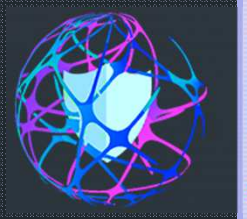


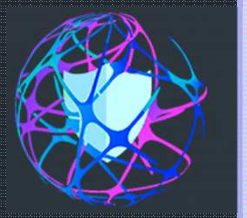
Bio morphis

Bio Morphic Perimeterisation Technology

Ransomware Eradication using Biomorphic Perimeterisation

Introduction

- *Types of Ransomware*
  - *Technology Perspective and Attacked Devices*
- *Ransomware Economy*
- *Security Conditions*
- *Biomorphic Perimeterisation*
- *How to generate a Biomorphic Perimeterisation*
- *Iimplementation Steps*
- *Mitigate Ransomware effects with Biomorphic Perimeterisation*



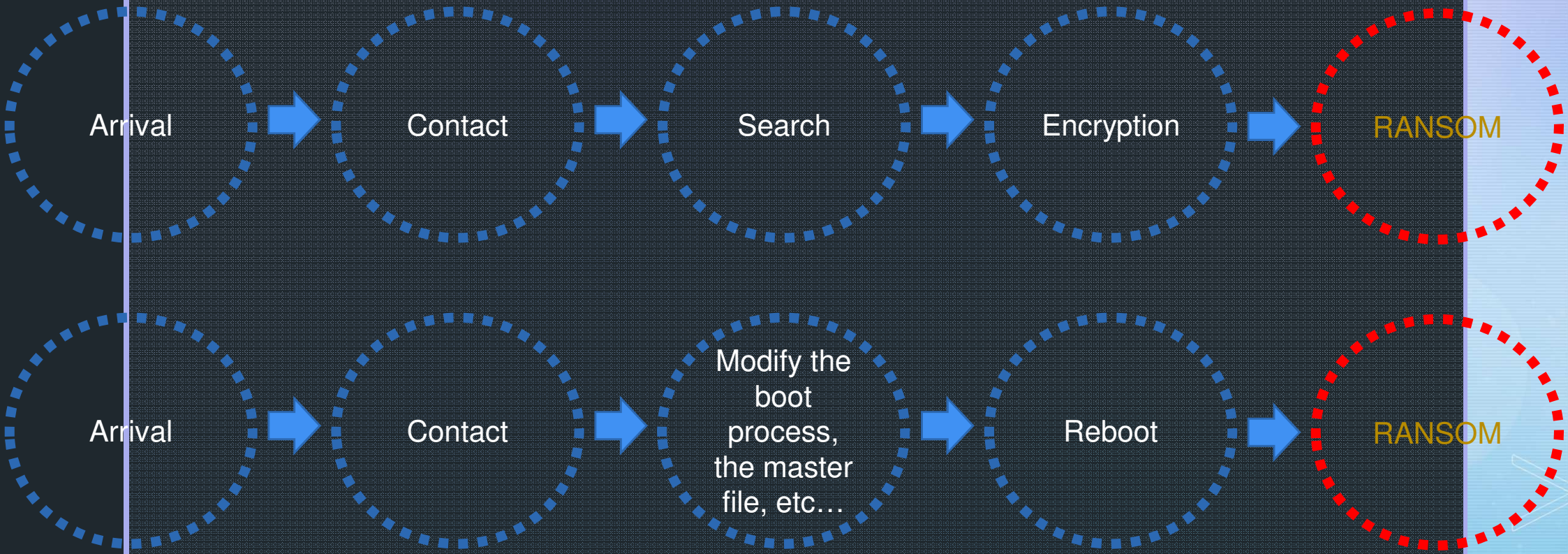
Bio morphis

Bio Morphic Perimeterisation Technology

Types of Ransomware

(Used Technology)

Ransomware in a nutshell



Types of Technology used for Ransomware

- **Encrypting ransomware**

  The attack utilized trojans that targeted computers. It propagated via infected email attachments, and via an existing botnets like Gameover ZeuS botnet; when activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, With the private key stored only on the malware's control servers. The malware then displays a message which offers to decrypt the data if a payment (through either bitcoin or a pre-paid cash voucher) is made by a stated deadline, and it will threaten to delete the private key if the deadline passes. If the deadline is not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in bitcoin. [2]

  Most Known encrypting ransomware

  - AIDS Trojan
  - CryptoLocker
  - Petya

Types of Technology used for Ransomware

- **Non-encrypting ransomware**
  Unlike the encrypting ransomwares, non-encrypting ransomware do not use encryption. Instead, they trivially restrict access by modifying the boot session, and asked users to send a premium-rate SMS to receive a code that could be used to unlock their machines. [1]

  Most Known encrypting ransomware
  - WinLock
  - Gpcode

1. http://searchsecurity.techtarget.com/definition/ransomware

Types of Technology used for Ransomware

- **Leakware (also called Doxware)**

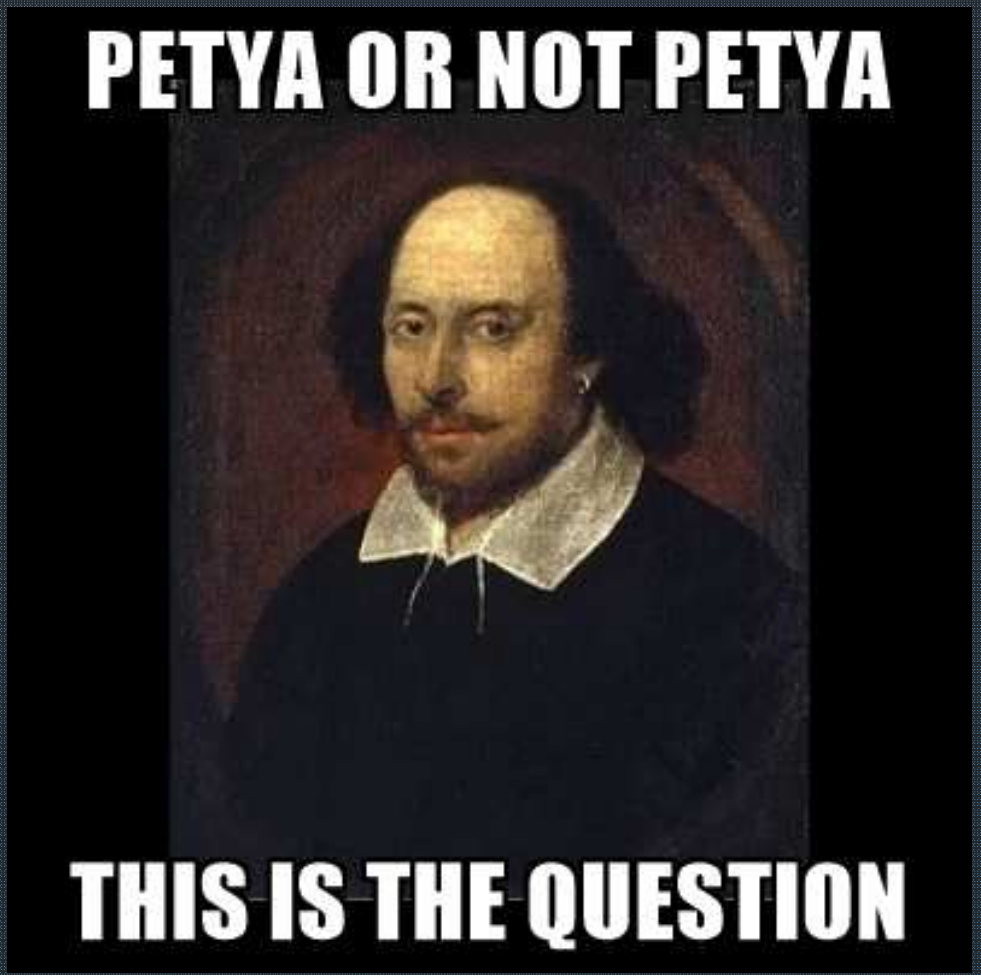
  The converse of ransomware is a **cryptovirology** attack invented by Adam L. Young that threatens to publish stolen information from the victim's computer system rather than deny the victim access to it. In a leakware attack, malware exfiltrates sensitive host data either to the attacker or alternatively, to remote instances of the malware, and the attacker threatens to publish the victim's data unless a ransom is paid. The attack was presented at West Point in 2003 and was summarized in the book Malicious Cryptography as follows, "The attack differs from the extortion attack in the following way. In the extortion attack, the victim is denied access to its own valuable information and has to pay to get it back, where in the attack that is presented here the victim retains access to the information but its disclosure is at the discretion of the computer virus“[4]

Most Known encrypting ransomware

- Popcorn Time
- WannaCry

4. https://en.wikipedia.org/wiki/Ransomware#Ransomware

The Not Petya Case

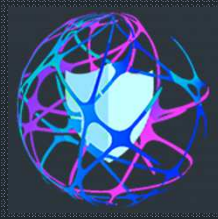


NotPetya isn't ransomware

NotPetya spreads on its own

NotPetya encrypt everything

You will never recover from NotPetya



Bio morphis

Bio Morphic Perimeterisation Technology

Types of Ransomware

(Device Target)

Ransomware Device Targets

Device Targets are Different

- **Computer Systems**
- **Smart phones and Tablets**
- **IoT**

Targets of Attacked Devices

- **Mobile**

  Mobile ransomware payloads are blockers, as there is little incentive to encrypt data since it can be easily restored via online synchronization. Mobile ransomware typically targets the Android platform, as it allows applications to be installed from third-party sources. The payload is typically distributed as an APK file installed by an unsuspecting user; it may attempt to display a blocking message over top of all other applications, while another used a form of clickjacking to cause the user to give it "device administrator" privileges to achieve deeper access to the system“[4]

