

Effects of Worms on Internet Routing Stability

Ido Dubrawsky 2003-06-11

The impact of worms on the Internet has increased significantly over the past five years. In particular worms such as CodeRed II, NIMDA, and the more recent SQL Slammer prove that the ability to effectively impact the Internet overall is here. This impact is not only felt at the connection endpoint where the worm takes residence and replicates itself but also on the infrastructure in-between. In the period of time that CodeRed II infection was at its most severe levels a unique effect began to be observed whereby global routing instability was detected throughout the Internet.

Border Gateway Protocol (BGP) Instability During CodeRed II / NIMDA Scanning and Propagation Phases

In their work "*Global Routing Instabilities during Code Red II and Nimda Worm Propagation*"^[1] James Cowie and Andy Ogielski of [Renesys Corporation](#) determined that such instability was not due to any specific telco point failure or fiber cut but rather from the propagation of the CodeRed II and NIMDA worms. These worms triggered a widespread end-to-end routing instability that originated at the Internet edge, which refers to endpoint or stub networks attached to an ISP core. In their work they postulate that while the majority of the traffic across the Internet flowed through the global backbones unaffected, the majority of the links at the Internet edge was markedly affected by the worms during their scanning/probing and propagation phases.

While unable to determine all of the possible reasons for such an effect Cowie and Ogielski speculate on possible causes. These include:

1. Congestion-induced failure of BGP (Border Gateway Protocol -- [RFC 1771](#)) sessions due to timeouts
2. Flow-diversity induced failures of BGP sessions due to router CPU overloads
3. Proactive response through disconnection of certain networks
4. Failures of other equipment at the Internet edge such as DSL routers and other devices

In support of item 4 above, [Cisco Systems, Inc.](#) released an [advisory](#) documenting not only Cisco products utilizing the Microsoft IIS web platform that were affected by the CodeRed worm but additional products that did not support the IIS software. These devices such as the Cisco 600 series DSL router, the 7960 IP Phone and the Aironet wireless products were affected due to *side-effects* instigated by the CodeRed II worm and not by

the worm code itself. Other vendors who also utilized the IIS web server in their products were similarly affected.

BGP, like all routing protocols, works on the basis of identifying the "best routes" to a given network.

To communicate changes in a given "best route" to a network prefix, a BGP router issues UPDATE messages to its defined peers. These peers then, in turn, update their routing tables. BGP is a TCP based protocol operating on port 179 on routers and hosts running routing software such as GateD or Zebra. Cowie and Ogielski used data gathered at several BGP monitoring points across Europe. The metrics used to identify instability in BGP were:

- Reachability and
- Rates of Change

Cowie and Ogielski define reachability as the measurement of "the number of prefixes that appear in a particular organization's routing tables at a given time."^[1] Rates of change were defined as the number of prefix announcements and withdrawals made in BGP UPDATE packets from a given organization over a specified period of time. Because of BGP's route dampening features the number of route changes to a given prefix that can be observed is on the order of once every 30 seconds. However, even given that limitation, a large number of BGP UPDATE messages are indicative of a rise in "diversity" among the observed network prefixes. Cowie and Ogielski note that these surges in BGP UPDATE messages are what distinguish routing instability from background noise. One concern is the ability to distinguish those surges that are due to CodeRed II and NIMDA from surges that are more common -- those caused by a peer BGP session undergoing a hard reset or those due to failure in the Internet infrastructure such as fiber cuts and other telco failures. The distinguishing characteristic between these surges is that surges due to telco failures result in short-term increases in the BGP prefix announcement rate that then return to the mean value within a very short period of time, on the order of several seconds or minutes. It is this characteristic (the duration of the surges and their growth rate) which determines whether something is normal background noise or a true global instability in the Internet.

In the case of CodeRed II and NIMDA, and SQL Slammer as will be noted later, the worms themselves were the source of this rise in BGP message rates lasting for a sustained period. The work done by Renesys after the CodeRed II and NIMDA worm assault on the Internet used BGP information collected from one of RIPE's Internet exchanges where approximately one dozen autonomous systems (AS) have BGP peering routers. The initial plot of the data from CodeRed is shown in Figure 1 below.

