A Snapshot of Global Internet Worm Activity

Dug Song, Rob Malan, Robert Stone
Arbor Networks
{dugsong,rmalan,robert}@arbor.net

November 9, 2001

Abstract

In this paper, we present a snapshot of Internet worm activity from September to November 2001, bearing witness to the rise of Nimda (and Nimda.E), the death of CodeRedII (and CodeRed.d), and a resurrection of the original CodeRed. We determine the demographics of the various worm-infected populations, and make predictions as to their future growth, attrition, and impact. These findings represent the early results of our ongoing research in "blackhole monitoring" - the instrumentation and analysis of an unused class A network, or 1/256 of the entire Internet address space, for evidence of global Internet attack activity.

1 Introduction

Internet worms have found fertile ground in the world's largest operating system monoculture - the widespread, default installations of Microsoft Windows-based operating systems. The resulting pandemic has had a measurable impact on the stability of the Internet at large [COPY01], while laying the groundwork for massively distributed denial-of-service attacks in the future [HW01].

Today's new Internet ecology largely consists of worms, viruses, and their opportunistic human scavengers. These network automata compete for hosts in a turbulent Internet land grab, leaving a trail of potential distributed denial-of-service zombies in their wake. By examining the impact these infected populations have on the global Internet, we hope to understand what the potential worst-case scenario for an Internet-wide epidemic might actually look like [SGJ01].

Our approach is to monitor as much of the unused Internet address space as possible, covering a significant subset of the uniform random distribution of IP addresses targeted in the propagation of such worms. From the purview of the network afforded by our class A monitor (corresponding to roughly 1/256th of the entire Internet address space), we may extrapolate details about worm activity across the globe.

2 Background

The year 2001 may very well go down in Internet lore as the Year of the Worm. Ramen, Lion, Adore, sadmind/IIS, CodeRed, CodeRedII, CodeRed.d, Nimda, Nimda.E. Cheese, CodeBlue, CodeGreen

3 Methodology

Our experimental "blackhole monitoring" platform consists of a 750 Mhz Pentium III server running custom packet capture and analysis software on OpenBSD 2.8, to which we terminate an unused but globally announced class A network (minus the allocation of a single legacy class B network) to capture backscatter and random scan traffic from the Internet at large. We have augmented the technique of off-ramping problematic traffic for inspection, first applied by Robert Stone for DDoS mitigation [St00] and more recently by David Moore, et. al in a DDoS measurement study [MVS01], with active network measurement and intrusion detection techniques for finer-grained traffic analysis. Our collected data consists of both raw and pre-processed packet traces, as well as unique application-layer payloads and their aggregate worm fingerprints.

In order to discriminate between different worms in their propagation attempts, we capture and reassemble the payloads of 1 out of every 100,000 TCP port 80 connection attempts. For each sampled SYN, we return a valid SYN/ACK advertising the maximal receive window, eliciting the contents of the HTTP request. The resulting HTTP requests, reassembled from ACK data, are then stripped of any variable HTTP headers (matching the case-insensitive regular expression '^(Host|Via|X-Forwarded-For|Cache-Control|Client-ip|Connection):') and saved in a payload file uniquely identified by MD5 signature, with a log maintained for each. Worm fingerprints are then simply identified as aggregates of such signatures after manual inspection of payload contents.

4 Results

4.1 Worm impact

In the seven-week period from September 19 to November 3, 2001, our blackhole monitor processed 2,500,365,946 TCP SYN packets destined for non-existent webservers in our class A network at a peak rate of about 2000 hits per second. Assuming a uniform random distribution of destination IP addresses attempted by each infected host, this translates to roughly 640 billion infection attempts seen across the Internet at large, or a minimum of 23 terabytes of TCP SYN traffic, alone. The actual amount of data transferred by these worms in their propagation was actually much larger, given that some fraction of these scans hit real webservers.

