Layer 8

And why people are the most important security tool

Damon “ch3f” Small

Special Thanks to…

- **Wall of Sheep**
- **My Employer**
- **My Wife & Editor**

You!

About NCC Group

GLOBAL CYBER SECURITY & RISK MITIGATION SPECIALIST

2000+ employees worldwide

35+ OFFICES ACROSS EUROPE, NORTH AMERICA, ASIA-PACIFIC & MIDDLE EAST

HELPING 15,000 ORGANIZATIONS WORLDWIDE TO MANAGE RISK & LIMIT THREAT OF CYBERCRIME

LISTED COMPANY FORMED IN JUNE 1999

GROUP REVENUE FOR YEAR END MAY 2016 £209.1m

Our Security Consulting Services

- Application Security
- Strategic Infrastructure Security
- Mobile Security
- Cryptography Services
- Digital Forensics & Incident Response
- Risk Management & Governance
- Security Training
- Bug Bounty Services

Office Locations

Europe
Manchester - Head Office
Basingstoke
Belgium
Cheltenham
Denmark
Edinburgh
Germany
Glasgow
Leatherhead
Leeds
Lithuania
London
Luxembourg
Milton Keynes
Spain
Sweden
Switzerland
The Netherlands

USA
Atlanta, GA
Austin, TX
Chicago, IL
New York, NY
San Francisco, CA
Seattle, WA
Sunnyvale, CA

Australia
Sydney

Canada
Kitchener, ON

Middle East
Dubai

About ch3f

Damon J. Small, Technical Director, NCC Group North America

- **In IT since 1995; Infosec since 2001**
- **Louisiana native – Geaux Tigers!**
- **Studied music at LSU; grad school in 2005 for Information Assurance (Norwich University)**
- **Blue Team Infosec**
  - Healthcare
  - Department of Defense
  - Aerospace (Johnson Space Center)
  - Oil & Gas

How This Slide Deck Came to be

- I am a digital pack-rat
- Found a couple of old whitepapers
- Was shocked that they were still relevant (thanks, Wall of Sheep)
- Techniques described are simple and old, but remain useful
- I love telling stories
- Coincidentally, WannaCry self-propagating ransomware happened

Audience Poll

Introduction

- **IT departments face myriad security-related products**
- **Businesses need to remain fiscally responsible**
- **Are we overlooking the value of human ingenuity and the skills of our practitioners?**

Finding the Needle

December 9, 2004

- **Primary firewall failed**
- **Large volume of tcp/135 traffic**
- **Periodic bursts of Internet-bound traffic on ephemeral ports**

Escalation

- **Malicious software suspected**
- **Barriers**
  - Spoofed source IP Addresses
  - Third-party-supported systems
  - 8,000 workstations
  - Networking team had protocol analyzers, but not the ability to monitor traffic in real-time
- **Due to these limitations, they could proceed no further**
- **Network team (begrudgingly?) engaged the infosec team**

We Needed to Know…

- From where the traffic came
- To where the traffic was going
- What was causing it
- How to get rid of it

Detective Methods

- **Commercial AV**
- **IPS**
- **WinDump**

```
windump -qn dst port 135
```

Identification Begins

- **Desktop team ran manual AV scans**
- **Found various self-propagating worms**
  - RPC/DCOM
  - LSASS buffer overflow
- **Looked like Blaster and Sasser**
- **Patches existed, but recall that it was 2004**

Botnet Worms

- **Command & Control via Internet Relay Chat (IRC)**
- **Worm logs into IRC channel & receives instructions from the bad guy**
- **Attacker can then use these “zombie” computers for other malicious activities**
- **NOTE TO SELF – enable egress filtering rules!**
- **Traffic from the worm propagating and logging into IRC channel crippled the network**

Gathering More Data

- **AV continued to be of limited value**
- **Security team enabled IRC login event rules on the IPS**
- **Found 3 malicious IRC channels**
  - xxx.xxx.xxx.189
  - xxx.xxx.xxx.94
  - xxx.xxx.xxx.228
- **Blocked IRC login events but this created another problem – we couldn't see the RFC1918 addresses**

Why Architecture Matters

- **IPS existed on the “dirty side” of the firewall**
- **IPS could only see NAT’d IP Addresses once we started blocking**
- **Was useful for stopping the infected hosts but couldn’t help us find them**
- **NOTE TO SELF – put the IPS *inside* the firewall**

Windump to the Rescue Again

Simply capturing traffic provided invaluable information, but was difficult to parse

```
windump -qn host xxx.xxx.xxx.189
or host xxx.xxx.xxx.94 or host
xxx.xxx.xxx.228
```

Snort to the Rescue

```
alert tcp $HOME_NET any -> $BOTNET any (msg:"BOTNET traffic
detected"; rev:1;)
```

