



eEye Digital Security®

Angel Recon System
Drew Copley


```
 /
i if (argc < 3)
{
printf ("\nwwwget - determine what httpd version a site is running\n");
printf ("== punkis@attrition.org ==\n");
printf ("Usage: wwwget [ip] [port]\n");
return 1;
}
host = argv[1];
sport = atoi(argv[2]);
hostinfo = gethostbyname(host);
if (!hostinfo)
{
fprintf(stderr, "Host: %s\n", host);
exit(1);
}
servinfo = getservbyname("http", "tcp");
if (!servinfo)
```

VULNERABILITY IS OVER



Angel Recon System : Introduction



- **Hacking is a martial art: an art of combat**
- **Like physical security, few reasons for pure offense**
- **Legitimate usage of offensive hacking is for intelligence purposes**
- **But, to be good at defense you must know offense**

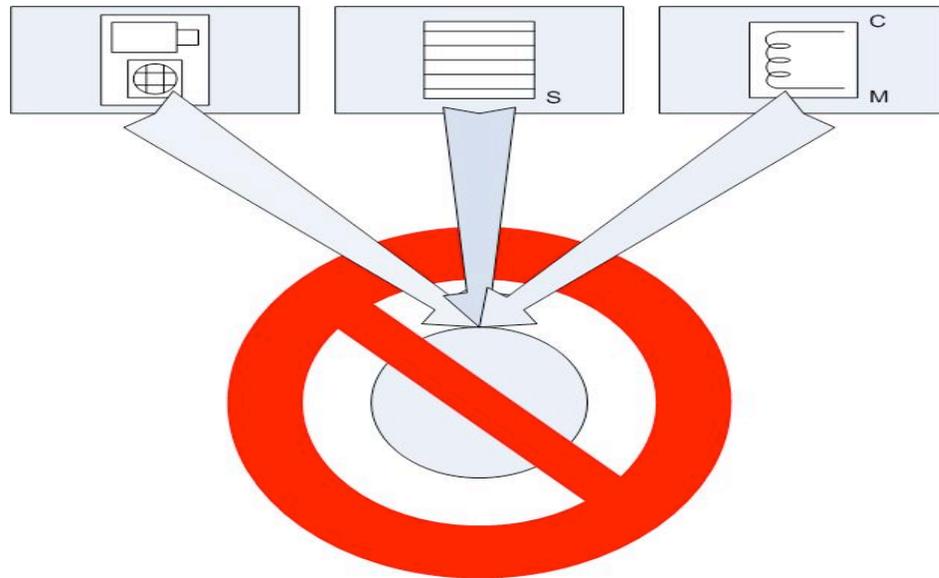
Angel Recon System: Introduction Part Two



- **ARS is designed to be an innovative and useful offensive hacking tool designed for intelligence purposes**
- **Yet, ARS is designed for training purposes**
- **Like vulnerability scanners, ARS can be both offensive and defensive in nature**

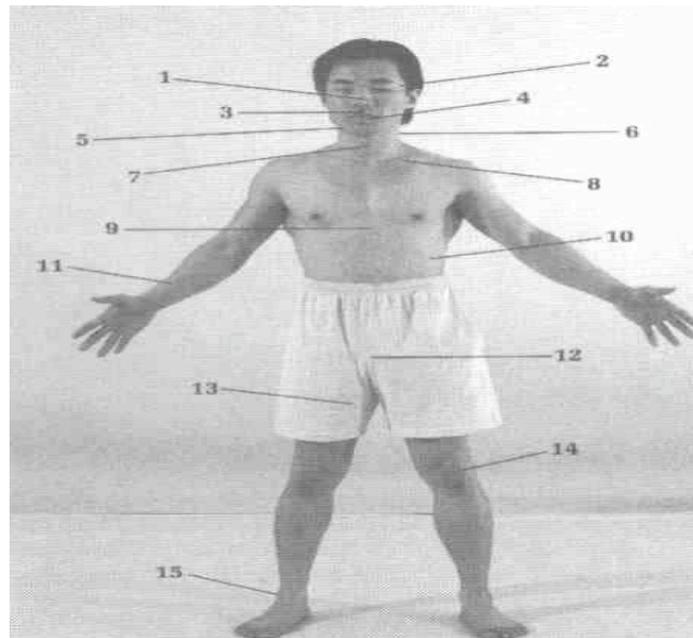
A Common Denominator for Security Products

6



- **Target the offending binary, target the offending process**
- **Signature AV, heuristic AV, Firewalling products, heuristic API products, system integrity agents, and others -- all have this common denominator**

Strike At Common Denominator



- Identify common denominators and strike at them
- Target systems have unknown defensives
- Common denominators are therefore essential strike points
- Most rootkits seek to strike at common denominator of lower level attacks



FIG. 52

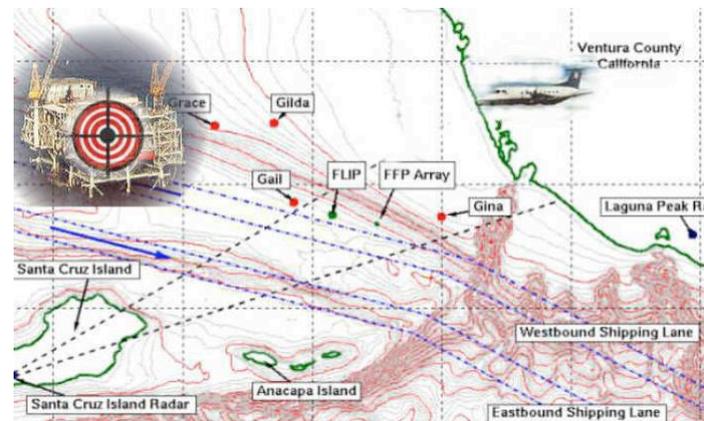
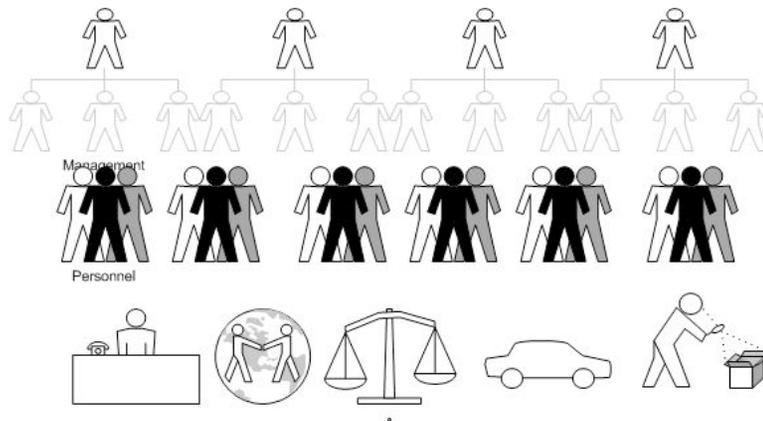
- **In offense or defense, first seek common denominator**
- **In physical attacks: throat or knees (everybody has em)**
- **In gun fighting: head shot (everybody has em)**
- **In hacking defense this might be heuristic and generic defenses against common denominators of attack products**

