Akili Bomba Cyber Security proposal

DRAFT

Table of Contents

Akili Bomba Cyber Security

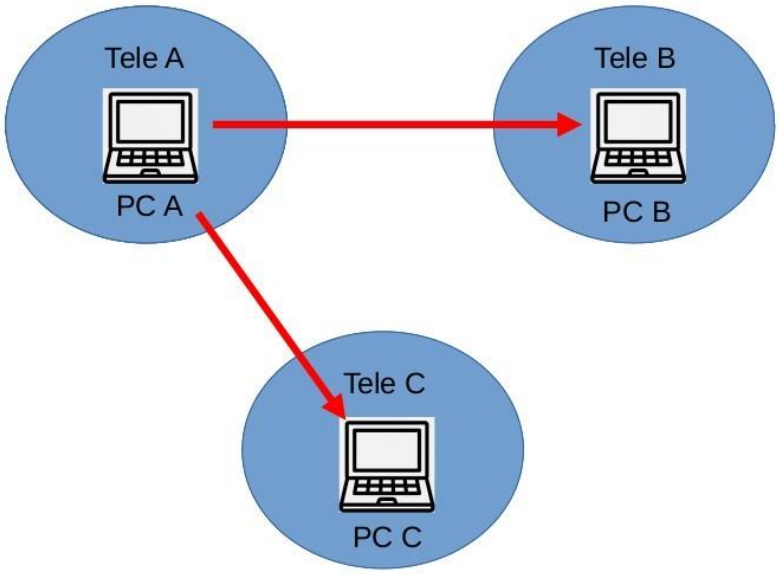
Akili Bomba is a local NGO in Kibra, Nairobi. Kibra is considered to be the biggest slum area in Africa. Over the last 3 years, Akili Bomba has worked with no governmental funding while helping people out of drug addiction and other mental problem with great success.

Cyber crime is a growing global problem costing the global society hundreds or billion USD annually. This could “easily” be rectified if the purpose was to solve the problem and not just profiting from it. We suggest Akili Bomba as the owner of such global secured network and are dedicated to making this a success. Below is a description of such network, how we’re planning to bring this about and how you can become part of this.

Conceptual description

It works like this:

- PC A is an infected computer inthe network of telecom company “Tele A”.
- PC A is used in an attempt toattack PC B belonging to Tele B. - The traffic is identifies as an attempt to hack by PC B’s firewall.
- The firewall informs Tele A thatit has been attacked by PC A - PC A is then used in an attempt to attack PC C
- Tele A wraps all traffic from PCA in a data package informing that this computer has been reported by others to be involved in attacks.



History of global cyber security

There is no doubt that there should be a global secured net. It has been tried before:

- America Online may have been the first attempt.
- IBM AS-400 was also an attempt to make a global secured network. But that fell with the growth or PCs.
- Microsoft NET was the next one. They came after Internet had matured enough to make it realistic. But nobody wanted Microsoft to “own” global security.

So why should anybody support Akili Bomba to do this job? There are a few organizations that could do the job. However, those IT corporations that would suffer financially from such net are probably so well invested there that they can easily prevent it from happening.
We think you should let us give it a try. And at the same time watch carefully how we’re doing it. If we don’t handle this in a good way, then a better alternative will emerge.

This document is explaining the full technology. Will someone steal it? We think it's great if they try. We will claim it's stolen and they will probably end up helping us. But that is up to our customers.

Consequences

Getting this implemented will be a big task. Gaining accept from the market will be an even bigger. But having a multiple billion USD market is normally a good foundation for generating good business. Our concept does it the smart way: The sending telecom company know who owns the infected computer and the receiver knows with 99.9% probability if it's legitimate traffic or not. The way it is being done today seems to be tailored to maximize the profit of the IT security industry without any care for the victims.

So what are the consequences if we are able to make this a global success?

- Once a computer is identified as infected, it can no longer be used in attack on computers belonging to partnering telecom companies
- Hackers will spend most of their energy on staying undetected and hacking will no longer be sustainable and will more or less stop.
- The value provided by partnering telecom companies will increase significantly and make "all" internet users who are interested in a safe connection switch to them.
- This will increase the pressure on non-partnering telecom companies and make the serious players join us.
- Those who lose will be criminals and IT security companies (they earn billions on the misery of others instead of implementing what's best for their customers)
- DOS attacks will also no longer be possible because companies can easily dismiss all traffic coming from infected computers. This can be handled automatically by telecom companies for servers that report abnormal traffic or too high load to us.
- Currently, telecom companies are reluctant to do "packet sniffing" because it's risky to start blocking traffic. By handling it our way, there's no spying or blocking of traffic and no other risk for telecom companies. They're just telling what others told them.
- With this system implemented, there will be less profit for the IT industry, but more for the telecom sector. However, there will be much more for those who partner. Those who don't will be left with scraps.
- All liberal societies are moving more and more to online solutions. This means that online security will (or at least should) be a major concern. This is especially true for countries that are new to this and have sparse resources. We are solving this. Meaning that societies can embrace this change.
- Cloud computing has seen huge growth. One concern with cloud computing is that you lock yourself to one provider with proprietary technology. If we gain trust as provider of online security, then we can tap into this market, either directly or with one or more selected partners. It is unclear what consequences our concept will have for this market isolated.