  Most Known encrypting ransomware

  - Popcorn Time

4. https://en.wikipedia.org/wiki/Ransomware#Ransomware

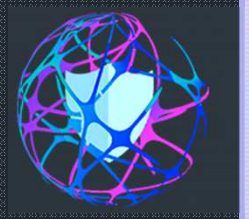
Targets of Attacked Devices

- **IoT**

  Smart devices are known to be a soft spot targeted by threat actors for various purposes. In August 2016, security researchers demonstrated their ability to take control of a building's thermostats and cause them to increase the temperature up to 99 degrees Celsius. This was the first proof of concept of this kind of attack, showing a creative way to put pressure on victims and drive them to pay ransom or risk consequences such as a flood or an incinerated house"

  In November 2016, travelers in the San Francisco MUNI Metro were prevented from buying tickets at the stations due to a ransomware attack on MUNI's network. In this case the attackers demanded $70,000 in BitCoins. In January 2017, a luxurious hotel in Austria was said to suffer an attack on its electronic key system, resulting in guests experiencing difficulties in going in or out of their rooms. The attackers demanded $1,500 in BitCoins. Whether or not this story is accurate, it demonstrates how creative this type of attack can get[11]

11. https://blog.checkpoint.com/2017/03/22/ransomware-not-file-encryption/



Bio morphis

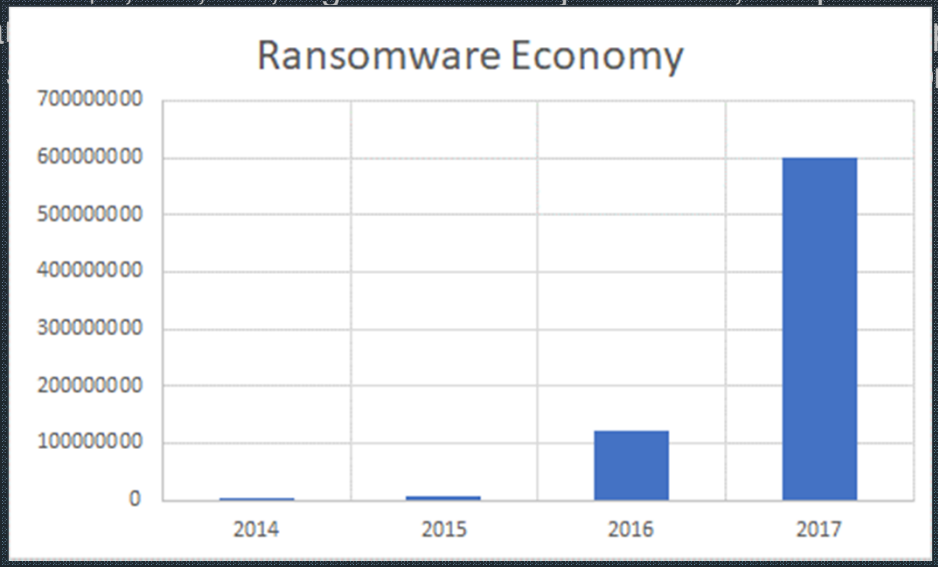
Bio Morphic Perimeterisation Technology

Ransomware Economy

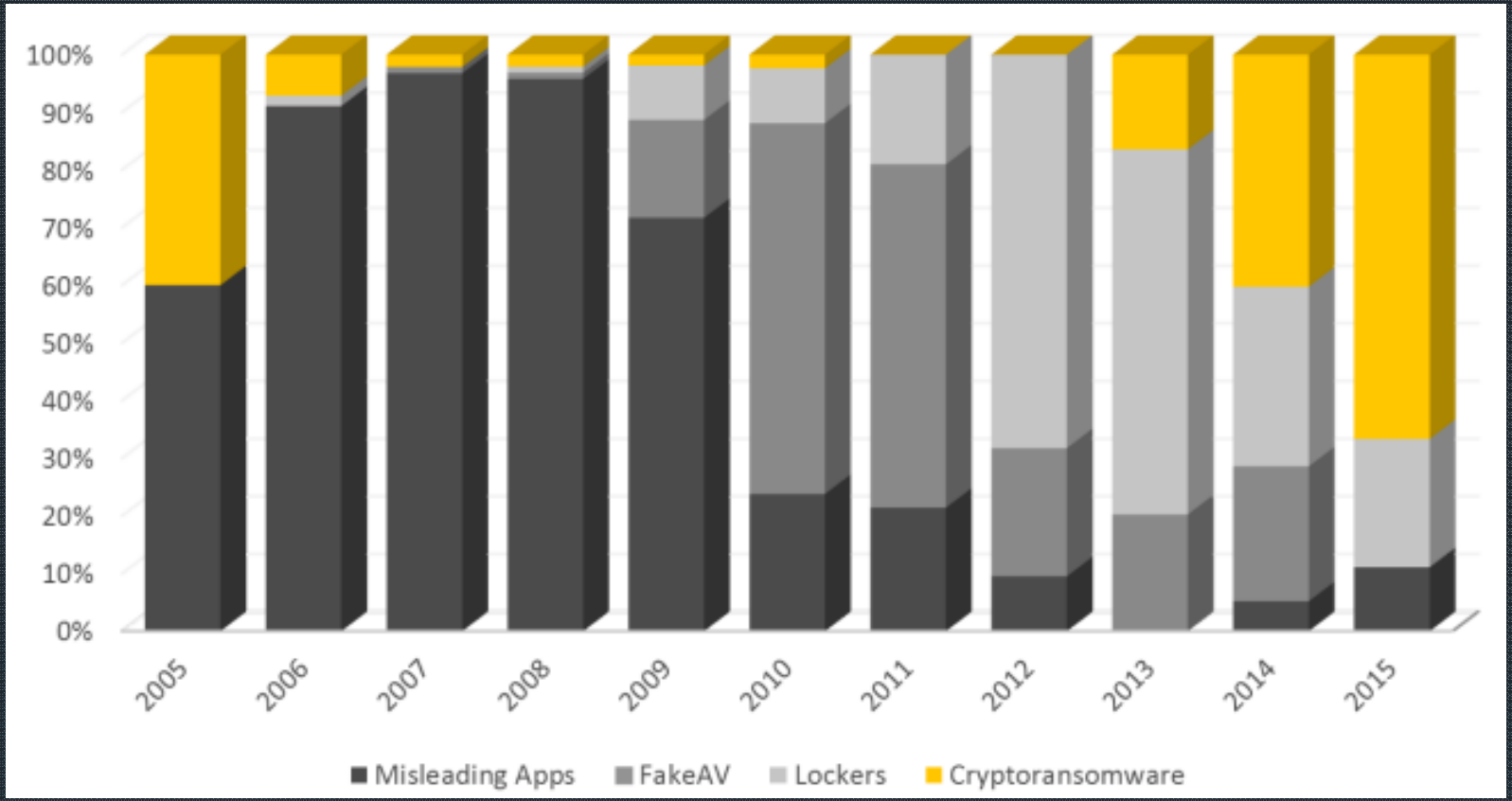
Ransomware Economy

- **Ransomware economy grows 2500 percent since 2016**

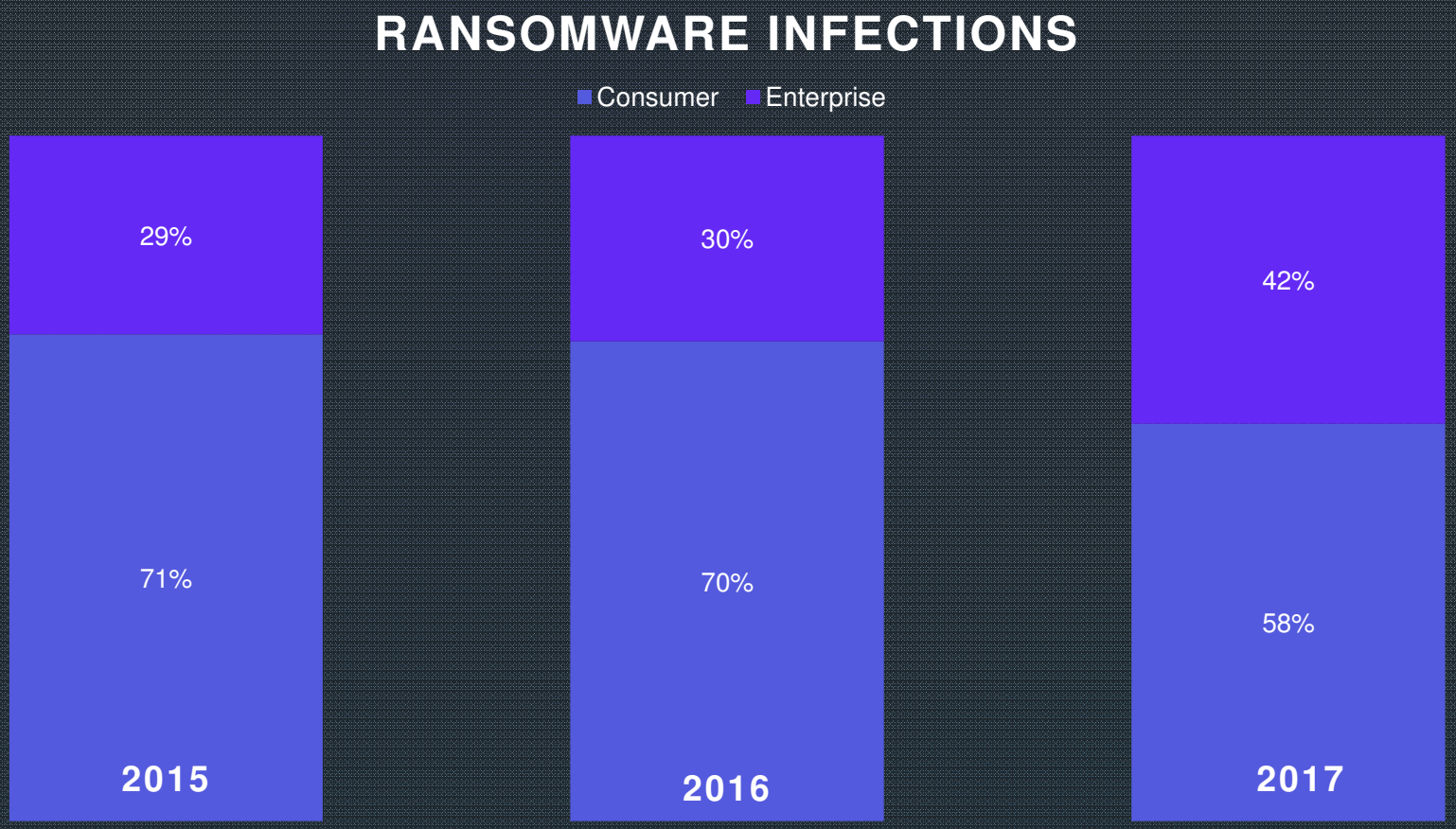
  Between 2016 and 2017 to date ransomware sales on the dark web have grown from $249,287 to $6,237,248, a growth rate of just over 2,500 percent. According to the FBI, ra p from $24 million in 201 r more annually..."[11]