A Brief Recap of Modern History of Recon



- **During Vietnam war a second front was fought in Laos**
- **North Vietnam supplied forces in South Vietnam through Laos**
- **Special Forces and CIA engineered concept of small recon forces who identified targets and called in air support for targeted strikes**

Target Identification Difficulties



- **In offensive hacking, first identifying a solid target is of utmost priority**
- **Identification can involve a great deal of effort**
- **Targetting may involve extensive use of intelligence**
- **Failed attack on target system may have severe physical and political consequences**

Unknown Defenses of Target System

11



- **A good attack plan involves many “Plan Bs”**
- **There are many defensive products out there**
- **New defensive products may always be invented, and unknown updates may be difficult to keep track of**
- **Manual defensive moves also involve, generally, a common denominator of striking at single binary and process**

Various Best Methods of Attack -- Upstream

12



- **Upstream Attacks for intelligence**
 - Lack of decryption capabilities, steg detection
 - (Most important information encrypted)
 - Requires information to be transmitted
 - Difficulty for remote targets, especially foreign
 - Danger of leaks, discovery

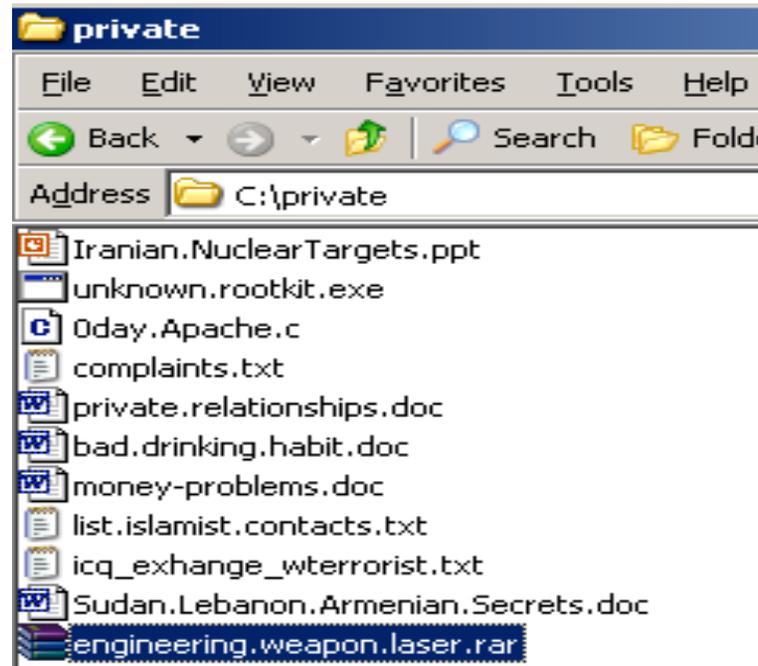
Various Best Methods of Attack -- Physical

13

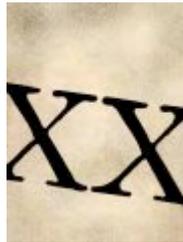


- **Hardware Attacks, eg, keyboard taps**
- **Video Camera pointing at typer, etc**
- **Generally, same problems as upstream attacks**
 - Advantage for stealth reasons in some cases
 - Great for local intelligence against criminals, horrible for foreign intelligence

Why Target Individual Systems



- Foreign difficulties overcome
- Remote Targets may be difficult to track down
- Ease of attack
- Incredible information resources usually found on system
- Ability to quickly build up target networks from single targetted systems
- Encryption/Protection schemes broken



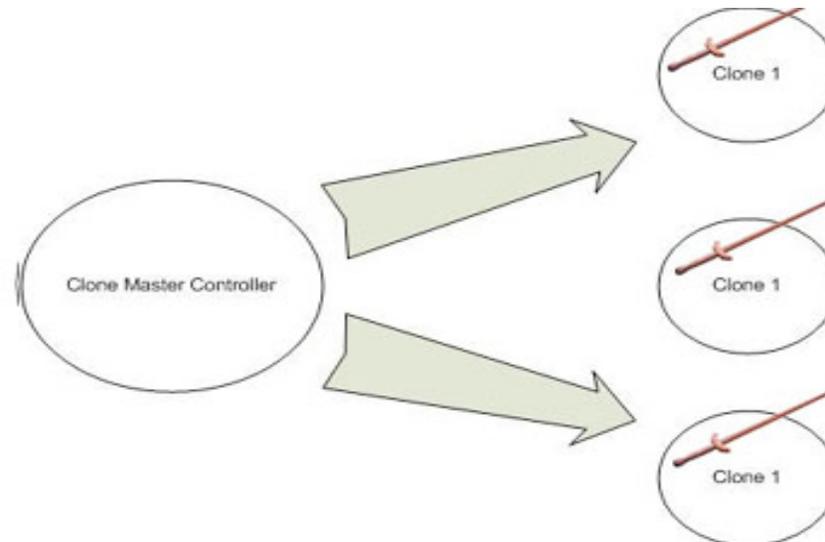
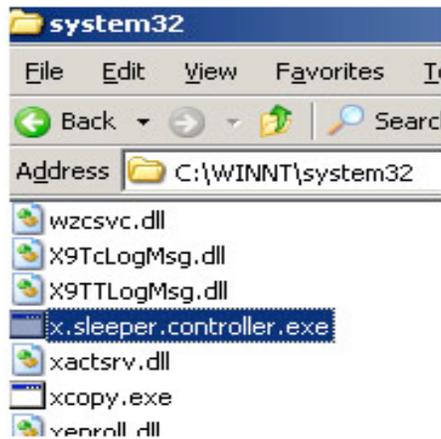
- **Compromised attack may never be disclosed to attacker**
- **If human resources involved, human resources may be physically attacked/turned**
- **Disinformation may be fed through compromised network – ala, Britain's infamous Double Cross system**
- **Target and Target network increases defenses, goes underground**

