NSCI National Security Cyberspace Institute

Malware Command and Control Overview

Kathryn Stephens, NSCI
December 30, 2010

Introduction

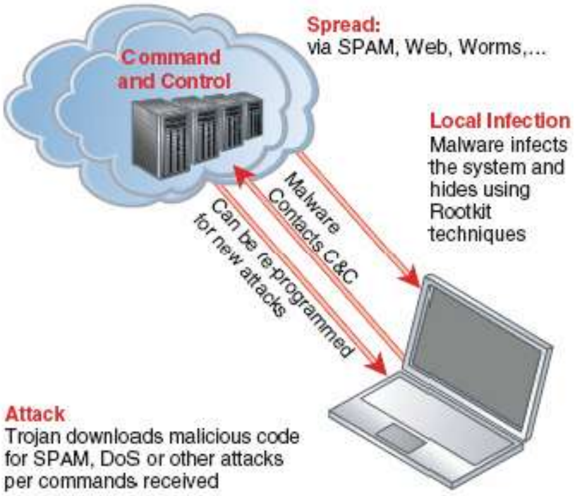
We've all heard about malware and threat it poses to cybersecurity. This paper is going to focus on how malware operates - the command and control (C2) aspects of the bot, botnet, and bot herder.

A botnet is a network of interconnected, autonomous computers that are infected with malicious software that is controlled by the owner of the malware, the bot herder. Once the software is installed in a computer, the bot is forced to carry out the commands of the bot herder, who can launch malicious attacks using some or all of the botnet's compromised computers. Botnets vary in size, complexity and sophistication. The botnet commander can use the botnet for denial of service attacks, spamming, traffic monitoring, identity theft and financial gain.

Each bot in a botnet communicates with the botnet's command-and-control center (C&C), and the herder has administrative privileges over all infected computers remotely from the C&C. A compromised computer communicates with the bot herder through covert communication channels such as IRC, peer-to-peer networks and social networking sites. The botnet's command-and-control center is used to send instructions to zombie computers, often over http or with more modern methods such as P2P and social networks. The most advanced way of controlling botnets is over P2P networks, which gives the herder the ability to switch servers quickly to avoid detection, and disabling botnets on these networks can be nearly impossible.[1] Uri Rivner, head of new technologies for consumer identity protection at RSA, says herders have four choices for C&C channels: herders can build their own C&C servers; use bulletproof hosting; use cloud services; or use social networks.[2]

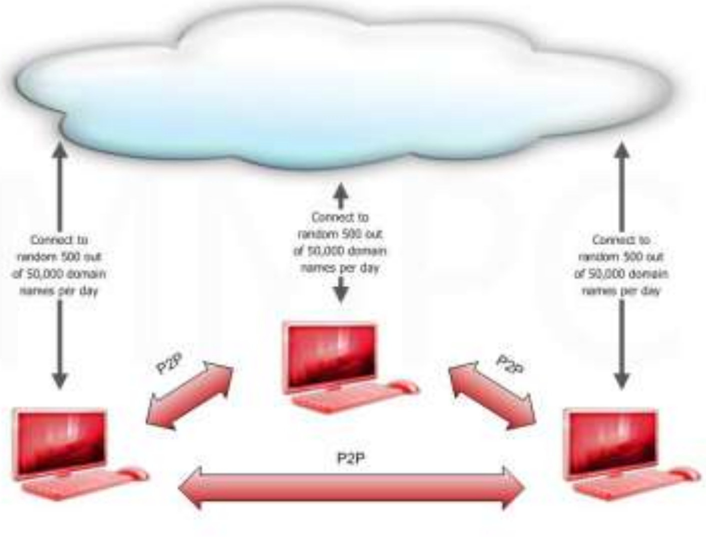
Internet Relay Chat (IRC) Command and Control (C2)

The first botnet codes were developed around Internet Relay Chat (IRC) channels, which is a form of real-time Internet messaging. IRC botnets are very centralized, which makes them easy to detect, trace and shut down.[3] Some botnets still use IRC channels. In June 2010, developers of the open source IRC server UnreallRCd reported that file servers code had been replaced by a version with a backdoor which allowed anyone to execute commands on the server running UnreallRCd. The backdoor was placed on file servers in November 2009, but was not detected.[4] IRC command-and-control channels have become less common since the IRC port is now usually blocked on most firewalls, and since the protocol is easily identified when analyzing network traffic.[5]


Command and Control
Spread:
via SPAM, Web, Worms,...
Local Infection
Malware infects the system and hides using Rootkit techniques
Malware Contacts C&C
Can be re-programmed for new attacks
Attack
Trojan downloads malicious code for SPAM, DoS or other attacks per commands received

[1] *How bots transparently control computers.* (2010, February 26). Retrieved November 23, 2010, from Security Park: http://www.securitypark.co.uk/security_article264343.html
[2] Fisher, D. (2010, July 19). *Attackers Moving to Social Networks For Command and Control.* Retrieved November 23, 2010, from Threat Post: http://threatpost.com/en_us/blogs/attackers-moving-social-networks-command-and-control-071910
[3] *How are bots and other advanced, persistent threats (APT) controlled?* (n.d.). Retrieved November 23, 2010, from FireEye: http://www.fireeye.com/resources/resources_page.php?id=9&keywords=Security_Vault_-_Understanding_Botnets
[4] *IRC server had backdoor in source code for months - Update.* (2010, June 12). Retrieved November 23, 2010, from The H Security: http://www.h-online.com/security/news/item/IRC-server-had-backdoor-in-source-code-for-months-Update-1020987.html
[5] Ferguson, R. (2010, October 15). *How botnets' rise foretells malware's future.* Retrieved November 23, 2010, from ZD Net: http://www.zdnet.co.uk/news/security-management/2010/10/15/how-botnets-rise-foretells-malwares-future-40090456/

