whalebone

Whalebone Threat Intelligence

Real Difference,
Real-Time

If there is one word to define the current global cyber threat landscape, it is the word “fast.” New threats, new techniques, and new vulnerabilities occur all the time. In order to always be one step ahead of cyber criminals, we face these challenges with new solutions, new algorithms, and new approaches.

Our research can be divided into the following 3 categories, which are described further in this document:

1. **Internal Research**
2. **Global Partnerships**
3. **Regional Partnerships**

Apart from descriptions of the different categories of our research, our continuous benchmark testing is presented. The document is concluded with an FAQ section and contact information of our threat intelligence experts.

Table of contents

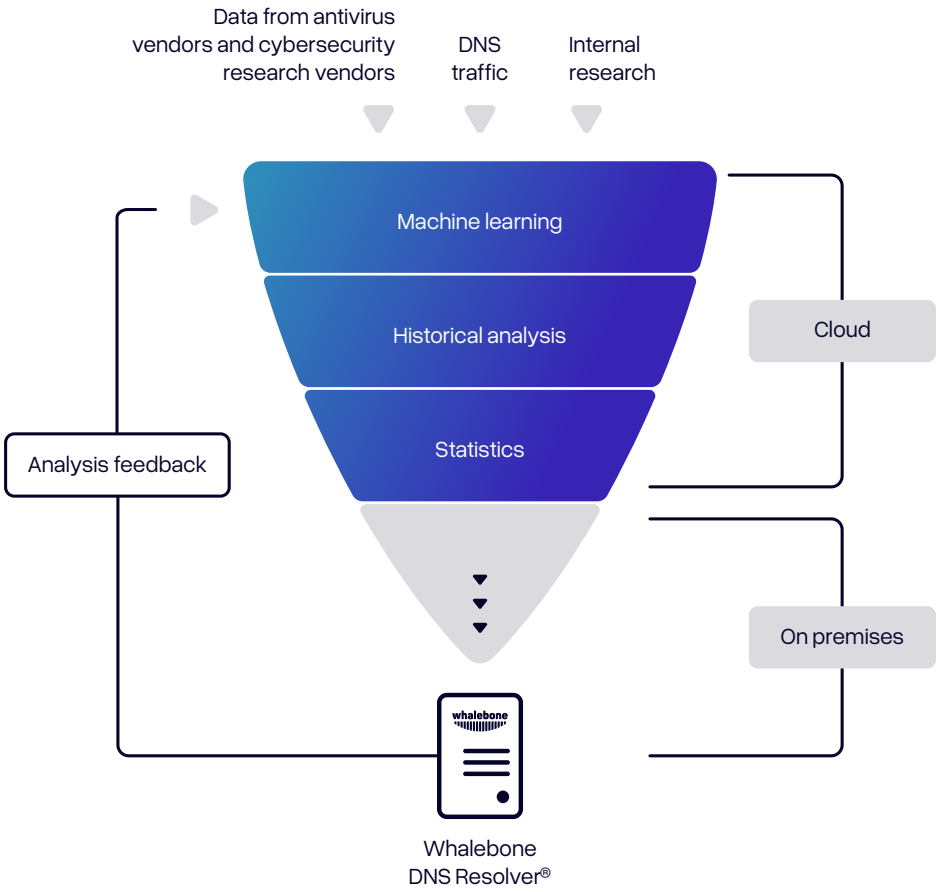
Internal Research

Our Threat Intelligence Team keeps testing and scoring all of our sources, including our own. We constantly reevaluate them to ensure that we are as up-to-date as possible, and we update our scoring algorithms based on emerging threats.

We analyze historical data, statistics, and utilize our unique technology to generate the best possible domain maliciousness evaluation. Multiple factors, including algorithms, are taken into account to determine whether a domain should be blocked or not.

Our internal research can be divided into four main categories:

1. Network Traffic Analysis
2. Automated Phishing Analysis
3. Whalebone Neural Networks
4. Dark Web Scouting Team



Network Traffic Analysis

An important pillar of our internal research is network traffic analysis. We look into the number of users communicating with domains over time, in different time ranges, from various regions. We inspect recent changes and use statistical analysis to expose irregularities or suspicious activities to be further investigated.

At the same time, we use machine learning of historical contacts for every single domain based on large traffic that we get to analyze. We always take into account standard user behavior and all possible meta information that we can access from DNS communication logs.

