The IMDDOS Botnet: Discovery and Analysis

Contents

Figure 4 represents the number of unique hosts (recursives or simple stubs) that are looking up the most popular authority CnC domain name for the IMDDOS botnet compared with the most popular domain name from Mariposa, Bobax, and Virut.

Consistently, over this period of investigation, the primary domain name from the new botnet was looked up from the same number of recursives as the Virut Domain name (visible from the Damballa monitoring standpoint) and twice the size of the most popular Bobax domain name (visible from the Damballa monitoring standpoint). It is important to note that these numbers do not necessarily reflect the infection population for each botnet; rather, they should be used as a rough scale of comparing botnet size from DNS infrastructure perspective.

The IMDDOS Botnet Website

The investigation of the IMDDOS Botnet led Damballa researchers to a Chinese website advertising a commercally available version of the service. There is a comphensive introduction to the IMDDOS service, attack metholodgy and tools, contact info, and other details important to the potential user/customer. The website states that only non-legitimate websites, such as gambling sites, can be added to the list of attack targets.

Figure 5: The main website advertising the IMDDOS Service

Figure 6 is a screen capture of the tool download page. It describes release logs for different revisions of the malware agents and supporting tool, as well as a list of the main features and functions. The latest revision is listed as V2.0, released on July 21, 2010. V2.0 has many new features including a smaller malware footprint for the infected host. Additional new features include support for new attack

methods and the reassignment of spare bots. It states that the current version is not compatiable with V1.5.

Figure 6: Tools Download Page

Figure 7: The Service Model: From Free to Paid Service

IMDDOS offers different service agreements, ranging from free to paid services, as depicted in Figure 7. Besides the free service, the website does not publicly list any pricing information for the paid services. A prospective customer would need to contact customer service via the QQ service (a Chinese chat

service) to a get a detailed price quote. There are three levels of paid services: monthly, annually, or lifetime. For the lifetime customers, there is 24x7 technical support. In addition, IMDDOS recruits resale agents to promote its business.

Figure 8: Contact information for support and service inquiries

Figure 8 shows IMDDOS contact info, including sales QQ number (Chinese chat service), discussion group, and email address.

Figure 9: CnC Rental Information

IMDDOS also allows customers to rent servers from its server pool – severs are selected based on desired location, computing power, etc. Figure 9 lists the servers' specifications, price, and location.

The first version of their commercial tool that Damballa identified in the wild appeared in May of 2010. There may have been earlier tools that are still undiscovered (especially during the testing phase of the botnet).

Tool revision history:

- V2.0 – July 30, 2010
- V1.5 – July 14, 2010
- V1.4 – July 5, 2010
- V1.3 – June 22, 2010
- V1.2.2 – May 29, 2010
- V1.2 – May 20, 2010
- V1.1 – May 14, 2010

Figure 10: Tool Screenshots