Peer-to-peer C2


Connect to random 500 out of 50,000 domain names per day
Connect to random 500 out of 50,000 domain names per day
Connect to random 500 out of 50,000 domain names per day
P2P
P2P
P2P

When researchers began to easily trace and shut down IRC botnets, herders moved to peer-to-peer (P2P) technology for their command-and-control systems. By using P2P technology, large botnets could be controlled with no centralized C&C server, making it more difficult to find and shut down the botnet C&C.[6] Symantec recently analyzed the Stuxnet botnet, and found that the malware was designed to spread completely through P2P communication channels. In a P2P command-and-control infrastructure, bots do not check in with a centralized server for updates and commands. Rather, the infected machines communicate with one another to see the latest updates. The machine having the latest malware version transfers it to the other computers, spreading the malware without the use of a centralized C&C server.[7] Command-and-control traffic on peer-to-peer networks is also heavily encrypted, which increases the difficulty and time it takes for the network to be detected and shut down.[8]

Social Network C2

Although IRC networks have been the most common malware command-and-control models, many herders are beginning to use social networks such as Twitter and Facebook as the command-and-control centers for their malware. Herders set up fake profiles on a social network and then post a specific set of encrypted commands to the profile. When a new machine is infected with the Trojan, the malware can then go to the profile for new commands. Uri Rivner says social networks have become so popular because they are extremely resilient and allow Trojans to run for months or years. Social networks are also popular with bot herders because of how easy it is to set up new profiles. If one malicious profile is found and taken offline, the herders can code a list of dozens or hundreds of malicious profiles into the Trojan.[9] Social networks also make it difficult to determine how much traffic is going to the botnet, and usually social networks cannot be blacklisted because of the number of legitimate users. Social networks are becoming the easiest, cheapest and most reliable infrastructure option for bot herders.

C2 in the Cloud

Another recent trend shows that herders are increasingly using cloud services such as Google's AppEngine for their command-and-control centers, allowing herders to use many of the same social engineering methods as social networks. AppEngine is particularly attractive to herders because the available capacity is very substantial,

[6] *How are bots and other advanced, persistent threats (APT) controlled?* (n.d.). Retrieved November 23, 2010, from FireEye: http://www.fireeye.com/resources/resources_page.php?id=9&keywords=Security_Vault_-_Understanding_Botnetss

[7] Schwartz, M. J. (2010, September 20). *Stuxnet Updates Through P2P Communications.* Retrieved November 23, 2010, from Information Week: http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227500247

[8] Dittrich, D., & Dietrich, S. (n.d.). *New Directions in Peer-to-Peer Malware.* Retrieved November 23, 2010, from http://staff.washington.edu/dittrich/misc/sarnoff08-dd.pdf

[9] Fisher, D. (2010, July 19). *Attackers Moving to Social Networks For Command and Control.* Retrieved November 23, 2010, from Threat Post: http://threatpost.com/en_us/blogs/attackers-moving-social-networks-command-and-control-071910

allowing users to serve over five million hits a month before they must pay for the service. AppEngine also allows the herder to stay completely anonymous by updating information on AppEngine from a public terminal.[10] In 2009, security researchers found an unauthorized command-and-control center for the Zeus botnet on Amazon's EC2 cloud computing infrastructure. This was the first time that Amazon Web Services' cloud infrastructure has hosted a botnet's C&C infrastructure. As it is becoming harder for criminals to host their C&C infrastructure in legitimate data centers, bot herders are moving to Web based services.[11]

Conclusion

Research shows that the trend for bot herders is to move from a single, centralized command-and-control mechanism, to several linked C&C servers. This makes it more difficult for researchers to detect and takedown malware operations. Even when experts are successful in taking down one botnet server, there are still several more that keep spreading the malware.[12] The Zeus Trojan, for example, is controlled by more than a dozen criminal gangs and includes more than 160 command-and-control servers. When one group is found and arrested, there is still little effect on the overall size of the Zeus Trojan.[13]

In order to limit the damage and size of botnets, users must be trained to protect themselves and their computers online. Some malware can be blocked by enabling a firewall and getting the latest computer updates for all installed software. Users should use up-to-date antivirus software and never open an attachment or accept a file transfer from a suspicious source. Avoid downloading pirated software, which often contains hidden malware, and use strong passwords. As botnet herders move malware command-and-control centers to social networks and cloud services, it is especially important to recognize the risk of social engineering attacks and be careful giving out any information online.

[10] Timmer, J. (2009, November 10). *Bot herders turn to the cloud for command-and-control.* Retrieved November 23, 2010, from Ars Technica: http://arstechnica.com/security/news/2009/11/bot-herders-turn-to-the-cloud-for-command-and-control.ars

[11] McMillan, R. (2009, December 9). *Hackers find a home in Amazon's EC2 cloud.* Retrieved November 23, 2010, from ComputerWorld: http://www.computerworld.com/s/article/9142058/Hackers_find_a_home_in_Amazon_s_EC2_cloud?taxonomyId=17

[12] Fisher, D. (2010, June 07). *Botnets Using Ubiquity as Security.* Retrieved November 23, 2010, from Threat post: http://threatpost.com/en_us/blogs/botnets-using-ubiquity-security-060710

[13] McMillan, R. (2010, September 30). *11 Eastern Europeans charged in UK Zeus bust.* Retrieved November 23, 2010, from ComputerWorld: http://www.computerworld.com/s/article/9188858/11_Eastern_Europeans_charged_in_UK_Zeus_bust