



Gathering Threat Intelligence

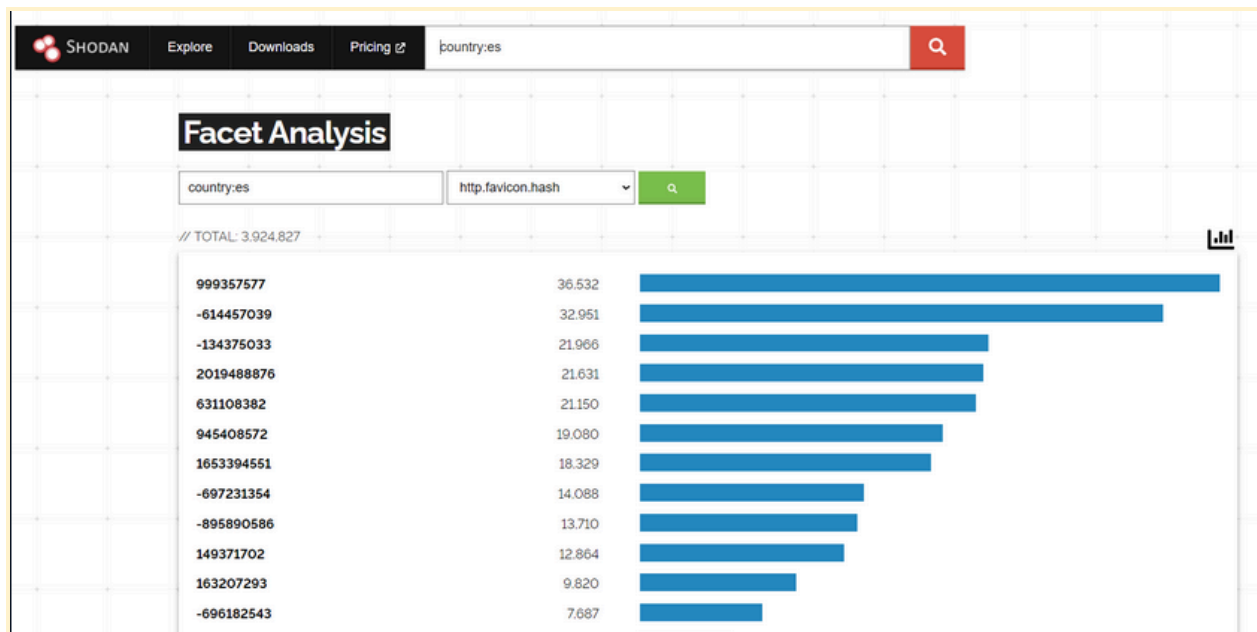
By: Ryan Stewart

One of the critical aspects of effective threat intelligence collection is maintaining a broad spectrum of data sources. When gathering threat intelligence, especially in the case of collecting **malicious hashes**, it is essential to cast a wide net by obtaining data from diverse sources. To ensure precision without inflating the false positive rate during source expansion, **setting a false positive limit value** and **implementing false positive filters** becomes imperative. This strategic approach allows the removal of sources that contribute significantly to false positive values from our intelligence repository.

Here I'll provide some of the prominent sources for collecting threat intelligence data and explore their potential equivalents:

Shodan

Shodan stands out as a web-based server search engine renowned for its popularity in its category. This robust search engine empowers users to explore internet-connected systems using specific filters. Searches can be tailored to focus on organizations or countries on a global scale. Shodan's adaptability allows users to customize searches according to their needs. **For instance**, it enables the identification of all systems from a particular country or organization with port# 21 that are exposed to the internet.



Many data can be accessed instantly by searching the interface on Shodan. Also, we may need to pull the data through the API as collecting intelligence manually is not possible.