Automated Phishing Analysis

We study newly registered domains and issued certificates and compare them with valid services and their domains to expose domains created or generated for phishing purposes. Our algorithms analyze both regular phrases and invisible metadata, including metadata from certificates. We analyze trends and patterns that cybercriminals use for the creation of hardly recognizable fake domains. This way, we get to block domains that trick everyday users by being similar to the services they use daily.

Whalebone Neural Networks

To constantly apprehend the activities of cybercriminals, we develop new technologies to both predict their next steps and react faster than humanly possible.

Whalebone DGA Sonar

Criminals often use domain generation algorithms (DGA) to prevent law enforcement from shutting down the rendezvous points of infected machines and command and control servers. They periodically generate large amounts of domains based on predefined rules that infected devices try to reach.

In collaboration with the Czech Technical University in Prague, we developed a unique neural network which can determine domains generated by DGA and predict domains to be generated in the future. This way, we always stay one step ahead.

Whalebone Virtual Analyst

Even though our Threat Intelligence Experts work meticulously to analyze suspicious domains, given the volume of the global traffic Whalebone handles, it is impossible to rely solely on manual work. That is why we have developed a powerful Virtual Analyst to help us.

This neural network mimics the behavior of a real-life analyst. It uses search engines to get more information about the domain, looks for articles that would discuss the domain, explores links to sandboxes, and makes qualified assumptions based on search results.

Whalebone Tunnel Block

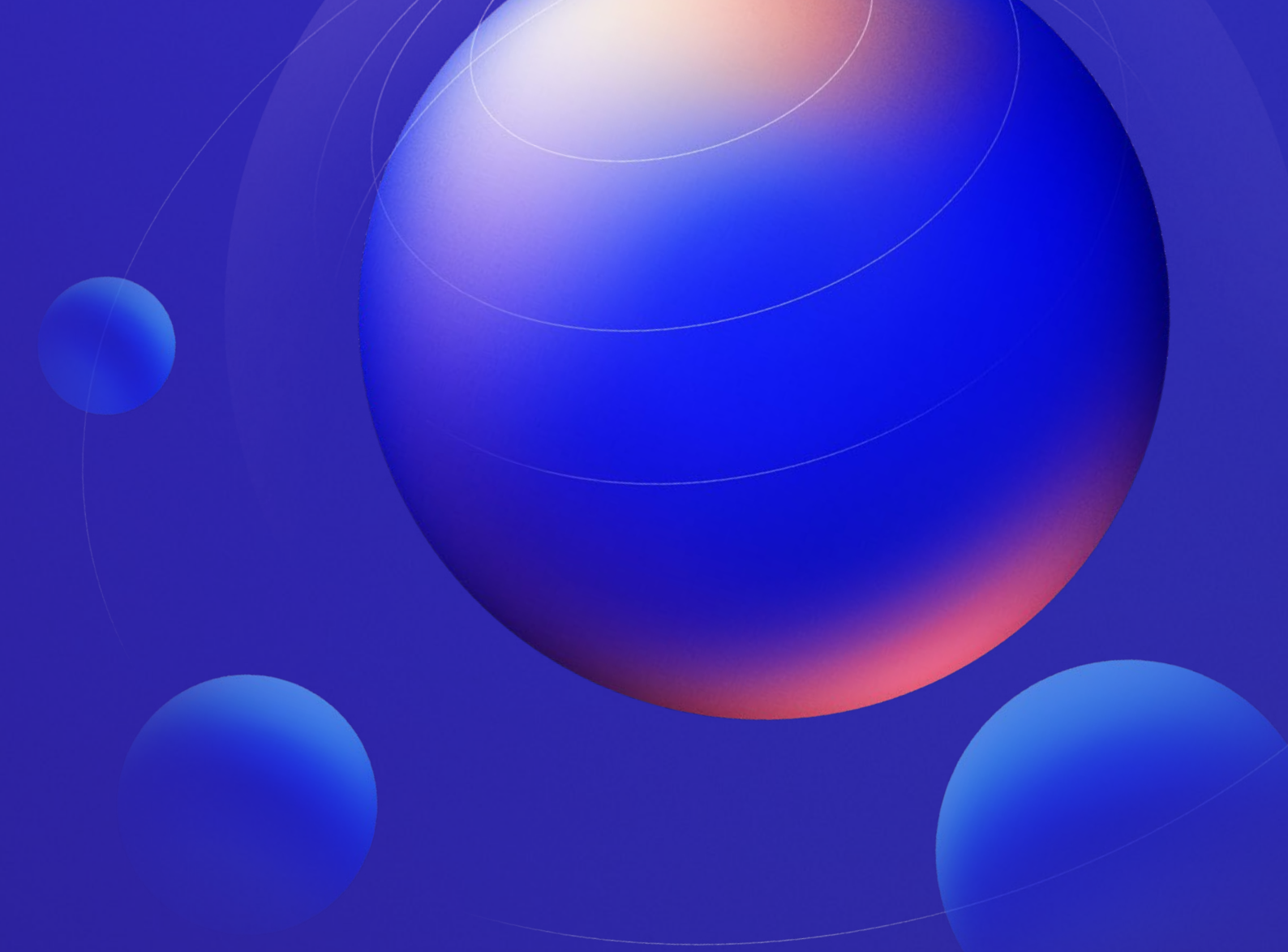
One of the very important malicious techniques that utilize the DNS protocol is so-called DNS tunneling. Hackers use DNS tunneling to smuggle encoded data in various formats through regular DNS communication.

