Active Defence
@
European Economic & Social Committee

Dimitrios Margaritis

IT Security Officer EESC

Few questions

1)What is Active Defence? Many definitions available...

2)What are the components of Active Defence and what they add to my existing security operations

3) Do I have to be in a high security maturity level to start with Active Defence?

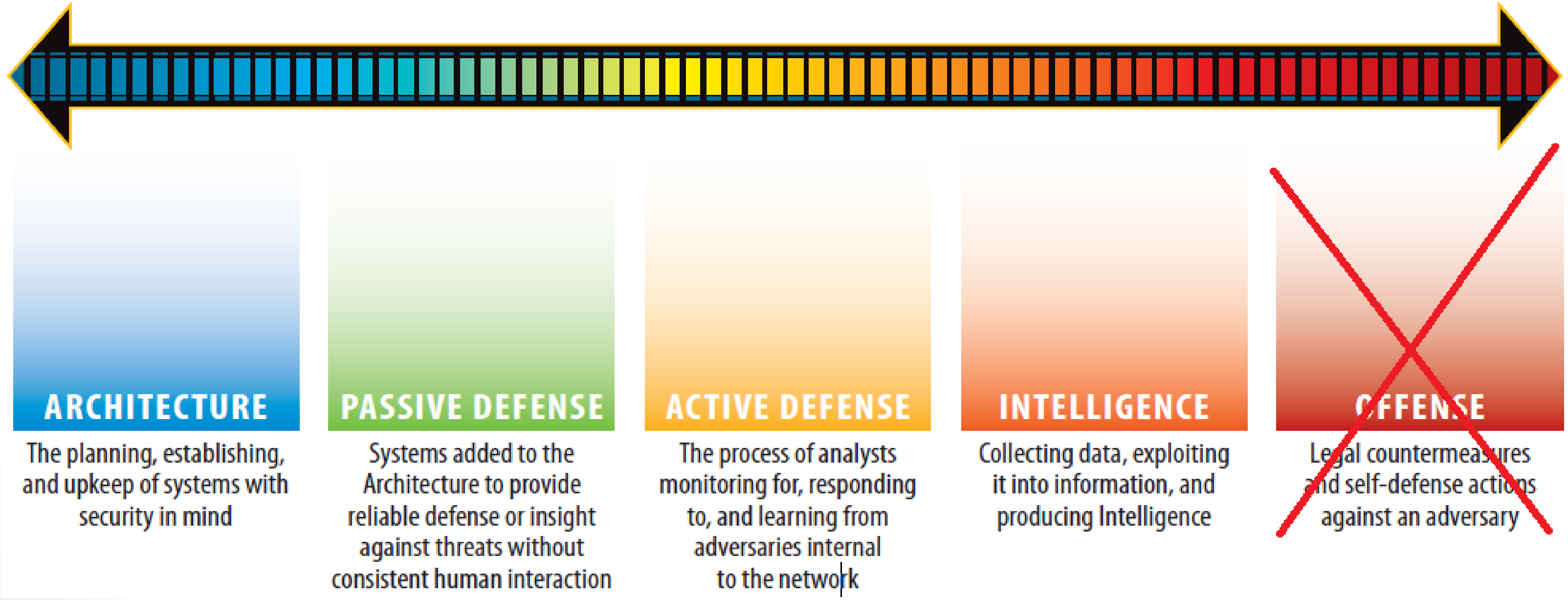
e.g from security architecture point of view, resources

My Definition

-Its not about hacking back (however for many people it is)

-Its not about one technical solution e.g deploy a deception tool

-Its about having a range of solutions and processes that go further to the traditional passive defence



ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE

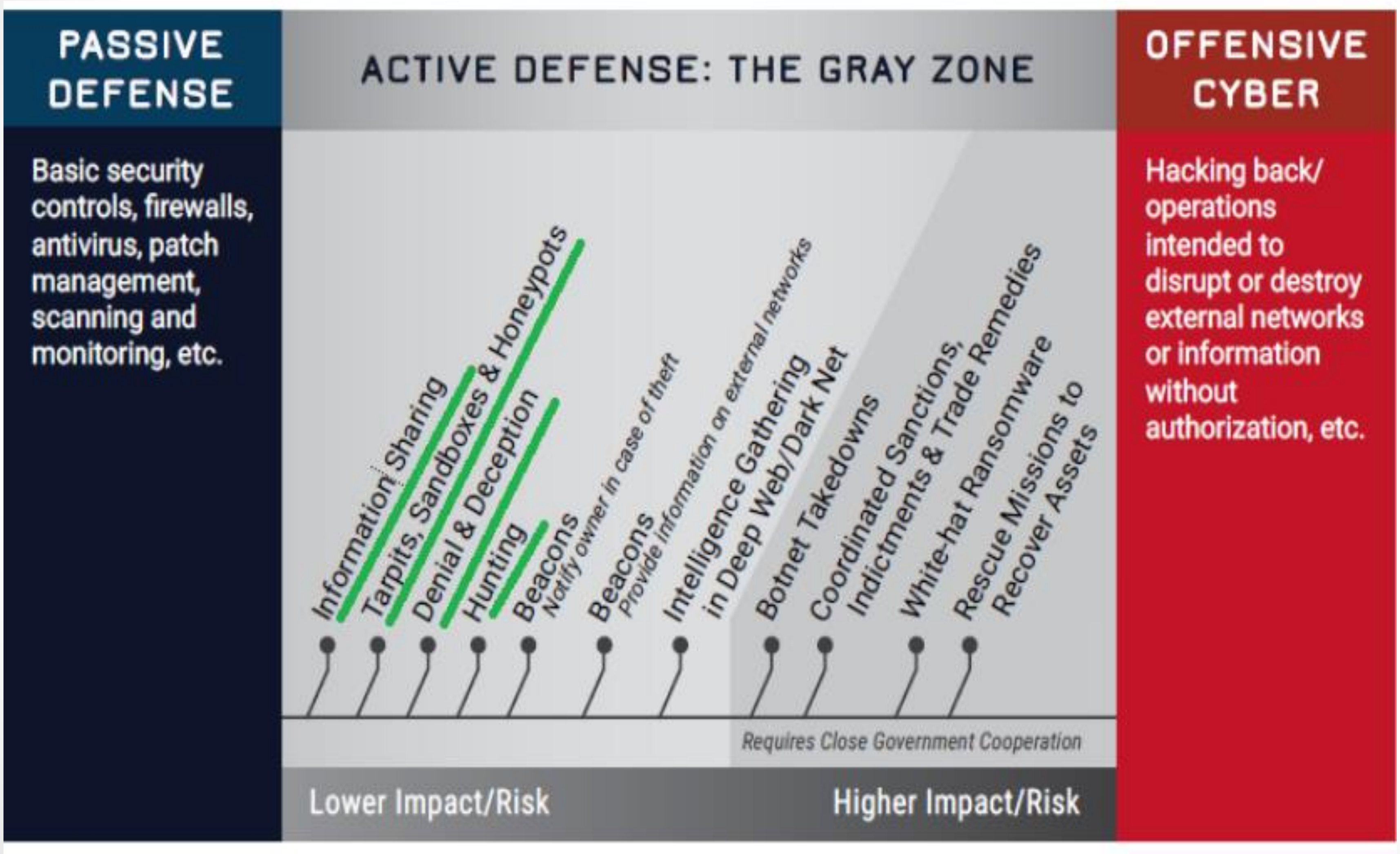
Collecting data, exploiting it into information, and producing Intelligence

~~OFFENSE~~

~~Legal countermeasures and self-defense actions against an adversary~~

SANS : The Sliding Scale of Cyber Security

Active Defence components



PASSIVE DEFENSE

Basic security controls, firewalls, antivirus, patch management, scanning and monitoring, etc.

ACTIVE DEFENSE: THE GRAY ZONE

- Information Sharing
- Tarpits, Sandboxes & Honeypots
- Denial & Deception
- Hunting
- Beacons *Notify owner in case of theft*
- Beacons *Provide information on external networks*
- Intelligence Gathering in Deep Web/Dark Net
- Botnet Takedowns
- Coordinated Sanctions, Indictments & Trade Remedies
- White-hat Ransomware
- Rescue Missions to Recover Assets

Requires Close Government Cooperation

Lower Impact/Risk

Higher Impact/Risk

OFFENSIVE CYBER

Hacking back/ operations intended to disrupt or destroy external networks or information without authorization, etc.