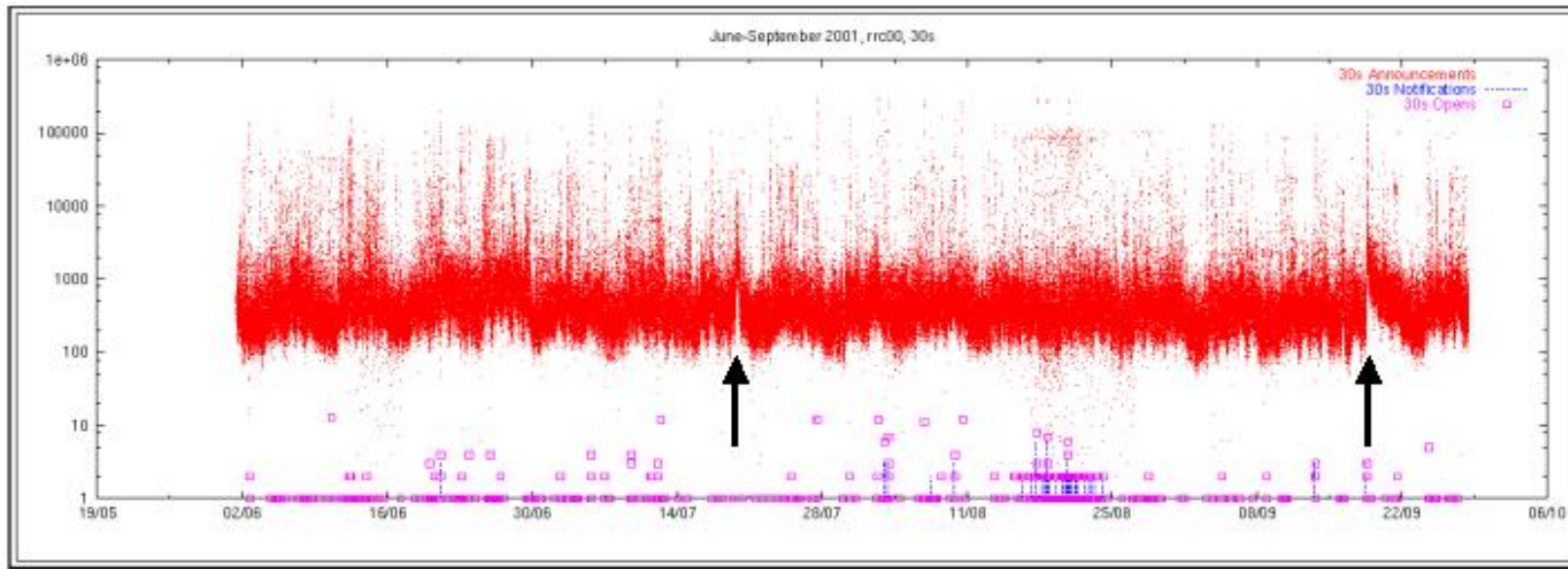


Figure 1: BGP Announcement Rates (from [1])

The two most interesting features in this plot are indicated by the two black arrows. These arrows indicate events which Cowie and Ogielski termed "BGP message storm(s)". The first arrow is an event that occurred on July 19th while the second arrow indicates a stronger event than the first occurring on September 18th. These events correlate with the main propagation phase of the two Microsoft worms, CodeRed II (in July 2001) and NIMDA (in September 2001). It is worthwhile to note that neither the Baltimore tunnel train wreck of July 18th (which severed several large fiber links) and the World Trade Center attacks of September 2001 do not impact the data in this graph at all. The reason being that each of those events, while significant in their respective locales, did not impact overall Internet routing stability *because* they were localized events. [1]

July 19th 2001 - The Impact of CodeRed II

CodeRed II began to impact the Internet on July 19th 2001. Within 14 hours over 359,000 systems had been infected with the worm [3]. The impact of the worm was easily detected through a dramatic increase in the scan rate of port 80 as shown in the two plots of Figure 2 below. The data used in these plots was recorded by the Internet Storm Center, analyzed in [1] and converted into histograms. The two plots show the scan rate for port 80 for two independent class B network spaces.