How ARS Attacks the Common Denominator



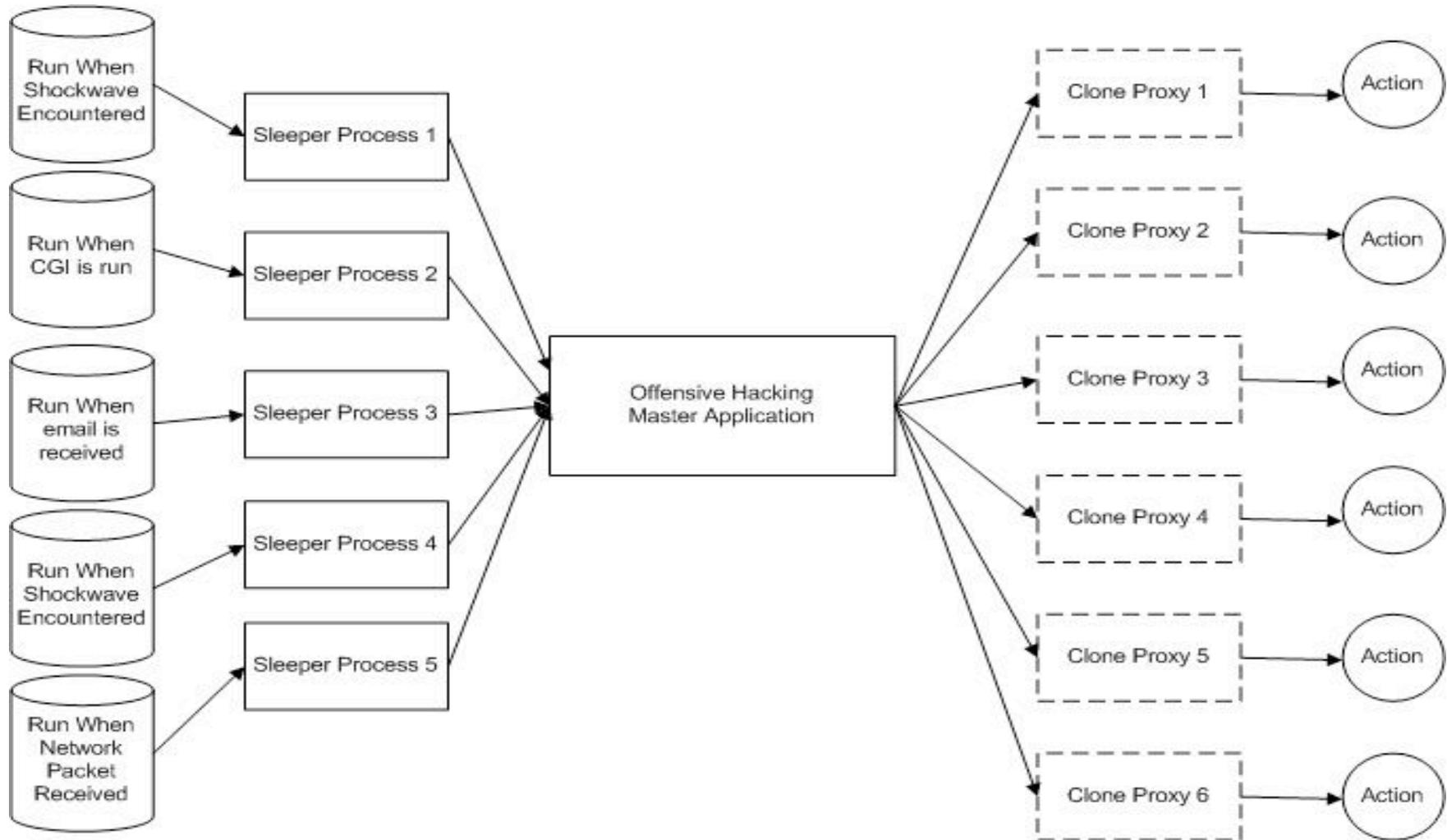
- **ARS attacks the common denominator of defense systems by having clones perform all of the work for it**
- **When a Binary or Process is discovered because of its' behavior, ARS itself stays alive to catalog this defensive move by the target system**

ARS Methodology of Cloning Logical Tree

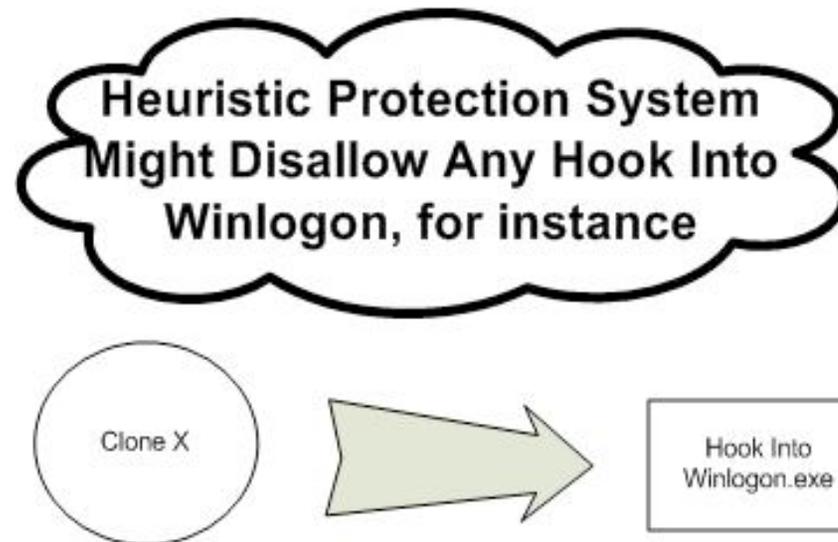


- **The ARS methodology is simple – while designed for a recon system which later might be used with a rootkit, ARS might also be defined as a system for rootkits in general**
- **ARS is flexible – the master process/binary may have several conduits to itself back, the master binary may not even be active, but secondary, third, and fourth controllers might be used**