- Server hosting is definitely a market we can tap into – especially the high end market that is concerned with security
- Cyber security as a service is a market we should tap into with partners.
- Global cyber security will be handled from a few hubs, maybe East Asia, Africa and America to cover all time zones. This means that lots of people will go there to have a say and for educational purposes. This should generate lots of spin off effects.
- IP version 4 is very limited and the world should shift to IP version 6. Introduction of our secured network is likely to boost this transition. This will further enhance the security because we can report back to the network owner which computer in the network is infected (only the owner will know which computer it is).
- Our network will have huge consequences for how nations do cyber defense and war – which we would like to discuss further.
- This is an opportunity to introduce a global digital ID (including global secure login). This will be good for digital users but not so good for oppressive regimes - probably.
- Currently, the strategy of the IT industry is not on solving problems, but rather as profiteering on people's misery. By shifting to solving problems, we can also start addressing problems like unsecured WiFi networks and infected private computers and provide the best tools for free as long as that also benefits our goal of making Internet secured. This may include free anti virus tools and encapsulating traffic from unsecured WiFi devices and warning the owner when there's communication with infected unit or attempt to hack other units in the network. Honey pots should also be implemented in all networks to expose threats and make hacking units in the secured network unsustainable.
- This is just a start. It's a "shift of paradigm". There will be new ideas in the years to follow.
- There are organized crime actors involved in cyber crime that is also involved in other kinds of crime. Profit is re-invested in more advanced breach technology to stay ahead of their victims. Profit from cyber crime is also re-invested in human trafficking, drugs, it boosts corrupt regimes and other crimes that cause a lot of damage. Removing the profit from cyber would help on all of this.
- We will generate many new IT jobs. This is a good combination with our work on mental health because poverty and lack of hope is a major reason for mental health problems.

About Akili Bomba

"Akili Bomba" means sound mind in Swahili. Our brain has strong functions for "helping" us maintain focus. But when our focus turns dark or distracted from what we should do, then those very same functions easily become our biggest problem and may turn into any mental problem, lack of social skills or other challenges.

We think the solution to mental problems is gathering a group working together to solve our problems and find peace of mind. The best therapists are champions who have overcome their own mental problems and can motivate others to do the same. Our vision is to build what we call "wellness sanctuaries" all over the world. By mixing mental health with solving cyber security

challenges, we can also generate lots of high quality jobs that give hope and income for many poor families.

The task

For implementing our global system for securing Internet, we need partners who see the value of a secured Internet and are willing to be part of the team and get their name engraved in history. We're looking for IT security, telecom companies, big corporations, governments and universities.

Hopefully the HQ will be in Nairobi, Kenya with branches elsewhere. So if you have a view on this, then you should contribute. We especially challenge those located in Nairobi to position themselves on the right side of history. Cyber crime is an ever escalating problem that costs corporations hundreds of billion USD every year. The big paradox is that it can easily be solved if there's good will to do what's best for our customers and not just what brings most cash in short term.

What are we looking for:
- Technical assistance in developing core systems for telecom companies to secure Internet
- Financial assistance in exchange for good name branding and a seat at the table
- Any other advice or assistance is also appreciated. Please also tell us if we're wrong. Then we can focus elsewhere.
- If you're willing to look for the above, then you're also welcome – especially if you also want to do something for mental health.

Akili Bomba Advisory Board

Akili Bomba does not have any cyber security skills and is planning to govern this network through advisory boards all over the world where we're hoping to have representatives from universities, government and big corporations. As time goes by, the role may change, but in the start, it will also have to do a lot of the work on the ground.

We're starting in Nairobi, Kenya, but we also want to have such advisory boards elsewhere. So we are looking for people who are willing and able to connect us with universities, telecom companies, government and big corporations to make this also happen in other countries. Those who contribute will be compensated as soon as there's income in the specific country.

Cyber Security Core System

We're planning to developer an open source system (maybe to be closed later) that:
- Handles traffic between telecom companies with tagged traffic

- Lets corporate clients receive the original traffic (requirement for partners yet to be decided)
- Lets telecom companies receive notifications about attacks and tag outgoing traffic accordingly- Central DB and related systems for handling partners, false positives, reports and miscellaneous - Handles the interface between partnering and non-partnering telecoms and others.