The image shows the Shodan API Reference page. It includes a navigation bar with 'SHODAN', 'Developer', 'Dashboard', 'API Reference', 'Integrations', and 'Pricing'. The main content area is titled 'API Reference' and contains two main sections: 'API Documentation' and 'Appendix'. The 'API Documentation' section lists links for 'Requirements', 'Introduction', 'Clients', 'REST API Documentation', and 'Streaming API Documentation'. The 'Appendix' section lists links for 'Banner Specification' and 'Search Filters'. The 'REST API Documentation' section provides the base URL for all methods: <https://api.shodan.io>. The 'Search Methods' section lists several GET requests for different endpoints.

Method	Endpoint
GET	/shodan/host/{ip}
GET	/shodan/host/count
GET	/shodan/host/search
GET	/shodan/host/search/facets
GET	/shodan/host/search/filters

- You can access the api documentation at <https://developer.shodan.io/api> and see how data can be retrieved via the API.

Other search engines alternative to Shodan are “BinaryEdge”, “Zoomeye”, and “Censys”.

****Resources Providing IOCs****

A **crucial strategy** for safeguarding against potential cyber threats involves the systematic collection of Indicators of Compromise (IOCs) such as **IPs, domains, hashes, and Command and Control servers (C2s)**. The acquisition of these artifacts associated with emerging threat actors empowers organizations to proactively detect malicious activities, fortify their systems, and take preemptive measures upon observing any related IOCs in their environment.

Several valuable resources, including Alienvault, Malwarebazaar, Abuse.ch, Malshare, **Anyrun**, **Virustotal**, **Hybrid-Analysis**, Totalhash, Phishunt, Spamhaus, Tor Exit Nodes, Urlscan, Zone-h, Rats, Sorbs, Barracuda, among others, offer a wealth of IOCs. A fundamental principle here is to maintain an extensive and diverse list of sources, regularly pulling data from them. Similar to Shodan, these sources often provide **data through APIs**, facilitating efficient data retrieval. Subsequent data refinement methods, such as whitelisting, help minimize false positives, ensuring a more accurate threat intelligence picture.

****Hacker Forums****

Hacker forums stand out as **pivotal hubs** for intelligence gathering. Threat actors frequently share their plans and preparations for attacks or campaigns against organizations or countries on these forums. Analyzing the content posted allows for insights into critical aspects of impending attacks, including the attack's direction, potential targets, attack methods, and identification of the individuals orchestrating the attack.

These forums may also host transactions involving the sale of access to compromised systems. In the event of a compromise, addressing remediation issues becomes paramount. This includes closing external access to systems, preventing access by more malicious actors, and conducting a thorough analysis to determine the root cause of the incident. The following section provides **visual representations** of content shared on hacker forums for illustrative purposes.



3500 HQ mails with amazon

[Follow](#)[Start new topic](#)[Reply to this top](#)

3500 HQ mails with amazon

[Report post](#)

In the presence of 3500 bold miles first hand with amazon.
I'll give it at % or at a fixed price to people with straight arms.
Hey guys in stock ~ 3500 HQ quality mails with amazon I one hand!!!
Work % or fix price



Connection :
jabber [redacted]
Telegram [redacted]

+ Quote

[redacted]

[redacted]



ESCO EXCEL (XLL) EXPLOIT BUILDER

[Report post](#)

Only use only valid contact address "[redacted]" or PMI (be wary of scammers.)
telegram directly contact link [https://t.me/\[redacted\]](https://t.me/[redacted])
(be wary of scammers.)

ESCO EXCEL (XLL) EXPLOIT BUILDER

Most of the vulnerabilities in macros have been closed. That's why Excel (xll) is now very good and stable as an alternative.
Once you have opened the file, just press the button that says enable once. And the file will be executed.

Videos

- [redacted]

Features

- Much better quality than silent and macro exploits.
- shows pop-ups when open it.
- Executing your file in one click.
- Works on all versions of Microsoft Office and Office 365 .net/native is compatible with all files.
- Gmail, Hotmail, Yahoo mail etc bypassing.
- Windows Defender and SmartScreen Bypassing Runtime.