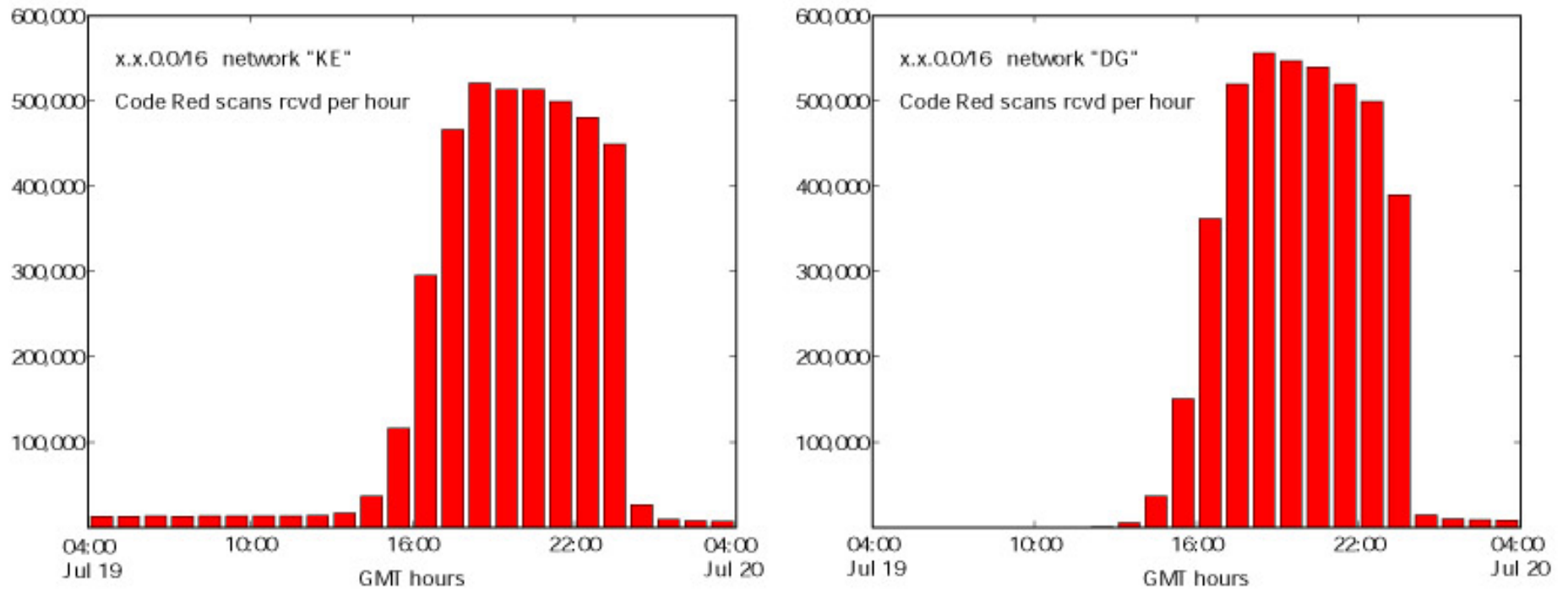


Figure 2: Port 80 Scan Rates Due to CodeRed II (from [1])

In addition to the high scan rate the CodeRed II worm propagation can also be correlated with an increase in the number of BGP route withdrawal announcements. In essence when a BGP speaking router can no longer reach a network that it transits traffic for it will announce a withdrawal of the route to that network in an UPDATE message. The increase in BGP route withdrawals is shown in Figure 3 below.