The Bigger Picture



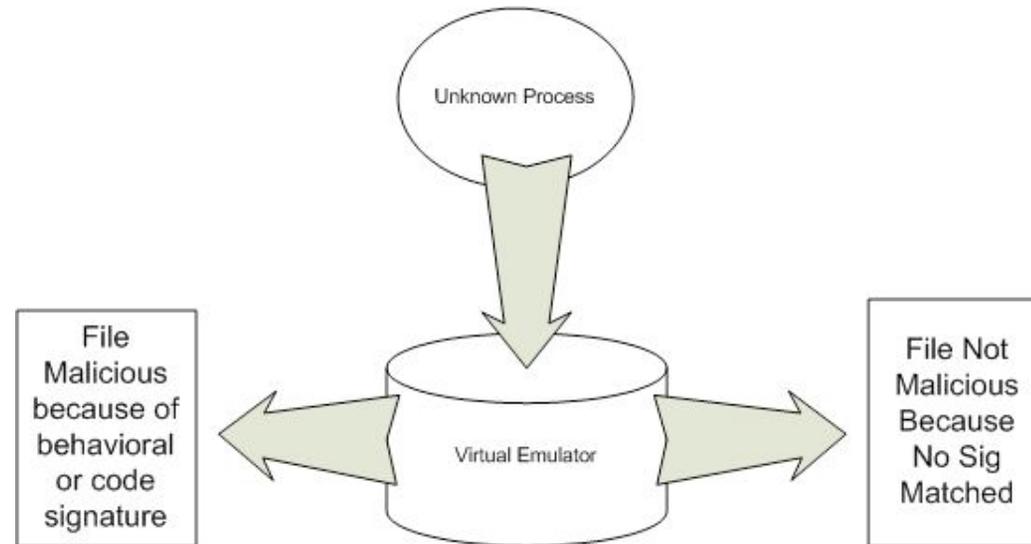
Principle of Clones to Perform Behaviors



- Any behavior which a trojan might perform which could be potentially called “malicious” or even “out of the ordinary” could reveal itself and compromise the attack
- This may be: hooking, sending messages, changing binary files, sending or receiving network traffic, even just process or disk activity

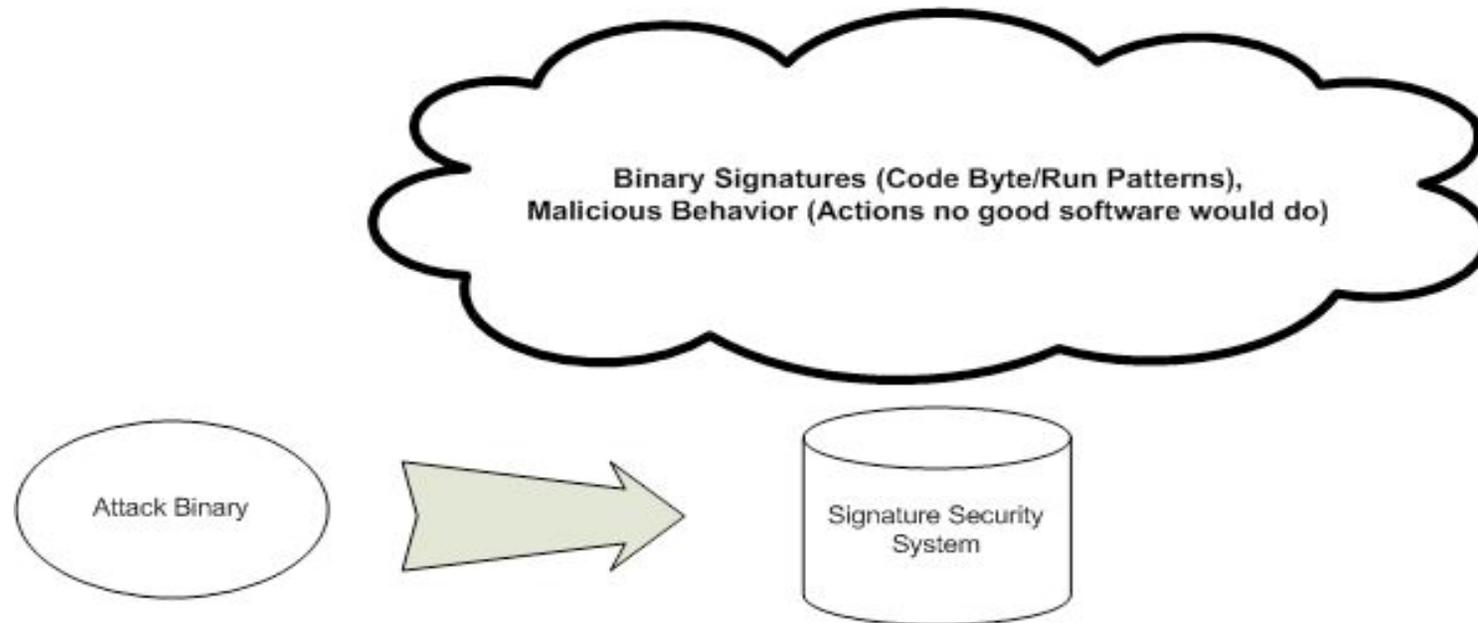
Signature Based Products: Heuristic and Fingerprint

