

Title: Measuring Global Denial of Service Attacks

Abstract

Cyberattacks as a tool for information warfare are not new and have been popular for well over a decade. Their growing prevalence, however, is a disturbing trend that requires study. Distributed Denial of Service (DDoS) attacks are one of the most widely crippling elements of many cyberwarfare campaigns. Designed to overwhelm a victim's infrastructure with junk traffic, their impact has been a significant element in some cyber warfare campaigns. As seen in Georgia, Estonia, and against dissident groups, these attacks can affect much more than just the specific targets. Furthermore, with the growing sophistication of attackers, we see that they can strike key infrastructure elements.

We have collected information on a number of events around the world from the past 10 years and have seen the growing use of DDoS attacks as a weapon to silence opposition both within countries and outside of them, as well as dissident organizations. As these organizations increasingly use the Internet to exercise freedom of speech, organize political campaigns or efforts to unseat governments, a new communications channel has become a target of a government's attention. The increasing prevalence of DDoS attacks shows that countries around the world recognize their potential impact. Especially after the spring 2007 attacks on Estonia, non-state groups have adopted these tools into their information warfare arsenal.

We have been able to measure several key elements in these attacks using a combination of measurement techniques. The first point of data collection is visibility into botnets and malware that are actively engaged in the attacks. The second point of our data collection is based on participating global flow instrumentation across network domains, which provide a unique data set to Arbor Networks. The third data set that we have for such events is a number of BGP feeds to discover changes in routing for a victim nation. Together, these three data sets can give a deep understanding of the popular movements that arise during cyber warfare campaigns and the impact of various attacks and tools.

Analysis of this data set across traditional disciplines suggests that these attacks will grow in severity and sophistication, while at the same time become easier to use and popular with a growing segment of the population. Because of this, we are concerned about the impact on future diplomatic friction in active regions as we see NATO expand into former Soviet Bloc countries and ex-patriot groups organize to counter Chinese and Burmese government activities.

Bio

Dr. Jose Nazario is the manager for security research at Arbor Networks. In this capacity, he is responsible for analyzing burgeoning Internet security threats, reverse engineering malicious code, software development, developing security mechanisms that are then distributed to Arbor's Peakflow platforms via the Active Threat Feed (ATF) threat detection service. Dr. Nazario's research interests include large-scale Internet trends such as reachability and topology measurement, Internet-scale events such as DDoS attacks, botnets and worms, source code analysis tools, and data mining. He is the author of the books "Defense and Detection Strategies against Internet Worms" and "Secure Architectures with OpenBSD." He earned a Ph.D. in biochemistry from Case Western Reserve University in 2002. Prior to joining Arbor Networks, he was an independent security consultant. Dr. Nazario regularly speaks at conferences worldwide, with past presentations at CanSecWest, PacSec, Blackhat, and NANOG. He also maintains WormBlog.com a site devoted to studying worm detection and defense research.