

Damballa: A Different Approach

Targeted attacks requires a new solution

Introduction

Targeted attacks such as BotArmies represent a dramatic change in the Internet threat landscape. Previously, a new threat might arise, but a defense to counter it would provide a more-or-less permanent solution. Targeted attacks take time and money to build. In addition, they exist to generate very large sums of money. As a result, they evolve constantly – typically far faster than traditional network security defenses can respond or be updated to respond. Traditional network defenses, including antivirus and antispyware, require hours or days to adjust, whereas targeted attacks can adapt within minutes. Most network security technologies simply move too slowly to provide complete protection against this threat.

Fortunately, targeted threats also contain fatal flaws that enable detection, analysis and mitigation. This paper details BotArmies and other targeted attacks, including how the online criminals who build these attacks operate. It then covers why this multi-network problem requires a multi-network solution that uncovers where attackers operate and how to respond to a sophisticated, constantly evolving threat.

In short, targeted attacks change the rules of network security. Security administrators need to shift the focus from detecting isolated attacks, as in traditional antivirus (AV) and intrusion detection/intrusion protection (IDS/IPS), to discovering the tell-tale signs of the targeted attacks:

- Compromise
- Propagation
- Command-and-control (CnC)
- Updates
- Attack/fraud activities

This wider approach helps organizations, literally, to think globally and act locally. Targeted attacks such as BotArmies take place across multiple networks. Therefore, it takes a multi-network approach to uncover critical CnC infrastructure and coordination protocols, and then track this activity back to individual compromised systems inside the network perimeter. This advanced data collection and correlation process represents the only truly effective strategy for combating targeted threats.

Other vendors focus on host-based malware and local intrusion attempts. Even when they claim to protect against malware and bots, they only see part of a much broader picture. Damballa attacks the entirety of a targeted threat, and it is this critical difference that makes Damballa's methodology and capabilities so effective.

Definitions

Security vendors, media outlets and analysts all tend to describe security issues within their own individual perspectives. Although many people may agree in concept on what something is, exact definitions can be maddeningly elusive. Therefore, this technical discussion of bots, botnets/BotArmies and BotMasters begins with a set of definitions that provide a consistent framework for the rest of the paper.

TARGETED ATTACK – According to a leading industry analyst firm, a **targeted attack** aims, “to achieve a specific impact against specific enterprises” and does so via malware that easily evades signature-based defenses or by hijacking critical network systems. BotArmies, for example, represent one of the fastest growing, most profitable examples of this organized, criminal online activity.

BOT – A **bot** :

- Is a compromised client or server system
- Communicates externally, and this communication often manifests itself as external control without the legitimate owner’s knowledge or consent
- Can take various actions prescribed by the BotMaster
- Comes preprogrammed with some attack capability

Bots communicate with BotMasters, take orders from them, and execute specific illicit tasks, all without the legitimate owner’s knowledge. BotMasters use bots to form BotArmies to perform coordinated attacks.

BOTARMY – A **BotArmy**, also called a bot network or botnet, is a logical grouping of bot-compromised systems, organized around specific command-and-control (CnC) infrastructure. This CnC is often hidden within the fabric of the Internet. BotArmies can contain hundreds of thousands or even millions of bots spanning tens of thousands of networks. Each BotArmy uses a common management and coordination layer to link members of the group into an effective, resilient and malicious weapon.

BOTMASTER – A **BotMaster** is an individual or a group that organizes bots into BotArmies, and then uses those BotArmies for coordinated and malicious activity. The BotMaster’s primary motivation is financial, which is why stealth is a crucial requirement for bot activity.

MALWARE – **Malware** is malicious software code that runs after it is downloaded onto a compromised device (computer, smartphone, printer, personal digital assistant, etc.). This broad category includes malware that turns compromised systems into bots, as well as more generic threats such as viruses, worms and Trojan horses.

VULNERABILITY – A **vulnerability** is a known weakness in an operating system, Web browser, database or application. Malware and human attackers use vulnerabilities as gateways to compromise systems, steal confidential data or turn machines into bots.

Unpatched systems are the easiest targets, although Zero-Day threats that utilize vulnerabilities for which there is no patch or defense are increasingly popular.

EXPLOIT – An **exploit** is a method, process or a piece of software code by which single or multiple vulnerabilities can be used to compromise a system. Multiple exploits are often grouped within a single attack to increase the likelihood of success.

ATTACK – An **attack** is malicious activity perpetrated by an individual computer or a BotArmy. Attacks can range from stealthy operations that steal confidential information to concerted denial of service efforts that prevent customers, partners and users from utilizing a network.

CnC – “Command and Control.” BotMasters use military-grade **CnC** to transform vast numbers of disparate machines into an organized, effective army. CnC points are located across the Internet, and often change to avoid detection and remediation.

Targeted Attack Tactics

BotArmies are the current targeted attack of choice for launching stealthy, profitable criminal enterprises. Security researchers have estimated that over 80% of spam now comes from BotArmies. Bots are also rapidly becoming the platform of choice for phishing, clickfraud, key logging, key cracking, copyright violations and denial-of-service (DoS) attacks

BotMasters use a variety of tactics to construct, maintain and deploy BotArmies. However, all targeted threat tactics are built around 3 key principles:

- Targeted attacks are **prolific**
- Targeted attacks are **profitable**
- Targeted attacks are **professional**

Targeted attacks are prolific

There are, of course, many ways to exploit a system via a targeted attack. BotMasters, for example, are in the business of building stable BotArmies that they can use directly for profit, rent out to other criminal elements, or both. Therefore stability is a key goal for a BotMaster. “Stability” means that the overall number of bots available to a BotArmy doesn’t change over time. New compromises keep up with – or exceed – bots lost on a network-by-network basis, either via malware removal or CnC disruption. As a result, a BotMaster can guarantee capacity and redundancy over time.

