BH USA 04 Digital Active Self Defense

Laurent OUDOT oudot@rstack.org http://rstack.org/oudot/

Some references

- Enforcer, Automated Worm Mitigation for private networks, Timothy M.Mullen
 - BlackHat Seattle, February 2003, AnchorIS
- Active Defense research project, Dittrich David
 - http://staff.washington.edu/dittrich/ad/
- Defending your right to defend: Considerations of an automated strike-back technology, Timothy M. Mullen
- Launch on Warning: Aggressive Defense of Computer Systems, Curtis E.A. Karnow
- Vigilantes on the net, Barbara Moran
 - NewScientist, 12 june 2004
- Symbiot, Adaptive Platform for Network Security
 - http://www.symbiot.com

Summary

- Introduction
 - The digital threats
 - From hardening to reaction
 - Active Defense...?
- Legal Issues
 - Proportional response
 - No adequate alternatives
- Technical considerations
 - Requirements
 - Honeypots
 - Internal computers
 - Internal threats
 - Examples
 - Technical limitations
- Conclusions

Introduction

Current threats

- Known limitations for defense technologies
 - Many solutions in the information security field
- Laws fail for certain kind of activities
- Cost of cyber threats
- Natural temptation
 - Fighting back attackers, counterstrike...
- Not so many solutions that use active countermeasure capabilities
 - Interesting field of research and development ?



The digital threats

- Though we use more and more security technologies, there are still security problems
 - Confidentiality, Integrity, Availability, Copyright, etc
 - Information Assurance
- External threats
 - Firewall, Proxies, Hardened services...
 - Ethical Hackers, Corporate spies, Cyber terrorists...
- Internal threats : easier/faster access
 - Authentication, In-depth Protection...
 - Trainees, Outsourcing, Employees...



From hardening to reaction

- A lot of technologies might be used to block evil traffic
 - Routers, Firewalls, proxies, etc
 - Allow the minimum that is needed
- But aggressors still find solutions like :
 - Bouncing in (bad security rules, bugs, etc)
 - Getting an access inside the minimum accepted (target services, target end-users with stupid clients, etc)

Countermeasure technologies

- While getting a sign of an attack (IDS...), security resources will respond by trying to stop the attack
- Could it be an interesting answer to handle some threats ?



Active Defense...?

• Usual methods would not always work ?

- Block incoming traffic
 - Might be problem for online services
- Apply rate limitation
 - Bandwidth adjusted
- Divert the traffic
 - Bait and switch technologies (honeypots)
- Fake responses (decoy)
- Should we use more aggressive methods ?
 - Self Defense
 - Counterstrike
 - Disable, destroy, control the attacker

Warning

Limitations

- Not a legal expert
- Legal issues might be different depending of the countries...

Legal Issues

- Toward a concept of *digital* self defense ?
- Self defense occurs when someone is threatened with imminent bodily harm
 - Might be applied to avoid injury to property
- Requirements
 - Necessity: No choice but using force
 - No adequate alternatives
 - Proportionality: This force is reasonable
 - Proportional response to the harm avoided
 - The threat is unlawful



Proportional response

- What could mean *proportional* ?
 - Risk of subjectivity / interpretation
- Need to create a classification of attacks to chose the appropriate response
 - Families of attacks and hierarchy
 - DDOS > DOS ?
 - Remote shell > Scan ?
 - . .
- Once it is done, you might be able to take a decision

No adequate alternatives

- Proving that you had no other choice ?
- Experts could argue that many other possibilities might be used :
 - First consideration : disconnect the victim(s) to avoid the attack ?
 - Self Defense doctrine does not require the victim to back away
 - Such a disconnection would result in a kind of denial of service on the victim
 - what about an e-business web server ?
 - Other possibilities : perimeter defenses ?



No adequate alternatives

- How can we explain that the counterstrike tools were able to fight back the attacker and that they could not block the attack ?
 - So many solutions of security to avoid an attack
- Conclusion : might be difficult to prove that you had no other possibility

Legal Issues and IW

- What about Information Warfare ?
 - Not officially recognized by The Hague and Geneva Conventions
 - No real example of act of war on the cyber battlefield
 - Individuals, groups, governments...
 - No real legal considerations



Self Defense Aggressor Victim Action Usual clients Scanners Exploits Trojan clients ... **Reaction**



Technical considerations

- Striking back ?
 - Identify the tools/methods/sources
 - IDS, logs, network captures...
 - Avoid spoofing...
 - Take a decision
 - White list / Black list : destination of counterstrike allowed
 - e.g. hacking back internal users
 - Strike back !



