Catching Worms at APNIC16

Philip Smith – APOPS BoF

APNIC16

Seoul, August 2003

Catching Worms

- No, this isn’t about feeding wildlife or preparing to go fishing!
- APNIC 16 conference network was seriously affected by both Blaster and Nachi worms

Background

- Conference network was a wireless 802.11b LAN and a terminal room of around 16 Windows XP PCs
  - On the same logical network
    - Bad design, did not allow separation of wireless and fixed networks
  - “Off the shelf” no-name basestations
    - No access, no control, no...

Diary – Monday 18th August

- Arrived at Lotte Hotel, Seoul-Jamsil, 8pm
- Network performing “poorly”
  - Router or WAN link problems suspected
- Obtained access to 7200 gateway router courtesy of local host
  - Repaired configuration, introducing AAA, inbound packet filters on WAN link, and other IOS best practices configuration
  - Switched on NetFlow, discovered attacks on tcp/135 emanating from several local hosts

18th August

- From looking at MAC addresses of the PCs in question, all from same manufacturer
  - Checked PC terminal room – match!
  - Most PCs seemed to be infected with Blaster
  - Infections were causing considerable amounts of network traffic
  - Requested the local hosts to install the Microsoft patch, and clean the systems

18th August

- Summary – at midnight:
  - Router Inbound filters – so hopefully no infections can come from the outside now
  - PCs requested to be cleaned and patched – so hopefully no more unsolicited network traffic from them

19th August – morning

- Calm before the Storm
  - Morning passed by, tutorials were taught, etc
  - Post tutorial, urgent request to investigate the router, as the wireless network had completely stopped, people were complaining, and router/routing or network problems were suspected

19th August – afternoon

- Chasing Worms
  - Netflow on 7200 revealed that many hosts on the conference network were ping flooding random IP addresses
  - Traffic on internal LAN was around 4Mbps inbound, 3Mbps outbound – tall order for an 11Mbps bridged wireless LAN
  - NetFlow also revealed that around 2Mbps of inbound ICMP flood was coming from the outside world

Chasing Worms: From the Inside

- Typical NetFlow signature:
  - show ip cache flow | i Null

```
SrcInt    SrcAddr        DestInt   DestAddr        Pr SrcPt DstPt Pkt
Fa0/0     221.143.6.155  Null      221.140.47.86   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.87   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.84   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.85   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.82   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.83   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.80   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.81   01 0000  0800   1
Fa0/0     221.143.6.155  Null      221.140.47.78   01 0000  0800   1
```

Chasing Worms: From the Outside

- Typical NetFlow signature:
  - show ip cache flow | i Null

```
SrcInt      SrcAddr          DestInt    DestAddr         Pr  SrcPt DstPt  Pkt
PO4/0       221.143.243.68   Null       221.143.6.55     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.56     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.57     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.58     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.51     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.52     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.53     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.54     01  0000  0800    1
PO4/0       221.143.243.68   Null       221.143.6.63     01  0000  0800    1
```

Chasing Worms

- Because of the level of ICMP, instant reaction was to block all ICMP
    - That got the wireless LAN usable again
- More refined configuration was to:
    - block ICMP echo in and outbound
    - Configurable ICMP unreachables on the 7200
    - Later in day, Nachi signature identified (92 byte ICMP echo), so ICMP echo permitted again, and specific Nachi ICMPs policy routed to Null0

Chasing Worms: Router Configuration

```
interface Null0
 no ip unreachables
!
interface FastEthernet0/0
 ip address 221.143.6.1 255.255.254.0
 no ip proxy-arp
 ip route-cache policy
 ip route-cache flow
 ip policy route-map nachi-worm
!
interface POS4/0
 ip address 211.214.255.66 255.255.255.252
 ip access-group 100 in
 ip access-group 101 out
 rate-limit input access-group 102 8000 8000 8000 conform-action transmit exceed-action drop
 rate-limit input access-group 103 32000 8000 8000 conform-action transmit exceed-action drop
 ip route-cache policy
 ip route-cache flow
 ip policy route-map nachi-worm
!
route-map nachi-worm permit 10
 match ip address 199
 match length 92 92
 set interface Null0
!
```

ICMPs dumped to Null0 don’t send unreachables back

NetFlow

Dump Nachi

Access-lists on next slide

Chasing Worms: Router Configuration

```
access-list compiled
! Inbound from the big BAD world
access-list 100 permit ip any host 211.214.255.66
access-list 100 permit ip any host 221.143.6.1
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any ttl-exceeded
access-list 100 permit icmp any any unreachable
access-list 100 deny   icmp any any log
access-list 100 permit tcp any any established
access-list 100 permit tcp any any eq 22
access-list 100 permit udp any any eq domain
access-list 100 permit udp any any eq ntp
access-list 100 permit udp any eq ntp any
access-list 100 permit udp any eq isakmp any eq isakmp
access-list 100 deny   udp any any eq 2049
access-list 100 permit udp any any gt 1023
access-list 100 permit ipinip any any
access-list 100 permit 41 any any
access-list 100 permit esp any any
access-list 100 permit gre any any
access-list 100 deny   ip any any log
```

Watching ICMP traffic

Someone we block until they get fixed

```
! What we let out
access-list 101 deny   udp any any eq netbios-ns
access-list 101 deny   tcp any any eq 135
access-list 101 deny   ip host 221.143.6.88 any
access-list 101 permit ip any any

! Rate limit ICMP echo/echo-reply
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply

! Rate limit new TCP connections
access-list 103 deny   tcp any any established
access-list 103 permit tcp any any

! Match ICMP echo for Nachi
access-list 199 permit icmp any any echo
```

Chasing Worms

- APNIC staff disinfected all the classroom PCs (which had mostly been patched, but not disinfected)
- Remaining infected systems were conference attendees using the wireless LAN
  - Harder job to track those down and fix them

Diary: Rest of Week

- Requested all attendees to ensure systems had latest Microsoft patch, and run WindowsUpdate
  - Made no difference
  - Conference week averaged around 2-5 infected laptops per day, peaking on Wednesday afternoon, after the initial cleanup on Tuesday afternoon

Diary: Rest of Week

- Brute force solution – no Internet access for perpetrators until laptops were patched and cleaned up
  - Added outbound IP filter to block miscreant IP address
  - Monitored NetFlow every 15 minutes or so
    - New miscreants added to filter, and announced at start and end of sessions

Summary

- Nachi contained, but had serious impact on wireless LAN early in the week
- Out of 180 DHCP leases, maybe 30-40 were infected overall
- Too many people had a desire to blame the router, the router configuration, the upstream ISP, or the general Internet
  - Problems were due to network traffic overload

Post Mortem Thoughts:

- PCs:
  - Connecting ANY Windows platform to the public Internet without the latest and current Microsoft patches is irresponsible
  - Not running WindowsUpdate is irresponsible
- Lack of basic filtering on and inappropriate configuration of WAN router at the start of the week was BAD
- Uncontrollable wireless base station use not recommended
- Wireless LAN must be on a separate LAN segment from PC terminal room