To make this happen, BotMasters have become experts at getting users to compromise their own machines. It is more than simple technical expertise. BotMasters understand human nature, and it is their ability to apply sophisticated social engineering that increases the danger.

Popular tactics to increase the propagation rate of bots include:

- “Drive-by downloads” – Web pages that use exploits to compromise machines without requiring the user to click on anything. Merely navigating to the site is sufficient
- Downloaded software that contains malware
- Hijacked DNS settings, in which a computer’s Web requests are surreptitiously routed through a rogue DNS server. This rogue DNS server then directs the target through a gauntlet of exploits designed to turn the computer into a bot-compromised system
- Redirected ads that download malware when clicked
- Malicious Web pages that ask for sensitive information such as credit card numbers
- Malicious Web pages that require a user to click prior to taking action (i.e., a “proprietary” video codec on an adult video site), then download malware when that link is clicked

These actions are triggered by convincing users that an email, a chat download, a multimedia text message, or a Web page is legitimate when it is not. The easiest means to make this happen is to appeal to holidays and popular culture. For example, spam aimed at spreading BotArmies concentrates on football at the beginning of the football season, Thanksgiving in November, controversial news stories, porn sites, celebrity gossip sites, wrestling sites, song lyric sites, social networking sites and other destinations where visitors tend to be impulsive rather than careful.

This strategy is very effective. The Storm BotArmy increased in size by 260% between Thanksgiving and New Years in 2007.

BotMasters also rely on compromised systems to betray trusted relationships between users and friends, family and coworkers. For example, some malware sends out emails from a user’s address book or social networking Web site that appears legitimate and contains an active link to additional malware. Since the email comes from someone the potential victims trust, they are much more likely to take an action that they would hesitate to do if the email came from an unknown source.

Targeted attacks are profitable

Continuing with the BotArmy example, BotMasters make substantial investments in building the malware that turns computers into bots, in constructing sophisticated and hidden CnC infrastructures, and in propagating BotArmies that represent stable platforms that exist for significant periods of time. There is one reason for this effort. BotMasters are in the business of making huge amounts of money.

BotMasters make money in a variety of ways, including – but certainly not limited to – the following:

- Leasing portions of their BotArmies to spammers and criminal organizations
- Building BotArmies for governmental or industrial espionage
- Replacing legitimate ads with their own advertising networks
- Creating false click-through traffic to generate revenue
- Stealing confidential information, then reselling it
- Launching for-hire DoS attacks

These businesses generate so much cash that front organizations for BotMasters operate traditional business offices in a number of locations around the world, in addition to open and underground online operations across the Internet.

Targeted attacks are professional

It is a serious mistake to think about targeted attacks such as BotArmies as more advanced versions of viruses or worms. BotMasters invest substantial sums of money into improving their product. They buy the same security products used by corporations so that they can build a more effective test environment for developing ways to evade traditional defenses. BotArmies, therefore, represent an ongoing evolution that constantly improves stealth, capability and robustness.

At its peak, the Storm BotArmy updated or changed the code within its bots as often as every 30 minutes. Each of these changes represented new targets, new CnC locations or new code that made each bot even harder to locate and remediate. The best antivirus vendors need hours or days to update their products. Clearly, the programmers who work for BotMasters have the talent to deliver a quality product within an astonishingly short development cycle.

It is this combination of long-lived BotArmies and profitability that drives the stealthy nature of bots. As a result, BotArmies represent a serious challenge to existing security mechanisms such as AV software, IDS/IPS, and the signature- or protocol-specific detection systems.

Since bots represent money to the BotMaster, a BotMasters has every incentive to keep the bots under his/her control for as long as possible. Therefore, bots often employ active evasion techniques to hide their activities. For example, botcode, or malware, can be packed to evade AV signature engines, and bots communicate using standard, common protocols like HTTP to mimic normal user activities.

These techniques are not new, even if the popular press is only now becoming aware of the problem. In fact, of the hundreds of thousands of samples of malware in Damballa's internal knowledgebase, more than 40% cannot be detected by any antivirus or antispyware solution. Some security organizations estimate that more than 80% of new malware is written specifically to evade existing network security defenses.

Even worse, the software used to create bots and BotArmies is relatively easy to find, and very easy to use. BotMasters want people to use their wares, and they understand, just like commercial software vendors, that a simple, visually attractive product quickly turns prospects into customers.