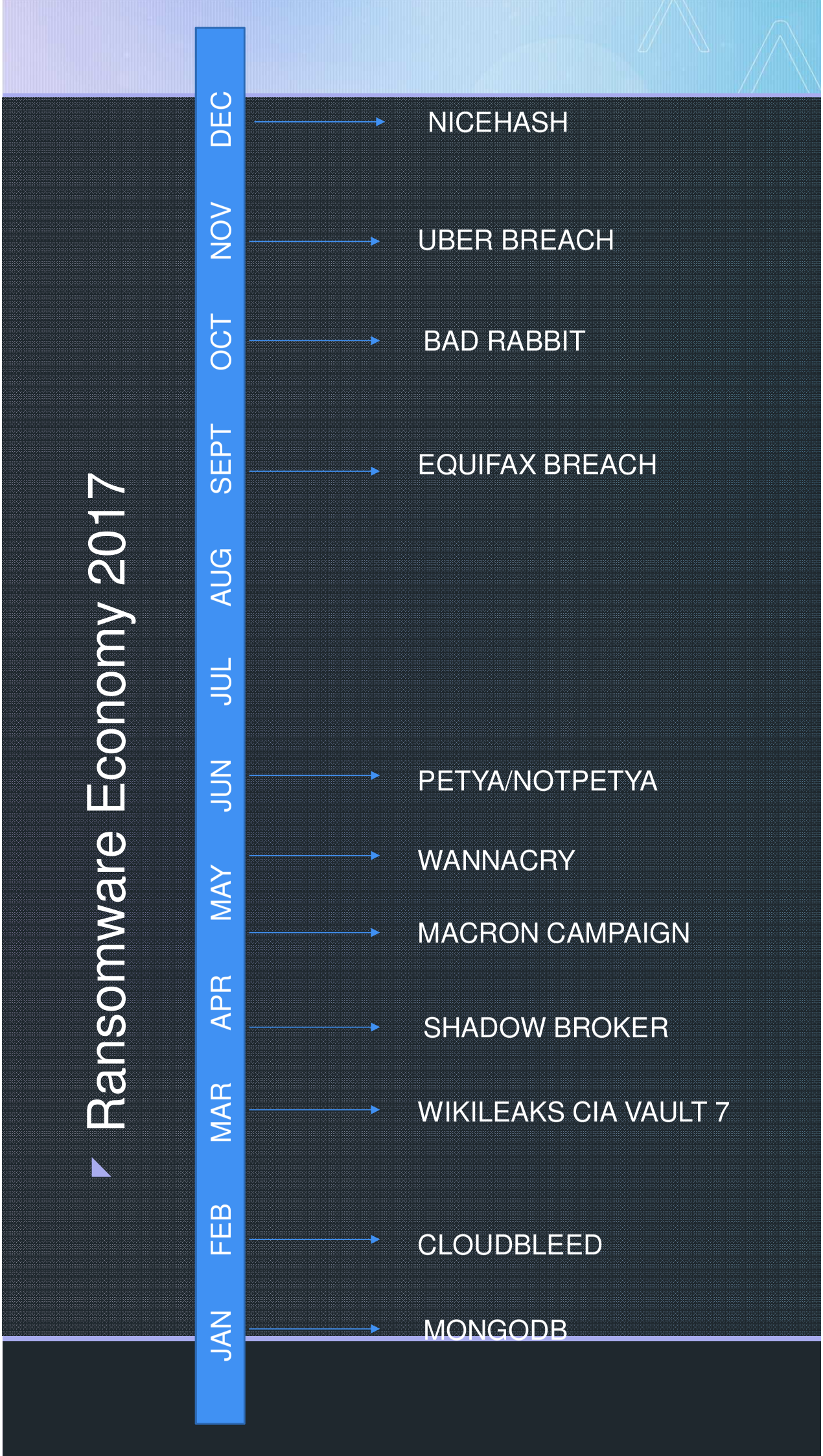
Ransomware Economy

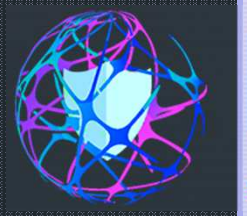


Ransomware Economy



SOURCE: SYMANTEC


Ransomware Economy 2017
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEPT
OCT
NOV
DEC
MONGODB
CLOUDBLEED
WIKILEAKS CIA VAULT 7
SHADOW BROKER
MACRON CAMPAIGN
WANNACRY
PETYA/NOTPETYA
EQUIFAX BREACH
BAD RABBIT
UBER BREACH
NICEHASH



Bio morphis

Bio Morphic Perimeterisation Technology

Security Conditions

Security Conditions

Security is based on assumptions that either are explicitly described, or implicitly assumed

- To respond correctly in a security issue:
  - *whether the posed question have been correctly answered*
  - *whether the right questions have been posed*

In most of the cases,

- People are answering correctly to the posed questions
- People do not pose the right questions

Security Conditions

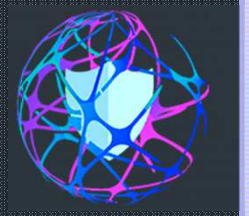
The right question is not:

- *How we can identify all exploits including zero-day exploits before any hacker or intruder invents them or install them in a computer system?*

The right question is:

- *How is it possible to maintain the systems most of the time safe and secure ?*

What will follows is a Paradigm shift



Bio morphics

Bio Morphic Perimeterisation Technology

Biomorphic Perimeterisation

Academic Approaches

Three academic approached propose improvement of Electronic Perimeter Protection:

- ***Deperimeterisation, Black Hat, Paul Simmonds, May 2004***
  A specific corporate policy for optimising corporate electronic perimeter, referring to Two Sided Triple Authentication as described in NIST-800 Handbook.

- ***Enforcing Policy at the Perimeter, SANS, Derek Buelma, June 2004***
  A specific corporate policy and architecture design for optimising corporate electronic perimeter, referring to security patches automation, Honey Pot strategies, and usage of Intrusion Detection Systems, Intrusion Prevention Systems and Vulnerability Management Systems.

- ***Fluctuant Perimeterisation, HES, M. Paschalidès, E. Viganò, March 05***
  A corporate dynamic policy generates electronic perimeter flexibility by dynamically modifying electronic perimeter, according to bioinformatics behaviour of evaluated micro-organisms and intelligent honey pot strategies.

- ***Biomorphic Perimeterisation, HES, M. Paschalidès,, October 11***
  Evolution of the Fluctuant Perimeterisation.

Principles of Enforcing Policy at the Perimeter

Derek Buelma has proposed Enforcing Policy at the Perimeter as follows

- ***Existence of a firewall and a firewall policy***
  - *Access control, including administrative access, access control lists, remote access, and physical security*
  - *Change management, including request protocol and response, firewall rule review and changes, and production review*
  - *Configuration management, including version control, security hardening, and vulnerability monitoring*
  - *Logging and alerting, including periodic risk assessment, audit logs, audit log reviews, audit log retention, access to audit logs, and alerts*
  - *Contingency planning*
  - *Architecture*
  - *Firewall banners*
- ***Existence of Intrusion Detection Systems***
- ***Patch Management and Need for Metrics***
- ***Existence of an Audit policy and respect of the Audit Policy***

Enforcing Policy at the Perimeter drawbacks

- ***VPS Issues***
  General purpose IP Sec / SSL VPN is the swiss-army knife of the security world

- ***Fortress Mentality Issues***
  - *Mobile computers*
  - *USB memories*
  - *PDA:s*
  - *Software*
  - *Internet access*
  - *Peer-to-peer*
  - *Voice over IP*
  - *Malware mail, viruses*
  - *Hacking tools*
  - *Ubiquitous Port 80*
  - *Remote execution*
  - *Remote access*
  - *Outsourced admin*

Principles of Deperimaterisation

Paull Simmonds of Jericho has proposed deperimeterisation as follows

- ***All devices should protect themselves***
- ***All devices should authenticate themselves***
- ***The data centre should be***
- ***Automation is the key to success***
- ***Keep network perimeter security such as conventional firewalls, but do not rely on them.***