Update and Detecting

- We are checking regularly, when is detect we are updating.
- Updates are free during your license period.
- Each new update is 1-0/30 FUD

Pricing



Sale wordpress admin/shells

ESCROW AVAILABLE IN THIS THREAD!

New deal

Watch

as bekdeniyor...

wp-login.php price from 0.3\$
zebra pattern from 0.4
sample from 1\$
Shell
from 1\$ it is also possible to upload your file
contact:

We attacked the [redacted] and leaked nearly 3.8TB of data, including core data from various key medical institutions across the country.
Organization Name: [redacted]
Contact us Telegram: [https://t.me/\[redacted\]](https://t.me/[redacted])

파일명 .확장자	크기 유형)	수정 시기	클릭수
최신 [redacted] _OLD_20191029.zip	7.75GB	2022/5/1	0
최신 [redacted] _OLD.MDF	55.98GB	2022/5/1	0
최신 [redacted] _OLD_1.LDF	1.00MB	2022/5/1	0
최신 [redacted] _BAK_Log.LDF	1.00MB	2022/5/3	0
최신 [redacted] _NEW_log.ldf	1.00MB	2022/5/3	0
최신 [redacted] _TEST_20190725.ldf	1.00MB	2022/5/3 1	0
최신 [redacted]	461.08MB	2022/5/3 1	0
최신 [redacted] _NEW.mdf	34.93GB	2022/5/4	0
최신 [redacted] _K_Data.MDF	38.42GB	2022/5/4	0
최신 [redacted] _ST_20190725.mdf	55.98GB	2022/5/5	0
최신 [redacted]	33.17GB	2022/5/5	0

Ransomware Blogs

The prominence of ransomware blogs has surged notably with the onset of the Covid-19 pandemic. Since 2020, ransomware groups have escalated their activities, using these platforms to publish data from victims who resisted payment and to announce their endeavors. Monitoring these blogs is imperative as they provide valuable insights into targeted organizations, the affiliations of specific groups, the countries under siege, motivations behind attacks, and a wealth of intelligence on ransomware groups.

Notable ransomware groups, such as **Lockbit**, **Conti**, **Revil**, **Hive**, and **Babuk**, are actively using these blogs. For an updated list of active ransomware groups and direct links to their blogs, refer to the following link:

http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgywyd.onion/

Accessing sites with .onion extensions requires the Tor Browser, as they are not accessible through regular browsers. Download the Tor Browser from torproject.org to navigate these links securely.

Ransomware Group Sites

If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:

DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhhgmb1

LTC: LXMDziBcT474Mava74r9BvkTyOxcAuk6MD

BTC/BCH: 1FyCD8kp9ek1TTgdyhftZrgzR1QCHV4i84

XMR: 48FgeW4fUpYjPDGxJdHaA441F5C9szYtLSVwbNv8T3Zxe9ZN3iLU55dA5of2vDQqdbgRYom9aMeQMWPQkr35PZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYP70N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open Open
Medusa	v3	Open
Midas	v3	Open
Moses Staff	v2	Open DEEP-WEB
Pandora	v3	Open
Pay2Key	v3	Open
Quantum	v3	Open
Ragnar_Locker	v3	Open
RAMP	v3	Open
Ransom Cartel	v3	Open
Ransom House	v3	Open

THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware



ZENTRALE
KRIMINALINSPEKTION
GÖTTINGEN

















































Federal
Criminal Police Office

****Black Markets****

Black Markets represent more organized versions of the "Selling" categories found in hacker forums. Within these markets, items such as credit cards, stealer logs, Remote Desktop Protocol (RDP) accesses, and prepaid accounts are commonly offered for sale.

While the data obtained from black markets may have limited standalone utility due to its restricted information, the significance emerges when connected to an established attack surface. As previously emphasized, if an attack surface exists and the collected data aligns with it, actionable insights can be derived.

