February 2013

Combating Botnets

Key Points

- Botnets are networks of compromised computers, controlled by remote attackers that perform such illicit operations as sending spam, facilitating fraud, or attacking other computers.
- Botnets are of concern to governments and businesses because they can harness large numbers of individual computers to direct an attack against the information technology infrastructure. By working with industry to fight botnets and by passing thoughtful, balanced regulation, governments can help protect their systems and citizens from botnet malware.
- Microsoft aggressively fights botnets by collaborating with governments and others to take them down. Microsoft also provides security tools and guidance to businesses, governments, and consumers.

BACKGROUND

A botnet is a network of compromised computers that can be illicitly and secretly controlled by an attacker without the knowledge of their owners, and then used to perform a variety of illegal actions. Computers in a botnet (also called nodes, bots, robots, or zombies) are usually ordinary computers in homes and offices around the world. A computer becomes a node in a botnet when attackers manage to install malicious software on it, often by using social engineering tactics that trick users into installing it.

The owners of infected computers are usually unaware that their computers are being used for malicious purposes. When a computer has been infected by botnet malware, the botnet owner secretly connects the computer to the botnet and uses it to send spam, host or distribute malware or other illegal files, or attack other computers.

Botnets pose a more dangerous threat than individual hackers to the information technology systems of enterprise and governments because botnets harness large numbers of computers that can be used to direct an attack. The raw computing power of botnets enables them to take down major websites and email servers, as well as other essential parts of critical communications, data, and electronic systems.

Additionally, botnets can pose a threat to IT supply chains. A 2012 Microsoft study found that cyber criminals infiltrated unsecure supply chains using the Nitol botnet, which introduced counterfeit software embedded with malware for the purpose of secretly infecting computers before they were even purchased. Botnets can also provide anonymity to the criminals who control them (known as *botherders*) by enabling them to hide the true source of their attacks behind their widespread network of computers.

MICROSOFT APPROACH

- Microsoft is determined to help fight cyber crime through technology innovation, legal action, and consumer education.
- Microsoft supports governments and law enforcement by giving them technical training, investigative and forensic assistance, and the continued development of new technology tools to combat cyber crime.
- The Microsoft Active Response for Security (MARS) initiative combines legal and technical acumen to proactively disrupt criminal infrastructure. This includes using private legal action and technology measures to take down botnets, seizing the infrastructure and domains criminals use to control them, and taking the information gained in those efforts to better protect the Internet community.

  Project MARS is a joint effort of the Microsoft Digital Crimes Unit, Microsoft Malware Protection Center, Customer Support Services and Trustworthy Computing. Recent examples of MARS successes include disruption and remediation of the Waledac, Rustock, Kelihos, Zeus, Nitol, and Bamital botnets.

POLICY CONSIDERATIONS

- **Public and private partnerships.** Microsoft welcomes the support of governments and law enforcement in fighting botnets. The company believes that cooperation with authorities is the most effective means for reducing cyber threats, and supports balanced regulation as part of that effort. This includes initiatives like the Anti-Bot Code of Conduct for Internet Service Providers recommended by the U.S. Federal Communications Commission. The company also believes that less onerous restrictions on industry allow for greater innovation and flexibility in implementing responses to cyber crime.
- **International cooperation.** Microsoft has joined with industry to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address online crime.
- **Strong enforcement and balanced regulation.** Microsoft strongly supports the enactment and enforcement of laws to combat botnets and the prosecution of cyber criminals. At the same time, it is important that these laws enable innovation and support the adoption of new technology.

Helpful Resources

The Microsoft Safety & Security Center offering security guidance
www.microsoft.com/security

The Microsoft Digital Crimes Unit
www.microsoft.com/dcu