QUESTNet 2004

Are You Spamming Today?

Matthew Sullivan <matthew@sorbs.net>

SORBS
Fighting spam by finding and listing Exploitable Servers.

Let there be light...

In the beginning there was the humble mailserver….

3rd May 1978 brought the first recorded 'Email' spam, though 5th March1994 was generally considered the birth of spam as we know it.

24th May 1988 brought the first recorded USENET spam (which is also is considered the first USENET scam)

References:
http://www.templetons.com/brad/spamreact.html
http://www.theregister.co.uk/2004/03/05/spam/

SORBS
Fighting spam by finding and listing Exploitable Servers.

Open SMTP Relays

The humble Open Relay SMTP Server
Mail Abuse Prevention System (MAPS)
Open Relay Blocking System (ORBS)
ORBZ, ORDB, SORBS, DSBL, NJABL….
OpenRBL, Moensted...

References:
http://www.mail-abuse.org/
http://www.openrbl.org/
http://www.moensted.dk/

SORBS
Fighting spam by finding and listing Exploitable Servers.

Open Proxy Servers

The Open HTTP Proxy Server
SQUID can be used for spam? Never!!
AnalogX, CCProxy, WinGate…etc…
The Open SOCKS Proxy Server
AnalogX, CCProxy, WinGate... Sound familiar?
Spam and Open Relay Blocking System (SORBS)
Blitzed Open Proxy Monitor (Blitzed OPM)
NJABL, DSBL, MAPS-OPS

References:
http://www.dnsbl.sorbs.net/proxy.html
http://www.sorbs.net/
http://www.blitzed.org/bopm/

SORBS
Fighting spam by finding and listing Exploitable Servers.

Quick Recap

The Open SMTP Relay Server
The Open HTTP Proxy Server
The Open SOCKS Proxy Server

More to consider..
The Open FTP Proxy Server
The Open HTTP Web Server

(cont.)

SORBS
Fighting spam by finding and listing Exploitable Servers.

What The!?!

The Open Cisco Router…
The Open Netgear DSL Modem…
The Open Cable Modem…
The Open Telnet Server…
The Open DOS Prompt…
The Open VNC Server...
The Open Web Server (scripts)

References:
http://www.dnsbl.sorbs.net/
http://www.unicom.com/sw/pxytest/
http://www.cisco.com/

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

SoBig

- A - Mails a notification to a certain user.
- C - Connects to a Predefined list of servers
- E - Connects to a Predefined list of servers
  Opens UDP ports 995 through 999
- F - Downloads code from predefined URLs
  Opens UDP ports 995 through 999
  Sends commands to UDP port 8998

References:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.E
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.F

Trojans and Viruses

Beagle/Bagle

- A - Opens Backdoor on TCP Port 6777
- B - Opens Backdoor on TCP Port 8866
- C/G - Opens Backdoor on TCP Port 2745
- I - Spreads via shares and email
- J - Opens Backdoor on TCP Port 2745
- L - Opens Backdoor on TCP 11117
  Introduces Banlist

Trojans and Viruses

Beagle/Bagle (continued)

- M - Opens Backdoor on TCP Port 2556
  Attempts to stop NETSKY from running.
- U/V - Opens Backdoor on TCP Port 4751
  Connects to remote server.
- X - Opens Backdoor on TCP Port 2535
  Attempts to stop NETSKY from running.
- Y - Opens Backdoor on TCP Port 18881
  Uses Banlist & sends IP and Port of it's Proxy

Trojans and Viruses

Mitgliedr

- A - Opens Backdoor on TCP Port 23888
- B/D - Opens Backdoor on TCP Port 39999
- C - Opens Backdoor on TCP Port 35555
- E - Opens Backdoor on TCP Port 39714
- F - Opens Backdoor on Ports 39999 & 3512
- H - Opens Backdoor on Ports 17771 or 14441
  Uses a downloaded banlist.