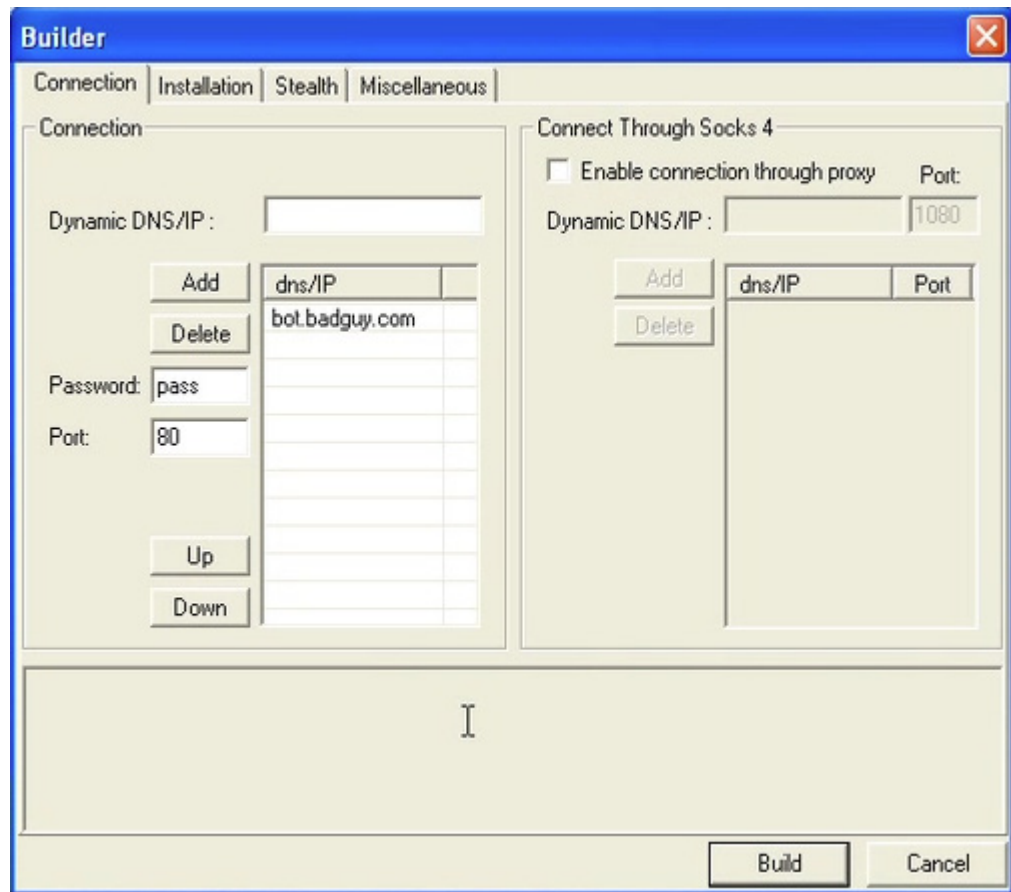
BotArmies now represent a mature ecosystem for conducting business, however illicit. There are different offerings for different markets. Point-and-click tools help unsophisticated users create and distribute malware with relative ease. These applications tend to support “script kiddies,” teens and young adults seeking a thrill, and angry individuals seeking to settle a score.

At a higher level, BotMasters control – and often compete to control – large BotArmies dedicated to specific types of activity, such as spam or click fraud. At the top, sit the criminal organizations that invest in the research behind bot evolution, commission the malware itself, and develop the IT infrastructure necessary to deliver robust, reliable BotArmy CnC.

A Malware-based Targeted Attack Example

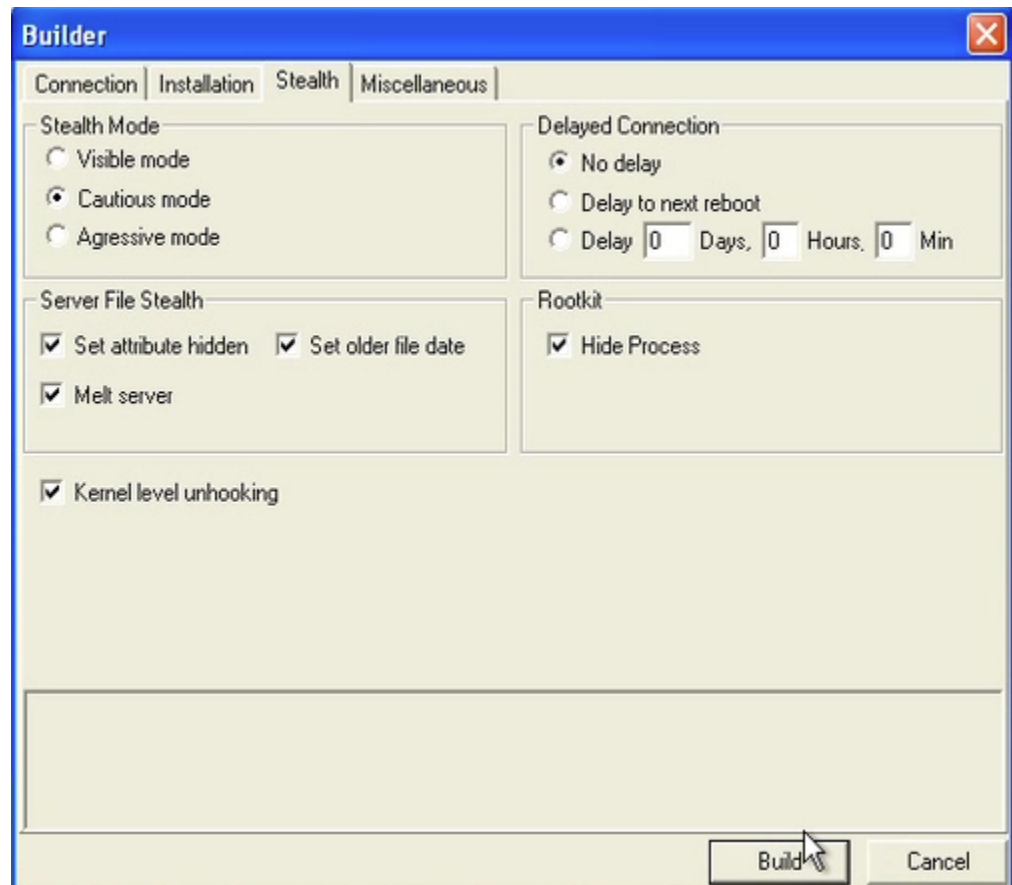
Targeted attacks are a powerful, resilient business model, and attackers have an amazing ability to build powerful, professional-grade bot malware. Even untrained attackers can easily purchase and download bot tools with graphical user interfaces (GUIs) that rival Windows and Apple in ease of use.