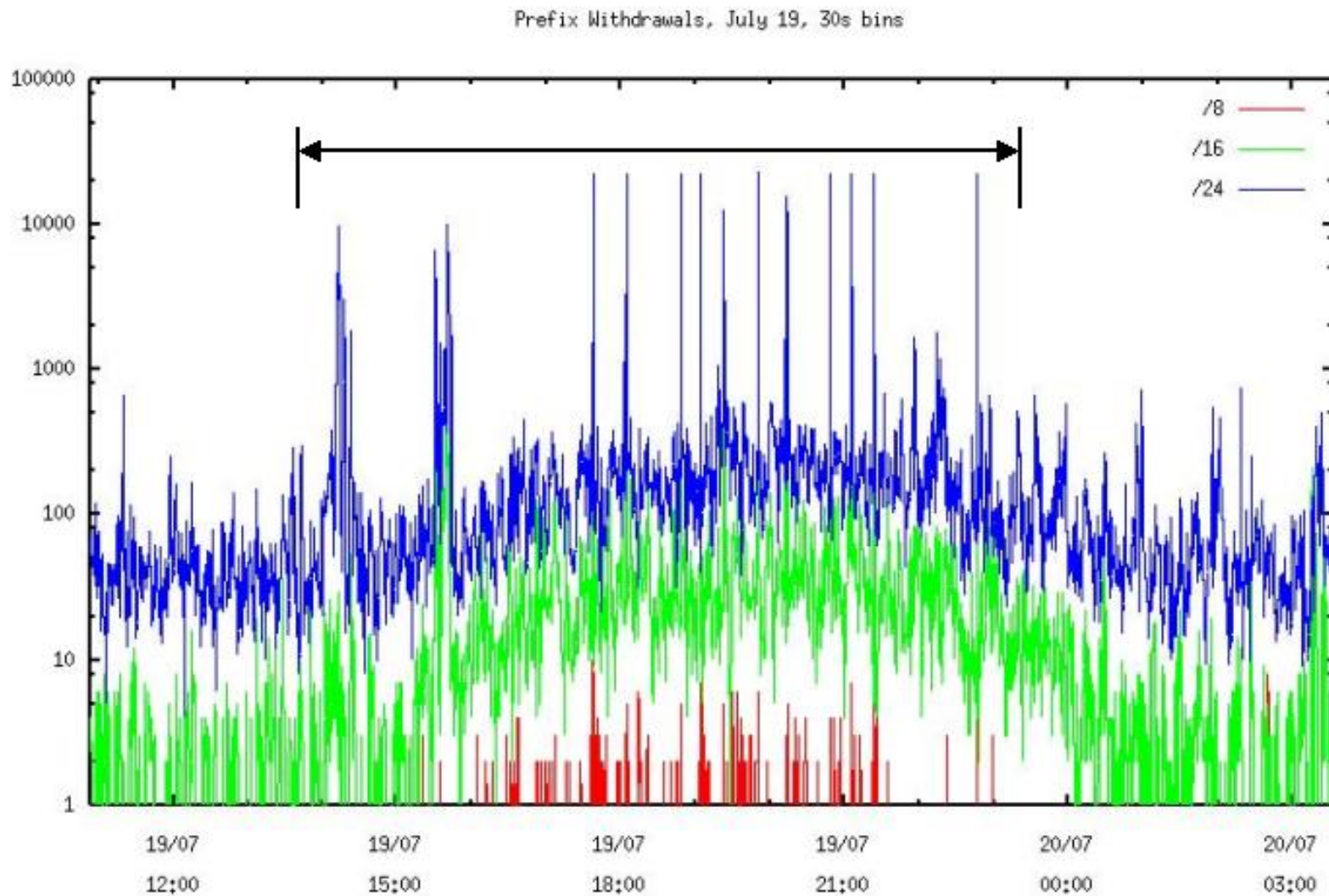


Figure 3: BGP Withdrawal Announcements (from [1])

The bracketed area includes several "surges" in the number of BGP route withdrawals being announced and tracked at the Internet exchange point where this data was collected. Only classful network boundaries are indicated on this plot. The surges in these announcements also is an indicator of overall BGP instability throughout the

Internet during the course of CodeRed II scanning and propagation.