Trojans and Viruses

Mitgliedr (continued)

- T - Opens random TCP Port as a Mail Server
  Employs a Banlist
- X - Opens SMTP Relay/Backdoor on Port 14247

Trojans and Viruses

NETSKY

- A - Propagates via P2P Networks
- B - Similar to .A
  Removes My.Doom Registry Entries
  Removes MiMail Registry Entries
- C - Notable for the included text:

<-<- we are the skynet - you can't hide yourself! - we kill malware writers (they have no chance!) - [LaMeRz->]MyDoom.F is a thief of our idea! - -
< SkyNet AV vs. Malware >- ->->

Trojans and Viruses

NETSKY (continued)

- D/E - Removed Registry Entries for:

MyDoom.A, MyDoom.B, MiMail.T

NETSKY.A, NETSKY.B, DEADHAT.B

Bagle.B, Nachi.B, Nachi.C, PE_Parite.A

Contains the following text:

be aware! Skynet.cz - -->AntiHacker Crew<--

Trojans and Viruses

NETSKY (continued)

- F - Removed Registry Entries for:

MyDoom.A, MyDoom.B, MiMail.T

NETSKY.A, NETSKY.B, DEADHAT.B

Bagle.A, Bagle.B, Bagle.E, Bagle.F

Bagle.G, Bagle.H, Nachi.B, Nachi.C

PE_Parite.A

Contains the following text:

Skynet AntiVirus - Bagle - you are a looser!!!!

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

NETSKY (continued)

- G - Removed Registry Entries for:

Bagle.A, Bagle.B, Bagle.C, Bagle.D

Bagle.E, Bagle.F, Bagle.G, Bagle.H

Bagle.I, Bagle.J, Bagle.K

Also removes entries listed in NetSky.F

Contains the following text:

“Netsky AntiVirus - Give up, bagle & mydoom, dude! You are fucking your mother! I want to meet you in the U,S.A, Road-App time enc:[fg.od.jgij], and the you will know what pain is”

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

NETSKY (continued)

- K - Opens Port 26 which will deinstall itself.

Contains the following text:

Skynet AntiVirus - We want to destroy malware writers business, including MyDoom & Bagle. To F-Secure and so on, we do not want damage systems, we only want to avoid that Bagle continues his dirty business. We have respect of your work (Your heuristic scan is not good enough! Make it better). When the beagle and mydoom loose, we wanna stop our activity. thats now. And personal words to mydoom: Your are so shitty i never seen in my life. A Sample is bin laden and saddam. Your are more, more as more. worse than bad, the only worst. I cannot describe you, you're so lame. And to the mydoom thiefs: You will go into the prison next time in texas, nice to meet the bagle author there. Eat my shit, its similar your food, you know. And do not watch too much porn. Last words to all AV firms: We are the Skynet, not netsky! You can use commands on port 26 to deactivate the Skynet!. This is the last version of our antivirus. The source code is available soon. Note that the optimization limit is also reached. You can't get more with smtp engines. bagle and mydoom can continue his dirty impact. The 11th of march is the skynet day.

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

NETSKY (continued)

- P - Removes Registry Entries as before.

Uses MIME exploit to auto execute

Contains the following text:

U'l't'i'm'a't'i'v'e 'E'n'c'r'y'p't'e'd 'W'o'r'm'D'r'o'p'p'e'r' 'b'y 'S
'k'y'N'e't'.'C'Z' 'C'o'r'p*'"D'r'o'p'p'e'd'S'k'y'N'e't"S'k'y'N'e'
t'F'i'g'h't's'B'a'c'k

B+a+g+l+e, d+o+ n+o+t+ d+e+l+e+t+e S+k+y+N+e+t.Y+o+u f+u+c+k+e+d
b+i+t+c+h! W+a+n+n+a g+o i+n+t+o
a p+r+i+s+o+n?W+e a+r+e t+h+e o+n+l+y A+n+t+i+V+i+r+u+s, n+o+t
B+a+g+l+e, s+h+u+t u+p a+n+d
t+a+k+e y+o+u+r b+u+t+t+e+r+f+l+y! -
M+e+s+s+a+g+e f+r+o+m S+k+y+N+e+t A+V T+e+a+m
+L+e+t+s +j+o+i+n +a+n +a+l+l+i-A-n-C-e-,+b+a+g+l+e+!

References:
http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

NETSKY (continued)

- S - Opens Backdoor on TCP Port 6789

Contains the following text:

SOW WE HAVE PROGRAMMED OUR BACKDOOR,
IT CANNOT BE USED FOR SPAM RELAYING
,ONLY FOR NKYNET DISTRIBUTION,
OUR ADVICE: EDUCATE THE USERS OR
UPDATE THE SMTP PROTOCOL, AND HEURISTICS
CANNOT DETECT NKYNET, BECAUSES
NUMEROUS SCAMBLER, COMPRESSORS, AND
PROTECTORS EXISTS INCLUDING PROGRAMMING
NEW FEATURES.
OHANKS TO RUSSIA, AND THANKS TO WWW
FOR SUPPORT.
09:34 J.H, XUSSIA

SORBS
Fighting spam by finding and listing Exploitable Servers.