The following is a GUI for building the Bifrost Trojan (also called Bifrose). Bifrose is the term used by antivirus companies. Bifrost is the term that attackers use.



This GUI requires only a single click to hijack the proxy settings of a victim's browser. Proxies exist almost exclusively within corporations, which may indicate the preferred target for this malware. The number of proxy servers running within the residential space is so small as to be inconsequential. Many corporations believe that a proxy will protect them against many Internet threats. Clearly, attackers know better.

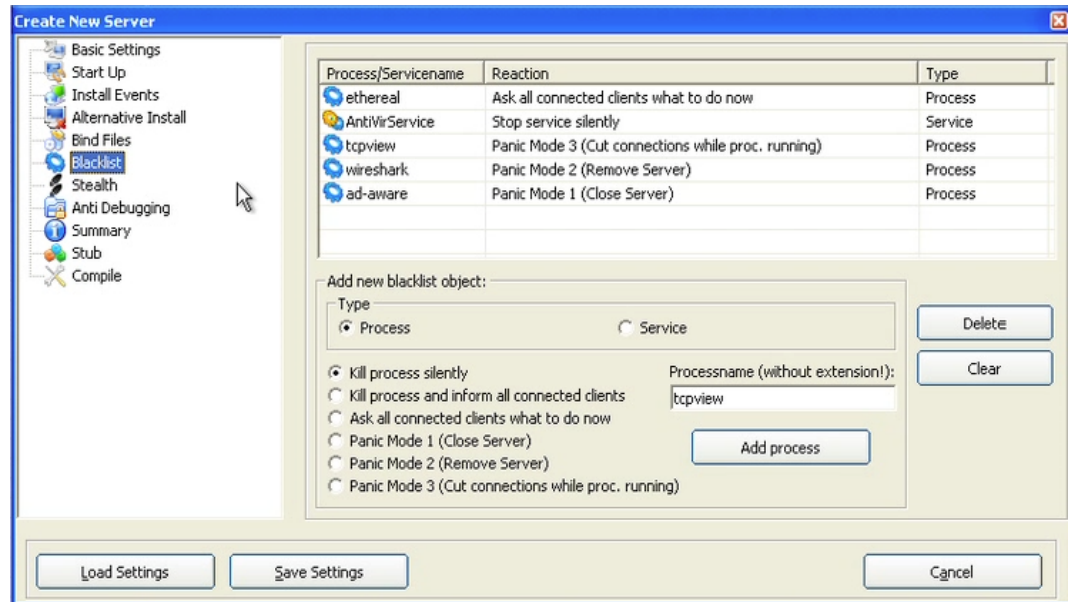
One other interesting feature is that the attacker can configure the malware to communicate on any port – even ports 80 and 443, which are necessary for HTTP and HTTPS Web traffic. Any network that allows outbound communication on these ports is at risk.



Bifrost's **Stealth Mode** settings are also interesting. The attacker can configure this bot to be completely hidden on a victim's computer – so well that AV cannot detect it. The root kit option adds an additional level of stealth that allows the malware to operate deep within the operating system kernel. Bifrost even has the ability to unhook a Windows firewall or an AV engine, so that it appears that these defenses are active when, in fact, they are not. This level of stealth means that, even if the AV engine had a signature capable of detecting the bot, the computer hardware itself would not allow the AV engine to detect it.

The **Server File Stealth** attributes ensure that there are no visible signs of the malware either on the computer's screen or within the file system of the device. **Melt Server** deletes its own installer once executed, which removes any trace that it ever existed. **Set Older File Date** makes forensic analysis more difficult since the malware acts like it installed long before it actually did.

These multiple evasion techniques mean that, once a machine is compromised, it can almost never be trusted as truly malware-free again. In fact, bot-oriented malware often requires reformatting a hard drive, or replacing the hard drive and destroying it to ensure that the malware is truly eradicated.



Finally, this screen shot illustrates Bifrost's ability to disable AV and antispyware software. **Kill Process Silently** disables the security software. It appears to run normally, but takes no useful action to stop the malware from operating.

