Active Defense Untangled

3

by Mohamed Bedewi

Senior Security Researcher and Penetration Tester

Introduction and Facts

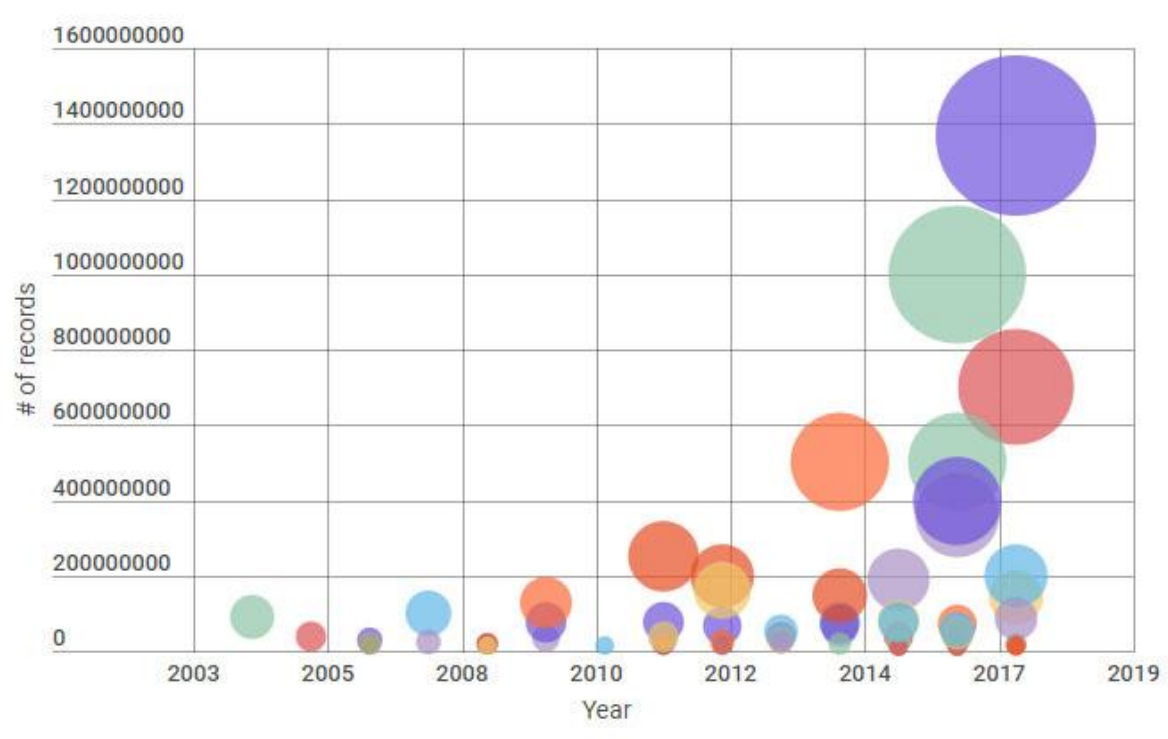
3-01

- The thread of Active Defense is spun throughout Sun Tzu's tactical teachings.
- Active Defense is a huge subject and was NEVER about hunting down hackers.
- Google exfiltrated a server in Taiwan and Facebook took down Koobface C&C.
- Hacking back is an offensive operation DON’T confuse it with Active Defense.
- DHS awarded NexiTech to implement Active Defense for industrial infrastructure.
- A new bill was proposed by Tom Graves last month to legalize Active Defense.

Would you let him do his job or interfere?

3-02

What's the Problem?



We have to understand that patch and pray strategy isn't serving us well as we expected, the threat landscape is massively increasing with no proper security whatsoever and our defense approach is flawed!

Passive Defense **vs** Active Defense

3-04

The comparison displayed below doesn't necessarily recommends a specific defense method over another; the best security is the one which can combine between both!

Passive Defense (Detection)

Depends on frustrating the attacker and pushing him to give up by making the network hard to exploit.

Relies on the Castle Approach to maximize defense in critical environments, pricey but very reliable.

Not effective against sophisticated cyber attacks and persistent threats which can operate, execute and persist for years totally undetected.

Active Defense (Prevention)

Depends on luring, misleading, trapping and hacking the attacker to understand and control the attack.

Relies on intelligence gathered to highlight the risk from every aspect to implement the right control(s).

Very effective against sophisticated cyber attacks and persistent threats since it can provide extremely accurate intelligence and control in critical timings.

Active Defense Advantages

3-05

Active Defense increases the cost of sophisticated cyber-attacks significantly.

Active Defense increases the efficiency and accuracy of Passive Defense controls.

Active Defense provides complete in-depth security control all over the network.