T

Principles of Deperimaterisation

This means

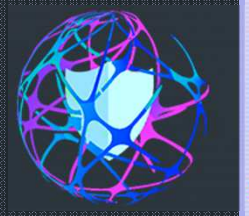
- ***Two-sided triple authentication of the user, software and device***
- ***Dedicated service provides AD user /group based filtering & anti-malware heuristics on all returned traffic***
- ***Existence of Macro-Perimeterised Services***

Deperimaterisation benefits

- ***Increased levels of Security***
  - *Connections to secure resources*
  - *Protocol-level authentication*
  - *Authentication to access individual secure resources*
  - *Secure protocol from device directly to secure resources*
- ***Network cost reduction***
- ***Simpler, less complex, more secure***
- ***Cheaper to run, easier to manage***
- ***Tomorrows technology with ability to gain business advantage***
- ***Flexible and adaptable solutions***

Deperimaterisation drawbacks

- ***Costs for security operations are increased****, because device protection requires more effort than perimeter protection. Patch management for 150,000 workstations and 4,000 servers is more difficult and time consuming than for one firewall, even if this process is fully automated. Dedicated service provides AD user /group based filtering & anti-malware heuristics on all returned traffic*
- *Protecting the networks using VLANs and VPNs requires* ***very intricate configuration*** *if the network must perform well and be secure at the same time. Managing a single firewall is far simpler. This means that managing deperimeterisation does involve a certain amount of additional risk*
- *Lots of* ***legacy machines*** *exist that* ***cannot be protected*** *or many applications hat will not work if you harden the platform, which means that* ***deperimeterisation cannot be implemented in one fell sweep*** *and requires careful and long-term planning*
- *Outsourcing and networked organizations are dynamic, making the* ***distinction of roles*** *in an organization difficult to define and maintain, which leads to* ***increased risk from social engineering attacks***



Bio morphis

Bio Morphic Perimeterisation Technology

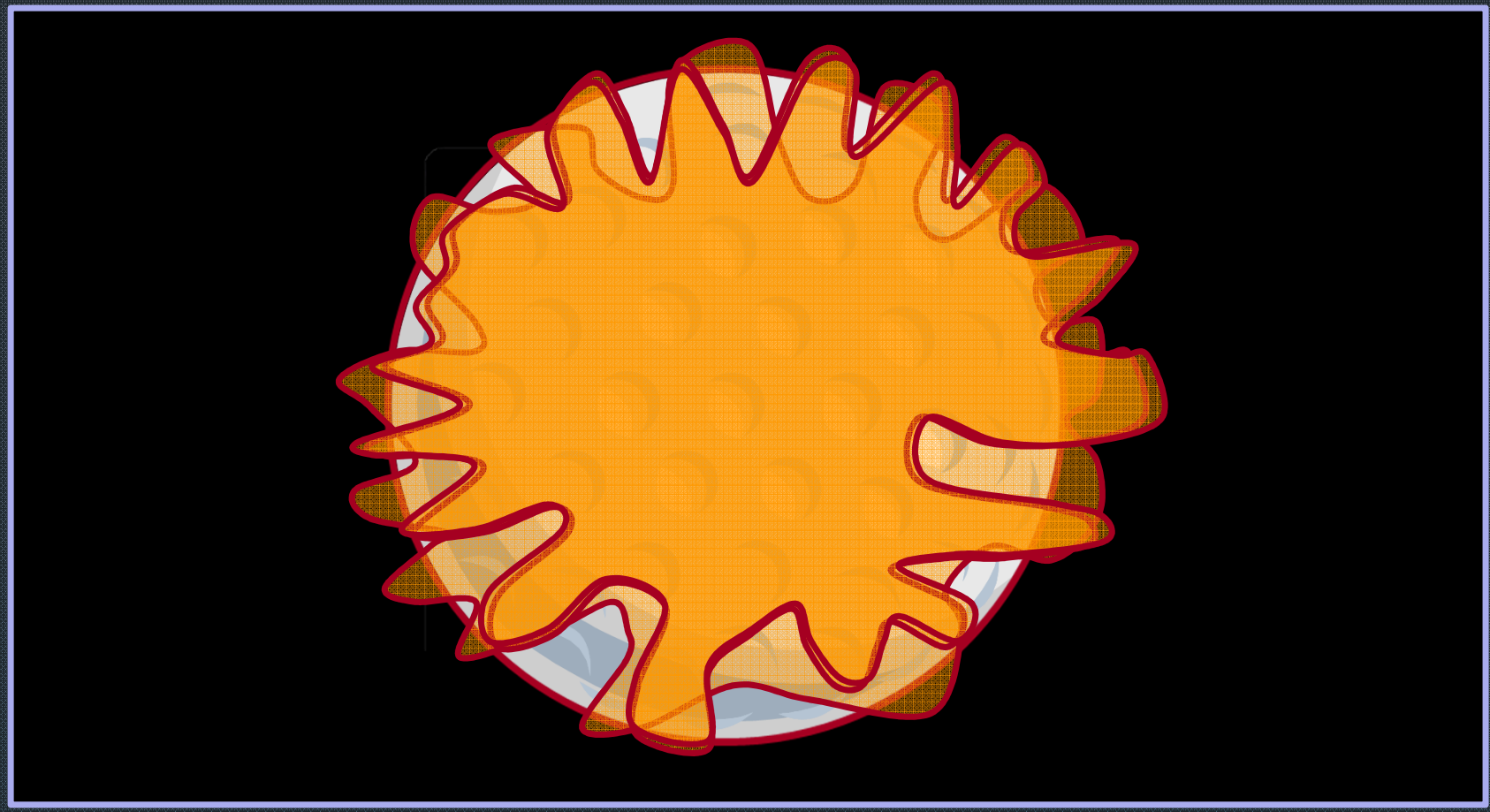
Fluctuant Perimeterisation

Fluctuant Perimeterisation

Fluctuant Perimeterisation is based on two principles

- ***HIV Immune System Principle***
- ***Fractalisation Principle***
- ***And will be based on Virtualisation***

Advanced Micro-organism Protection System



The Gateway Problem

Proposing a Fluctuant in Time Perimeterisation generates a handshake issue based on a gateway problem for any information that has to be pulled from organisation's electronic perimeter / demilitarized zone (DMZ).

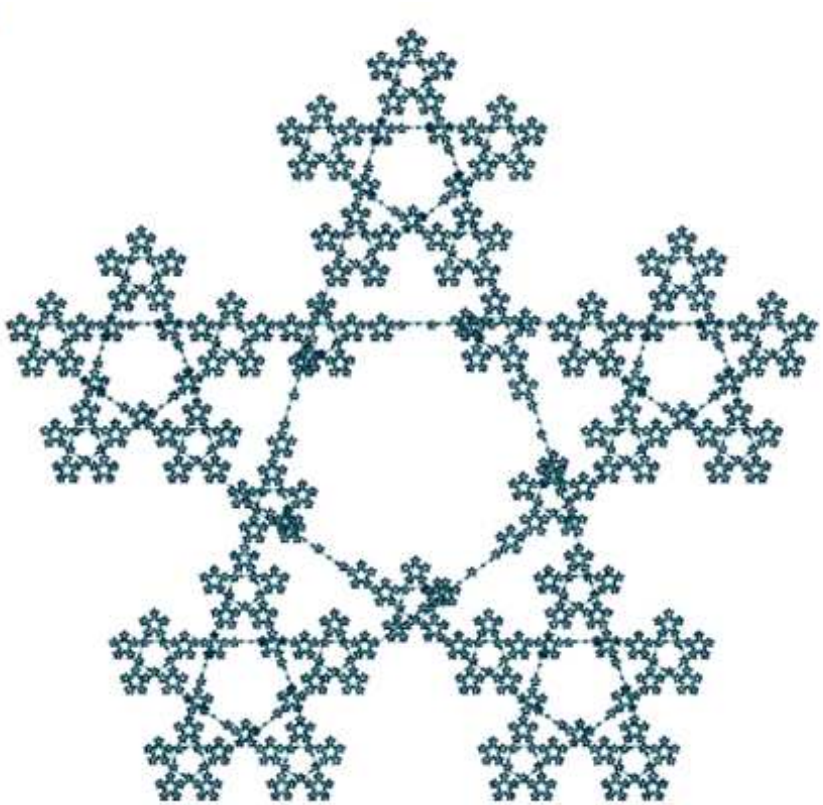
Because, in case the organisation decides to maintain a fixe gateway, the intruder can overpass the Fluctuant in Time Perimeterisation Security and attack organisation's electronic perimeter.

In such a case, the fixe gateway becomes the main problem of intrusion, that can be seen as a border condition issue of the internet model.

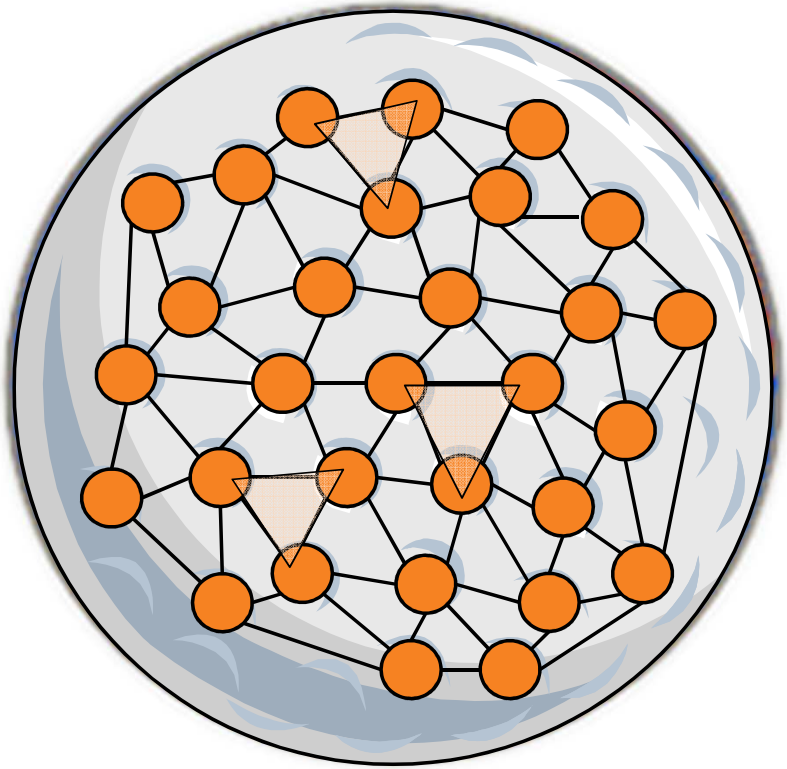
Indeed, Internet allows overcoming of a disruption of a specific node, a part from the borders.