20



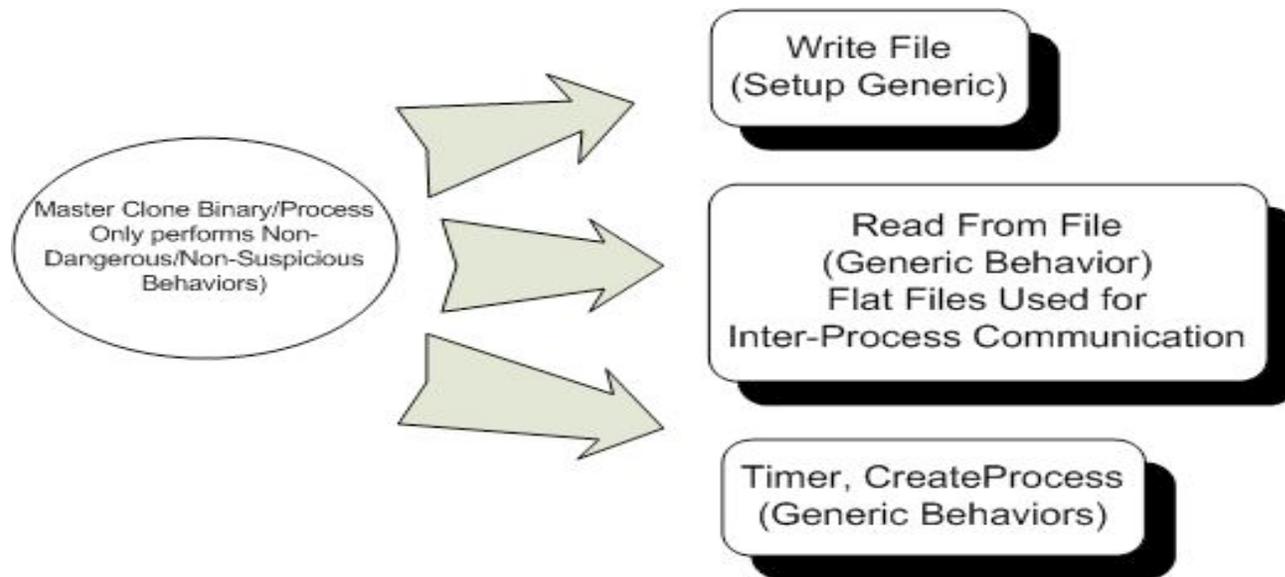
- **Most heuristic based systems do have signatures**
- **Often the most sophisticated kind utilize emulation to run the code: throwing up multiple binaries and having the master binary do no harm can throw such systems for loops**
- **It should be noted, however: any system which is revealed to the public is compromised by default because of signature systems**

Evading Signature Based Systems Not Problem



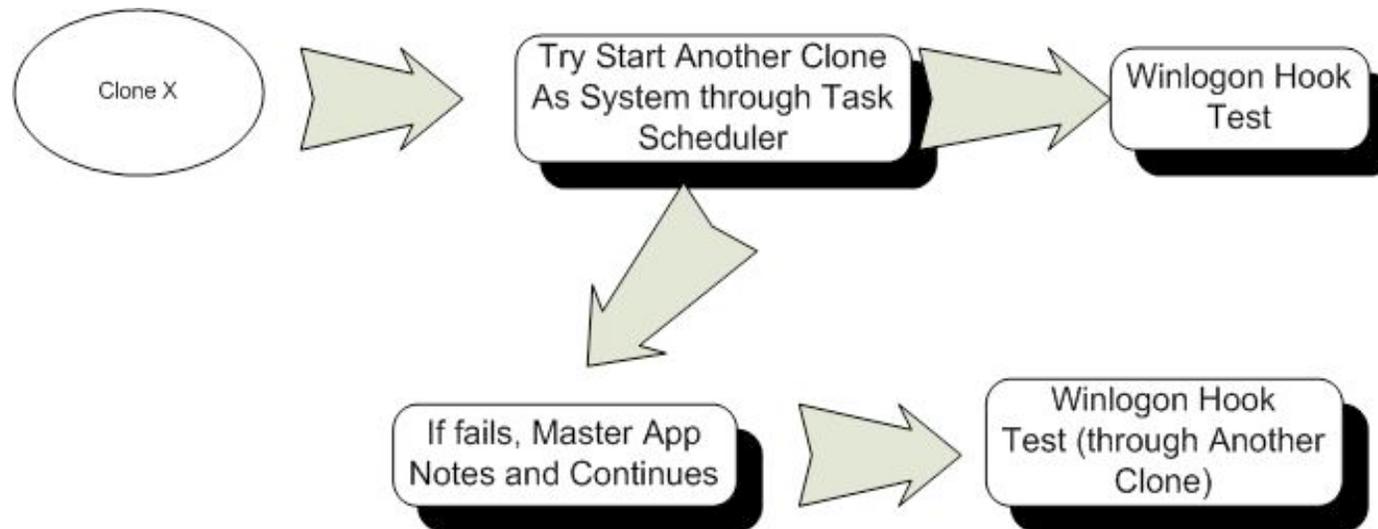
- **Evading Signature based systems is not a problem, so it is not countered here**
- **The signature can be based on the behavior of the application or on the blind code fingerprint of the binaries themselves (which is essentially same thing)**
- **Unknown trojans by default evade such signatures – that is the best assurance and extremely simple**