September 18th 2001 -- NIMDA

On September 18th 2001 the NIMDA worm first appeared on the Internet. Unlike CodeRed II which had one infection vector, NIMDA infected hosts using a variety of mechanisms including:

- client to client via email
- client to client via open network shares
- web server to client via browsing of compromised web sites
- client to web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities ([VU#111677](#) and [CA-2001-12](#))
- client to web server via scanning for the back doors left behind by the "Code Red II" ([IN-2001-09](#)), and "sadmind/IIS" ([CA-2001-11](#)) worms [2]

NIMDA's impact on the Internet was significantly more dramatic than CodeRed II. This can be seen from the magnitude of the second "BGP storm event" in Figure 1 above. NIMDA hit faster and produced a more pronounced spike in the BGP announcements than the one produced by CodeRed II on July 19th. As described in [1], from approximately 1300 GMT till about 1500 GMT the aggregate BGP announcement rates increased by a factor of 25 jumping from approximately 400 per minute to over 10,000 per minute with occasional "super-bursts" in the range of 200,000 per minute. Over the next week the rate of announcements slowly decreased until they finally reached pre-NIMDA levels around September 24th.

The number of BGP route withdrawals also show similar bursts of activity during this period as shown in Figure 4 below. Like CodeRed II the first withdrawals come from smaller, /24, networks. However, unlike CodeRed II there is no similar withdrawals from larger networks. Cowie and Ogielski theorize that this may be indicative that the routing instabilities caused by NIMDA originated at the Internet edge and never made it to the core. Thus NIMDA's effects were more transient and did not result in long-lasting losses of reachability to edge networks.[1]