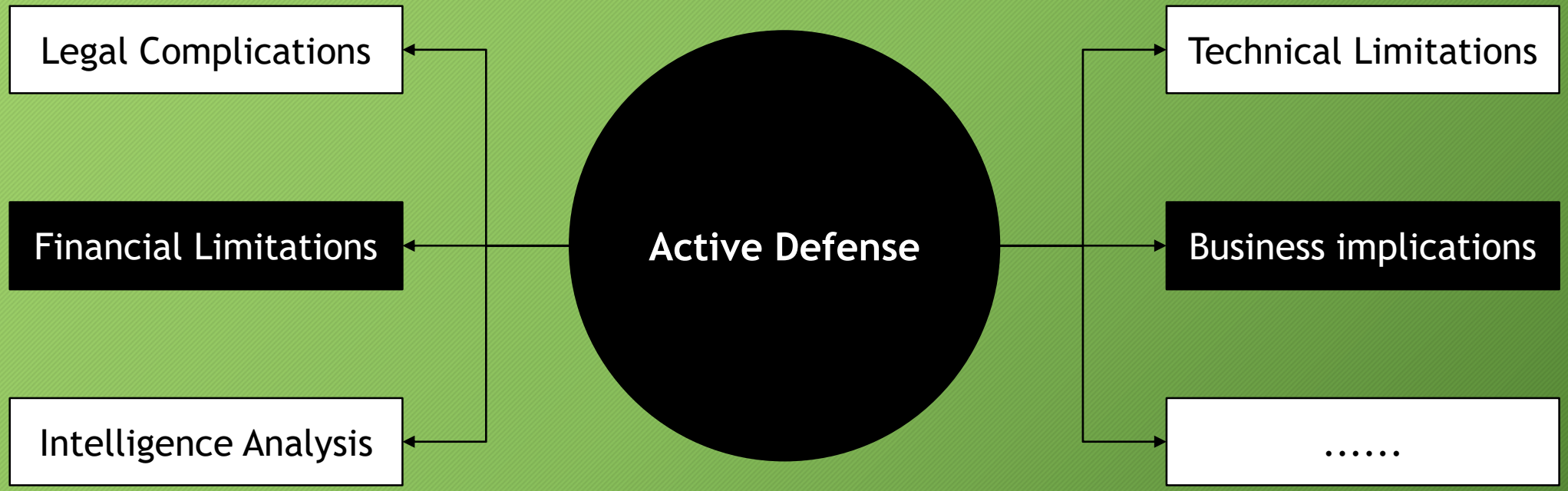
Active Defense provides full risk and attack control in case of a security breach.

Active Defense minimizes investigation and tracking time for law enforcements.

Active Defense generates an extremely accurate risk and tactical intelligence.

Active Defense Challenges

3-06



Attack is the secret of defense; defense is the planning of an attack.

Sun Tzu, The Art of War

How to Implement Active Defense?

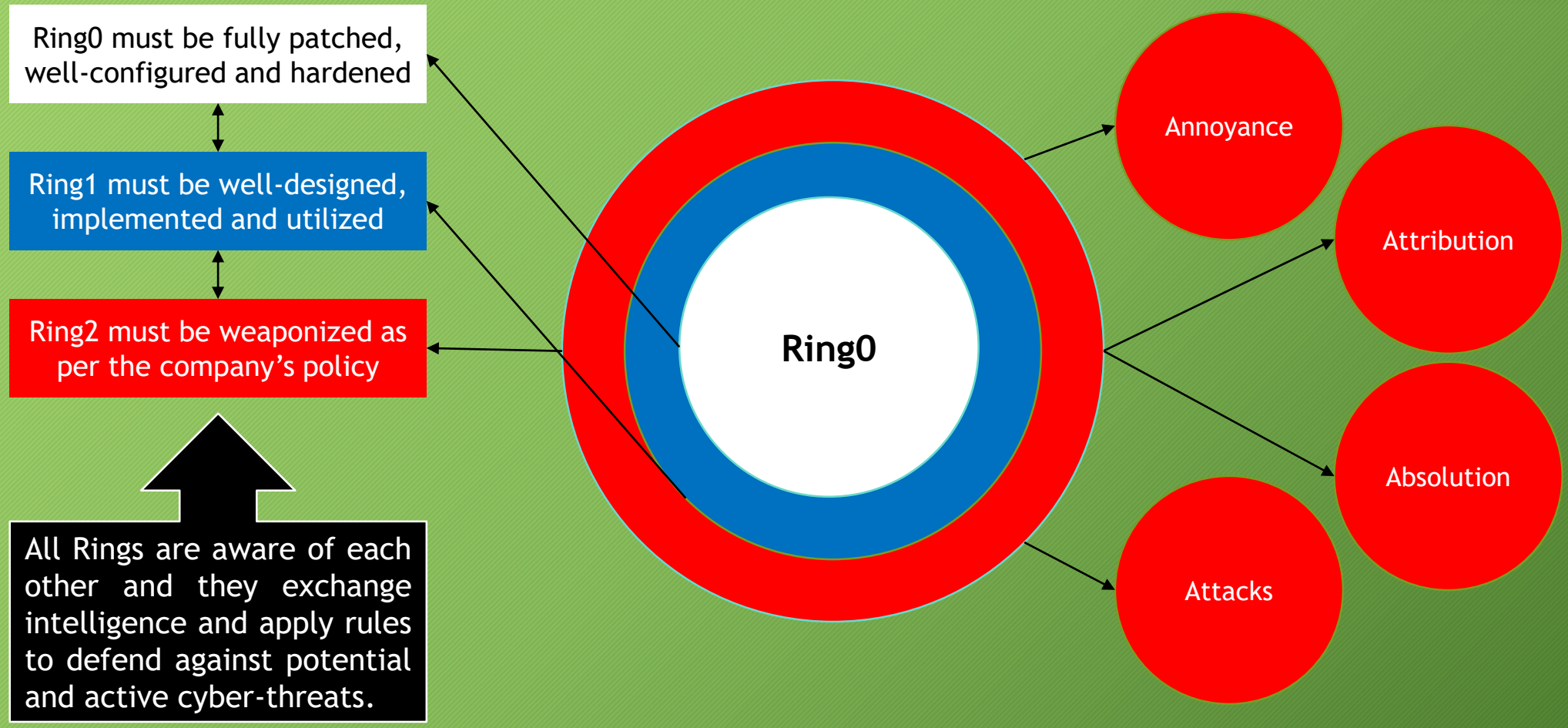
Technical Responsibilities:

- Technically experienced dedicated teams preferably blue and red.
- Hardware and software expansion along with major modifications.
- Threat intelligence analysis to predict and defend cyber-attacks.

Management Responsibilities:

- Financial flexibility to invest in Active Defense and its integration.
- Management board support of Active Defense and its operations.
- Legal understanding of Active Defense and how to fully leverage it.

Active Defense in Action



Examples of Active Defense Traps

Integrity Monitors

One of the simplest yet sometimes it can be a game changer as if an attacker tried to dump/modify files or directories into your systems, the trap will trigger and inform you with all needed intelligence to take an action

Advantages:

- Breaches early alarm.
- Intelligence like a fox.
- APT enemy since ages.

Honeyfiles

Another simple trap which focuses more on deception by luring the attacker to fetch and execute files from your systems which can lead to taking full control of his machine and pinpointing his accurate location information

Advantages:

- Threat and risk control.
- Intelligence level ninja.
- Identification is easier.

Scraper Deceivers

Relies on the fact that to discover a website, an attacker needs to crawl it and if this was automated, unlimited dynamic pages will be generated which will put the scanner in infinite loop causing OS crash or fat drive

Advantages:

- Attack cost multiplier.
- Skiddies traffic filter.
- ActiveRecon defender.

Examples of Active Defense Traps

Honeyinfo

Every successful cyber-attack started with a detailed Recon to identify used technologies and patch level but if the collected patch level was all wrong, the attacker will run all sort of triggers trying to exploit the wrong service

Advantages:

- Attack cost multiplier.
- Skiddies traffic filter.
- ActiveRecon defender.

Honeyports

Ports are the entry point to any computer system and this is where the attacker starts scanning for open ports to attack services but what if all ports where open and any unauthorized connect triggers a trap which bans and alerts

Advantages:

- Attack cost multiplier.
- Skiddies traffic filter.
- ActiveRecon defender.

Honeytokens

Fictitious words or records that are added to legitimate databases, documents, config files and webpages which once used by the attacker, it triggers a trap which bans, alerts and in some cases takes full control of his machine

Advantages:

- Threat and risk control.
- Intelligence level ninja.
- Identification is easier.

More Active Defense Traps

ADHD is a Linux distro based on Ubuntu LTS. It comes with many tools aimed at active defense preinstalled and configured. The purpose of this distribution is to aid defenders by giving them tools to “strike back” at the bad guys.

ADHD has tools whose functions range from interfering with the attackers’ reconnaissance to compromising the attackers’ systems. Innocent bystanders will never notice anything out of the ordinary as the active defense mechanisms are triggered by malicious activity such as network scanning or connecting to restricted services.

Final Thoughts and Closure

- Cyber-threats became complicated in a way which requires us to fully understand it.
- Passive Defense alone won’t solve the security problem since there’s always away.
- Active Defense integrates with Passive Defense to ensure reliable dynamic security.
- Threat intelligence must be analyzed, researched properly and leveraged to serve.
- Incident response will evolve to achieve full threat control and better identification.
- Cyber-threats prediction will significantly evolve with the accurate threat intelligence.

Thanks and Have a Great Day