Unlike some other sources, black markets typically do not provide data through Application Programming Interfaces (APIs). Extracting data necessitates sending requests through scripts and parsing the responses. The following section includes visual representations with screenshots from various black markets for illustrative purposes.

#	Type	Bin	Bank	Class	Level	EXP	Database	Country	State	City	Zip	SSN	DOB	Vendor	Price	Action
#			BANK	CREDIT	OPTIMA	06/2024	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	07/2024	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	06/2022	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	10/2023	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	06/2022	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	01/2023	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	DEBIT	RELOADABLE PREPAID	10/2024	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	CREDIT	CONSUMER LENDING	07/2024	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	CREDIT	OPTIMA	07/2024	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
#			BANK	CREDIT	OPTIMA	10/2022	5.7/usa vr/90% (REFUND 5 min)							ya####08 (platinum)	\$ 12.00	Buy
<div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>8</div><div>9</div><div>10</div><div>»</div></div>																
Mask	Country	State / City	Details						Info	Vendor	Blacklist	Price	Action			
35.182.**** ISP: Amazon Technologies Inc.		Ontario Toronto	OS: Win10(2022) Proc: Intel Core i5 RAM: 6 GB @: 1000 / 1000 Mbit/s						Admin: Yes Paypal: No NAT: -	 Pr####dp (platinum)		\$ 8.00	Buy			
35.183.**** ISP: Amazon Technologies Inc.		Ontario Toronto	OS: Win10(2022) Proc: Intel Core i5 RAM: 6 GB @: 1000 / 1000 Mbit/s						Admin: Yes Paypal: No NAT: -	 Pr####dp (platinum)		\$ 8.00	Buy			
3.99.**** ISP: Amazon Technologies Inc.		Ontario Toronto	OS: Win10(2022) Proc: Intel Core i5 RAM: 6 GB @: 1000 / 1000 Mbit/s						Admin: Yes Paypal: No NAT: -	 Pr####dp (platinum)		\$ 8.00	Buy			
35.183.**** ISP: Amazon Technologies Inc.		Ontario Toronto	OS: Win10(2022) Proc: Intel Core i5 RAM: 6 GB @: 1000 / 1000 Mbit/s						Admin: Yes Paypal: No NAT: -	 Pr####dp (platinum)		\$ 8.00	Buy			
3.96.**** ISP: Amazon Technologies Inc.		Ontario Toronto	OS: Win10(2022) Proc: Intel Core i5 RAM: 6 GB @: 1000 / 1000 Mbit/s						Admin: Yes Paypal: No NAT: -	 Pr####dp (platinum)		\$ 8.00	Buy			
20.80.**** ISP: Microsoft Corporation		Virginia Boydton	OS: Windows 11 Pro Proc: Intel Xeon Platinum 8370C CPU 2.80GHz 2.80GHz RAM: 16 GB @: 698 / 989 Mbit/s						Admin: Yes Paypal: No NAT: Yes	 qw####11 silver		\$ 12.00	Buy			
20.80.**** ISP: Microsoft Corporation		Virginia Boydton	OS: Windows 11 Pro Proc: Intel Xeon Platinum 8370C CPU 2.80GHz 2.80GHz RAM: 16 GB @: 686 / 989 Mbit/s						Admin: Yes Paypal: No NAT: Yes	 qw####11 silver		\$ 12.00	Buy			

Chatters

Platforms enabling both bilateral and multi-party written and audio-visual communications hold significant relevance in the world of threat intelligence. Threat actors **often share** sensitive information or divulge crucial details and documents related to attack preparations through these communication channels. Therefore, it is imperative to monitor these chatters comprehensively, capturing and archiving pertinent information in our database.

Keeping a vigilant eye on chatters is essential due to the potential disclosure of valuable intelligence during these interactions. Presently, threat actors favor popular chatter applications

such as Telegram, ICQ, IRC, and Discord. Within specific groups on these platforms, one may encounter posts advertising the sale of credit cards, accounts, and direct access to companies. For a visual representation, refer to the accompanying screenshots showcasing content from various chatters.