Technical Overview of ARS



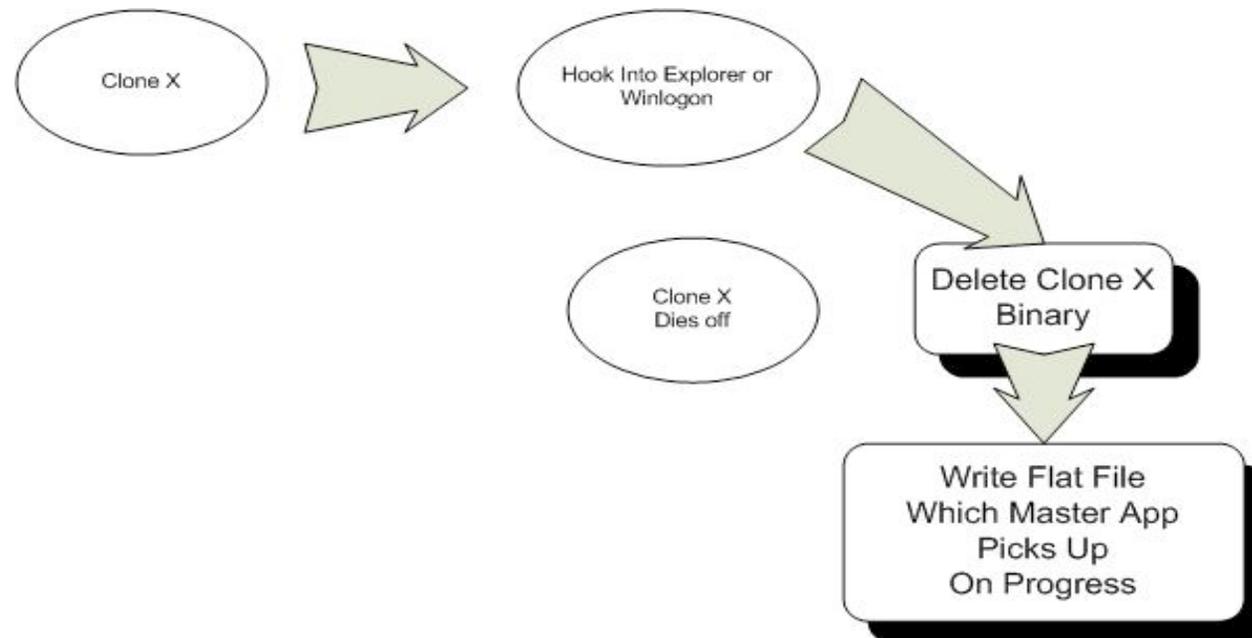
- **ARS runs, creates first clone and first timer**
- **First clone attempts to perform minor operation, getting list of user context privileges**
- **If first clone fails, ARS gets report, if first clone succeeds, privileges gotten lead to next goal**

ARS Stage Two



- **First clone kills itself, deletes itself**
- **Second clone starts up, if it has admin, it attempts to get to system by using at.exe trick**
- **If Task Scheduler not started or enabled, it enables it, starts it**
- **If fails, third clone goes into operation**
 - Etc, etc

Other Various ARS Attacks

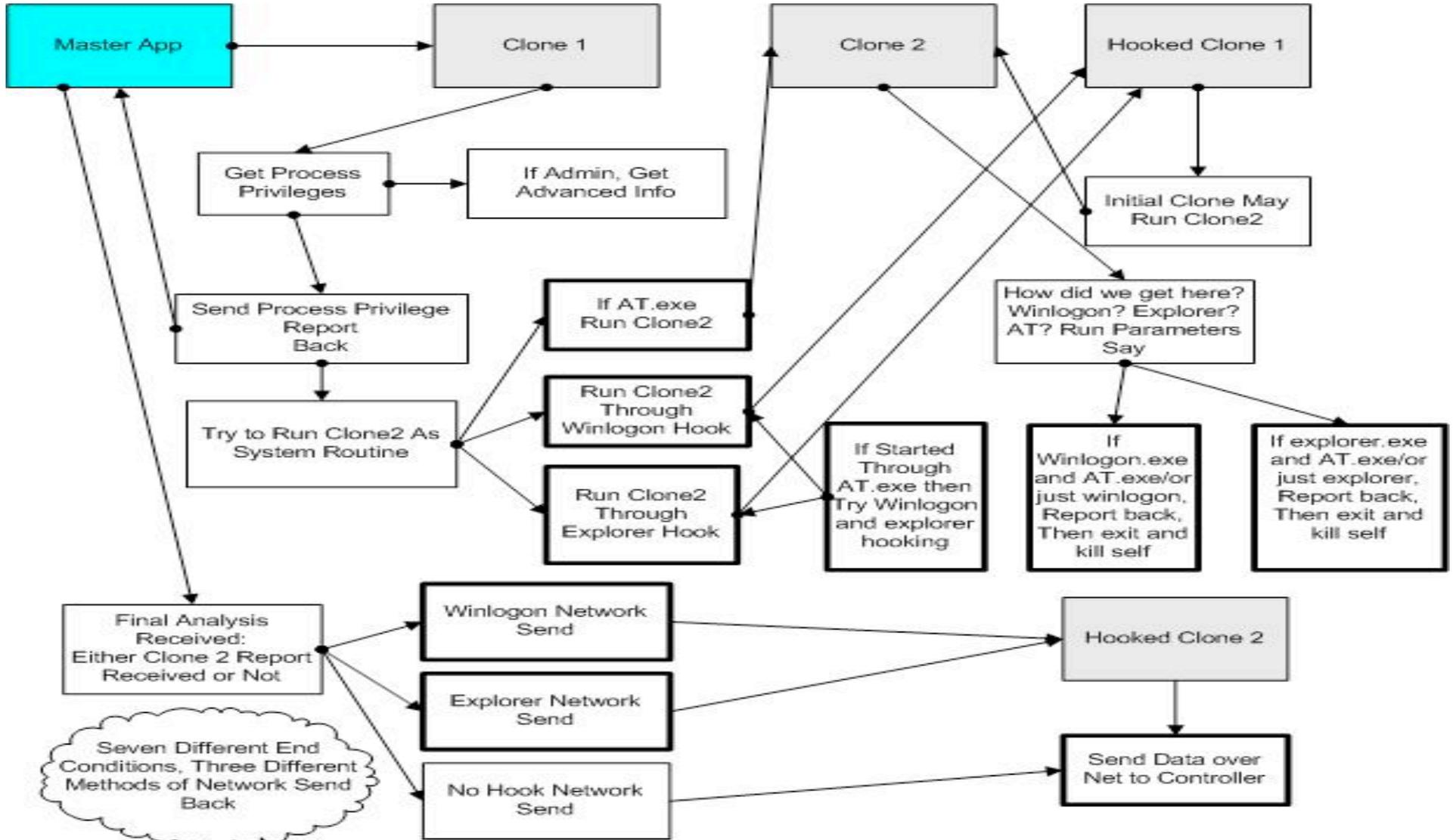


- **Secondary diagnostic attack involves attempting to hook into winlogon and running another clone as system through this attack**
- **One clone attempts further to hook into explorer.exe to run another clone**
- **Hooking is important for further obfuscation of clones**
- **If hooking fails system and/or local, all is reported to master system**