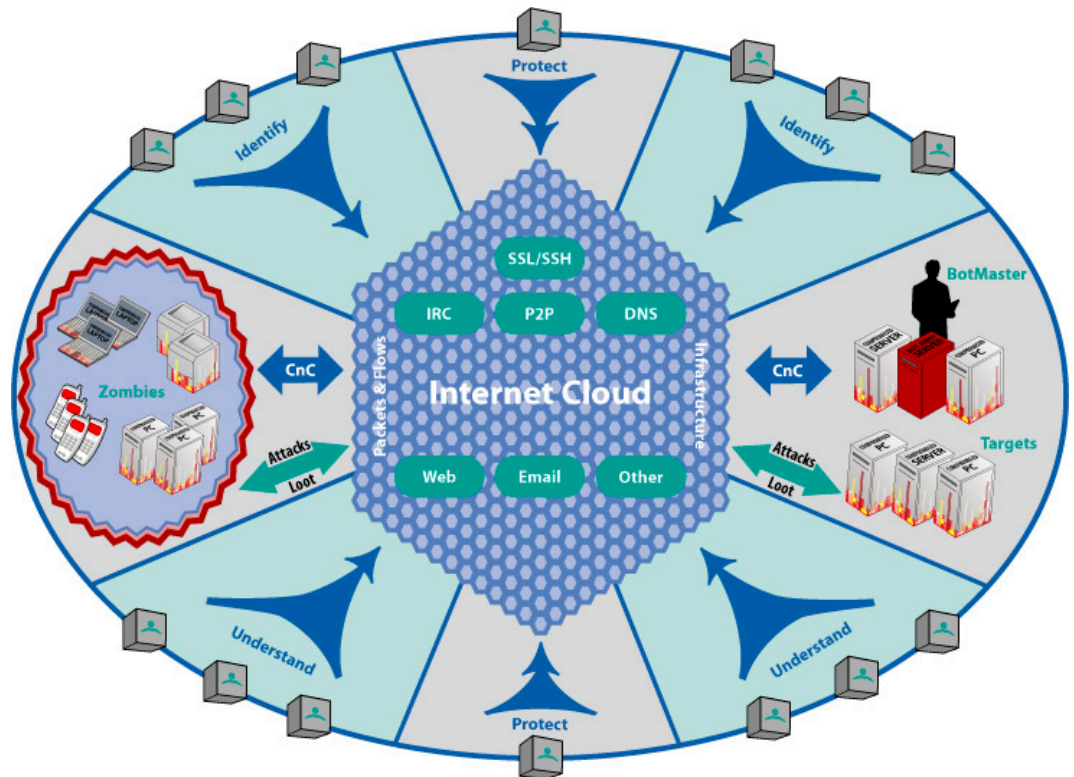
Multi-Network, Internet-wide Targeted Threat Detection

Most targeted threat detection techniques rely on host- or single LAN segment-based solutions to find individual bots. They almost never connect them to broader criminal activity. Therefore, risk assessment for any particular threat is almost impossible. Also, this approach is less than effective for a number of other reasons.

BotArmies represent a truly dynamic, constantly evolving targeted attack. By definition, they extend across corporate network boundaries and law enforcement jurisdictions. Individual bots are very difficult to locate, especially in enterprise environments encompassing thousands of IP-connected devices, and bot malware evolves rapidly enough to evade most host-based detection tools. In addition, individual bots do not generate sufficient network traffic within a typical enterprise network perimeter to trip behavioral-based defenses.

A practical, effective detection technology must move beyond host and LAN detection techniques. It must begin by understanding what distinct targeted threats do, and how attackers communicate with individual compromised systems. These CnC links are the most vulnerable element of a targeted attack. After all, a bot that cannot communicate with a BotMaster or other bots is a very low-level threat.

Damballa employs a multi-network approach to focus on CnC. This trans-Internet visibility (LAN and Internet) into threat activity pinpoints compromises, even well-hidden ones. The following diagram illustrates the fundamental differences between Damballa and other vendors.



Damballa’s Global Surveillance Network is a series of sensors and data feeds that span the Internet. This intelligence grid provides constant feedback that is collected, correlated and analyzed to provide real-time, highly accurate intelligence on targeted threats, BotArmies, bot CnC, specific bot activities and locations of compromised machines.

Damballa supplements this information with additional sensors installed immediately in front of or behind corporate firewalls. This additional information enables a more granular understanding of activity from internal compromised machines as they attempt to connect to CnC nodes, and of external attempts to reach internal corporate resources.

In short, we cover the same landscape as the enemy, and so we know where and how the attackers operate. This multi-network, Internet-wide approach means that Damballa is truly able to:

- **Identify** targeted attack activity and differentiate it from legitimate Internet activity
- **Understand** what an attack is attempting to do
- **Protect** our clients from malicious activity

Damballa uses a wide variety of detection and prevention techniques. Many of these are significantly more advanced than anything else on the market, and originate from an ongoing commitment to innovative Internet security research. More importantly, Damballa's technology directly addresses the needs of enterprise organizations seeking to limit targeted attacks, such as:

- Timely, accurate information on BotArmies and BotArmy intent
- Rapid, accurate identification of internal compromised systems
- Identification and understanding of malware that evades other solutions
- Efficient protection without additional IT complexity or headcount

This paper outlines four of these approaches: (a) DNS-based monitoring, (b) network-based anomaly detection, (c) passive honeypots, and (d) trap-oriented technology and correlation analysis. The following sections describe Damballa's unique approach in these areas, and the technologies that make it effective.

Damballa Identification Technologies

Damballa has multiple techniques that it uses to identify targeted threats on the Internet and within enterprise networks. Much of this knowledge comes from advanced research that Damballa turns into powerful products and services that protect against targeted attacks, and we remain highly focused on constantly developing new innovations that identify how attackers control their malicious assets.