4.2 Worm demographics

From 16,433 hits to 113 unique payload signatures, we identified 5 major worm fingerprints: CodeRed, CodeRedII, CodeRed.d, Nimda, and Nimda.E, based on early analyses of these worms from independent third parties [PM01] [MRRV01]. Other signatures identified web robots, various misdirected web requests (e.g. for AOL Instant Messenger), and other network flotsam and jetsam. In Table 1, requests matching the payload signatures for each worm ranked Nimda slightly higher than CodeRed and CodeRedII combined, most likely due to CodeRed's periodicity, and CodeRedII's timely death. In the breakdown of these infection attempts

Worm type	hits	% of total
CodeRed	1592	10
CodeRedII	1884	12
CodeRed.d	2655	16
Nimda + Nimda.E	9928	62

Table 1: Infection attempts at 1/100,000 sampling

by country, and top-level domain in Table 2, .net and Korean hosts figure prominently, comprising more than half of all worm-infected hosts. This may be due to the high concentration of cable modem and DSL providers in .net, and the singular broadband Internet phenomenon in Korea. According to a March 2001 Nielsen/Netratings study of 21 countries worldwide, Korean users are the world's most active Internet surfers, leading the world in the number of visits to the World Wide Web, the number of unique sites visited, the number of pages downloaded, and time spent on the Internet per session and per month [NN01]. In August 2001, Nielsen/Netratings reported the near-saturation of the Korean broadband market, with 15.8 million broadband users, representing 95% of all Korean web surfers [Ya01].

4.3 Worm behavior

The graph of CodeRed, CodeRedII, and Nimda infection attempts in Figure 1 illustrates the peculiarities of each worm's propagation and their interactions. For example, Nimda's initial propagation begins with a sudden, dramatic burst, and then closely follows CodeRedII's lead - most likely due to contention for the same hosts (one of Nimda's infection vectors includes the `root.exe` backdoor left on IIS servers by CodeRedII). Similarly, the time-coded limits to CodeRed and CodeRedII's propagation stages, originally identified by eEye security researchers in their disassembly of these worms, are borne out in the graph with CodeRedII's sudden demise on October 1st, and CodeRed's short-lived resurrection from October 1st to 19th. The appearance of the new Nimda.E variant on November 1st also results in a minor resurgence, before returning to current levels.

While CodeRedII appears to be effectively finished (and likely is, due to time-coded October and year 2002 propagation limits), CodeRed is apparently here to stay, its infected population exploding from the 1st to the 19th of every month like a swarm of Internet locusts. As vulnerable hosts are patched or otherwise protected from re-exploitation, the maximum size of this population may shrink. Otherwise, the global impact of CodeRed's next phoenix-like rebirth may be on the order of 40 billion infection attempts scattered across the Internet, spread across 19 days, based solely on its performance in October. From our monitoring of CodeRed, it should be possible to track down infected hosts with significantly skewed clocks (ground zero for the next outbreak), to help eliminate CodeRed once and for all - or at least until someone launches it again manually.

Nimda, although stable, shows no sign of slowing

CodeRed	%	CodeRedII	%	CodeRed.d	%	Nimda	%
.net	49	.net	46	.net	47	.net	53
Korea	16	Korea	27	Korea	32	Korea	21
.com	11	.com	13	.com	8	.com	11
.edu	6	China	4	China	4	China	5
Germany	2	Germany	3	Germany	3	.edu	2
Italy	2	.edu	3	.edu	2	Germany	2
Brazil	2	France	2	France	2	Taiwan	2
Spain	2	Italy	2	Italy	2	USA	2
Netherlands	2			Taiwan	1	Canada	2
China	2						
France	2						
Denmark	2						

Table 2: Percentage of infection attempts by type, country and TLD

down. With no time-coded end to its propagation stage in sight, Nimda may be with us for quite some time, accounting for at least 5 billion scans across the Internet each day (Nimda implements "island hopping", preferring to target hosts first within its class B network (with 50% probability), then its class A network (25% probability), and finally, a completely random target).

5 Future work

With roughly 30 GB of raw and pre-processed network traces left to analyze, there are probably many more interesting discoveries to be made, such as the recovery rates of the infected populations, identification of factors in their recovery (timely security advisories, automated software patching, publication of articles in the mainstream press, migration to Apache, etc.), the analysis of older worms, etc. AS concentration and bandwidth estimates for the infected populations, as well as demographic information about the attackers scavenging the Internet at large for these hosts would help to characterize and quantify the latent DDoS risks presented by these epidemics.

We have already begun mining the corpus of data collected for insight into vulnerability scanning across the entire Internet, the prevalence and severity of distributed denial-of-service attacks following recent current events, and the incidence and implication of other non-malicious, random chaff we see floating around the Internet.

6 Acknowledgments

We would like to thank David Langhorst for his valiant efforts in trying to save the previous two months of data (for July and August, spanning the rise of CodeRed and CodeRedII), which we lost in a massive RAID disk failure with the first version of our blackhole monitor. Disk is cheap, but unfortunately you get what you pay for.