Trojans and Viruses

NETSKY (continued)

- T - Opens Backdoor on TCP Port 6789

Launches DoS on a few sites

Contains the following text:

Now we have programmed our backdoor,
it cannot be used for spam relaying
,only for Skynet distribution,
our advice: educate the users or
update the smtp protocol, and heuristics
cannot detect Skynet, becauses
numerous scambler, compressors, and
protectors exists including programming
new features.

Thanks to russia, and thanks to CCC
for support.

09:34 A.M, Russia

Trojans and Viruses

NETSKY (continued)

- V - Spreads via IE vulnerabilities

Uses Ports 5556 and Port 5557 for copying the virus from machine to machine

- W - Opens Various ports for remote control

Deletes Registry Entries for Bagle etc..

Has a new message which comments are for various political entities.

Trojans and Viruses

NETSKY (continued)

- X - Launches DoS attacks on websites.

- Y - Opens TCP Port 82 which is used to remote load and execute code.

Launches DoS attacks on websites.

- Z - Opens Backdoor on Port 665

Launches DoS attacks on websites.

Trojans and Viruses

AgoBot/rBot/rxBot

Uses RPC DCOM Buffer Overflow to spread.

Opens Ports 22226, 135 & 445

Connects to IRC servers and perform a number of IRC actions.

Performs Remote Network scanning.

Performs DoS attacks on command.

Perform remote updates.

Trojans and Viruses

Sasser

Uses LSASS Buffer Overflow to spread.

Opens Ports 5554 (FTP Protocol) & 9996

Performs remote updates.

What can be done?

Team Cymru (kum-ree)

Bogon Route Server

Dark Net

CERT & AusCERT

Alerts - Get them! Use them!

Report Incidents to LEAs & CERTs

(cont.)

References:
http://www.cymru.com/
http://www.auscert.com.au/
http://www.cert.org/

What can be done?

SORBS

ISP Alerts

Vulnerability Database & Dark Net

Spam Database

Proxy Databases

(cont.)

SORBS
Fighting spam by finding and listing Exploitable Servers.

What can be done?

PATCHING!!!!

(cont.)

SORBS
Fighting spam by finding and listing Exploitable Servers.

What can be done?

Some thoughts and ideas

Default Blocking of incoming connections..?

Default Blocking of SMTP connections..?

Rate limiting/throttling of SMTP connections..?

Default Static Allocations..?

Cleanup Fees..?

The Internet “Drivers” License..?

SORBS
Fighting spam by finding and listing Exploitable Servers.

Default Port Blocking

Default Blocking of incoming connections..?

Default Blocking of outgoing connections..?

Quarantine pools..?

Booting/Scanning Bots..?

Cleanup Fees..?

References:
http://www.washingtonpost.com/wp-dyn/articles/A25845-2003Sep4.html
http://www.nessus.org/

SORBS
Fighting spam by finding and listing Exploitable Servers.

A Final Note...

SPF, Domain Keys, etc….

SPF (Sender Policy Framework)

```
;; QUESTION SECTION:
;sorbs.net.                     IN TXT

;; ANSWER SECTION:
sorbs.net.              86400   IN TXT     "v=spf1 mx a:oblivion.isux.com
a:ppp.isux.com a:mail.isux.com include: uq.edu.au -all "

;; QUESTION SECTION:
;sorbs.net.                     IN MX

;; ANSWER SECTION:
sorbs.net.              21600   IN MX 5    stealth.sorbs.net.
sorbs.net.              21600   IN MX 10   goliath.sorbs.net.
sorbs.net.              21600   IN MX 15   corkscrew.sorbs.net.
sorbs.net.              21600   IN MX 20   oblivion.sorbs.net.
```

References:
http://spf.pobox.com/
http://spf.pobox.com/wizard.html

SORBS
Fighting spam by finding and listing Exploitable Servers.

Questions..?

SORBS
Fighting spam by finding and listing Exploitable Servers.


Thank You
Matthew Sullivan
SORBS
Fighting spam by finding and listing Exploitable Servers.