Whalebone Tunnel Block is trained to block data exfiltration without disrupting the regular, harmless DNS resolution requests.

Dark Web Scouting Team

For our Identity Protection security layer, we have a dedicated team of specialists who daily explore both publicly available and hidden forums to keep our database of leaked credentials updated. At the same time, we inquire into data that was stolen by malware and mass dumps from malware, spyware, keyloggers, etc.

We prioritize privacy in storing all this information. For instance, we retain only the data indicating that leaked passwords were found, but not the passwords themselves. Occasionally, we may share parts of stolen credentials with end customers, ensuring that it poses no harm when stored.



Global Partnerships

We believe that #ConnectedMeansProtected – even when it comes to connecting R&D teams and utilizing the learnings of researchers from all over the world.

That is why we carefully choose, evaluate, and continuously test various partners and threat intelligence sources to ensure the best possible results.

Trusted Partners

We collaborate with vendors specializing in various fields and continuously analyze the landscape of potential partners.This process involves continuously scoring and reevaluating different sources whose quality changes over time for different malware types, regions, etc. To ensure the highest quality of the pool of sources, they need to be rigorously tested.

Apart from vendors, we also collaborate with takedown services that inform us about domains that have proven to be malicious.

Joint Research

We collaborate with universities and research institutes to move both DNS Security and Identity Protection forward. We participate in research projects when solving specific problems and continuously collaborate with universities such as the Czech Technical University in Prague and research institutes such as the Polish National Research Institute (NASK).

OSINT

Another source of information for our Threat Intelligence Engines are standard Open Source Threat Intelligence Feeds. We carefully evaluate their quality, particular strengths and weaknesses, to utilize them to their full potential. Apart from that, we also make use of other publicly available sources to run automatic analyses of online malware discussions — for example, we automatically analyze social media discussions to detect domains that are being discussed as malicious.

Regional Partnerships

While there are many global trends and campaigns in cybersecurity, the ability to zoom in and focus on localized Threat Intelligence is what makes all the difference when it comes to regional or specialized threats.

That is why we greatly focus on regional partnerships as well as systems and processes that enable local Threat Intelligence sharing. Most visibly, this affects our product for governments, Immunity DNS4GOV, and activities connected to DNS4EU, the European Union's initiative for securing critical infrastructure and services for Europeans, but these efforts have strong positive impacts on all of our products and services offered globally.

We work with Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), National Centers for Cybersecurity (NCSCs), and DNS4EU Consortium Members and Associated Partners that include: CZ.NIC (CZ), Czech Technical University in Prague/CVUT (CZ), DNSC (RO), NASK (PL), SZTAKI (HU), ABILAB (IT), DESEC (DE), TIME.LEX (BE), CESNET (CZ), F-SECURE (FI), Centro Nacional de Ciberseguranca (PT), and the Ministry of Electronic Governance (BG).

