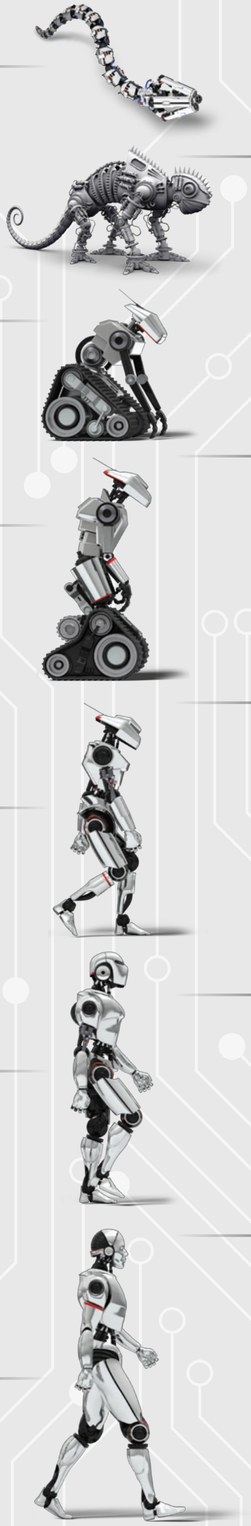
The Evolution of Botnets

...and the Fight Against Them

CYREN

◎ = BOTNET TAKEDOWN



1988

☁ Robert Morris, Jr., a Cornell grad student, releases the Internet's first worm, also designed to "phone home" to a command & control server at Berkeley.

1999

☁ A trojan and a worm—Sub7 and Pretty Park—are believed to be the earliest known malware connecting the victim's machine to an IRC channel to listen for malicious commands.

2004

☁ Phatbot, a descendant of Agobot, is among the first bot malware to use P2P instead of IRC.

2006

☁ Zeus (Zbot) malware first appears giving cybercriminals the ability to steal banking credentials and recruit the victim's computer into a botnet.

2008

☁ Grum originates and in four years' time expands with a capability of distributing 39.9 billion messages per day.

◎ Storm botnet abandoned after multiple takedown attempts and removal of bots.

2010

☁ Zeus code is integrated into SpyEye malware and marketed to high-end criminal customers.

◎ Waledac spam botnet is taken down by Microsoft.

2011

☁ 'Gameover Zeus' emerges using a P2P protocol for contact with C&C sites.

◎ Cyren reports spam levels drop over 30% after March 2011 takedown of Rustock botnet.

2012

◎ Grum botnet taken down with coordinated activity across Russia, Ukraine, Panama, and Netherlands.

2013

☁ Security professionals report the first android botnets, such as MisoSMS.

◎ Joint law enforcement and private sector takedown of multiple Citadel botnets, responsible for thefts of $500 million from consumer and business bank accounts.

2014

◎ Operation Tovar: U.S. Department of Justice (DOJ) along with law enforcement agencies in multiple countries, grab control of Gameover Zeus botnet.

2016

☁ The first IoT botnets take hold. Hundreds of thousands of devices are infected.

2017 & Beyond »

☁ IoT botnets will expand and become the botnet of choice for a number of years, faciliated by the fact that many IoT devices, such as home appliances, lag in security protection.

☁ Botnet developers will continue to get more creative and stealthy, building botnets that are increasingly difficult to disrupt.