The Botnet vs. Malware Relationship

The one-to-one botnet myth

By Gunter Ollmann, VP of Research

Introduction

A common misperception of cyber-crime botnets is that a one-to-one relationship exists between a malware bot agent and an individual botnet. Even if this had been a true statement back when botnets first began to appear, it is not true today. The key is the development of commercial build-it-yourself malware kits. These professional-grade tools lower the entry-level requirements for creating a malware bot agent, constructing a Command-and-Control (CnC) structure, and controlling the resultant botnet.

As a result, sophisticated botnets are well within the grasp of any technically-savvy user who knows how to use an Internet search engine and build a Web site. Enterprise organizations must change their focus from identifying malware by name to identifying the criminals behind individual botnets in order to keep up with this evolving threat.

Single DIY Botnet Kit

The major problem with the one-to-one botnet myth is that a single piece of malware does not correspond to a single botnet under the control of a cyber-criminal. This fallacy is easily exposed by observing the way in which a single popular malware DIY kit is used.

The bot agent itself is created using an off-the-shelf malware creator kit. These kits come in a variety of flavors and capabilities. Even free (or pirated) versions can create custom malware with a full spectrum of malware features capable of bypassing most antivirus technologies (e.g. keylogging, network sniffing, rootkit hiding, deactivating host protection, encrypted backdoors, etc.). “Professional” malware kits cost a few thousand dollars, but provide even more advanced features and often come with 24x7 support and money-back guarantees for evading of antivirus.

Consider the Zeus malware creator kit. The latest versions typically retail for around $400-700. Older versions can be purchased for $20-50 through software pirating channels. Even older versions can be obtained for free via newsgroups and torrent networks. The newer versions, of course, have more malware capabilities and better management features.

Armed with a Zeus creator kit, a would-be criminal can build new families of Zeus infector files with customizable parameters such as CnC channel, encryption keys, administration passwords and methods of communication. The final result is a custom variant of a Zeus bot agent.

To make things a little more interesting, this would-be criminal can undertake two additional development steps that increase the probability of success:

1) **Serial-Variant Preparation –** Savvy malware creators can generate multiple variants of the infector agent in advance of public release, and then release them sequentially at a pace slightly faster than antivirus vendors can release new signature updates. The assumption is that even if a Zeus agent is caught and a signature is made to detect that particular variant, the criminal is already using a previously created new variant by the time the signature is distributed by the antivirus company. The Serial-variant vector was a major reason for the success of the Storm botnet.
2) **Malware QA Verification –** Malware creators can also apply any of a number of tools and subscription services that manage multiple antivirus engines to automatically verify whether a particular malware sample can be detected and what different vendors have named its signature. Some of the more advanced tools automatically modify malware samples to evade antivirus signatures. When combined with a Serial-variant preparation plan, our criminal can be assured that his Zeus bot agents have no antivirus signature recognition.

The net result is that multiple variants of a single bot agent report to the same CnC and are controlled by the same criminal, but use different passwords and encryption, and require different signatures to detect their presence.

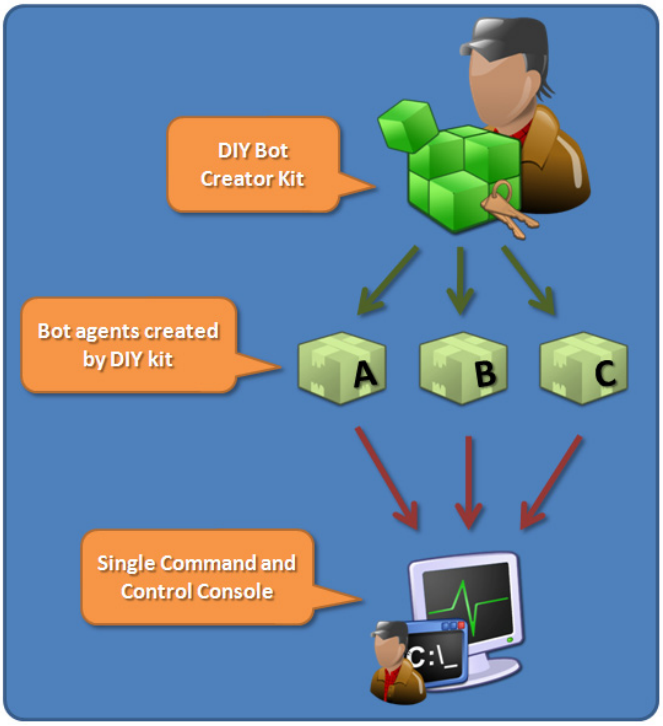

Figure 1: The DIY bot creator kit is used by the criminal to create multiple bot agent variants (A,B and C). All bot agents are configured to report in to a single CnC infrastructure operated and maintained by the criminal.