Requirements

- Graduated response : level of reactions to strike back with a **proportional** response
- Determination of hostile hosts (level of threats)
 - Behaviour, intrusion detection analysis, etc
 - Risk: false positive (huh! sorry)
- Profiling the attack
 - Probes, scanners, exploits, clients, malware, worms, Dos, etc
 - Choose the appropriate strike back possibility
 - Real life example: DEFense CONdition
 - DEFCON 5 Normal peacetime readiness
 - DEFCON 4 Normal, increased intelligence and strengthened security measures
 - DEFCON 3 Increase in force readiness above normal readiness
 - DEFCON 2 Further Increase in force readiness, but less than maximum readiness
 - DEFCON 1 Maximum force readiness.



Fighting back usual clients

- Imagine what would happen if the aggressors used vulnerable or mis-configured clients ?
 - Web clients (IE...),
 - SSH clients (Putty, OpenSSH...),
 - Mail clients (Outlook...),
 - DNS resolvers,
 - IRC clients...
- Then a remote control/crash would be possible
 - Very interesting for Self Defense !



Fighting back usual clients ??

- This is a not a so easy task
 - Is it just theory ?
- Fighting back a listening client (mail client, etc) might be easier because you can try an attack multiple times (multiple mails...)
- Fighting back an incoming client may be a one shot operation (web client, etc) during a specific phase
- You will need specific information to launch such an attack :
 - Operating System/Hardware (p0f...)
 - Version ("Banner")...



Specific opportunities

- Though lawyers could argue that Self
 Defense is a very dangerous response to a digital threat, one can think about :
 - Honeypots
 - Internal Threats

Honeypots

- « A honeypot is a security resource whose values lies in being probed, attacked or compromised »
 - This is a non production system
 - Used to delude attackers
 - Incoming traffic is suspicious
 - That implies that the decision of launching a counterstrike is probably easier
- Honeypots are really interesting technologies for aggressive defense purpose



Internal Computers

- Official remote administrator access might be possible on internal computers/devices
 - On a final destination (potential attacker)
 - Near potential attackers
 - Network devices at one or two hops...
- Self Defense might be used inside your own network in order to protect it
 - Might be an easy and clean method (no exploits, etc)
 - Stop processes, add firewall rules, reboot/halt, modify files, patch...
 - Might be very useful to avoid fast propagation of worms...



Handling internal threats

- Local Area Network
- Striking back your own computers
 - Those computers are under your legal control
 - If you have the right to « pentest » them, why could'nt you strike back in their direction ?
- Very useful to find evil end users
 - Corporate hackers, zealot end-users...
- Potential risk: spoofing is easier on a LAN
 - Layer 2 attacks, etc



Real examples...

- Code Red II / Anti code red II « default.ida » script
 - Strike back that abuses the remote CRII
- Attack occurs over a TCP session: might be the real source
- Problem with attacks over simple UDP flows
 MS SOL Server, UDD 1424, Litchfield (couple)
 - e.g. MS SQL Server, UDP 1434, Litchfield / exploit
- Symbiot.com technologies
- Limitations : imagination + laws + technics
 - Imagine a web server that could gather extended info about an attacker (email...) while reacting by hacking back an evil IE client playing with SQL injection...

Possible goals

- Stop / limit the attackers
 - One attack / one attack and next attacks
- Gather more info about the aggressor (trial...)
 - Passive methods
 - Active methods
 - Almost stealth (network interaction low level)
 - Not really stealth (footprinting, banner grabing, etc)
- Taking the control of the remote attacking host
 - To add special marks on the computer (proofs / trial)
 - To gather more information
 - To follow a chain of hosts owned and used to bounce
 - Same trojan used with same passwords, etc
 - To definitly stop the threat



Technical limitations

- Counterstrike technologies might not exist for some kind of threats
 - Might need « remote exploits » for each worms, evil tools, etc [!]
- False positive
- Spoofing
- Collateral damage

Conclusions

- Technology
 - Really interesting
 - Feeling of doing something right
 - New possibilities to explore in order to protect an infrastructure
- Organization
 - Legal issues
 - Counterstrike might be used to target internal computers/devices
 - Add In-Depth Security capabilities (kind of advanced intrusion prevention system)
 - Information Warfare battlefield ?
- Blackhats
 - Yet another way to attack (attackers ?!)
 - e.g. Evil Honeypots

• Questions ?

 Greetz : « MISC Mag », Dave Dittrich, Jennifer Granick, Barbara Moran...