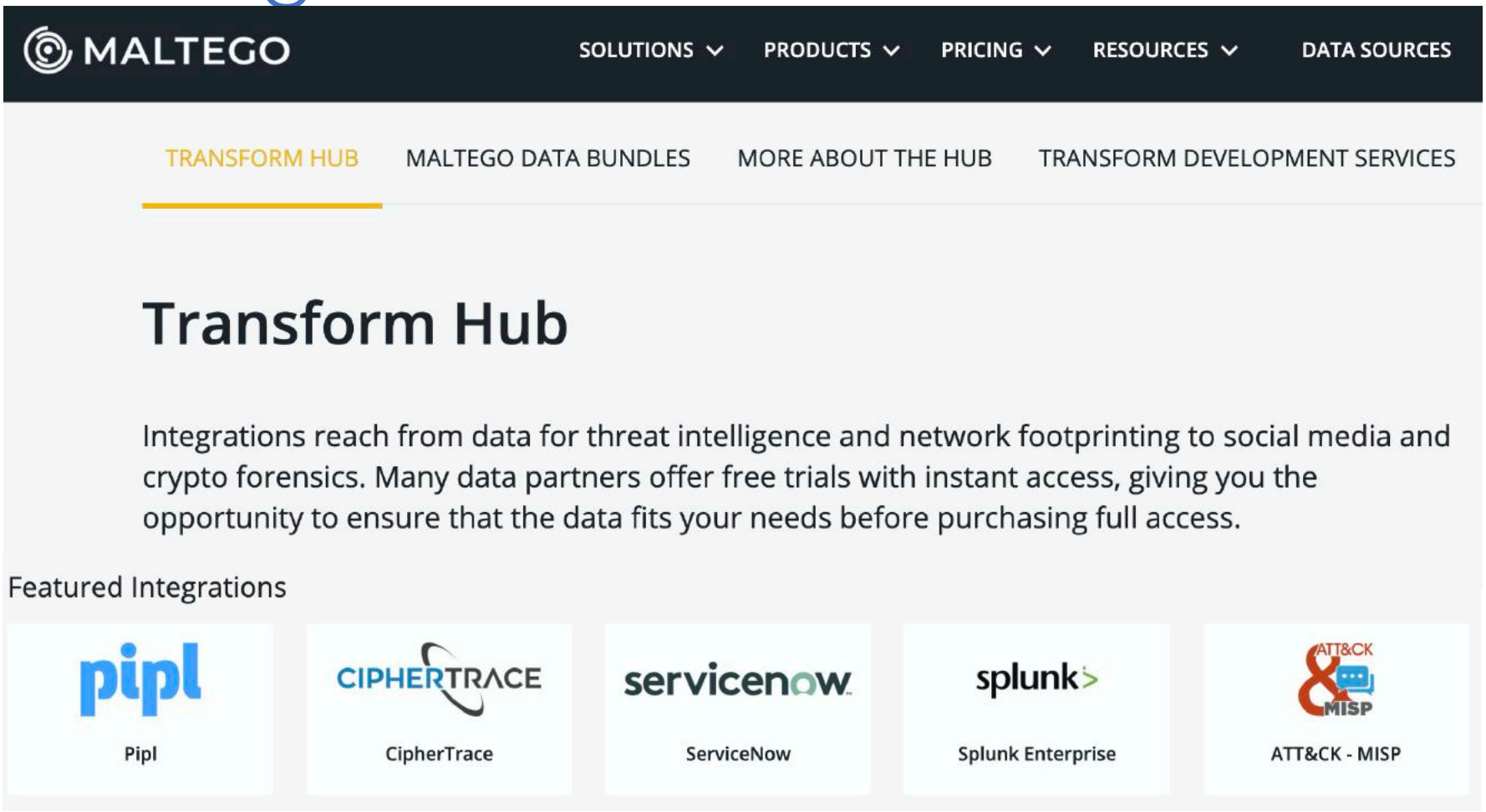
Sync.me/Truecaller/OpenCNAM



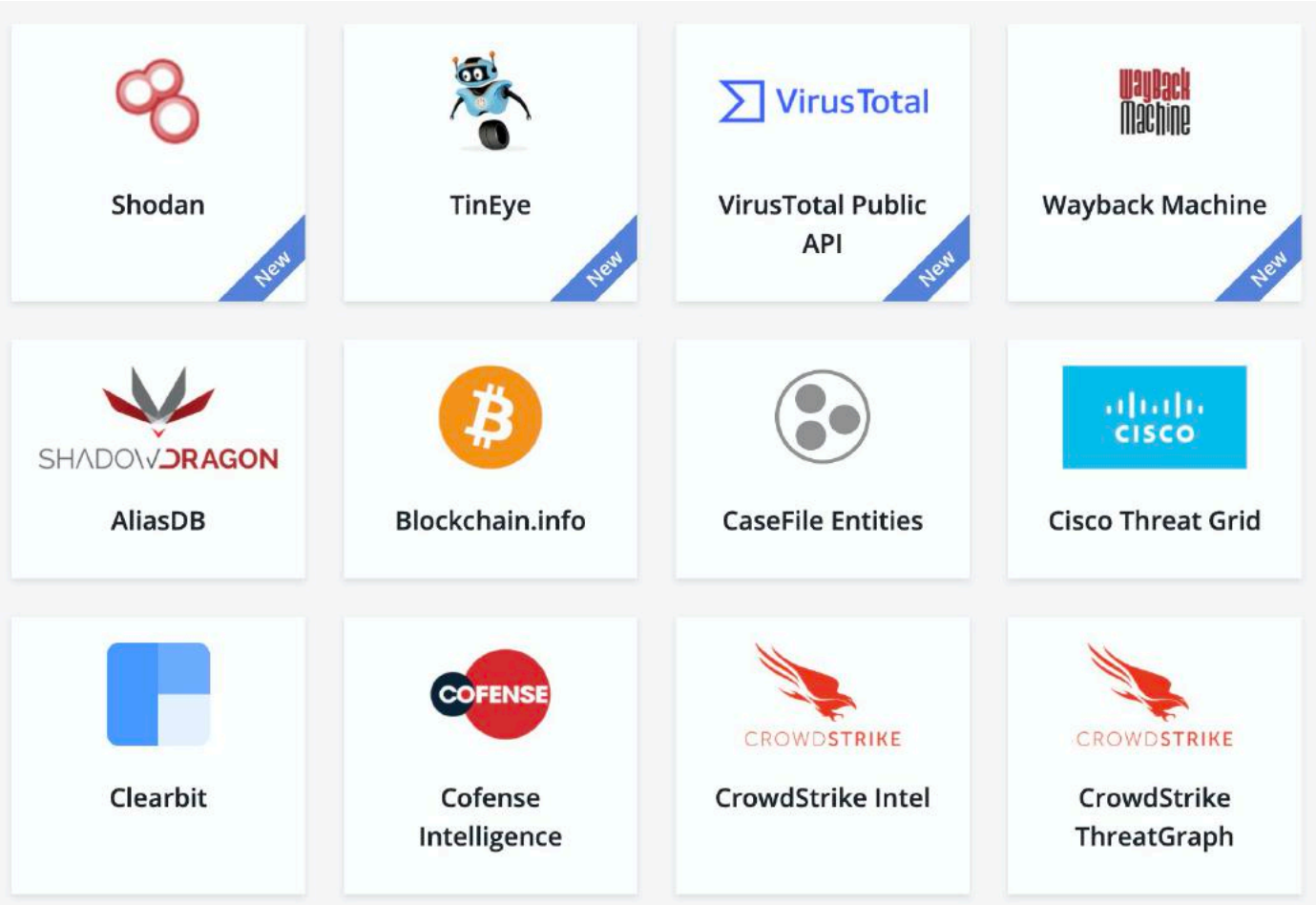
Maltego


Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12 50 255 10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Entity Palette
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
A range of IP version 4 addresses
URL
An internet Uniform Resource Locator (URL)
Tracking Code
Represents a tracking code for a web service.
Website
An internet website
Run View
Transforms
Machines
Prune Leaf Entities
Machine to prune leaf entities
Home
New Graph (1)
Layout
Freeze
View
108.174.10.11
108.174.10.10
108.174.10.14
185.63.144.0-185.63.
64.74.0.0-64.7
91.225.248.0-91.225.251.255
129.152.38.136
156.154.66.23
156.154.67.23
156.154.65.23