Damballa's products apply these technologies via a security foundation that allows our customers to stay ahead of the criminals who are behind targeted attacks. For enterprise customers, internal appliances focus on compromises inside the network perimeter, external appliances recognize attempts to connect to internal systems and powerful analytics correlate this granular data with global threat activity to provide comprehensive, real-time reporting and feedback on active threats. For OEM partners, Damballa delivers an integrated, modular platform that delivers internal and external CnC identification, active blocking for malicious communications, targeted threat inference for indeterminate cases and advanced reporting.

Whether enterprise or OEM, Damballa delivers a flexible, extensible model that allows customers and partners to plug-in what they need today, then implement additional capabilities in the future. Damballa will continually respond to emerging threat vectors, providing scalable solutions and powerful analysis that keeps customers and partners ahead of targeted threats.

The following sections represent a sampling of Damballa's analysis and identification techniques. This is not an all-inclusive list. However, it is a good beginning for understanding why Damballa is uniquely effective.

DNS-Based Analysis

DNS monitoring and analysis plays a central role in Damballa's solution. In fact, our work in this area arguably pioneered the use of DNS for BotArmy identification. Damballa focuses on rallying behavior – when malware contacts CnC nodes to receive new commands. This rallying behavior is often a predictor of future attack activity.

For example, bots are not intelligent. They need a command to attack in order to attack, and all bots do not receive the attack commands simultaneously. Many, if not most, bots come with some sort of pre-programmed propagation or attack capability. Key logging and spam are the most common. Bots also often seek address books on compromised hosts, using them to issue socially engineered emails to the contacts within those address books to maximize the spread of the malware.

In spite of this built-in risk, it takes time to distribute new attack instructions to tens of thousands of individual bots, or to coordinate bot activity across the Internet. Only then can bots simultaneously launch an attack that maximizes the end result. Damballa uses this time window to identify the BotArmy, disrupt bot-oriented CnC and protect our clients.

Damballa extends its insight into bot-rallying and focuses on the invariants therein: the organization of bots into networks. For example, IRC was once widely used to organize bots. This protocol now has been abandoned by professionally-run BotArmies. DNS, however, remains viable because (a) BotArmies trying to avoid the use of DNS resolution via static routing have brittle, centralized networks, and (b) DNS provides BotArmies with the network agility (e.g., DNS fast flux) required to evade detection. Thus, we expect DNS to remain a rallying vehicle for BotArmies as well as an instrument for abuse by BotArmies.

DNS allows bots to find the CnC point. CnC can occur over any predefined channel. Therefore, the channel by which bots talk to CnC may change, but the need to find the CnC continues. Damballa's focus on identifying the command and control rather than one specific source for the traffic allows our solutions to evolve ahead of the threat.

Damballa uses data that encompass existing, commercial feeds of DNS metrics, such as fast-flux host lists, and related intelligence. While useful, these technologies will also become less popular with BotMasters over time. Damballa is developing several distinct, independent and complementary technologies for DNS-based analysis that will continue to refine our ability to track and mitigate BotArmy activity. Of those, DNSBL data-mining and passive DNS replication and analysis are discussed here.

DNSBL Data Mining

Black-lists of known malicious hosts have been used to reduce spam (e.g., MAPS). These black lists typically are distributed over DNS, and are called DNSBLs. Many Internet service providers (ISPs) and enterprise networks use DNSBLs to track IP addresses that originate spam so that future emails sent from these IP addresses can

be rejected. For the same reason, BotMasters are known to sell clean bots that are not listed in any DNSBL at a premium. Critically, *BotMasters themselves must perform reconnaissance lookups to determine their bots' blacklist status.*

The fact that BotMasters have to consult the BLs provides an opportunity for passive monitoring. Damballa has created technology to identify threats performing DNSBL lookups. In essence, we observe that malware must be used to lookup whether other compromised systems are listed in a BL set. The DNSBL queries therefore become a data stream from which additional compromises can be found. We will continue to refine our existing techniques for DNSBL counter-intelligence and identify compromised systems performing reconnaissance.

Damballa hosts numerous BLs. To host a DNSBL mirror, one must first obtain permission and consent of the DNSBL data owners. Each DNSBL has a different set of network policies and serves different communities (some with contracts, some with licenses, some with undefined access rights). Damballa is continually expanding our existing suite of DNSBL mirror-derived data to improve our detection capabilities. Furthermore, we consistently invest in techniques and heuristics that observe the simultaneous, illicit use of the DNSBL mirrors by malicious operators. This is easily accomplished by having cooperating mirrors send IP access lists covering short epochs that are within an interval less than the time for an RTT failure for a DNS lookup.

Our analysis of our mirror infrastructure shows that bots performing DNSBL counter-intelligence will be witnessed at multiple mirrors. That is, bots checking on the DNSBL listing status of other bots have been observed making requests across the entire Internet. Damballa also monitors this activity for additional attack-oriented intelligence.

Passive DNS Replication

For years, BotArmies have been using fast-flux DNS resolution services. In essence, compromised systems use other bots to provide DNS hosting services. A BotArmy cloud acts as a recursive or authority NS service. Similarly, the DNS answers provided by this cloud point to Web servers hosted in BotArmies. Bots use these bot-based DNS services to point victims to services hosted in other BotArmies.