CERTs

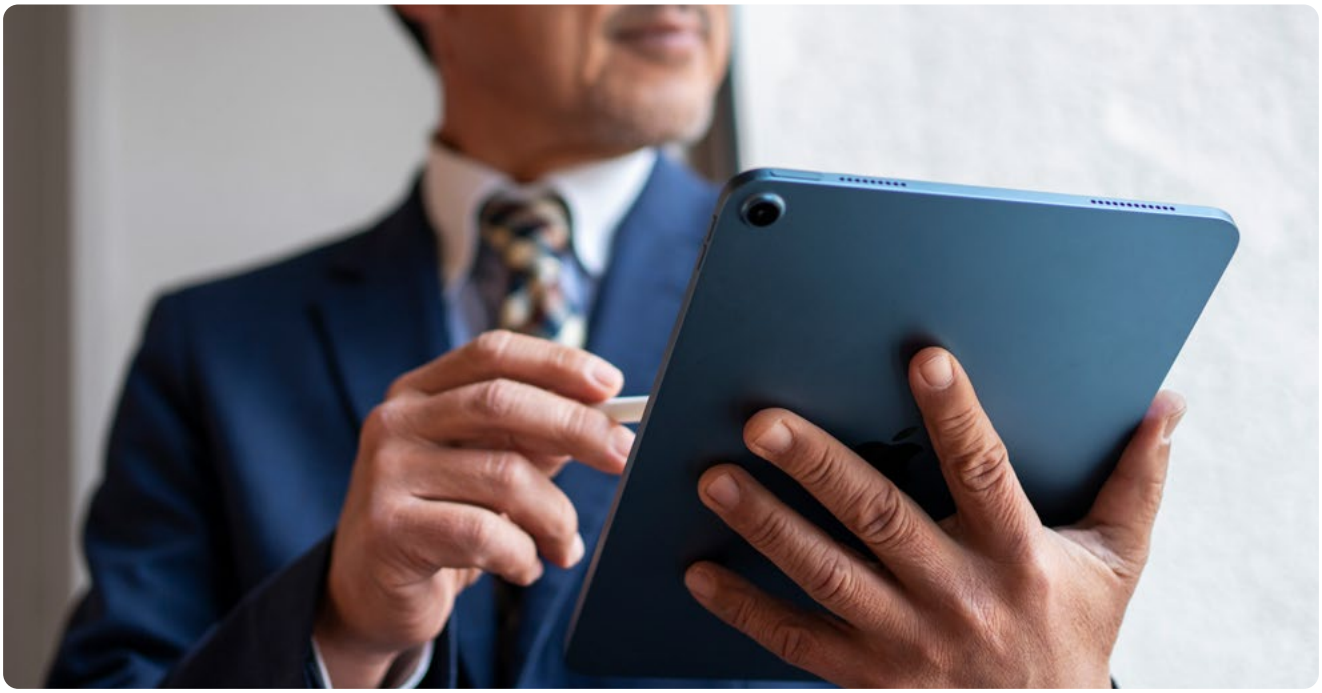
We actively establish relationships with local CERTs and other government agencies to improve our regional Threat Intelligence. Since we run DNS resolution for significant parts of populations of many countries due to our partnerships with telco operators, it is a mutually beneficial relationship. We provide a tool for CERTs to block malicious domains for many citizens, while our regional Threat Intelligence is enhanced.

Apart from that, we collaborate with CERTs when implementing DNS4EU.

European Commission (DNS4EU)

DNS4EU is the European Union's official secure and private DNS resolution for citizens, institutions and governments. We were tasked by the European Commission to lead the consortium responsible for the development and implementation of secure and privacy-compliant DNS resolution for European citizens and countries. To reach DNS4EU goals, we collaborate with ENISA, the European Commission, and lead a consortium of 11 key institutions from 9 European countries.

This project allows us to significantly improve our Threat Intelligence and collaborate with governing bodies on the improvement of the overall security posture of whole countries. Learn more about the project **here**.



Telco Fraud Prevention Teams

With the highest number of telco consumer cybersecurity deployments, our collaboration with hundreds of telco security experts cannot be overstated. Working together with internal teams of telcos significantly improves our threat intelligence.

For successful integration, we have a standardized methodology and many options for the connection of telco teams. At the same time, we are ready to accommodate our technology to telco capabilities for Threat Intelligence sharing and adjust both the processes and the system.

Regional OSINT

Wherever there are regional OSINT feeds available, we allocate resources and efforts to analyze them, evaluate their merit, and potentially properly integrate them into our existing algorithms. With the growth of regional campaigns tailored to specific audiences and regions, all sources for better regional Threat Intelligence need to be thoroughly evaluated and analyzed.