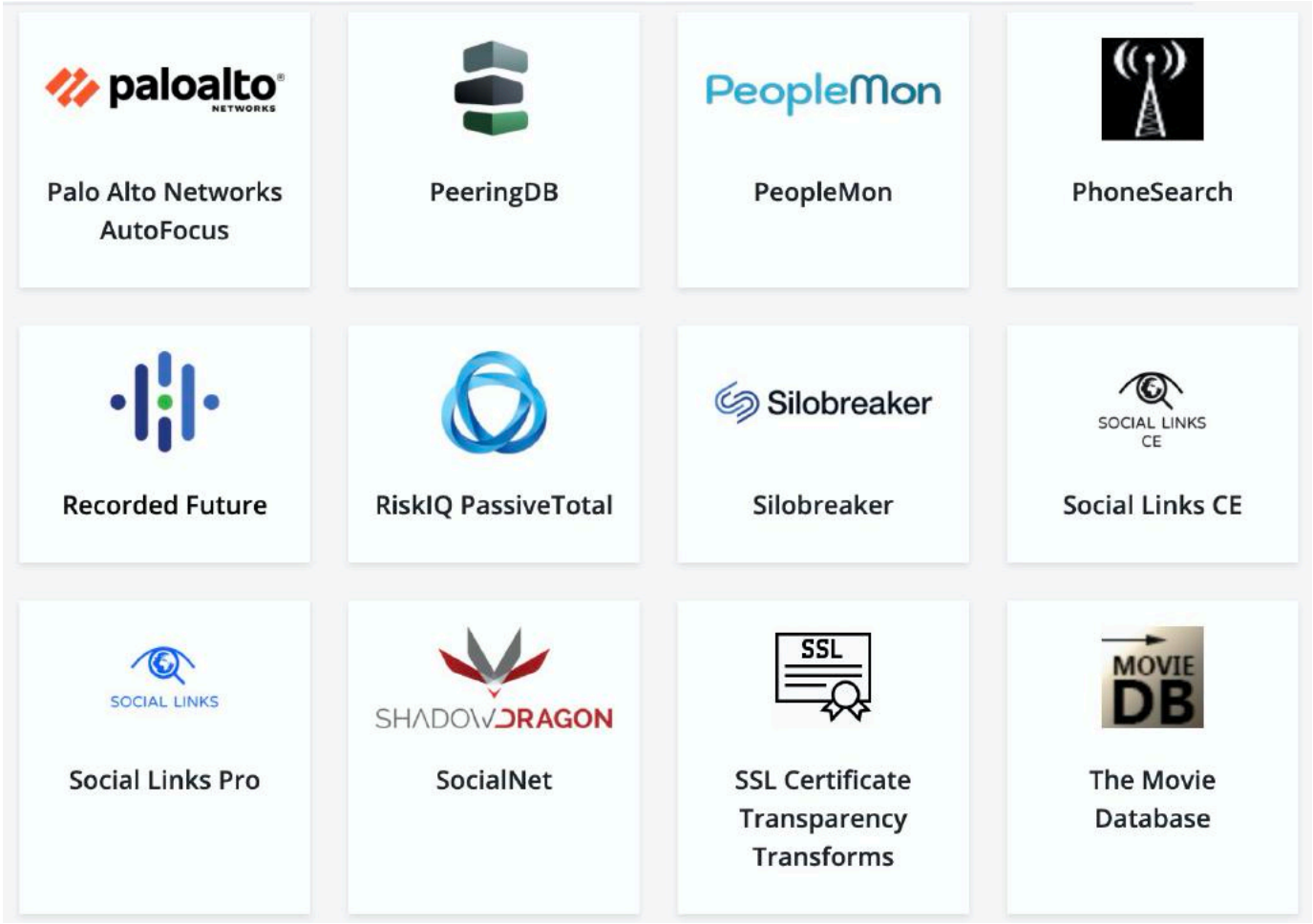
Maltego


MALTEGO
SOLUTIONS
PRODUCTS
PRICING
RESOURCES
DATA SOURCES
TRANSFORM HUB
MALTEGO DATA BUNDLES
MORE ABOUT THE HUB
TRANSFORM DEVELOPMENT SERVICES
Transform Hub
Integrations reach from data for threat intelligence and network footprinting to social media and crypto forensics. Many data partners offer free trials with instant access, giving you the opportunity to ensure that the data fits your needs before purchasing full access.
Featured Integrations
pipl
Pipl
CIPHERTRACE
CipherTrace
servicenow
ServiceNow
splunk>
Splunk Enterprise
ATT&CK
&
MISP
ATT&CK - MISP