Where $BOTNET = xxx.xxx.xxx.189, xxx.xxx.xxx.94, xxx.xxx.xxx.228

```
NICK [UL]987199
USER fvxtkcav 0 0 :[UL]987199
:0wnd.us 001 [UL]987199 :Welcome to the hi
IRC Network [UL]987199!
fvxtkcav@172.16.21.50
:0wnd.us 002 [UL]987199 :Your host is
0wnd.us, running version Unreal3.2.1
:0wnd.us 003 [UL]987199 :This server was
created Fri Nov 19 2004 at 05:01:26 MST
:0wnd.us 004 [UL]987199 0wnd.us
Unreal3.2.1 iowghraAsORTVSxNCWqBzvdHtGp
lvhopsmntikrRcaqOALQbSeKVfMCuzNT
```

:**0wnd.us** 005 [UL]987199 MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTARGETS=20 AWAYLEN=307:are supported by this server
:**0wnd.us** 005 [UL]987199 WALLCHOPS WATCH=128 SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(ohv)@%+ CHANMODES=beqa,kfL,l,psmntirRcOAQKVGCuzNSMT NETWORK=hi CASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT :are supported by this server

:0wnd.us 251 [UL]987199 :There are 1 users and 4253 invisible on 1 servers
:0wnd.us 252 [UL]987199 3 :operator(s) online
:0wnd.us 253 [UL]987199 5 :unknown connection(s)
:0wnd.us 254 [UL]987199 24 :channels formed
:0wnd.us 255 [UL]987199 :I have 4254 clients and 0 servers:0wnd.us 265 [UL]987199 :Current Local Users: 4254 Max: 7852

:0wnd.us 332 [UL]987199 #UL# :.asc lsass_445 100 5 99999 -b
PRIVMSG #UL# :[SCAN]: Sequential Port Scan started on 10.32.0.0:445 with a delay of 5 seconds for 99999 minutes using 100 threads.

PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.1.93.
PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.2.43.
PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.2.120.
PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.2.194.
PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.2.230.
PRIVMSG #xpl-ul# :[lsass_445]: Exploiting IP: 10.32.3.129.

```
:l0ngb0ng!b0ng@cows.are.great PRIVMSG #UL#
:.syn xxx.xxx.xx3.14 6667 600 0 -s
:l0ngb0ng!b0ng@cows.are.great PRIVMSG #UL#
:.syn xxx.xxx.xx0.14 6667 600 0 -s
:x3n!admin@admin PRIVMSG #feck :!ddos.udp
xxx.xxx.xxx.158 1000 9500 15 6667 -s
```

Mitigation/Cleanup Process

- **Anti-Virus was ineffective**
  - Non-functional
  - Third-party-supported devices
  - Biomedical devices (don’t get me started on FDA 510K)

Sniff for the C&C IRC Channels

- We knew to where the infected hosts were phoning home
- We knew which hosts were infected
- We knew which port the infected host was using

```
23:24:46.665481 10.11.3.134.1303 >
192.168.163.189.18067: tcp 0 (DF)
```

Finding the Offending Process

- **Use fport to find which process is using which port**

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.

Pid    Process        Port   Proto  Path
[…]
1292   AClntUsr ->   1132   TCP    C:\Program
Files\Altiris\AClient\AClntUsr.EXE
664    shellker ->   1133   TCP    C:\Program
Files\Altiris\CarbonCopy\shellker.exe
8      System ->     1295   TCP
232    lsass ->      1300   TCP    C:\WINNT\system32\lsass.exe
1420   w32usb2 ->       1303   TCP    C:
\WINNT\system32\w32usb2.exe
8      System ->     1306   TCP
```

Stopping the Malicious Process

- **In those days, removing involved simply deleting the file**
- **You can’t delete files that are in use**
- **We stopped the process remotely using PSKill**

```
C:\tools\forensics\pstools>pskill \\10.11.3.134 w32usb2

PsKill v1.03 - local and remote process killer
Copyright (C) 2000 Mark Russinovich