INTO THE GRAY ZONE : Center for Cyber and Homeland Security 2016

Information Sharing

- Based on CERT-EU CTI process

  -Reactive approach

  -Focus on IOCs

  -Necessary but not effective in targeted attacks

Tools for Deception-Honeyxxx

- Commercial
  - TrapX
  - Cymmetria
  - Illusive Networks
  - CounterCraft
  - TopSpin Security
  - Javelin Networks
  - …….

- Open source
  - MHN- Modern Honeypot Network
  - ADHD - Active Defense Harbinger Distribution
  - ……..

Honeydocs

- Looking at your defence from the perspective of how an attacker operates is a good idea

- Creation of deception docs based on the experience from Red Team Exercises (simulation of targeted attacks)

Questions :

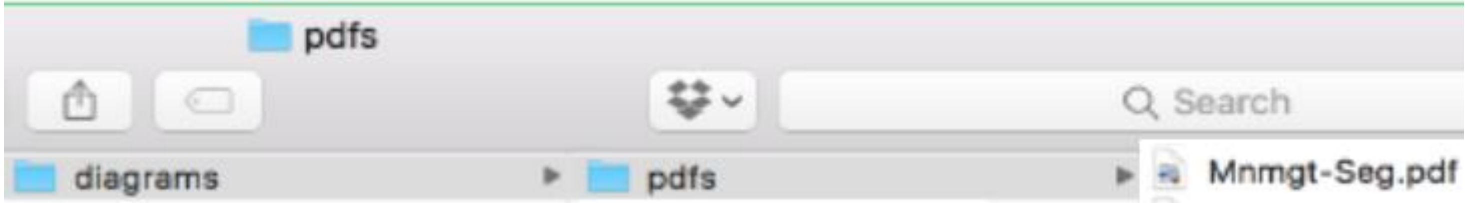
- How do we create a Honeydoc?
- Where can be stored?
- How to get alert that it was accessed?