The principal question is whether it is possible to avoid such border issues

Fractalisation



Internet Fractalisation



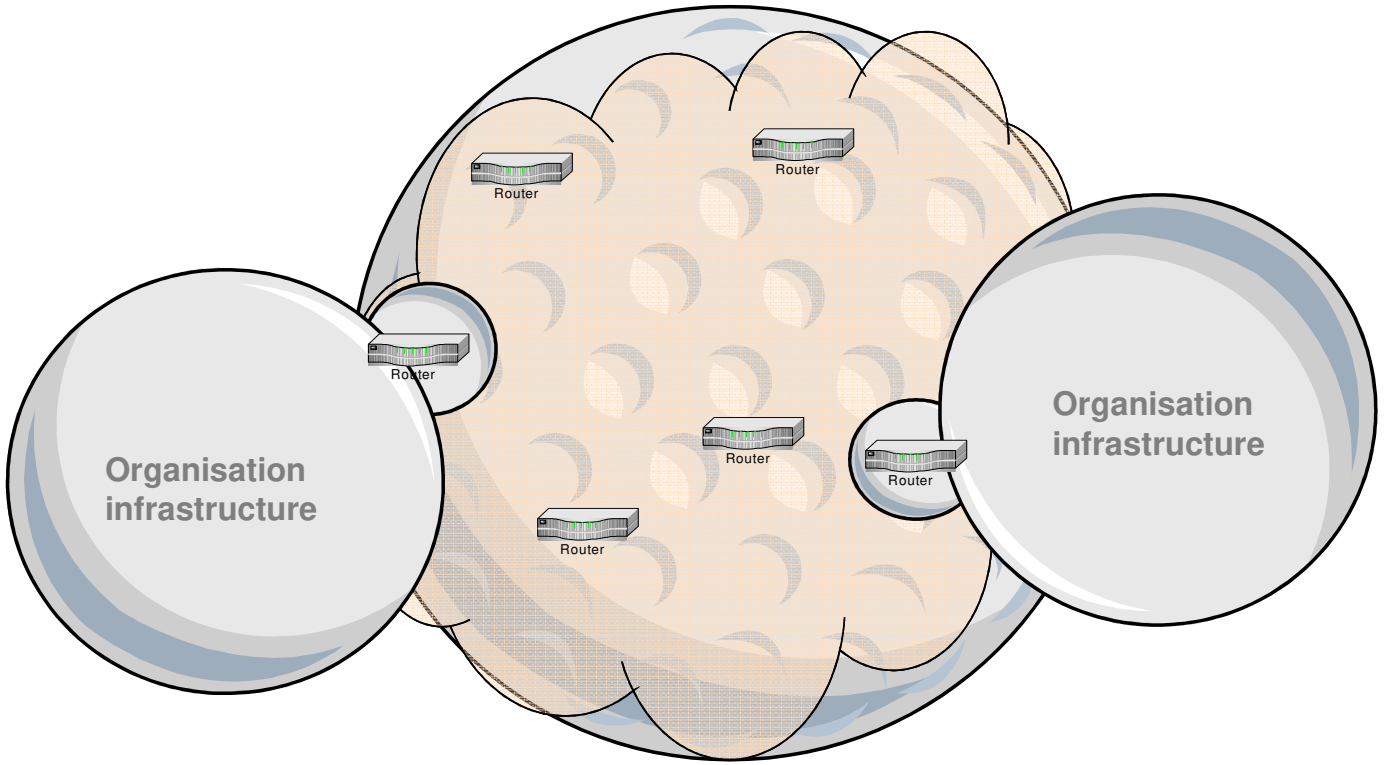
Internet Representation

Internet can be seen as a set of interconnected electronic devices (nodes).

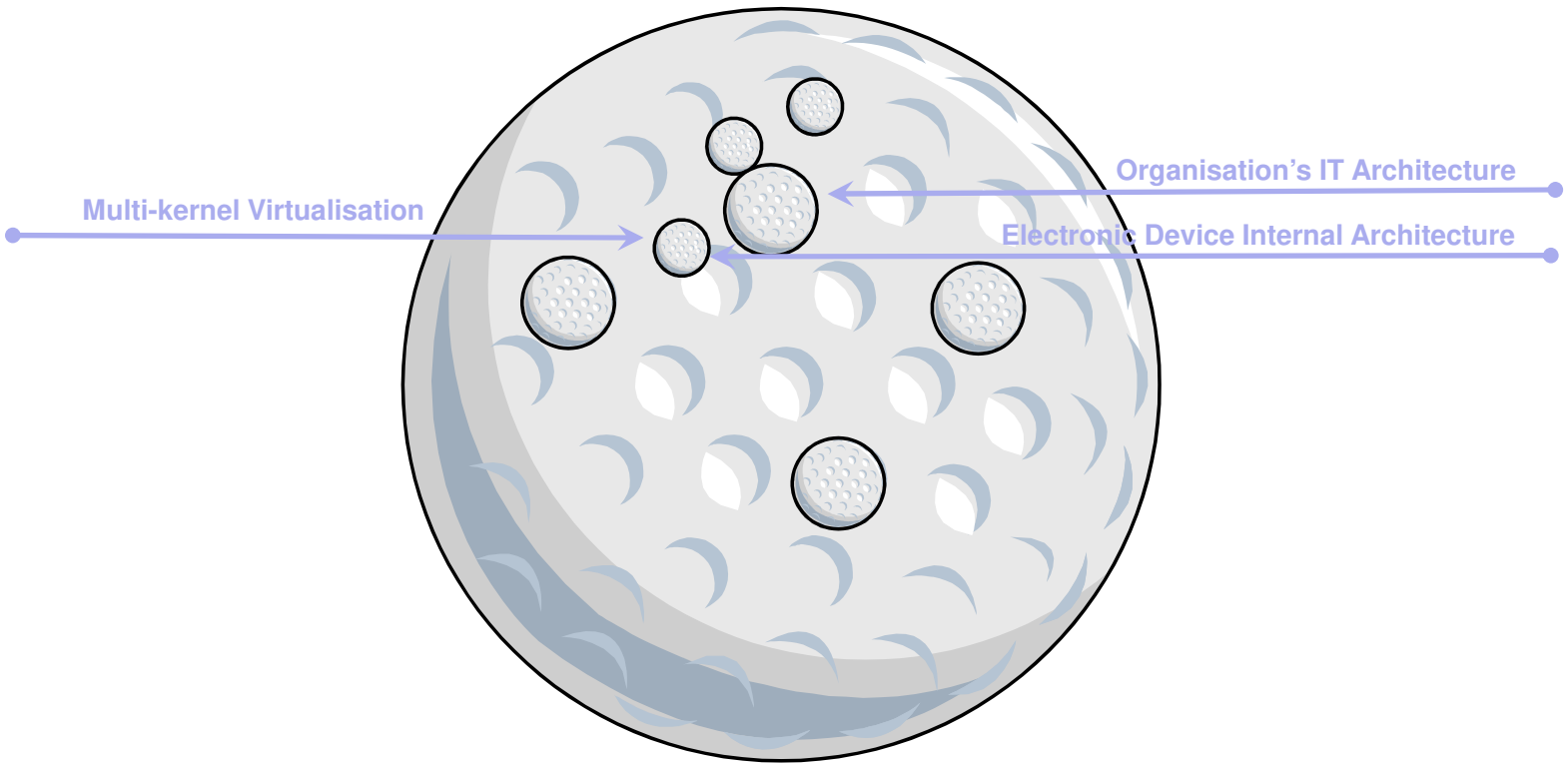
This interconnectivity avoiding all points of disruption is valid everywhere, a part from the ending points, (border effect).

From a geometrical perspective, these nodes present a triangular fractal behavior.

