Prolexic is a network security company that focuses on Distributed Denial of Service (DDOS) mitigation and digital threat intelligence gathering. Prolexic is headquartered in Hollywood, FL and has a Security Operations Center (SOC) that is staffed 24 hours a day with additional senior level engineers operating on call for escalation over rolling shifts. These engineers fight the largest and most sophisticated DDOS attacks on the internet today. The company boasts over 800Gbps of bandwidth that front-ends 20+ discreet layers of protection against DDOS attacks, located in four global scrubbing centers. It's those 20+ layers in their defense-in-depth model that allow Prolexic to claim they are "undefeated" in terms of mitigating DDOS attacks in which they are engaged.

The Prolexic approach is that no single solution, hardware or software, can mitigate all types of DDOS attacks seen in the wild today. Prolexic fills that void by using multiple measures to reduce the impact of an attack, including several that were developed by in-house engineers. This approach is seen again in Prolexic's use of a proprietary algorithm for some encrypted data transmissions. Security is at the core of this organization's strength, and has been since the beginning.

Prolexic's history is cloudy at best, with rumors of protecting gambling sites in the early days, with Russian gangstas thrown in somewhere along the timeline for added flavor. In addition, there are whispers that Prolexic plays both sides of this DDOS game. For whom better to thwart the attacks of the malicious than those with access to the battle plans, the attack targets, the timing…the source code? Meanwhile, Prolexic is busy protecting some of the largest institutions on the planet and is known by both those who lease botnets to attackers and the malicious actors alike, for their ability to stop the impact of a DDOS attack in a matter of minutes.

As one might expect, Prolexic has standardized on Linux and Apple, avoiding pretty much all things Microsoft. Oh, they like Bill Gates and all, but Windows machines dominate the botnet landscape at the moment. Botnets are those pesky machines that are infected with just the right level of malware to allow a remote Command and Control server to direct its nefarious actions. Those actions often include DDOS attacks-turned-campaigns, so it's easy to understand why Windows isn't the Operating System of choice in Hollywood. On the data side, Prolexic's utilizes several databases on the back-end for all sorts of tasks ranging from threat analysis to retention of attack and threat data. Correlation engines run on custom-built Security Information Event Monitoring (SIEM) machines, thrashing though Terrabytes of real-time data looking through tiny bits that might indicate that an attack is coming. Still others parse through mountains of residual attack data piecing together the puzzle that paints the landscape of the current threat environment. Gigabit fiber connects everything inside the 800Gbps of pipe, because speed is the minimum expectation of bandwidth. And when the pipe is saturated with enough ingress traffic to sink the ISP equivalent of the Titanic, mitigation streams need to move at the speed of…well light. One might summarize Prolexic this way: massive pipes front-end an array of proprietary technologies.

If you read the news, you've seen the dramatic increase in focus on cyber security. From Face the Nation to FBI to the President, it's all over the wire. Cyber attacks are on the rise as banks and the U.S. government work to deflect the onslaught. Among the most common and effective attack strategies deployed today is a DDOS attack. And as it stands, there's still one company in the defense space that claims to be undefeated. That company defends against DDOS attacks. That company is Prolexic.