CC → [- ✓ -] 52 727|06|25|761
MSG → Thanks for subscribing!
GATE → SA (A)
TOOK → 4.97's
CHKD BY → 12.5K 19:14

CC → [- ✓ -] 40 78|05|2026|207
MSG → Thanks for subscribing!
GATE → SA (A)
TOOK → 6.47's
CHKD BY → 12.6K 19:15

January 10

CC → [- ✓ -] 49 82|03|23|369
MSG → Thanks for subscribing!
GATE → SA (A)
TOOK → 4.54's
CHKD BY → 9204 18:33

1734 members

4
5
5
5
5
5
5

PAYMENTS BY BTC ONLY

I AM ACTIVE 24/7
I ACCEPT ESCROW
RIPPERS STAY OFF
WHATSAPP:

13:09

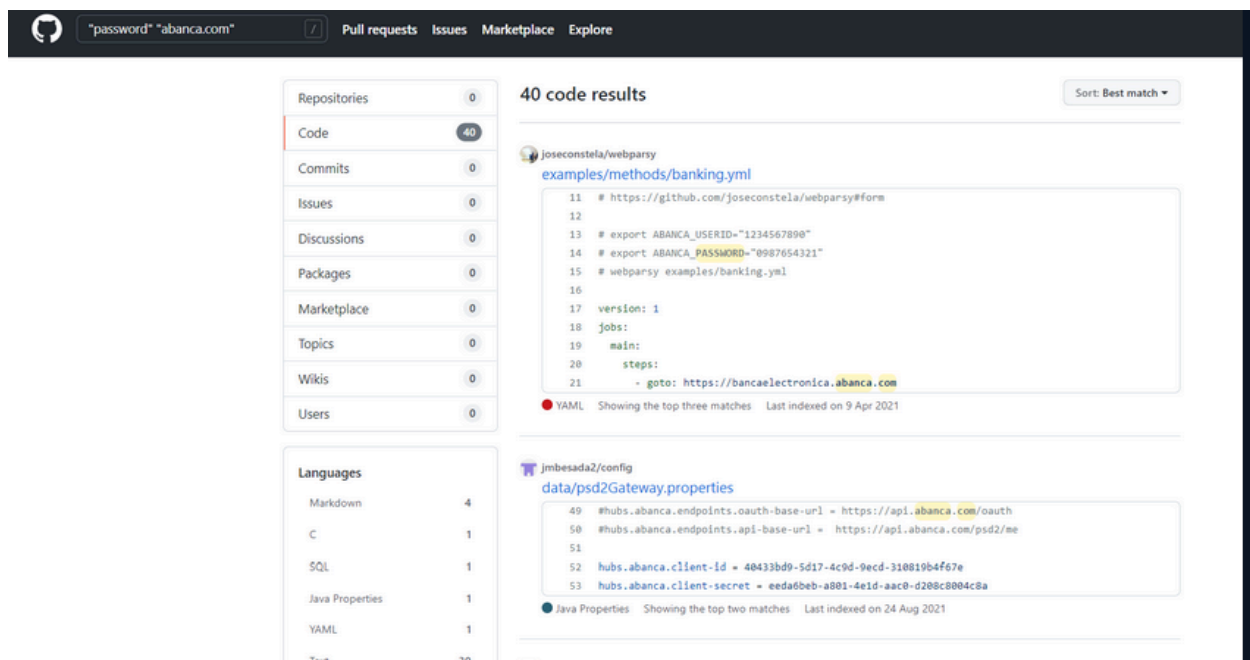
✓ I Have In Stock spam Tools - Smt - Cpanel
cpanel mailer - CFO/CEO leads - Company Jobseeker
RDP/VPS ✨ Localhost Scampage + Letter any country
Email extractor - SMS Bulk Sender Professional,
✨ Passport Driving Licence -SSN - USA -UK-ID Driving
Any Type And Any Country i Can Make it
✨ Make Documents complete message me at cheap price ✓