Multiple Kit Operators

DIY bot kits are purchased by a wide variety of would-be criminals. Each operates independently from the others, selecting unique CnC channels, encryption keys, administrative passwords and methods of communication. This swarm of different botnets use the same malware creator kit, but require different malware detection signatures and are operated independently by criminals with a variety of motivations.

All subsequent botnets share the same malware family name – even if they are operated by different criminals using different CnC channels. The method of compromised host cleanup, however, will be the same. In other words, the same remediation processes can typically be used for all malware created by a *specific version* of the same creator kit – regardless of which criminal happens to control a particular botnet based on that kit.

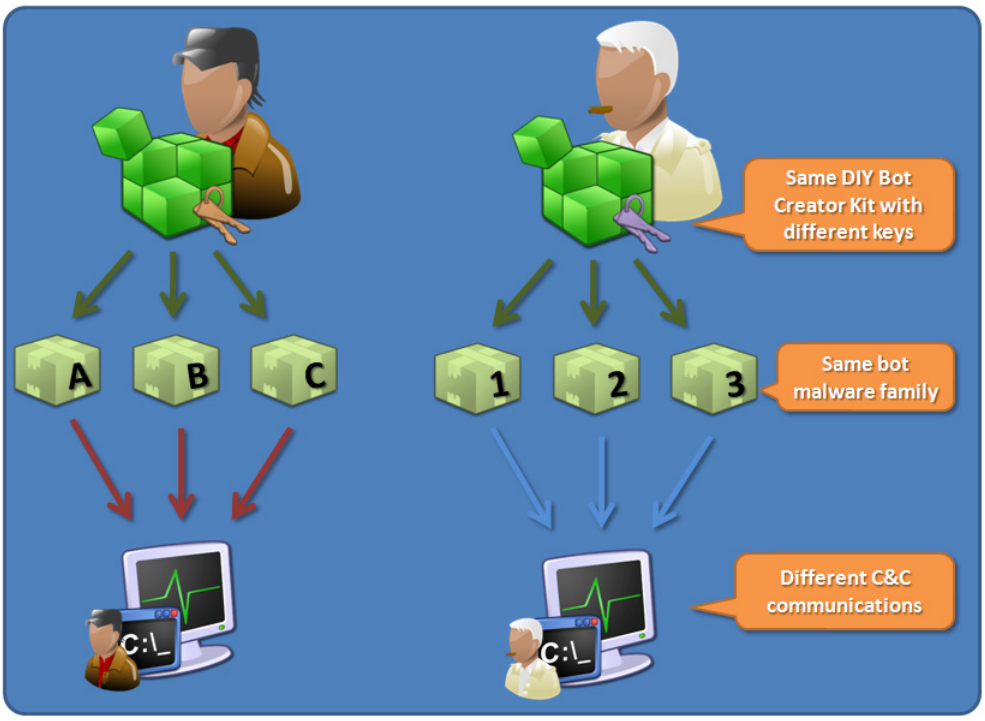

Figure 2: Two criminals both purchase the same DIY bot creator kit and produce their own bot agents. The first criminal creates bot agents A, B and C that point to a single CnC infrastructure under his direct control. The second criminal uses his own copy of the DIY bot creator kit to build bot agents A, B and C, and then points them to his own CnC infrastructure. All six bot agents are variants of the same malware type, but are operated by two independent criminals.

Multiple DIY Botnet Kits

This increasingly large pool of DIY botnet creator kits is a major contributor to sustainable botnet growth. The development and sale of these DIY kits is a business unto itself, and a highly competitive one at that. As such, any would-be criminal can select from a growing list of multi-function DIY kits – each one capable of producing its own unique family of bot agents and malware.