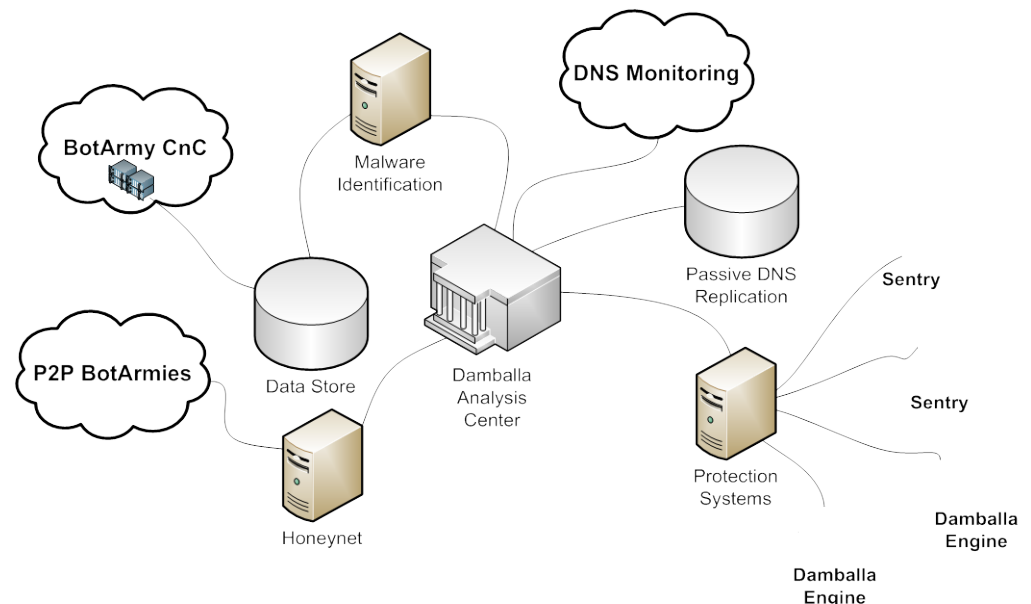
This technique creates two resolution paths for victims: the normal forward resolution using valid DNS, such as ISP-provided servers, and a subverted resolution path to rogue DNS servers, usually controlled by criminal organizations. Damballa has also witnessed the creation of a "second secret authority" or alternate resolution path for illicit DNS activity on the Internet. Fast-flux is but one component of this problem.

Damballa addresses fast-flux DNS and the related use of similar rogue DNS servers by deploying and leveraging a large passive DNS replication system. ***Passive DNS*** is a monitoring system that records the answers to DNS queries seen on selected

networks. By remembering how external domains were once resolved (as opposed to merely their current resolution), passive DNS provides a complete history of a domain. This greatly helps abuse response and law enforcement.

A conceptual view of passive DNS appears in the following figure. In order to reach the CnC server, compromised hosts perform a DNS lookup of the domain. If we assume a low caching time for the domain, then the recursive server for their network eventually contacts the SOA or the domain. The attacker has a variety of CnC servers at the ready. Mitigation of one does not stop the attack because the attacker also has the ability to update the DNS entry with the authority server.

Passive DNS records all of the resolutions performed within a network. This technique enables Damballa to detect domains with wide splay resolution trees.



Clustering Attack Traffic

Some of the most challenging aspects of identifying targeted attack activity include the dynamism of IP addresses that are involved in the attacks. IP addresses of malware such as bots are continually changing, not only through dynamic address pools of clients but also because IP addresses of bots are eventually blacklisted, so these bots must assume new identities. The ability to predict whether a machine is a member of a BotArmy solely based on its *behavior*, rather than on an ephemeral identity such as an IP address, is a critical part of Damballa's next-generation reputation technologies.

As part of this process, Damballa has developed clustering algorithms that observe traffic and fingerprint behavior that is characteristic of certain malicious behaviors, so that the compromises can be detected and quarantined based on the automated behavior of connecting to a CnC node, even if the IP addresses of the bots or the CnC nodes change. Observing and fingerprinting compromise behavior has two notable

benefits. First, this approach is more dynamic than existing blacklisting approaches, which must be continually updated as the IP addresses of bots change. Second, malicious traffic can be observed from many diverse locations. This diverse monitoring capability helps operators observe groups of related IP addresses that may exhibit organized behavior. In other words, Damballa has the potential to expose targeted attack and BotArmy membership simply by clustering IP addresses that emit similar attack behavior.

Compromise-Oriented Network Anomaly Detection

The goal of targeted attack network anomaly detection is to identify abnormal traffic patterns that may suggest inappropriate activities. Damballa's approach is to develop heuristics based on the intrinsic characteristics of targeted attacks, bots and BotArmies, inclusive, rather than on bot activity alone, then separate that behavior from activity typical of groups of human users.

These threats rely on frequent communications with CnC nodes and/or with each other to get updates and coordinate their activities. Further, such communication activities from malware such bots of the same BotArmy are driven by the same code. Thus, network activities of bots within the same BotArmy can be correlated with each other and even with their own previous behavior.

Damballa's anomaly detection systems capture the spatial-temporal and correlation properties of targeted attack CnC activities across an enterprise network. For example, we can detect CnC traffic in IRC in a port-independent manner. The advantages of our anomaly detection algorithms include: (1) they do not require prior knowledge of CnC servers or content signatures, (2) they are able to detect encrypted CnC traffic and (3) they do not require a large compromise presence in the monitored network.

For example, most bots that communicate using a specific channel are likely to respond to a command from the BotMaster at a similar time. On the other hand, it is very unlikely for many users in a normal channel to send similar messages at almost the same time. Bots hence have much stronger synchronization in sending messages than do normal users. After observing several rounds of such (group) message transmission, Damballa computes and aggregates the degree of synchronization or homogeneity from each round of messages to identify whether these hosts are bots of the same BotArmy.