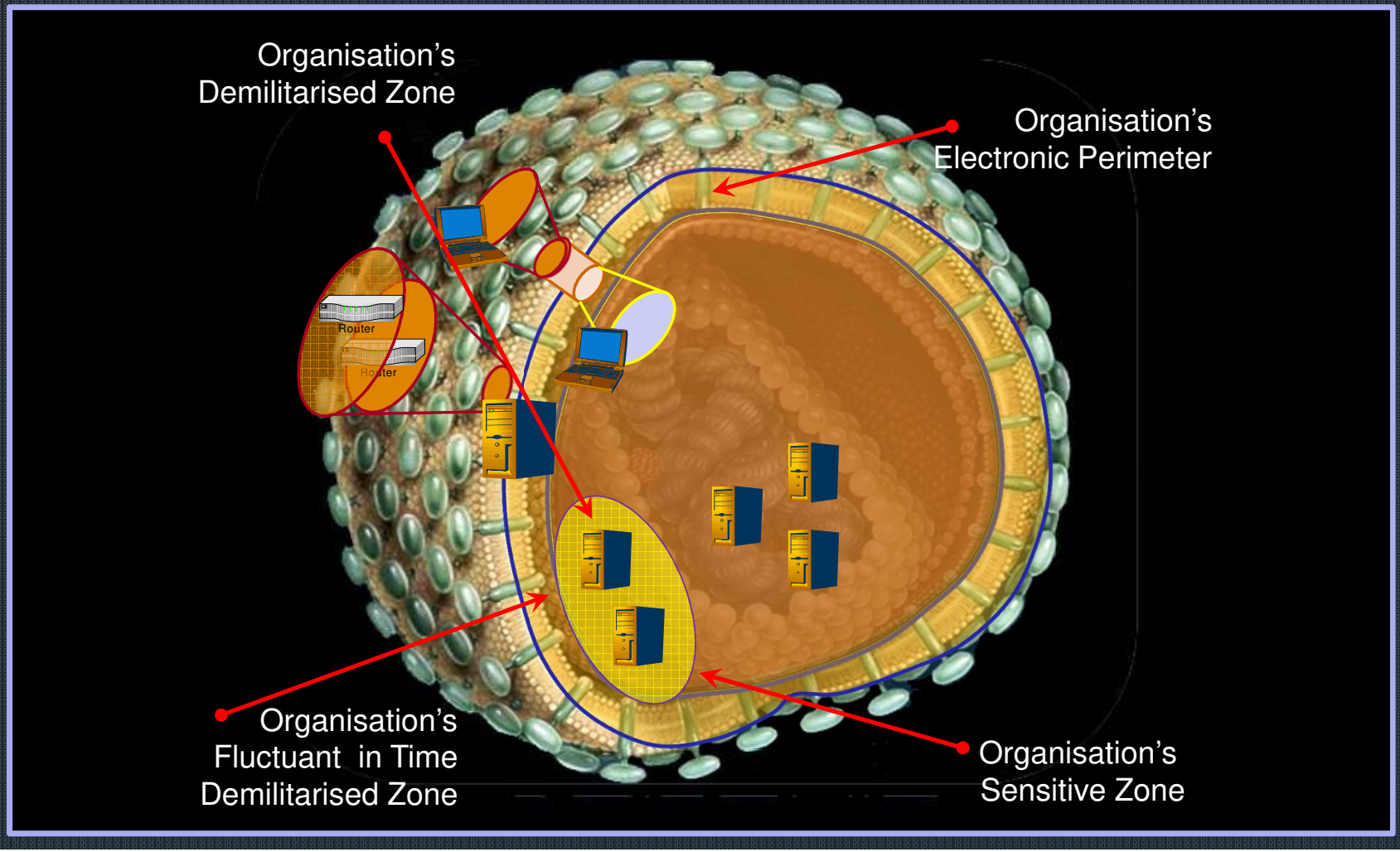
Internet Fractal Behaviour

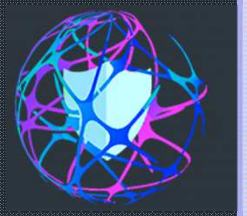


Extending Internet Fractal Behaviour



Fluctuant Perimeterisation Implementation





Bio morphics

Bio Morphic Perimeterisation Technology

Biomorphic Perimeterisation

Human Immune System

The immune system is a host defence system comprising many biological structures and processes within an organism that protects against disease. To function properly, an immune system must detect a wide variety of agents, known as pathogens, from viruses to parasitic worms, and distinguish them from the organism's own healthy tissue. In many species, the immune system can be classified into subsystems,:

- *the innate immune system*
- *the adaptive immune system, or humoral*

Macrophage function of Human Immune System

Macrophages are a type of white blood cell that engulfs and digests cellular debris, foreign substances, microbes, cancer cells, and anything else that does not have the types of proteins specific to healthy body cells on its surface in a process called phagocytosis. These large phagocytes are found in essentially all tissues, where they p potential pathogens by amo vement. the innate immune system

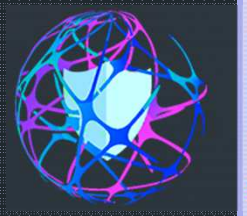
From Fluctuant to Biomorphic Perimeterisation

Biomorphic Perimeterisation is

- *HIV like immune system*
- *Fractalisation*

Plus

- *Human Immune System macrophage function*



Bio morphics

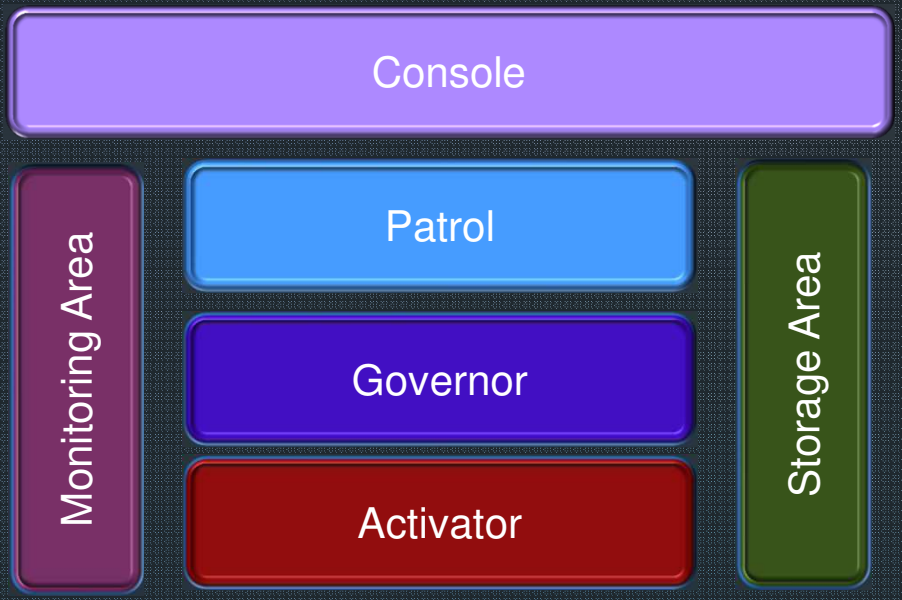
Bio Morphic Perimeterisation Technology

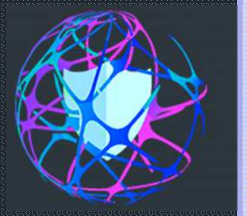
How to ganarate Biomorphic Perimeterisation

System Architecture

The system is based on the following components:

- *Patrol systems*
- *Governor*
- *Activator*





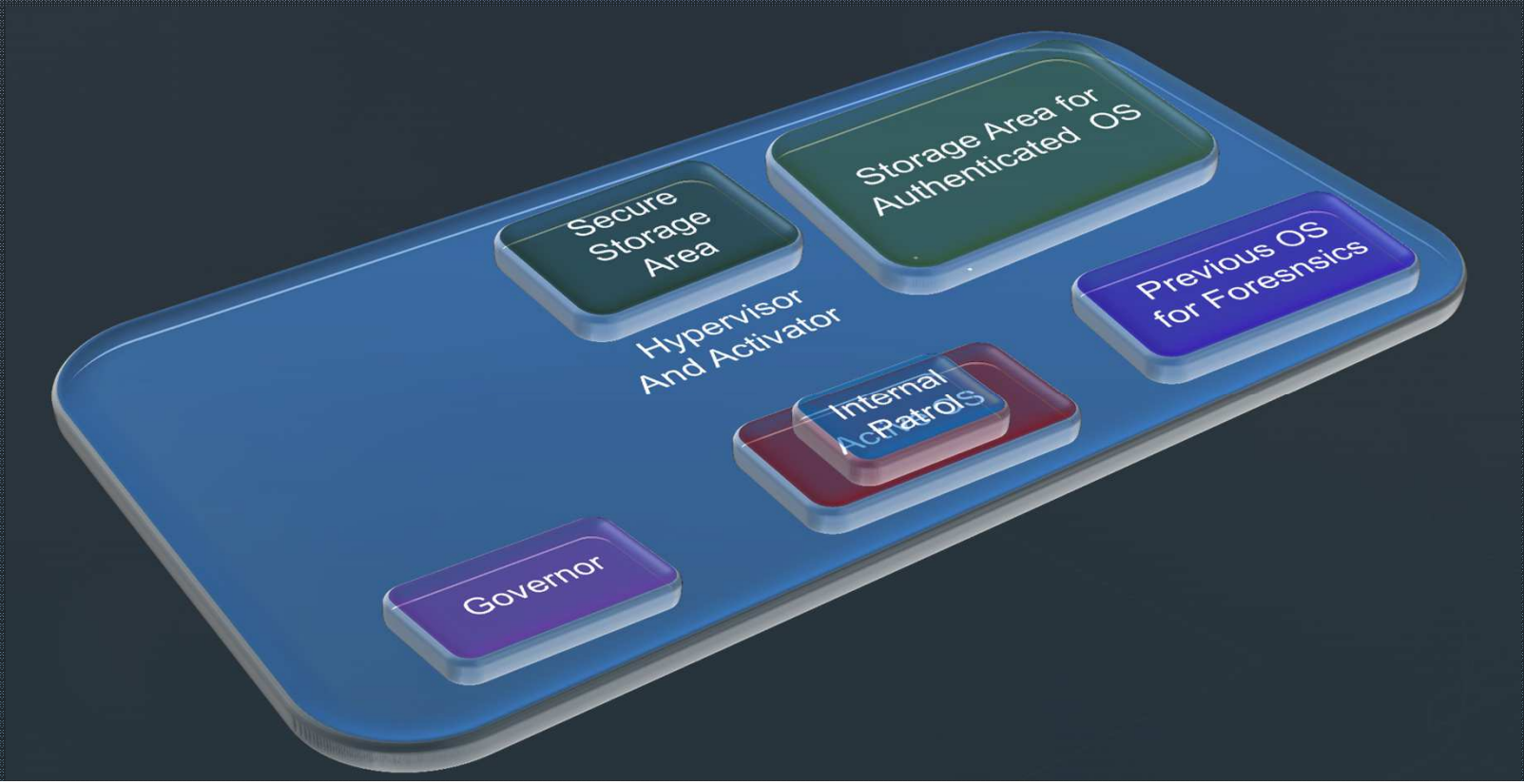
Bio morphics

Bio Morphic Perimeterisation Technology

Biomorphic Architecture

The System

Hypervisor and Virtualisation are key issues for



The Patrol

The Internal Patrol agent monitors all modifications effectuated in:

- *Files*
- *Database fields*

And

- *Store them in Secure Storage Area*

The Governor

The Governor System controls whether the Active Operating System is responding

Whenever the Active Operating System is no longer responding,

- *he sends a message to the Activator System, so to inform the end user that the system is no longer answering*

The Two Activation Solutions

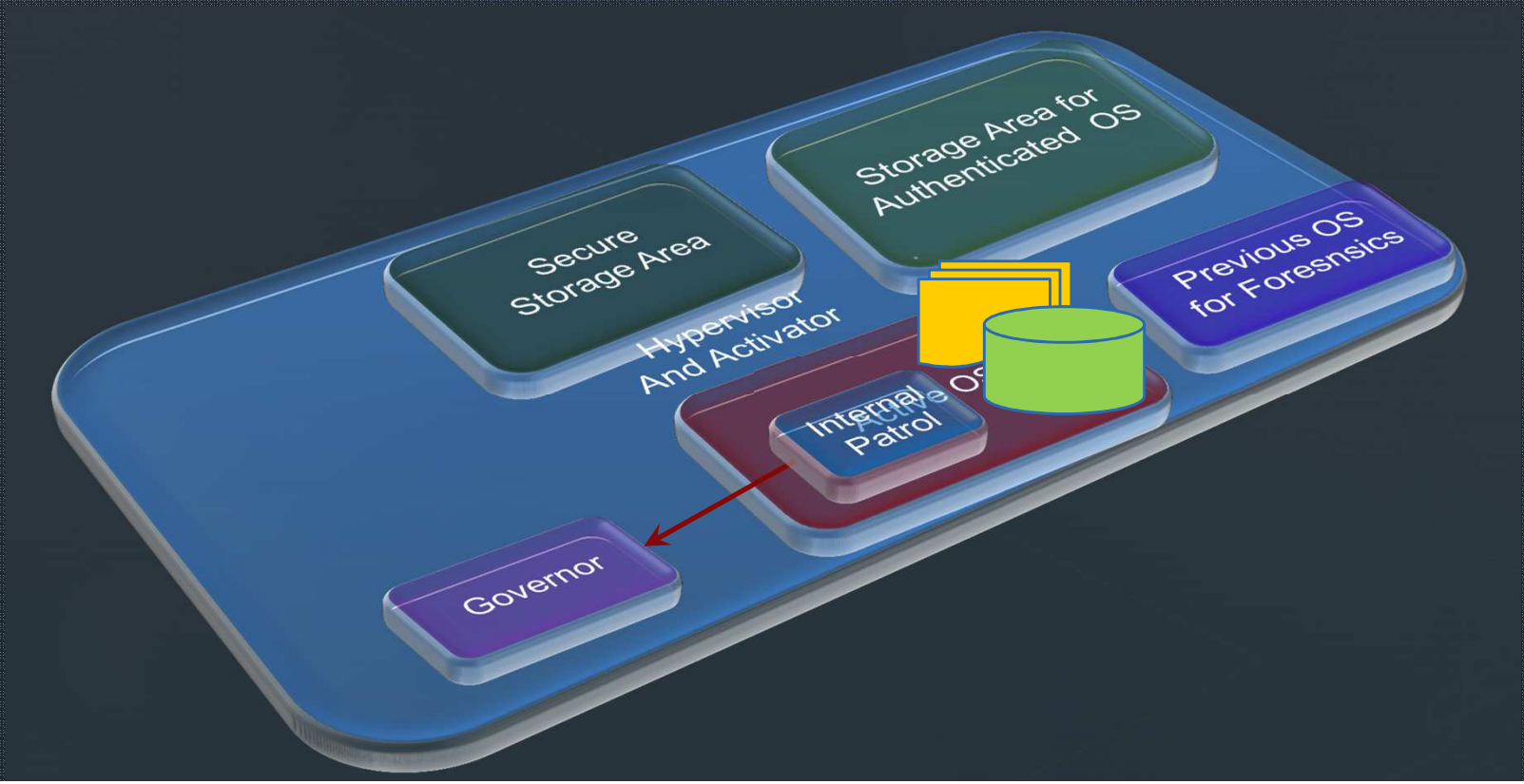
There are two way to rebuild the system after a Ransomware attack :

- *Either restoring a full backup (Software, license and initial data) and the incremental data backup*

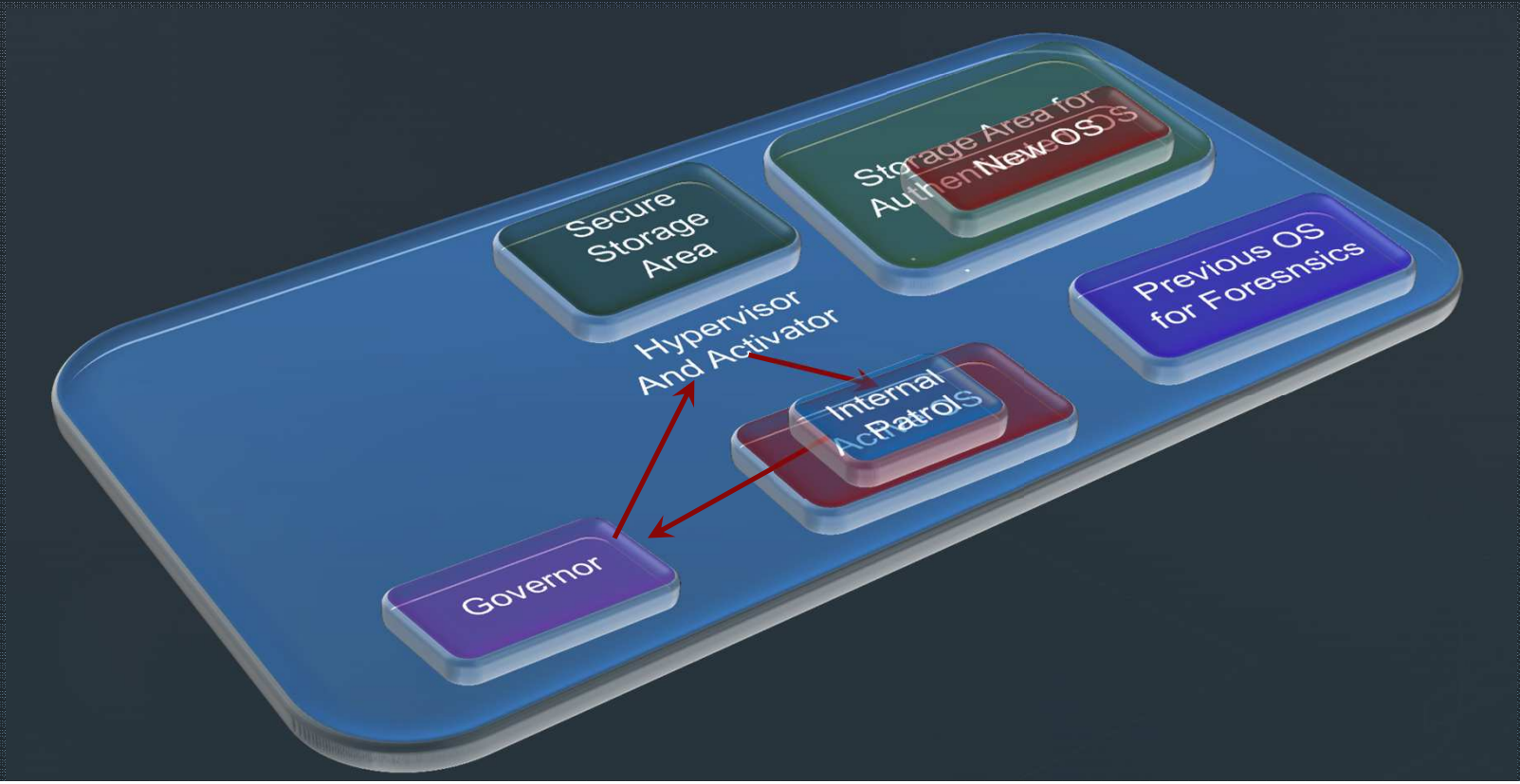
Or,

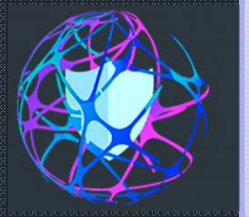
- *An initial data backup and then the incremental data backup installed in a new system*

How the System Works Normally



How the System Works in case of an Attack





Bio morphics

Bio Morphic Perimeterisation Technology

Implementation Steps

Initial Step

Provide a backup of the system in time T

Either

- *Full Backup (Software, License, and Data) in Time T*

or

- *Data Backup in time T*

Intermediate Steps

Provide an incremental backup of the data for the system in times dT

This incremental back up includes

- *Files and Folders*

and

- *Data base tables and fields*

Final Step

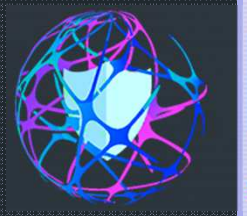
When your system has been corrupted by a Ransomware