How to connect

For now, our main communication channels are:

The Facebook group page "Mental health awareness and solutions" (click the link to join)

A whatsapp group called "Global Cyber Security" (click the link to join)

The core team

Felix Kokonya, founder and chairman of Akili Bomba CBO, +254 113068435 	Øystein Torsås Source of the idea. +47 99647892 	Leo Nancy Entrepreneur and IT professional. +254 726 325397 

Investment opportunity

Akili Bomba and Taransvar are non-profit organization. We don't have the capital to develop and launch this in an optimal way. So we are looking for financial partners who are willing to avail the necessary capital in exchange for a fair share of the future profit. Please contact us if you have any suggestion on this.

Modular system/project description

Introduction

This is just a draft for a document that is meant to evolve for as long as Internet exists. The intention is that each chapter becomes a separate sub project to be handled by separate project group. Such sub project may be assigned to a university or other external entity. Since this document contains strategic evaluations, it must be kept confidential unless otherwise decided by the board.

Definition++

- AB-router is whatever implementation we have of this system to be installed at telecom and other partners (clients).

- Client is whatever corporation or organization that has AB-router delivered by us
- Unit-ID is a unique ID assigned by clients that as good as possible uniquely identifies the sender unit or network (unlike IP/port, which may change).

What does already exist?

Modern routers and firewalls have advance features for inter-communication and encapsulation. This project may be more or less implementable with what already exists. This should be investigated. Speed will always be an issue, so using already optimized HW will significantly increase the speed.

Central DB design and implementation

There will be a global central database containing information about:

- Clients and their implementation of AB-routers (Akili Bomba routers).
- Presumed infected units for each partnering telecom

Communication between firewalls and AB-router

Most relevant firewalls will have functions for communicating with “Security Operation Centers” (SOC). For test/developement and to be able to provide services to SMB market, we may also develop such communication also for other firewalls.

Communication between AB-router and telecom routers

A key component in the system is that sending telecom companies link together traffic that comes from the same computer/network even when it’s assigned a new IP address/port. This will also distinguish presumed infected traffic from other traffic using the same IP pool, making detection of malicious traffic far more accurate. This will happen using a unique ID assigned by the sending telecom company that will follow that specific unit/network. We need to talk with telecom companies to figure out how this can be handled.

Internal comm central DB - AB-routers

The central DB and the AB-routers installed by any kind of client will form a virtual private network that will communicate closely. Should this be implemented as database calls to the central database or some other kind of IP packages?

Encapsulation

The AB-routers will have functionality for encapsulating traffic to (and from?) IP-ranges that are defined to belong to our secured network.

- What protocol should be used?
- What record layout should we use?
- Will the AB-router also handle traffic to and from non-clients?

System for administration of clients

This system will include (among other functions):

- Registration of clients
- Registration of AB-routers with IP-ranges defined as our secured network
- Billing information
- Security system – this is top level admin system

System for manual handling false positives and similar

There will be many false positives in the system. Any attempt to log in to a computer secured by a malconfigured firewall will end up as a false positive in this system.

Automatic system for handling false positives

Arificial Intelligence (AI) will provide significant information on what is legal traffic and what is not. This should probably be implemented somehow.

Certification of clients

To prevent abuse, there must be a system for certification in place for those implementing the ABrouters and also for any entity to receive encapsulated traffic.

Requirements for telecom companies:
- Unique (anonymous) identification

- Maintaining the system, communication lines and - Prevention of spoofing

Requirements for other entities:
- Confidentiality
- No kind of reverse engineering.
- We should not give this to just anybody. Reason why they need it should be given and also requirements for size, reputation and other operational criteria.

Electronic ID

Handling a global electronic ID would probably be a controversial topic. Many countries would probably not like it for good and bad reasons (we could start conducting global polls and there are of course also privacy issues)… There would also be many attempts to gain a fake ID.

Security as a service

We should think new on how we can provide a much wider range of security services than what was natural when the Internet was not secured.

We can offer complete login systems for any kind of computer system that include global ID and two factor authentication and handling of malicious attempts to login.

What about e-mail systems? We can make them secure by implementing two factor authentication and automatic spam-marking of e-mails sent from units that are not properly secured.

Systems for ordering filtering of traffic

DOS-attack is a major threat to web system and also a huge producer of garbage on internet. With our routers in place, clients can instruct other clients not to send specific traffic. This can potentially clean up lots of the garbage traffic on internet and thus limit the need for big investments.

Spoofing (fake sender IP address or email) should not be allowed. How is this currently handled?

Other possible spin off products

This concept will be shift of paradigm providing lots of spin off products. Most (maybe all) advanced IT products require security. By implementing a segment on internet where security and governance is implemented as core features, we make ourselves relevant to all future system development on Internet. Our main business is about fixing mental health globally. We’re a threat

to nobody except the cyber criminals and cyber crime profiteers (the IT security industry). So we are open to any kind of collaboration.

Any ideas?

- Consultancy
- Penetration testing (white hat hacking)
- Certification for white hat hackers, firewalls and other security products