References

[MVS01] D. Moore, G. M. Voelker, S. Savage. "Inferring Internet Denial-of-Service Activity." Proceedings of the 10th USENIX Security Symposium, August 2001.

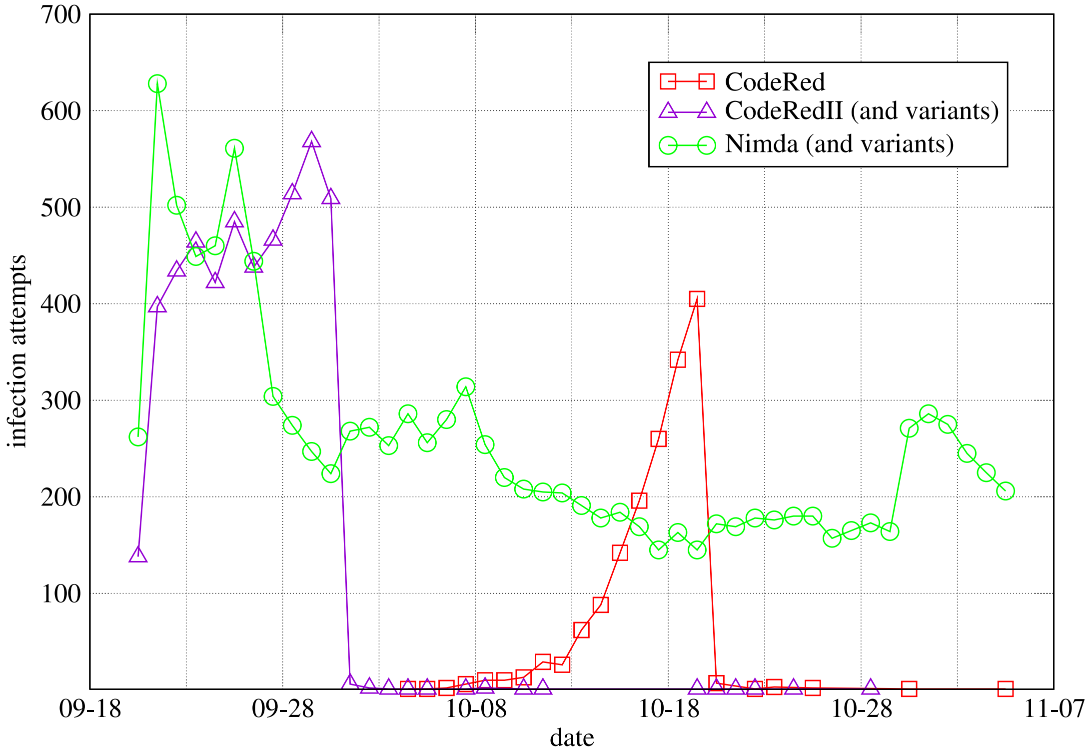
[St00] R. Stone. "CenterTrack: An IP Overlay Network for Tracking DoS Floods." Proceedings of the 9th USENIX Security Symposium, August 2000.

[HW01] K. Houle, G. Weaver. "Trends in Denial of Service Attack Technology." CERT Coordination Center, `http://www.cert.org/archive/pdf/DoS_trends.pdf`, October 2001.

[SGJ01] S. Staniford, G. Grim, R. Jonkman. "Flash Worms: Thirty Seconds to Infect the Internet." `http://www.silicondefense.com/flash/`, August 2001.

[COPY01] J. Cowie, A. Ogielski, B. Premore, Y. Yuan. "Global Routing Instabilities during Code Red II and Nimda Worm Propagation."

Figure 1: Worm infection attempts at 1/100,000 sampling, aggregated daily



http://www.renesys.com/projects/bgp_instability/, September 2001.

[PM01] R. Permeh, M. Maiffret. eEye Digital Security Advisories AL20010717 and AL20010804. http://www.eeye.com/html/Research/Advisories/, July 2001.

[MRRV01] A. Mackie, J. Roculan, R. Russell, M. Van Velzen. "Nimda Worm Analysis." http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf, September 2001.

[NN01] Nielsen/Netratings. "Findings show Koreans the keenest Internet surfers in the world." http://www.eratings.com/news/20010313b.htm, March 2001.

[Ya01] S. Yang. "Broadband penetration nears saturation in Korea." The Korea Herald News, online edition, http://www.koreaherald.co.kr/SITE/data/html_dir/2001/09/27/200109270007.asp, September 27, 2001.