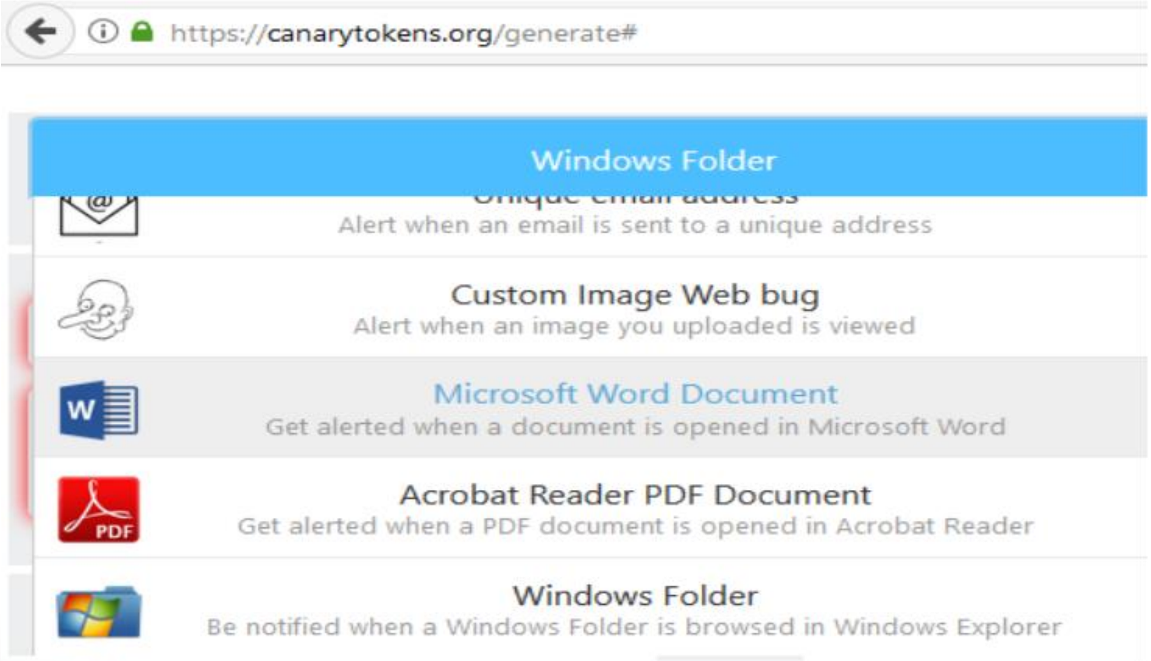
Examples

<u>A well chosen honeydoc should attract attacker's attention</u>

-Word files, shared folders with attractive names

-Fake Keepass databases,fake network diagrams




https://canarytokens.org/generate#

Windows Folder

Unique email address
Alert when an email is sent to a unique address

Custom Image Web bug
Alert when an image you uploaded is viewed

Microsoft Word Document
Get alerted when a document is opened in Microsoft Word

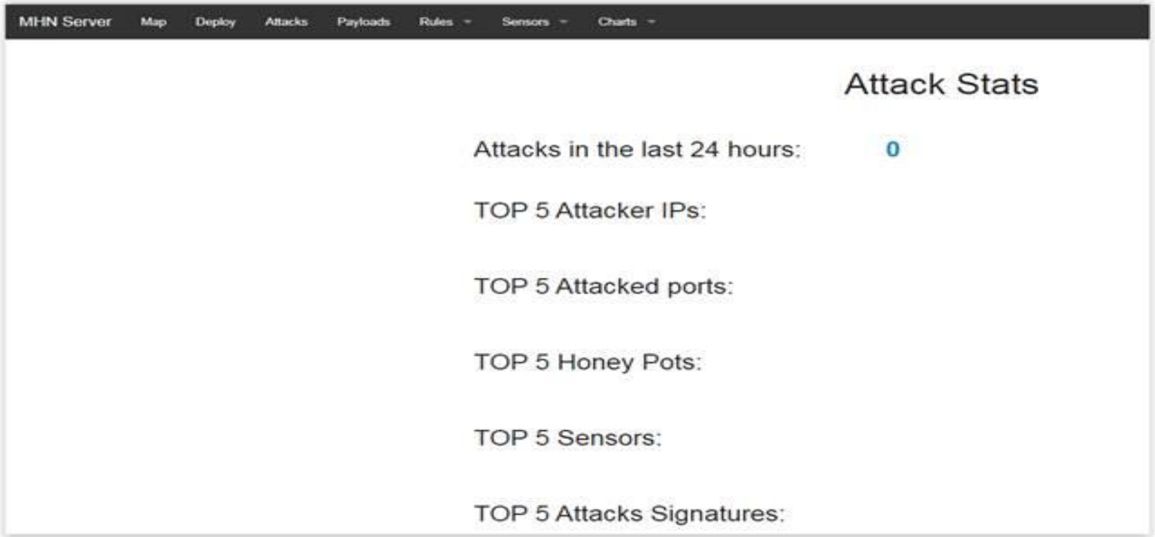
Acrobat Reader PDF Document
Get alerted when a PDF document is opened in Acrobat Reader

Windows Folder
Be notified when a Windows Folder is browsed in Windows Explorer

Low interaction honeypot

- Deploy few honeypot servers based on Modern Honeypot Network

- Relatively Easy to deploy – Still configuration needed so banners don’t say “This is a honeypot….” ☺



Attack Stats

Attacks in the last 24 hours: 0

TOP 5 Attacker IPs:

TOP 5 Attacked ports:

TOP 5 Honey Pots:

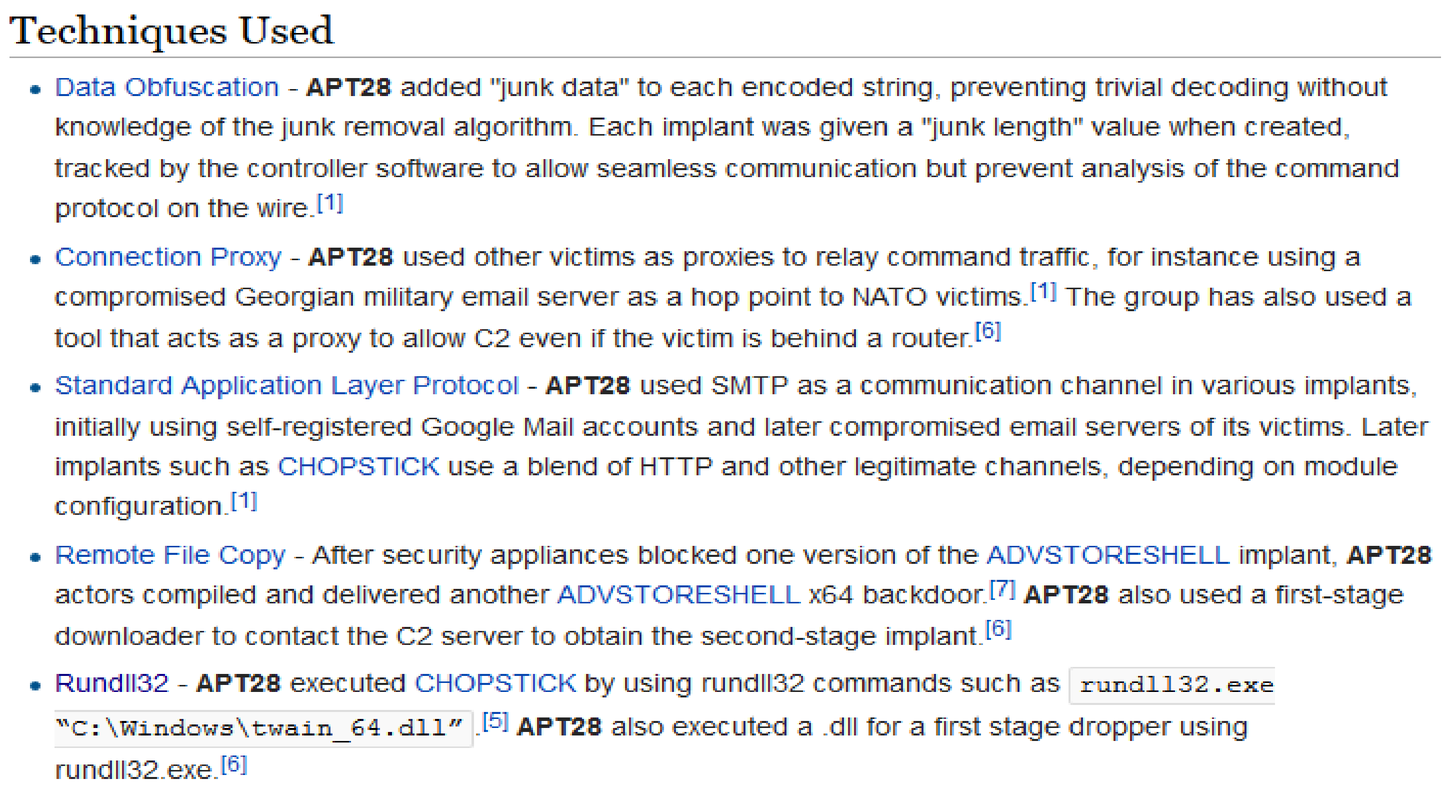
TOP 5 Sensors:

TOP 5 Attacks Signatures:

- Example : How we gather CTI info in a targeted attack using a custom honeynet

Hunting

- Actively looking for presence of attackers following the MITRE ATT&CK and CAR frameworks
- Based on CTI info focus on TTPs of the adversaries active in our sector
- Baseline – Stacking, Grouping, Clustering - Alert near-real time



Techniques Used

- Data Obfuscation - **APT28** added "junk data" to each encoded string, preventing trivial decoding without knowledge of the junk removal algorithm. Each implant was given a "junk length" value when created, tracked by the controller software to allow seamless communication but prevent analysis of the command protocol on the wire.[1]
- Connection Proxy - **APT28** used other victims as proxies to relay command traffic, for instance using a compromised Georgian military email server as a hop point to NATO victims.[1] The group has also used a tool that acts as a proxy to allow C2 even if the victim is behind a router.[6]
- Standard Application Layer Protocol - **APT28** used SMTP as a communication channel in various implants, initially using self-registered Google Mail accounts and later compromised email servers of its victims. Later implants such as CHOPSTICK use a blend of HTTP and other legitimate channels, depending on module configuration.[1]
- Remote File Copy - After security appliances blocked one version of the ADVSTORESHELL implant, **APT28** actors compiled and delivered another ADVSTORESHELL x64 backdoor.[7] **APT28** also used a first-stage downloader to contact the C2 server to obtain the second-stage implant.[6]
- Rundll32 - **APT28** executed CHOPSTICK by using rundll32 commands such as `rundll32.exe "C:\Windows\twain_64.dll"`.[5] **APT28** also executed a .dll for a first stage dropper using rundll32.exe.[6]

- Expensive, requires skilled personnel