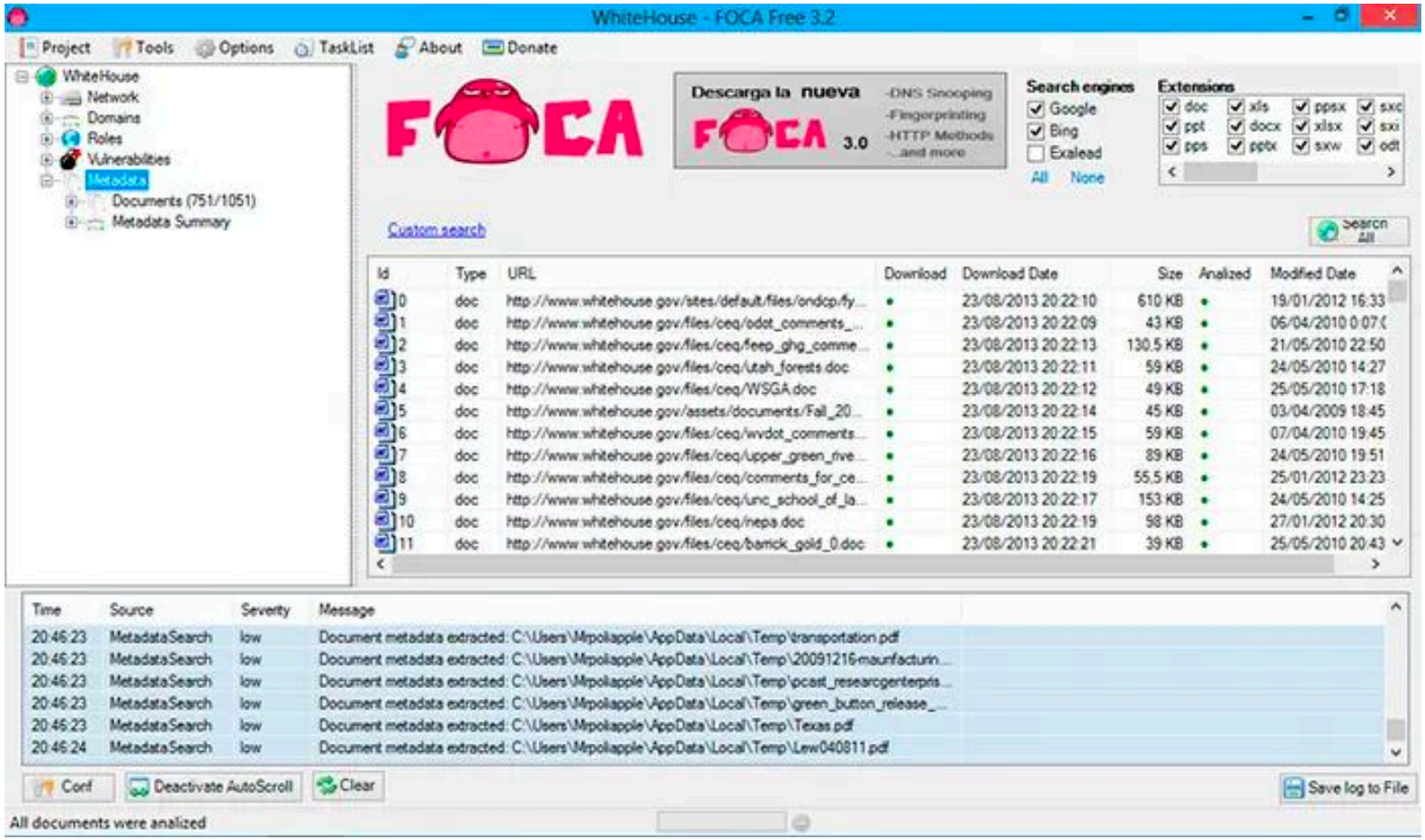
Maltego


Shodan
New
TinEye
New
VirusTotal Public API
New
Wayback Machine
New
AliasDB
Blockchain.info
CaseFile Entities
Cisco Threat Grid
Clearbit
Cofense Intelligence
CrowdStrike Intel
CrowdStrike ThreatGraph