Criminals construct botnets that are even more resilient to existing host-based detection technologies by using multiple kits to create armories of bot agents. If a popular antivirus tool detects all offspring created by a version of a popular DIY bot creator kit (or a new behavioral technique for identifying a popular infection vector), it could potentially destroy the criminal's botnet. Therefore, no single detection algorithm (or cleanup process) will be capable of wiping out an entire botnet if the deployed bot agents were created using multiple and different DIY kits.

The significance of this tactic is that a single criminal operator can employ entirely different malware components that all utilize the same CnC infrastructure, yet still control them as a single botnet. In other words, this botnet operates independently from the type of bot agent used, which greatly complicates remediation. The identification of one strain of the botnet's agents will no longer counter the entire botnet threat.

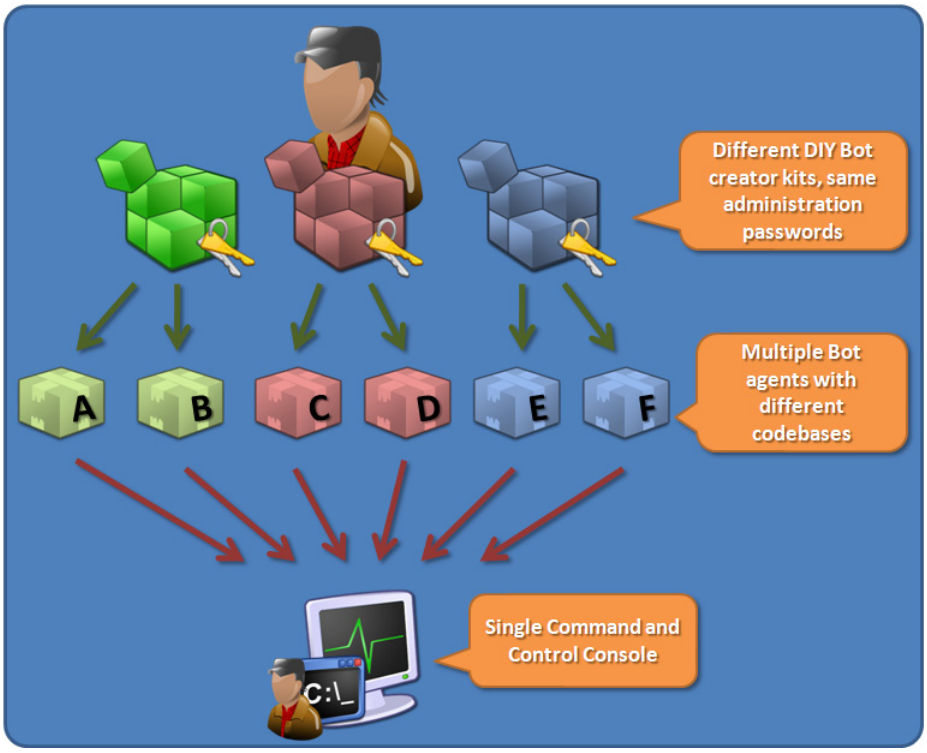

Figure 3: A criminal botnet operator procures three different and unrelated DIY bot creator kits and uses them to create a sequence of distinct bot agents (A-F) prior to distribution. All botnet agents are configured to use the same CnC infrastructure.

Conclusion

The use of DIY bot creator kits is a growing concern that has a direct impact on the way in which organizations must evaluate and protect against the botnet threat. The relative ease of access to such DIY kits makes it trivial for criminals to construct new botnets that are statistically immune to host-based protection systems, yet appear to

be almost identical from a malicious software perspective and communicate with a single CnC.

Because organizations have traditionally classified the botnet threat by their malware name rather than by the criminals who operate them, they have found it difficult to grasp the dynamics of building botnets and have faltered in building suitable defense strategies. By understanding the fallacies of the one-to-one malware to botnet myth, organizations should be in a better position to focus upon the criminal entities that target their business. The goal is to counter the threat at its source within the network layer – and more efficiently employ remediation solutions for compromised hosts.

About Damballa, Inc.

Damballa protects businesses from bot-driven targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control that coordinates botnet attacks to rapidly identify compromised systems and enable immediate control of malicious activity. Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa is privately held and headquartered in Atlanta, Georgia.