In Thomas Chen and Jean-Marc Robert’s article “Worm Epidemics in High-Speed Networks,” their main focus is on the future possibility of fast-spreading worms. At the beginning of the article, Chen and Robert describe that many machines are already vulnerable to worm attacks and a majority of organizations are affected by malicious software. They then report that with the emergence of high-speed internet, worms like Code Red and SQL Slammer will become even more dangerous, and there is no current defense mechanism for such quick attacks. Chena and Robert then briefly outline how worm outbreaks begin slowly at first but skyrocket exponentially in infection rates after some time, and eventually tapers off as the infectible population becomes totally infected, using an epidemic model equation to express the point.

Then, the authors describe the Code Red and SQL Slammer worms. The Code Red worm took advantage of a buffer overflow in Microsoft’s Internet Information Server software. While the first version of Code Red was slow and somewhat ineffective, CRv2 and Code Red II (the third) were extremely effective and each infected over 350,000 machines. SQL Slammer was a much smaller program that focused more on its scans for uninfected machines than duplicating itself, so while it reached a maximum of 55 million scans per second, the actual infection of machines was smaller than Code Red.

Chen and Robert then describe how high-speed internet will make these worms exceptionally more dangerous. An increase in bandwidth will allow these types of worms more scans and therefore exceptionally more infections. Furthermore, worms able to avoid inefficient scanning either through the program itself or by waiting to launch at full throttle until a list of vulnerable machines is drafted could cause hundreds of thousands of machine infections in mere seconds. Current detection mechanisms such as Misuse and Anomaly detection struggle with detecting what is “malicious,” either because of the scope of the search or the definition of what is “not malicious” within the system.

While in 2004, internet worms were somewhat new and frightening, with high speed internet that blows 2004 internet away, I suppose great solutions must have been found for defending against worms in the next 16 years. I am curious as to how both worms and defense mechanisms evolved in that time, and what modern day threats are like.