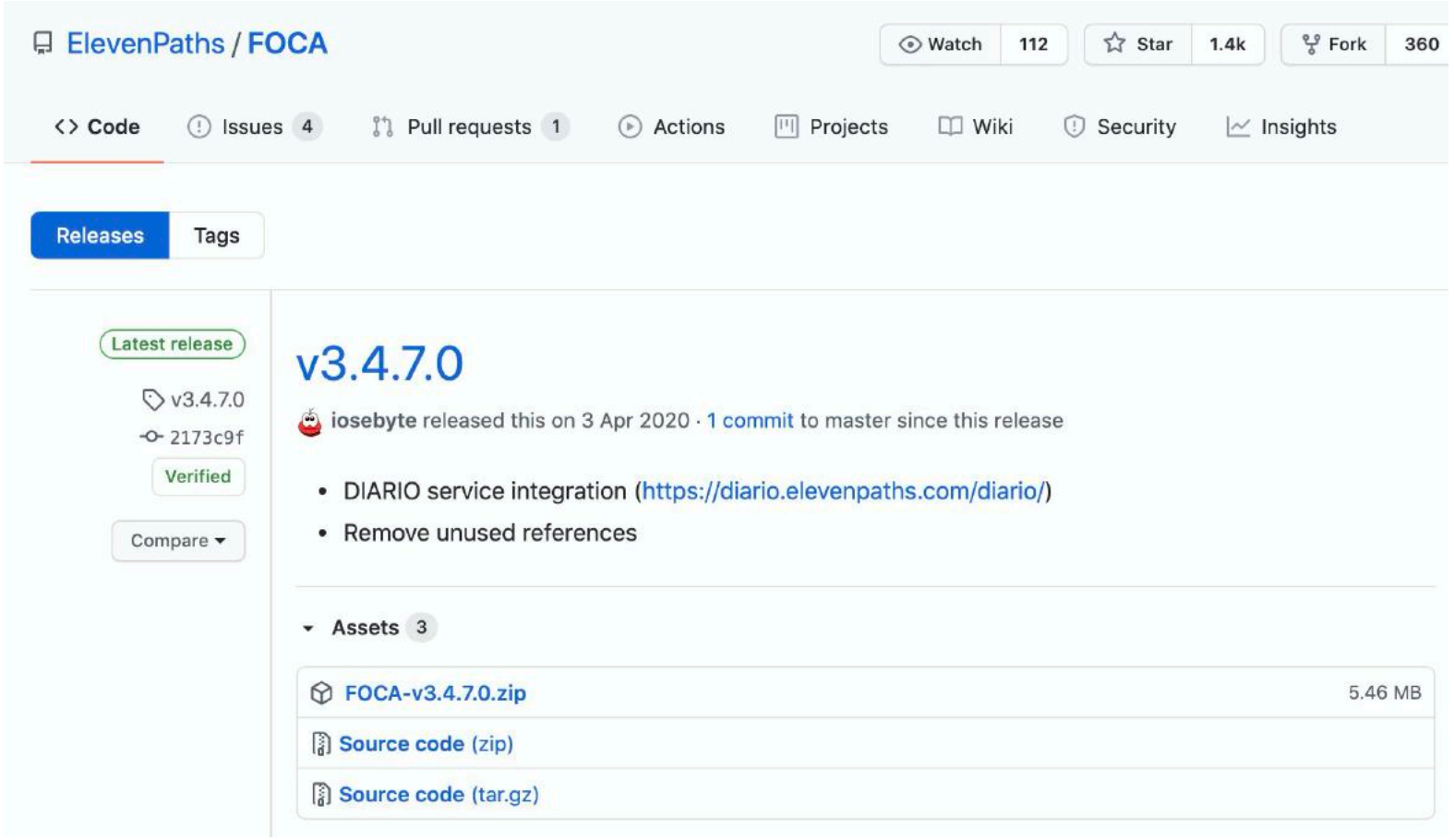
Maltego


paloalto NETWORKS
Palo Alto Networks AutoFocus
PeeringDB
PeopleMon
PeopleMon
PhoneSearch
Recorded Future
RiskIQ PassiveTotal
Silobreaker
Silobreaker
SOCIAL LINKS CE
Social Links CE
SOCIAL LINKS
Social Links Pro
SHADOWDRAGON
SocialNet
SSL
SSL Certificate Transparency Transforms
MOVIE DB
The Movie Database