Process w32usb2 killed on 10.11.3.134.
```

Botnets Discovered

In all, we found at least 4 different botnet worms

- **Spybot or Wootbot10**
  - Infected file: w32usb2.exe
- **Randex, Spybot, Rbot, or SDBot11**
  - Infected file: bling.exe
- **SDBot, Rbot, or Spybot12**
  - Infected file: crsss.exe
- **Rbot.JP13**
  - Infected file: mswctl32.exe

Lesson

“Knowing which screw to turn.”

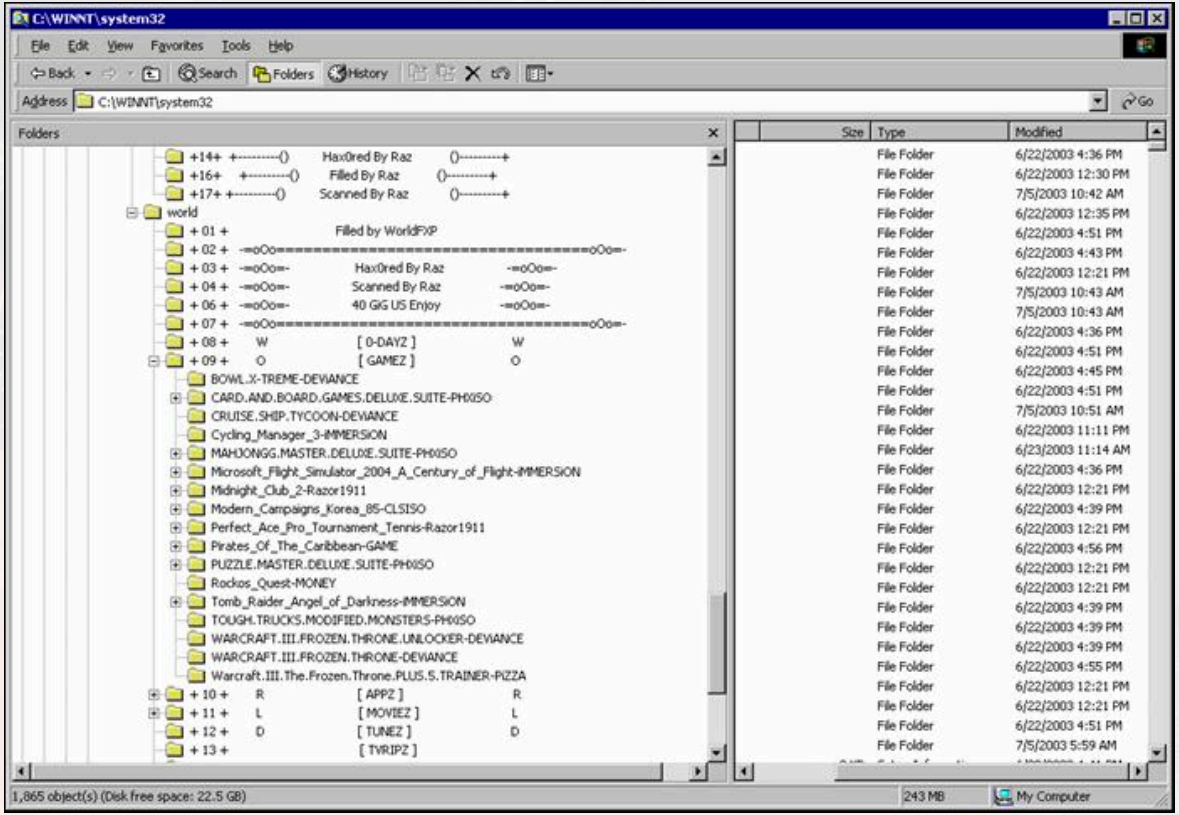
- **None of what we did was difficult**
- **Most of what we did relied on basic tools**
- **Understanding the nature of the problem in the context of the incident, based on decades of collective experience by talented infosec staffers, resulted in the malware being eradicated**
- **These years-old techniques are still relevant**

WebDAV

DMZ Server got pwned on July 5, 2003

- **Rogue FTP site**
- **Disks filled**
- **Patches applied by hacker**

Checked C:\ When Suddenly…



Nmap to the Rescue

```
# nmap (V. 3.00) scan initiated Sat Jul 05 10:19:26 2003 as: nmap -O -oN d:
\nmap.complete.log -p 1-65535 <IP address deleted>
Interesting ports on <IP address deleted>:
(The 65521 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
135/tcp    open        loc-srv
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
445/tcp    open        microsoft-ds
[…]
1978/tcp   filtered    unknown
2003/tcp   open        cfingerd
3372/tcp   open        msdtc
3389/tcp   open        ms-term-serv
3460/tcp   open        unknown
```

Fport Again

- **Showed port 2003 being used by “winmgnt”**
- **Not to be confused with the legitimate process “winmgmt”**

Telnet to port 2003 (1 of 2)

```
                    -= Welcome To =-
                 -= Antoher Raz Stros =-

                 -=PERSONAL INFORMATION=-

 ¤ Your login is : ............................... %Name
 ¤ You are connected from the address ip : .... %IP
 ¤ Your current repertoire : ........................... %Dir
 ¤ You are connected since : ............................ %TconM Min
```

Telnet to port 2003 (2 of 2)