Crowdsourcing

We help many of our larger customers create options for their end users to report a suspicious activity. There are many tried and tested options available that we can help our customers with.

This way, regular consumers also participate in enhancing our Threat Intelligence and protecting their fellow citizens.

Whalebone Threat Intelligence Performance

To ensure the highest quality of our Threat Intelligence, we actively compare our engines with different cybersecurity vendors on the market, using data provided by impartial expert sources. We conduct regular testing to eliminate any deviation from our standard quality of service.

Furthermore, we regularly collaborate with AV-TEST GmbH, which is an independent German research institute for IT security. In collaboration with AV-TEST, we compare our products with relevant network security competitors. Whalebone consistently receives highly favorable results from all types of benchmark tests.

> “Whalebone is continuously delivering reliable protection with a near-perfect false positive rate.”
>
> **AV-TEST REPORT**

Read a detailed benchmarking report here ▶

FAQ

What is Threat Intelligence?

Threat Intelligence consists of collecting, analyzing, and interpreting data about current and potential cyber threats. This information is used to understand and anticipate cyberattacks. It enables proactive defense measures, allowing organizations and individuals to stay one step ahead of attackers and mitigate risks before they cause harm. In essence, threat intelligence transforms raw data into meaningful information that enhances cybersecurity readiness and response.

How often do you update the threat intelligence database?

We update our threat intelligence database in real time. Our systems continuously analyze data and propagate updates instantly to ensure the most current protection against new and evolving threats.

How would your Threat Intelligence target local threats in our country?

We collaborate with regional experts, such as local CERTs and internal security teams of telcos, to enhance our understanding of localized threats. This allows us to tailor our threat intelligence to address specific regional threats effectively.

How do you score the domains?

We use a combination of network traffic analysis, machine learning, metadata and historical data to evaluate the maliciousness of domains. Our scoring algorithms consider various factors to determine whether a domain should be blocked, ensuring high accuracy with minimal false positives.

Do you have honeypots or your own telemetry?

Yes, we use our own telemetry and deploy honeypots to gather data on potential threats. This proactive approach helps us detect and analyze malicious activities before they can impact the end-customers.

Do you work with user traffic? Anonymized or full?

We analyze anonymized user traffic to ensure privacy while still gathering valuable data for threat detection. This approach helps us enhance our threat intelligence without compromising user confidentiality.

What does the „AI“ in your detection engine do?

Our AI-driven detection engine leverages machine learning and neural networks to identify and predict threats more efficiently than traditional methods. It mimics human analysis, evaluates domain behavior, and predicts future malicious activities to stay ahead of cybercriminals.

You can read more about our AI modules in the Internal Research chapter.

Do you cluster botnets/ campaigns?

Yes, we identify and cluster related botnets, phishing and malware campaigns.. By understanding these connections, we can more effectively combat coordinated attacks and disrupt the operations of cybercriminal networks.

Can you stop newly observed domains? How?

Our system can block newly observed unknown domains in real time by analyzing patterns, metadata, and behaviors that are indicative of malicious activity. Our algorithms and AI models assess these factors to prevent potential threats proactively.\

How is this better than a PiHole?

While PiHole blocks ads and known malicious domains, Whalebone‘s Threat Intelligence offers advanced, real-time threat detection, machine learning capabilities, and regional threat analysis. Our solution provides a more comprehensive approach to cybersecurity, protecting against a wider range of threats with greater accuracy and up-to-date intelligence. On top of that, our products focus on user-centricity that allows mass adoption globally and hence protection of millions of everyday Internet users, while usage of tools such as PiHole is limited to more experienced users.

Conclusion

"Whalebone Threat Intelligence goes beyond keeping pace with the rapid evolution of cyber threats to anticipate and proactively protect against them. By integrating our deep internal research with insights from global and regional partners, we have crafted a dynamic, real-time defense system that evolves as quickly as the threats it counters."

ROBERT SEFR
WHALEBONE CTO

This is not just about staying ahead; it is about reshaping the battleground entirely, turning the tide in favor of those who rely on us for protection.

Would you like to discuss our Threat Intelligence with an expert?

Feel free to contact our Threat Intelligence Lead

Martin Stehlík
Whalebone Threat Intelligence Lead
martin.stehlik@whalebone.io
+420 608 438 928

Follow us

www.whalebone.io