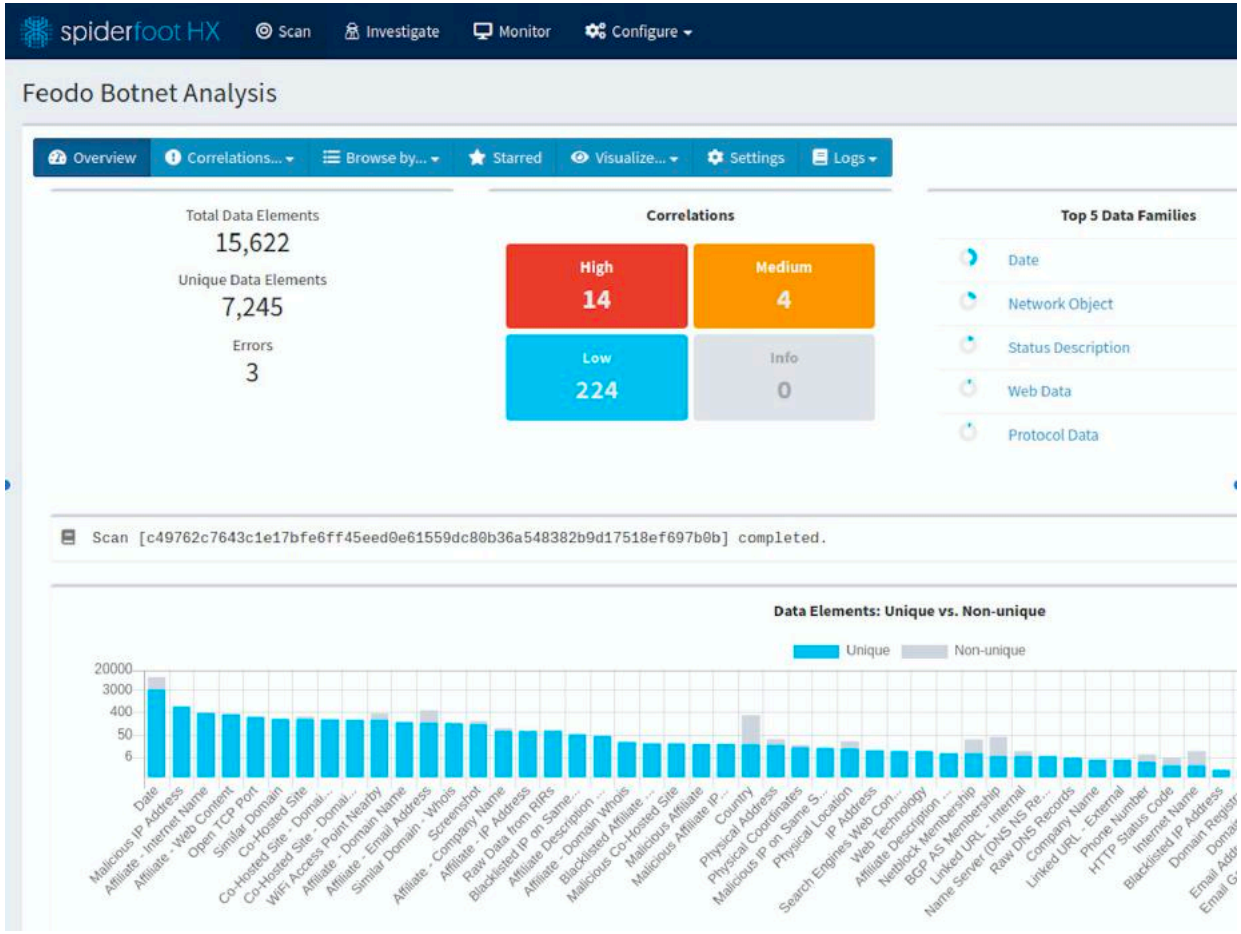
Foca


WhiteHouse - FOCA Free 3.2
Project
Tools
Options
TaskList
About
Donate
WhiteHouse
Network
Domains
Roles
Vulnerabilities
Metadata
Documents (751/1051)
Metadata Summary
FOCA
Descarga la nueva
FOCA 3.0
-DNS Snooping
-Fingerprinting
-HTTP Methods
...and more
Search engines
Google
Bing
Exalead
All
None
Extensions
doc
xls
ppsx
sxc
ppt
docx
xlsx
sxi
pps
pptx
sxw
odt
Custom search
Search All
Id
Type
URL
Download
Download Date
Size
Analized
Modified Date
0 doc http://www.whitehouse.gov/sites/default/files/ondcp/fy... 23/08/2013 20:22:10 610 KB 19/01/2012 16:33
1 doc http://www.whitehouse.gov/files/ceq/odot_comments_... 23/08/2013 20:22:09 43 KB 06/04/2010 0:07:(
2 doc http://www.whitehouse.gov/files/ceq/feep_ghg_comme... 23/08/2013 20:22:13 130.5 KB 21/05/2010 22:50
3 doc http://www.whitehouse.gov/files/ceq/utah_forests.doc 23/08/2013 20:22:11 59 KB 24/05/2010 14:27
4 doc http://www.whitehouse.gov/files/ceq/WSGA.doc 23/08/2013 20:22:12 49 KB 25/05/2010 17:18
5 doc http://www.whitehouse.gov/assets/documents/Fall_20... 23/08/2013 20:22:14 45 KB 03/04/2009 18:45
6 doc http://www.whitehouse.gov/files/ceq/wvdot_comments... 23/08/2013 20:22:15 59 KB 07/04/2010 19:45
7 doc http://www.whitehouse.gov/files/ceq/upper_green_rive... 23/08/2013 20:22:16 89 KB 24/05/2010 19:51
8 doc http://www.whitehouse.gov/files/ceq/comments_for_ce... 23/08/2013 20:22:19 55.5 KB 25/01/2012 23:23
9 doc http://www.whitehouse.gov/files/ceq/unc_school_of_la... 23/08/2013 20:22:17 153 KB 24/05/2010 14:25
10 doc http://www.whitehouse.gov/files/ceq/nepa.doc 23/08/2013 20:22:19 98 KB 27/01/2012 20:30
11 doc http://www.whitehouse.gov/files/ceq/barrick_gold_0.doc 23/08/2013 20:22:21 39 KB 25/05/2010 20:43
Time
Source
Severity
Message
20:46:23 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\transportation.pdf
20:46:23 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\20091216-maunfacturin...
20:46:23 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\pcast_researcgenterpris...
20:46:23 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\green_button_release_...
20:46:23 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\Texas.pdf
20:46:24 MetadataSearch low Document metadata extracted: C:\Users\Mrpoilapple\AppData\Local\Temp\Lew040811.pdf
Conf
Deactivate AutoScroll
Clear
Save log to File
All documents were analized