Either come with the old system and effectuate

- *Initial Full Backup (Software, License, and Data) in Time T*

and

- *Incremental back ups*
  - *Folders and Files*



Bio morphis

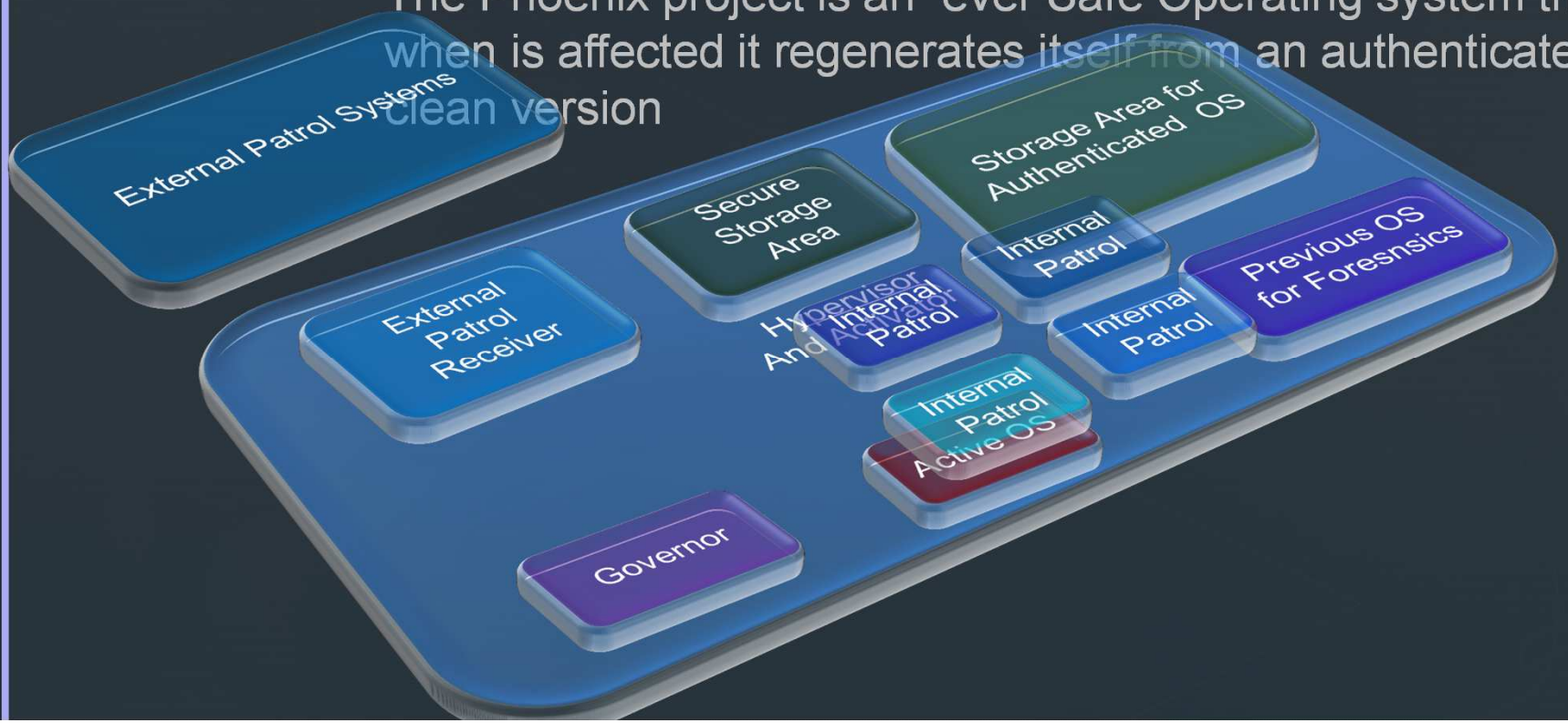
Bio Morphic Perimeterisation Technology

Next Visionary Steps

The Phoenix Project

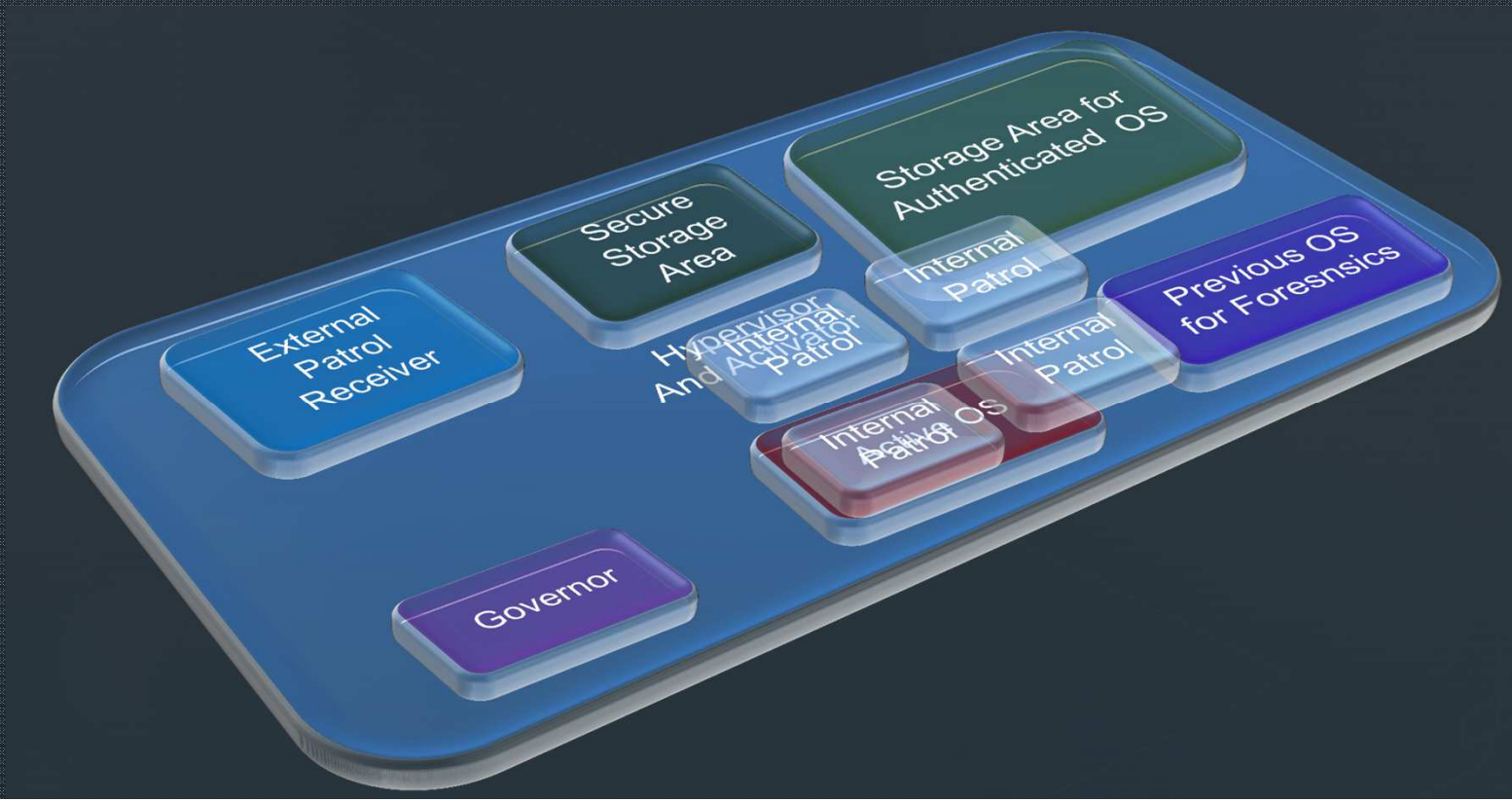
- **An Immune Operating System Recovering Every Time from its Infection**

The Phoenix project is an ever Safe Operating system that when is affected it regenerates itself from an authenticated clean version



The System

Hypervisor and Virtualisation are key issues for



Bio morphics

Bio Morphic Perimeterisation Technology

Conclusion

Biomorphis

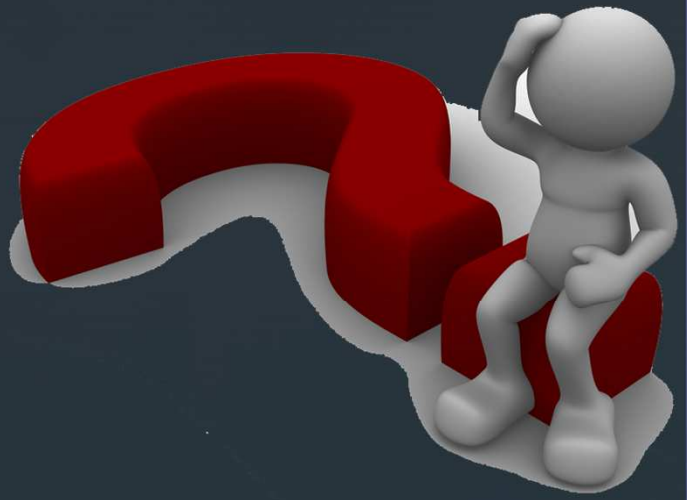
Proposes a solution which is a Paradigm Shift

- **An Immune System that recovers every time from its Infection, a System that never dies as it reborn from its ashes**

- **An Immune Operating System Recovering Every Time from its Infection**

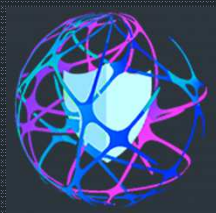
  The Phoenix project is an ever Safe Operating system that when is affected it regenerates itself from an authenticated clean version

Questions



Bio morphics

Bio Morphic Perimeterisation Technology



Bio morphis

Bio Morphic Perimeterisation Technology

Contact

- info@bio-morphis.com