Final ARS Stages

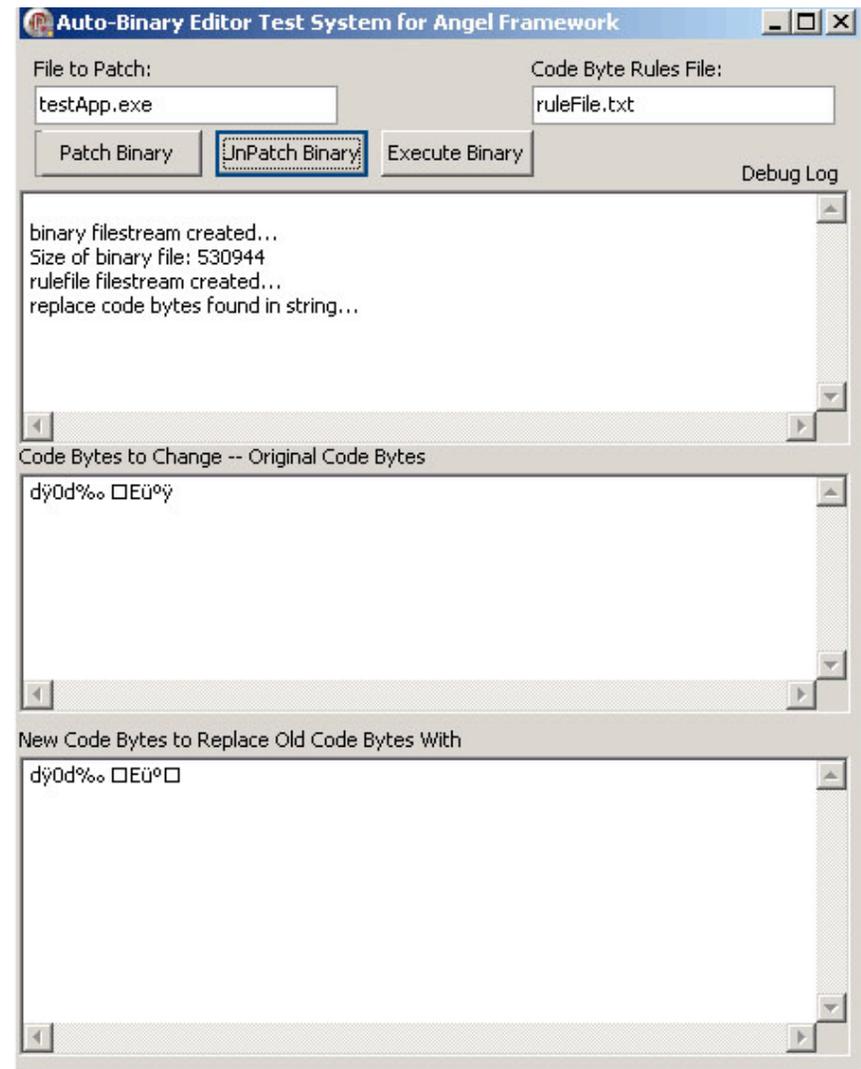
- **Final Stage of ARS is simple:**
 - NH-U (No Hook Userland)
 - NH-S (No Hook System)
 - UH-U (User Hook Userland)
 - UH-S (User Hook System)
 - SH-S (System Hook System)
 - SH-A (System Hook Admin No AT.EXE)
 - Never ran clone

Visual Tree of ARS Runthrough



Two Example Attack Endpoints to ARS

- **Two Example Attack endpoints ARS might have in offensive applications:**
 - Additional timer binaries which sleep on system controlling master binary for optimum survivability
 - Secondary backdoor mechanism, such as illustration where third party apps are changed minor byte to introduce backdoor security flaw



Defensive Application of ARS

```

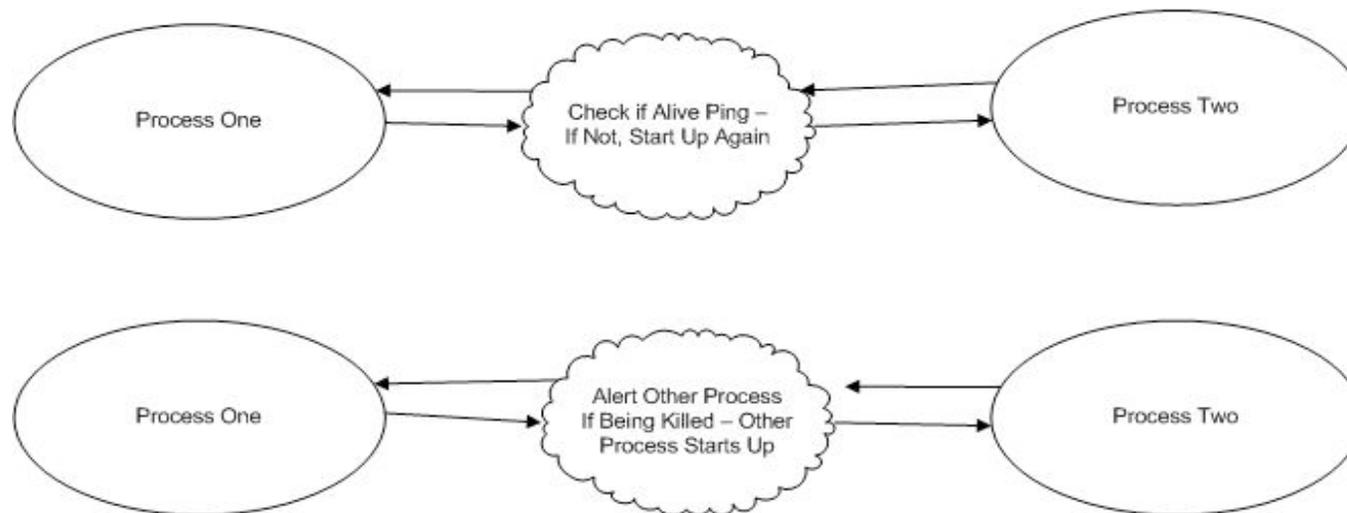
ARS Central Reporting Server Prototype
7001 Stop Start Local Test (Visible) Start Local Test (Invisible)
Raw Debug Output
...Clone One Killed Off After Stage One...
...Clone Two timer started...
...
...
... timer one for clone one shut off...
... wait now for one minute for Clone Two to start up...
... timer two starting up
... SUCCEEDED: Clone Two Created As System through AT.EXE ...
... now trying hooking winlogon.exe, if failed, explorer.exe...
... SUCCEEDED: clone two setup file found and deleted...
STAGE THREE INITIATING
... wait while timer two runs again to test hooking...
... SUCCEEDED: Clone Two Created As System through Winlogon Hook ...
... SUCCEEDED: System Level Hook ...
... SUCCEEDED: Run as System Through AT.EXE Also ...
... SUCCEEDED: clone two setup file found and deleted...
SH-S (System Hook System) AT.EXE
  