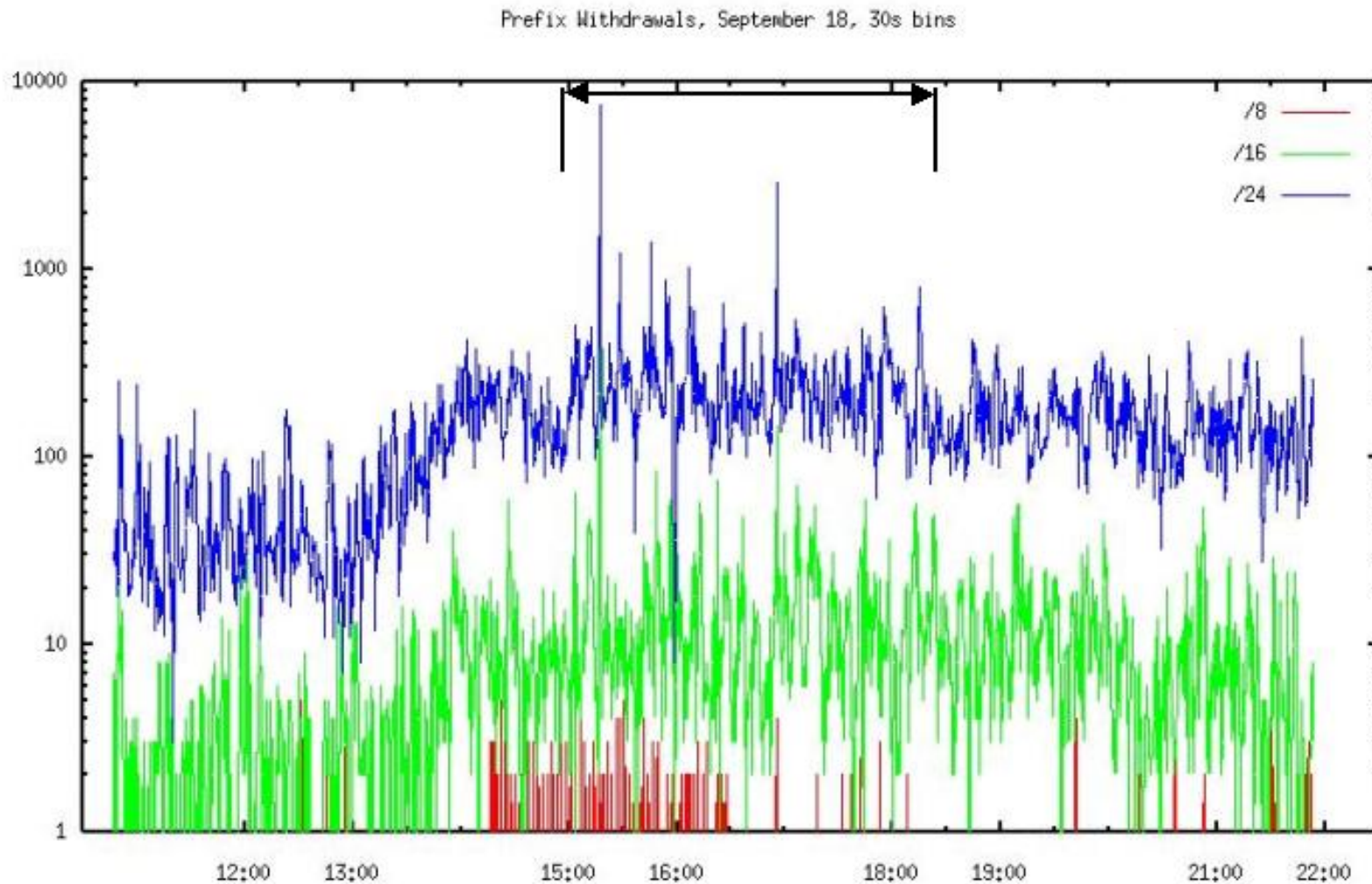


Figure 4: BGP Prefix Withdrawals for NIMDA (from [1])

January 25th 2003 -- The Impact of SQL Slammer

The SQL Slammer (aka sapphire) worm began to appear around 0530 GMT on Saturday January 25th. This

suite or had the Microsoft SQL Server Destop Engine (MSDE) installed. SQL Server spread faster than any other worm ever seen, infecting the majority of vulnerable hosts within 10 minutes of appearing on the Internet and some 75,000 hosts overall. CodeRed required over 14 hours to acheive its saturation impact limit of 359,000 hosts.

Unlike CodeRed II and NIMDA, SQL Slammer was a UDP-based worm that impacted the Internet through bandwidth consumption. The worms reached its full scanning rate of 55 million scans/second within three minutes of the start of infection and had a doubling rate of 8.5 seconds. CodeRed II's doubling rate was on the order of 37 minutes.

The effect of SQL Slammer can be seen in the dramatic decrease of BGP best routes shown in Figure 5. The immediate drop in BGP routes at the same time as the SQL Slammer worm first appeared provides excellent correlation between the worm and Internet routing instability. Additionally, Internet backbone disruption was significant enough that various peering points became saturated due to worm traffic as shown in Figure 6.