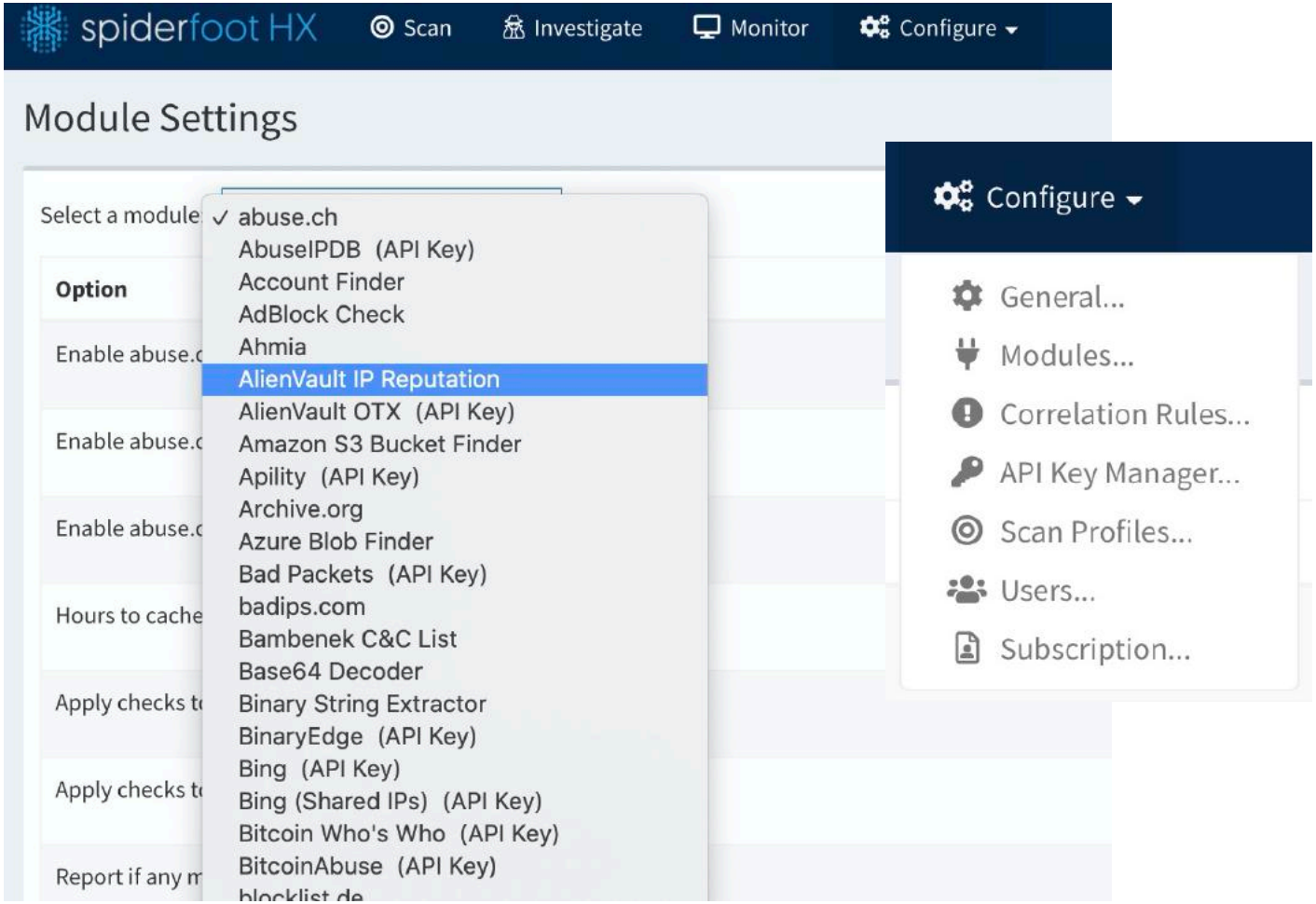
Foca


ElevenPaths / FOCA
Watch 112
Star 1.4k
Fork 360
Code
Issues 4
Pull requests 1
Actions
Projects
Wiki
Security
Insights
Releases
Tags
Latest release
v3.4.7.0
2173c9f
Verified
Compare
v3.4.7.0
iosebyte released this on 3 Apr 2020 · 1 commit to master since this release
DIARIO service integration (https://diario.elevenpaths.com/diario/)
Remove unused references
Assets 3
FOCA-v3.4.7.0.zip 5.46 MB
Source code (zip)
Source code (tar.gz)

Spiderfoot


spiderfoot HX
Scan
Investigate
Monitor
Configure
Feodo Botnet Analysis
Overview
Correlations...
Browse by...
Starred
Visualize...
Settings
Logs
Total Data Elements
15,622
Unique Data Elements
7,245
Errors
3
Correlations
High
14
Medium
4
Low
224
Info
0
Top 5 Data Families
Date
Network Object
Status Description
Web Data
Protocol Data
Scan [c49762c7643c1e17bfe6ff45eed0e61559dc80b36a548382b9d17518ef697b0b] completed.
Data Elements: Unique vs. Non-unique
Unique
Non-unique
20000
3000
400
50
6

Spiderfoot


spiderfoot HX
Scan
Investigate
Monitor
Configure
Module Settings
Select a module
Option
Enable abuse.c
Enable abuse.c
Enable abuse.c
Hours to cache
Apply checks t
Apply checks t
Report if any m
✓ abuse.ch
AbuseIPDB (API Key)
Account Finder
AdBlock Check
Ahmia
AlienVault IP Reputation
AlienVault OTX (API Key)
Amazon S3 Bucket Finder
Apility (API Key)
Archive.org
Azure Blob Finder
Bad Packets (API Key)
badips.com
Bambenek C&C List
Base64 Decoder
Binary String Extractor
BinaryEdge (API Key)
Bing (API Key)
Bing (Shared IPs) (API Key)
Bitcoin Who's Who (API Key)
BitcoinAbuse (API Key)
blocklist.de
Configure
General...
Modules...
Correlation Rules...
API Key Manager...
Scan Profiles...
Users...
Subscription...

In alternativa… ;-)

Programming & Tech › Data Analysis & Reports › Data Mining/Scraping

I will do professional OSINT report

fiverr.

arulselvar

€4.34

3 Days Delivery

Grazie per l'attenzione

paolo@dalchecco.it
@forensico