13:19

****Code Repositories****

Code repositories serve as repositories of **potentially forgotten sensitive data**, presenting a risk for organizations and individual users alike. Within these repositories, crucial information such as database access credentials, login details, sensitive configuration files for applications, and secret API keys may inadvertently be left behind. This oversight opens avenues for malicious actors to discover and exploit these vulnerabilities in their attacks. Consequently, monitoring public code repositories becomes essential from a threat intelligence perspective.

Furthermore, code repositories often become depositories for newly announced vulnerabilities and their corresponding exploits. Identifying and tracking these developments is critical for staying ahead of potential threats. Popular code repository platforms like **Github**, **Gitlab**, and **Bitbucket** are commonly used for hosting code. By employing specific search parameters within these platforms, one can uncover sensitive data. For instance, a search query like "password" "abanca.com" on Github may reveal pertinent information, as illustrated in the following example.



The screenshot displays the GitHub search interface with the query "password" "abanca.com". The search results are categorized by type, with 40 code results shown. The first result is a YAML file named "examples/methods/banking.yml" by user joseconstela/webpary. The code snippet shows environment variables for ABANCA_USERID and ABANCA_PASSWORD, and a goto command pointing to "https://bancaelectronica.abanca.com". The second result is a Java Properties file named "data/psd2Gateway.properties" by user jmbesada2/config. The code snippet shows OAuth and API endpoints for Abanca, along with client ID and secret values. The search results are sorted by "Best match" and show the top three matches for the first result and the top two matches for the second result.

Category	Count
Repositories	0
Code	40
Commits	0
Issues	0
Discussions	0
Packages	0
Marketplace	0
Topics	0
Wikis	0
Users	0

Language	Count
Markdown	4
C	1
SQL	1
Java Properties	1
YAML	1
Text	30

As the screenshots show, we have 40 results for our search for "password" and "abanca.com" keywords. When we review these results we clearly see that the secret API key of Abanca is left open in the second file.

```
47 #hubs.abanca.client-id = 4fa3368a-5f64-43d4-90c2-1078d7fb36d0
48 #hubs.abanca.client-secret = 8ffd7ef3-ffc9-4b08-80e9-e342e3a1bbe2
49 #hubs.abanca.endpoints.oauth-base-url = https://api.abanca.com/oauth
50 #hubs.abanca.endpoints.api-base-url = https://api.abanca.com/psd2/me
51
52 hubs.abanca.client-id = 40433bd9-5d17-4c9d-9ecd-310819b4f67e
53 hubs.abanca.client-secret = eeda6beb-a801-4e1d-aac0-d208c8004c8a
54 hubs.abanca.endpoints.oauth-base-url = https://api.abanca.pt/oauth
55 hubs.abanca.endpoints.api-base-url = https://api.abanca.pt/psd2/me
56
57 hubs.abanca-dummy.client-id = 4fa3368a-5f64-43d4-90c2-1078d7fb36d0
58 hubs.abanca-dummy.client-secret = 25088050-ef29-482a-b475-a36d360d28ab
59 hubs.abanca-dummy.endpoints.oauth-base-url = https://api.abanca.com/oauth
60 hubs.abanca-dummy.endpoints.api-base-url = https://api.abanca.com/sandbox
```

This information may belong to the organization or a third party that provides services, but either way, it is obvious that it is highly risky that this data is open in this way.

****File Share Sites and Threat Intelligence****

File share sites serve as actively utilized platforms by many threat actors, enabling anonymous sharing of files. The uploaded files on these platforms may pertain to specific organizations or even entire countries. In the event of a breach, confidential documents from organizations may find their way onto these file share sites. Monitoring these platforms is crucial from a threat intelligence perspective, as it allows for awareness of shared content related to organizations under scrutiny. Detecting such shares promptly enhances the ability to identify breaches at an early stage.