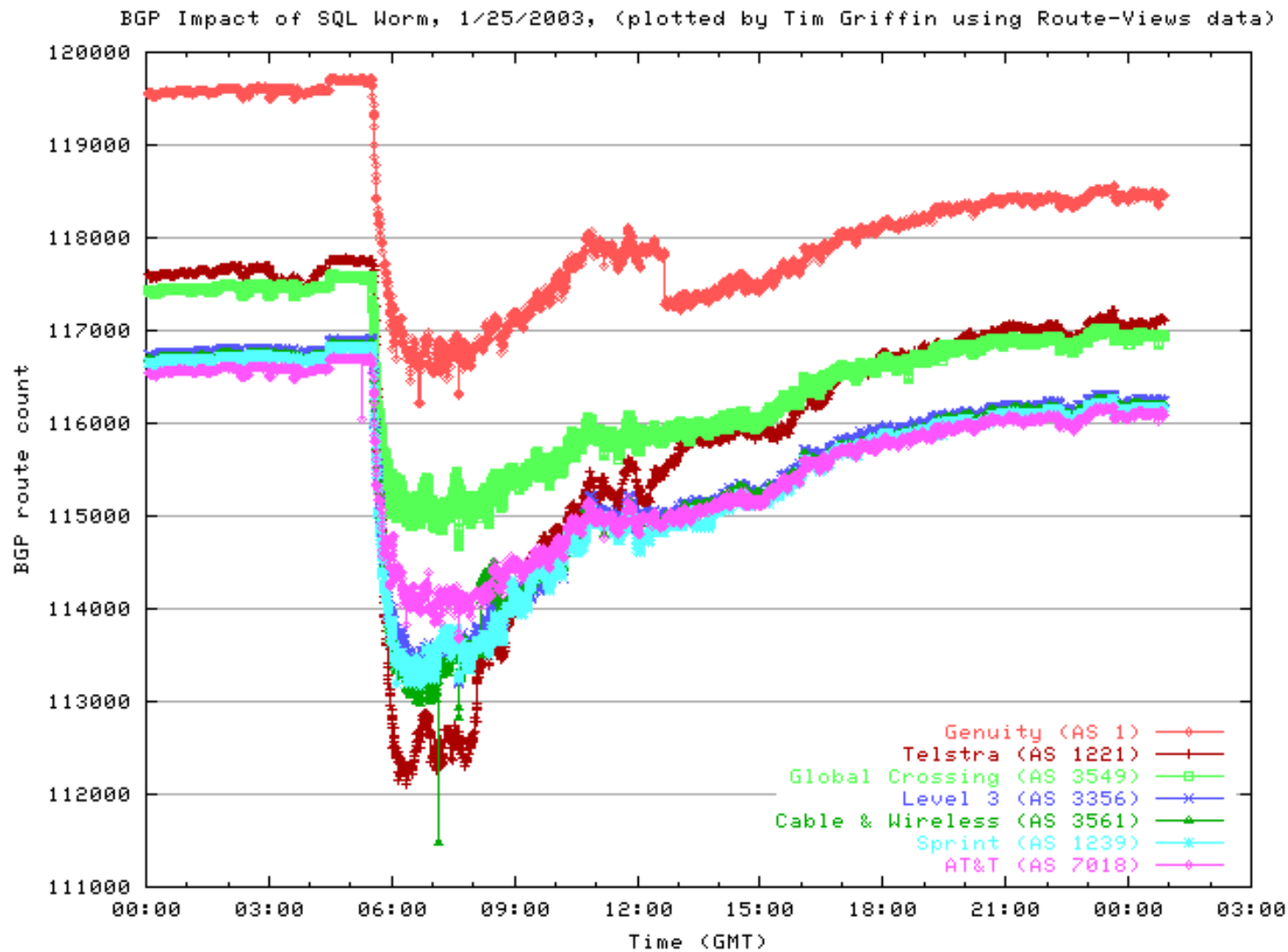


Figure 5: SQL Slammer Effect on BGP Best Routes (from [4])

The Internet Health Report (Last Hour)