```
-=SERVER STATISTICS=-

   ¤ Hour and local date : ................. %time at %date
   ¤ This server is up since:.............. %ServerDays Days, %ServerHours Hours,
%ServerMins Mins, %ServerSecs Secs
   ¤ Times since the last revival : ..... %ServerDays days,%serverHours hours,
%serverMins mins and %serverSecs secs
   ¤ Usage since the last ones 24 H : .................. %U24h
   ¤ Users since the beginning : ..................... %UAll
   ¤ Current users : ............................. %UNow
   ¤ Files transferred : ............................. %ServerFilesDown files
   ¤ Total transferred in Kbytes : ...................... %ServerKbDown
   ¤ Files uploaded : ................................ %ServerFilesUp files
   ¤ Total uploaded in kbytes : ......................... %ServerKbUp
   ¤ Actual bandwidth : ........................... %ServerKBps Kb/sec
   ¤ Average bandwidth : ............................ %ServerAvg Kb/sec
   ¤ Free space on CD : ............................. %Dfree
```

RB.bat – install script for FTP Site

```
SET MXHOME=C:\winnt\system32\wins\
SET MXBIN=C:\winnt\system32\wins

C:\winnt\system32\wins\firedaemon -i servU "C:\winnt\system32\wins" "C:
\winnt\system32\wins\winmgnt.exe" "" Y 0 0 0 Y

C:\winnt\system32\wins\firedaemon -i secureNt "C:\winnt\system32\wins" "C:
\winnt\system32\wins\SecureNetbios.exe" "" Y 0 0 0 Y

C:\winnt\system32\wins\firedaemon -i secureBT "C:\winnt\system32\wins" "C:
\winnt\system32\wins\secure.bat" "" Y 0 0 0 Y

net start iroffer
net start servU
net start secureNt
net start secureBT
```

Hacker Patched our System…

```
echo ------------------------------------------------------------
echo This Tools Disable The W3SVC / IISADMIN / ISSRESET
echo (c) 2003 by Granny Smith // Admin of DarkStormFXP
echo ------------------------------------------------------------
echo.
echo Disabling Services...
echo.
net stop w3svc
net stop iisadmin
IISRESET.EXE /STOP
IISRESET.EXE /DISABLE
echo.
echo Creating Reg-Entry for Disable the WebDav...
echo.
echo Windows Registry Editor Version 5.00 > protect.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servi
ces\W3SVC\Parameters] >> protect.reg
echo "DisableWebDAV"=dword:00000001 >> protect.reg
regedit /s protect.reg
reg.exe IMPORT protect.reg
del protect.reg
echo.
echo All Done ... Enjoy It ...
echo
pause
echo on
```

…Then Began Looking for New Victims

```
COMMAND: sfind -webdav xxx.xxx.0.0 xxx.xxx.255.255
xxx.xxx.34.14 Webdav Enabled!
xxx.xxx.39.145 Webdav Enabled!
xxx.xxx.39.148 Webdav Enabled!
xxx.xxx.44.220 Webdav Enabled!
xxx.xxx.47.11 Webdav Enabled!
xxx.xxx.53.6 Webdav Enabled!
xxx.xxx.57.235 Webdav Enabled!
xxx.xxx.81.41 Webdav Enabled!
xxx.xxx.86.146 Webdav Enabled!
xxx.xxx.86.228 Webdav Enabled!
xxx.xxx.153.39 Webdav Enabled!
xxx.xxx.153.35 Webdav Enabled!
xxx.xxx.153.51 Webdav Enabled!
xxx.xxx.153.137 Webdav Enabled!
xxx.xxx.153.147 Webdav Enabled!
xxx.xxx.153.151 Webdav Enabled!
xxx.xxx.153.155 Webdav Enabled!
xxx.xxx.154.135 Webdav Enabled!
xxx.xxx.153.237 Webdav Enabled!
Scan Complete!
```

Hacker’s Calling Card

¸,ø¤°``°¤ø,¸¸,ø¤°``°¤ø,¸ ¸,ø¤°``°¤ø,¸¸,ø¤°``°¤ø,¸ ¸,ø¤°``°¤ø,¸¸,ø¤°``°¤ø,¸¸,ø¤°``°¤ø,¸

ScaNNed By Raz
HaCKed By Raz
FiLLed by WorldFXP
SpaCe FiLLed 37 GB

Several technological challenges conspired against the team during these incidents. Using both commercial and freely obtainable tools the team was able to overcome these obstacles in a resourceful and cost-efficient manner. The analysts' actions demonstrate that problems can be solved creatively using limited resources. While companies must regularly evaluate commercial products, properly trained personnel can be more valuable to an organization than any hardware or software device.

What Can We Do?

As information security professionals…

- **Spend on people first, technology second**
- **When ready to spend on technology, consider the skills of the people you already have**
- **Identify gaps**
  - Spend on training first, hiring second
- **Work outside of your organizational silos**

Thank you!

Please stay in touch

- damon.small@nccgroup.trust
- @damonsmall