Among the popular file share sites enabling anonymous file uploads are platforms such as Anonfiles, Mediafire, Uploadfiles, WeTransfer, and File.io. Unlike traditional methods, direct file downloads from these sites are not feasible. Therefore, alternative methods, beyond API usage, are required to extract data from them.

Two distinct methods exist for downloading data from these sites. The first involves a sophisticated process: by employing a guessing algorithm to determine the unique keys associated with a file on these platforms, a request to the application server with that key can retrieve the file in the server's response. However, this method is resource-intensive and requires significant processing power.

The second method is simpler and cost-effective. When a file is uploaded to these sites and marked as public, browsers index these files over time. By utilizing Dork, which are specialized search queries, a script can capture and pull these indexed files to our servers. This method provides an efficient and economical approach to acquiring data from file share sites.

****Public Buckets and Cloud Security****

Bucket applications, residing in **cloud-based environments**, serve as storage spaces for organizations or individuals to safeguard their data. Ideally, these environments should be tightly secured, permitting access only to authorized users within the organization. Unfortunately, this is not always the case, and instances of these environments being inadvertently left wide open are not uncommon. Such lapses can lead to the exposure of sensitive and confidential data, turning **public buckets into potential sources of threat intelligence**.

Detecting these public buckets and identifying their endpoints can be achieved through proactive measures, including brute force attempts. By systematically testing potential bucket names within a structure like **"bucketname.amazonaws.com,"** one can uncover existing public buckets and subsequently search for files under those endpoints. The efficacy of this approach is heightened by utilizing a **wordlist containing potential organization names**.

Prominent applications offering bucket storage include Amazon S3 Buckets, Azure Blobs, and Google Cloud Storage. It is paramount for organizations to be vigilant in securing their cloud-based environments to prevent inadvertent data exposure and mitigate potential threats to their sensitive information.

****Honeypots: Decoy Systems in the Pursuit of Attackers****

Honeypots stand out as a highly effective method for luring and apprehending attackers. These systems, intentionally designed with security vulnerabilities, are strategically disconnected from critical servers or systems, operating on the principle of deception. By presenting an enticing target for attackers, honeypots actively capture Indicators of Compromise (IOCs), including attacker IP addresses, allowing organizations to enhance their threat intelligence.

Creating a custom honeypot tailored to specific needs is an option, or alternatively, organizations can leverage existing popular honeypots. Examples of widely used honeypots include **Kippo, Cowrite, Glastopf, Nodepot, Google Hack Honeypot, ElasticHoney, and Honeymail**. The primary goal is to entice attackers to engage with these decoy systems, enabling the collection of valuable data that can be used to bolster the security of the organization's own systems.

Whether opting for a bespoke solution or leveraging established honeypots, incorporating these deceptive systems into the security strategy provides organizations with a proactive means of actively monitoring and gathering intelligence on potential threats.

****SIEM/IDS/IPS/Firewalls: Safeguarding Through Intelligent Logs****

In the face of numerous daily attacks, an institution's defense mechanisms, guided by rules embedded in security products like **IDS, IPS, and Firewalls**, play a pivotal role in thwarting potential threats. The logs generated by these security products, when centralized in a Security Information and Event Management (SIEM) system, become a goldmine of intelligence. Analyzing these logs, particularly those containing details about blocked IP addresses by firewalls, provides valuable insights into the nature and patterns of attackers.

By filtering these logs, an institution can compile a list of attacker IPs, enhancing situational awareness. Additionally, within the SIEM, the hash of a malicious file captured serves as a crucial piece of intelligence. Recognizing the significance of these security products and viewing them as critical resources allows organizations to stay a step ahead of potential threats. Employing effective rules and scripts to extract pertinent data from these sources ensures the proactive and strategic utilization of security measures. This approach enables organizations to not only prevent attacks but also cultivate a proactive security stance to safeguard critical assets.