About this site

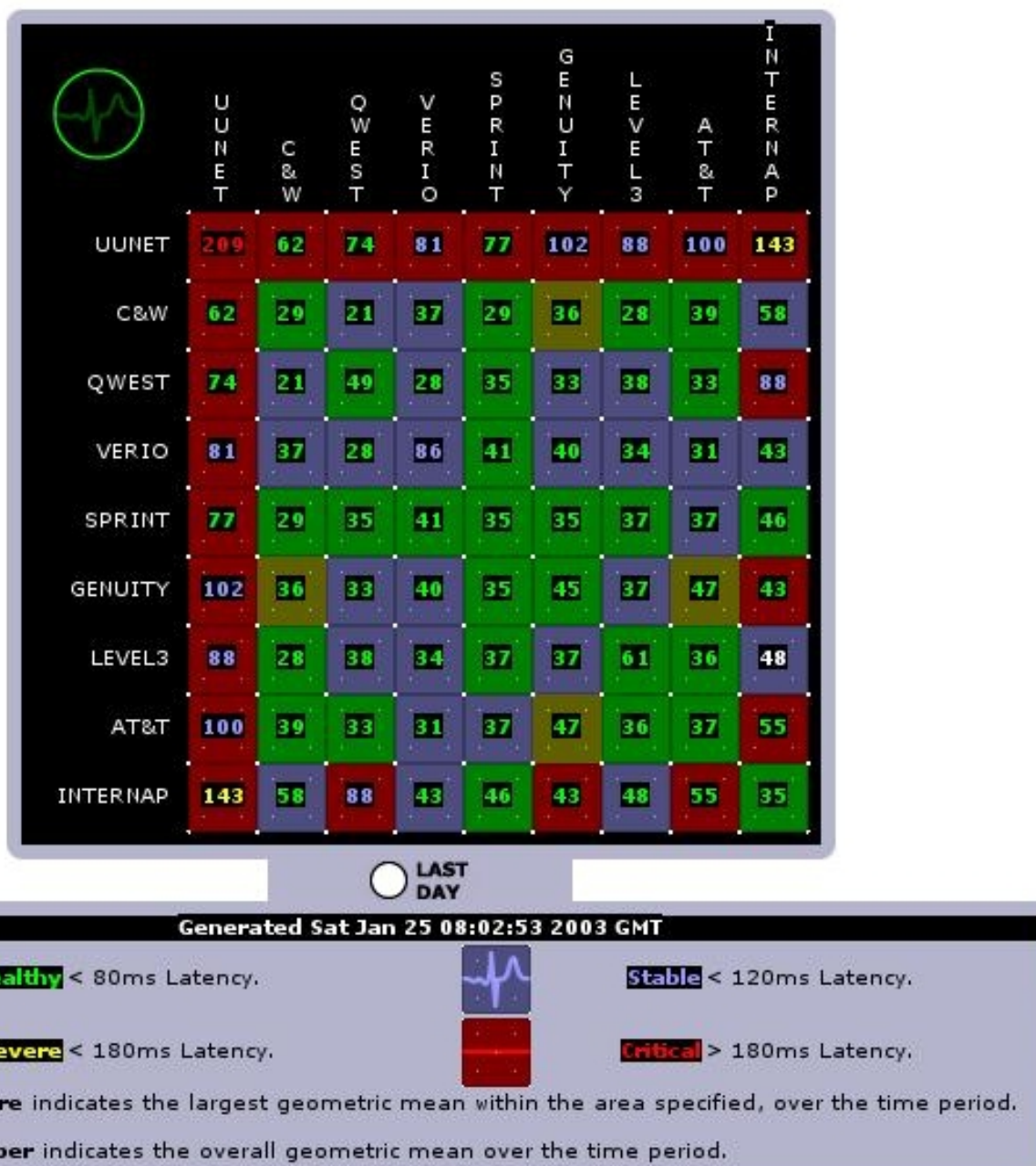


Figure 6: SQL Slammer Effect on Backbone Peering (from [5])

SQL Slammer also affected multicast space by scanning some Class-D addresses, thereby generating an unusually large number of Source Announcements (SAs). The impact of these scans was that some Multicast Source Discovery Protocol (MSDP) speaking routers had a large number of SAs in their caches and in some cases several ASes lost Multicast BGP (MBGP) connectivity in the immediate aftermath of the attack. [6]

One of the key results of SQL Slammer was the transformation of the theoretical possibility of flash worms, that is worms that can infect hosts on a global scale in the Internet in a matter of minutes, into reality.

Conclusions

Worms have had a significant impact on the operation and stability of the Internet for many years. The Morris Worm of the mid-1980s was the first in a long line of worms to disrupt peaceful day-to-day operation of the Internet. The impact of the CodeRed II, NIMDA, and SQL Slammer worms shows that even today's global Internet is as vulnerable to cataclysmic events as the Internet was in the mid-1980s. The focus in the future must be to build even greater resiliency into the Internet infrastructure to prevent such events from recurring with even more impact.

References

- [1] Cowie, J., Ogielski, A., Premore, B., and Yuan, Y. (2001) "Global Routing Instabilities during Code Red II and Nimda Worm Propagation." http://www.renesys.com/projects/bgp_instability, September 2001.
- [2] CERT® Coordination Center, "Nimda Worm", CERT® Advisory CA-2001-26, <http://www.cert.org/advisories/CA-2001-26.html>
- [3] Cooperative Association for Internet Data Analysis, "CAIDA Analysis of Code-Red", <http://www.caida.org/analysis/security/code-red>, 2002
- [4] Griffin, Tim, "BGP Impact of SQL Worm, 1/25/2003", http://www.research.att.com/~griffin/bgp_monitor/sql_worm.html, January 2003
- [5] "Internet Health Report - 1/25/2003", http://www.digitaloffense.net/worms/mssql_udp_worm/internet_health.jpg

[6] Rajvaidya, Prashant, "Sapphire Worm: January 2003, Effects of Sapphire Worm on MSDP", <http://www.nmsl.cs.ucsb.edu/mantra/ries/sapphire/>

[Privacy Statement](#)

Copyright 2006, SecurityFocus