```

```

C:\Documents and Settings\drew.DCOPLEY\Desktop\@Angel\@Angel_Server\Angel_Recon_System.e...
W32Time
W3SVC
winmgmt
wuaucler
WZCSVC
... end list of active services...
... AT Running...
... SUCCEEDED STAGE ONE ...
...Clone One Killed Off After Stage One...
...Clone Two timer started...
...
... timer one for clone one shut off...
... wait now for one minute for Clone Two to start up...
... SUCCEEDED: Clone Two Created As System through Winlogon Hook ...
... SUCCEEDED: System Level Hook ...
... SUCCEEDED: Run as System Through AT.EXE Also ...
... SUCCEEDED: clone two setup file found and deleted...
STAGE THREE INITIATING
SH-S <System Hook System> AT.EXE
  
```

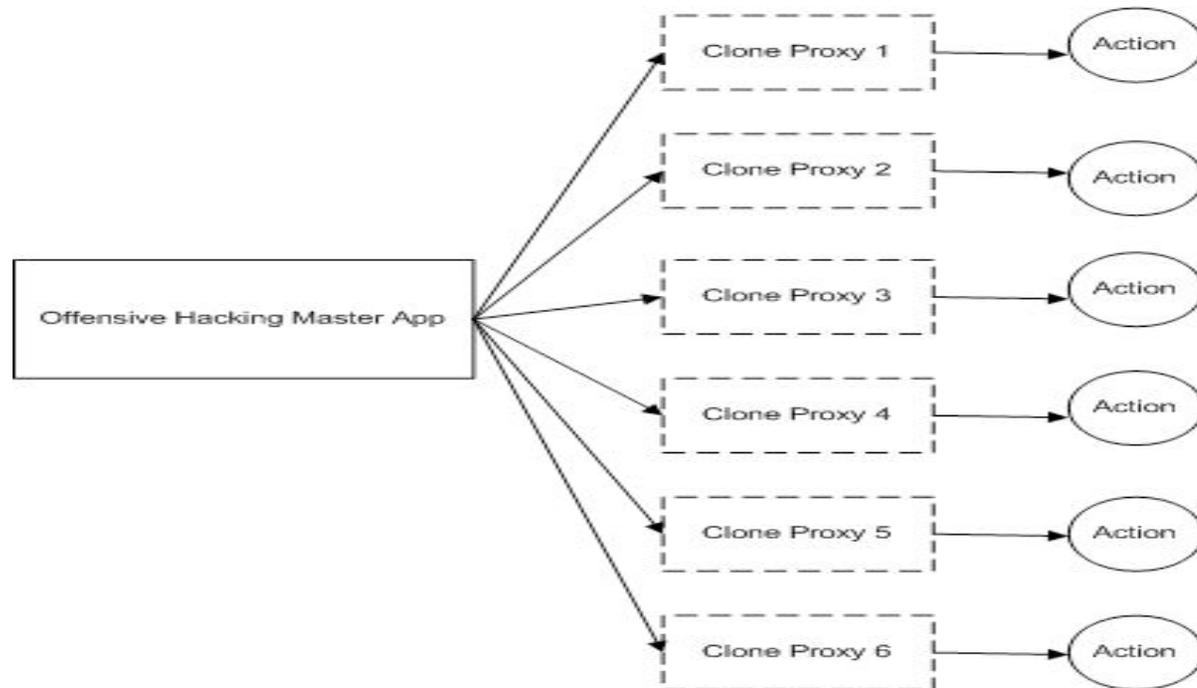
- **Defensive applications of ARS**
- **Created server system which reads in remote ARS information**
- **A little heuristic vulnerability analysis system**

Previous Work Similar to ARS



- **Oddly, there is not a lot of similar previous work to ARS**
- **Several applications have had dual process/binary systems for survivability – kill one process, the other process starts that process up again**
- **At least one app used ARS type functionality to test application firewalls**
- **Rootkits & Spyware**
- **Multiple Backdooring not new and common sense**

Multi-Layered Process/Binary Protection



- Consider this like a malicious threading model: only where malicious actions are performed by cloned, temporary processes and binaries
- Linear progression likely best, however, to ensure stealth

Conclusions

- **ARS was created for training purposes for US government employees**
- **ARS was designed to highlight the concepts spoken of here**
- **The means *IS* the end**
- **Thinking different is required in security – thinking different is empathy, empathy for your enemy is required to attack and defend against your enemy**
- **9/11 tells us all how crucial intelligence and counter-intelligence is to national defense and global defense... intelligence is the one thing that could have prevented 9/11**
- **Intelligence is all about information and IT is all about Information Systems**