Honeynet-Based Detection

While IRC will continue to be an area of concern as kit-based and do-it-yourself BotArmies proliferate, the large, million-member BotArmies of today no longer use IRC. Instead, professionally-run BotArmies increasingly use Web and peer-to-peer technologies. The Storm BotArmy, for example, uses the Overnet peer-to-peer protocol to communicate.

Damballa's honeynet infrastructure permits the tracking of BotArmies utilizing distributed CnC protocols, such as Web and peer-to-peer in addition to legacy, centralized CnC protocols, such as IRC. For example, when BotArmies use a centralized command and control, analyzing the BotArmy behavior is straight forward. One merely has to compromise a honeypot, and it will join the CnC node. If IRC is used, other bots of the same BotArmy can be enumerated. If other technologies are used for CnC, then observation of bot behavior in the honeynet can be used by other sensors to enumerate other bots in the network.

In a peer-to-peer network, however, any individual honeypot sees only a few peers in the overall BotArmy cloud. Running hundreds or thousands of honeypots is cost prohibitive and requires large power installations, monitoring staff, and significant equipment costs. Damballa's high-speed, light-weight bot emulation technology enables the measurement, enumeration, and selective disruption of these distributed Web and peer-to-peer networks. This technique permits the rapid measurement of peer-to-peer BotArmies.

For example, Damballa is able to map the entire Storm BotArmy every hour. This process yields an enumeration of victims, details about the search behavior of hosts, and insights about the degree of connections found in hosts.

Damballa's capabilities also include:

- Automatic classifications of P2P malware. Damballa's classification heuristics identify which of the thousands of malware samples collected each day exhibit P2P behavior
- Reporting on P2P malware. Clients and partners receive reports covering likely P2P behavior found in malware
- Victim Enumeration. Damballa provides a list of peers participating in malicious P2P networks for distribution to clients and partners

Correlation

Targeted attacks have a long life-cycle and can engage in a variety of fraudulent activities. Those defining characteristics are why multiple sensor technologies of the sort described thus far are needed. Each sensor focuses on one aspect or one part of a threat. The output of these sensors then needs to be correlated in order to yield more accurate and comprehensive information of a targeted attack.

Damballa's correlation engine supports a variety of network sensors, each charged with detecting specific stages of propagation, compromise, communication, and attack (e.g., exploit activity, downloading, outbound bot coordination dialog, etc.). Our correlation engines then tie together the dialog trail of in-bound intrusion alarms with those outbound communication patterns according to a targeted threat semantic

model (i.e., steps/flows activities in BotArmy compromise, propagation, CnC, and attack/fraud) that are highly indicative of successful internal compromise.

Threat and Malware Analysis

As stated in an earlier section, malware authors are keenly aware of the practical limitations of antivirus software. Attackers routinely use automated means to create new binaries that appear different to signature-based antivirus and antispymware systems but have semantically identical behavior.

As a result, security researchers collect thousands of new malware samples every day, even though there may be only a few hundred that are semantically different. Damballa's technology automates this process via a high-performance engine that dramatically streamlines unpacking, analysis, behavior extraction and classification of malware.

Damballa's capabilities also include directed mapping of malicious sites that exploit browsers and serve malware and an expansion of the automated unpacking technology to allow for prioritized submission and unpacking of malware. This system allows Damballa to understand evolving both Internet-based and P32 binary threats far faster and more accurately than is possible with manual or semi-automated research and analysis methodologies. As a result, Damballa can update overall protection solutions in a very short period of time, so that our clients' defenses can better respond to the rapidly changing nature of targeted attacks.

Mitigation

The recovery from targeted attack compromises presents technological and policy barriers on many levels. Most victims are located in networks with heterogeneous policies. Even in situations where compromises are found in organizations with a common network (e.g., a business where a single group or individual decides how to mitigate), other policy barriers arise. For example, throughput issues may make network engineers very cautious about adding additional in-line devices on critical network segments.

An alternative to host-based mitigation is to control the malicious traffic within the network itself. Typical methods quarantine compromised hosts or unwanted traffic by utilizing inline filtering/blocking devices. Damballa understands how different malware control-plane infrastructures work, and how to disrupt each one. One type of disruption technique manipulates routing through use of DNS itself.

At the client's authorization, Damballa can manipulate the client's DNS server to change the CnC domain resolution from the real CnC server point on the Internet to a local device controlled by Damballa. In this way, Damballa is able to neuter the compromise without the legitimate user even realizing what is happening. Our ability to effectively neuter many types of malware, including bots, without being in-line

provides a valuable window in which clients can safely operate a compromised system until an effective mitigation and remediation strategy can be put in place. The host must still be remediated. However, Damballa provides a window for remediation that was not available previously.

Competing Methods and Deficiencies

A wide variety of network security vendors claim that their technologies can stop targeted attacks. None of these alternatives takes Damballa's trans-Internet approach and so have severe limitations on their effectiveness.

As discussed above, signature-based solutions such as AV, antimalware and IDS/IPS are very limited when it comes to combating malware such as bots. Many of these products now include a behavioral element that claims to detect bot activity on hosts. These solutions miss a great deal of bot activity because bots increasingly mimic legitimate traffic, or utilize HTTP or HTTPS for communicating with BotArmy CnC and/or piggy-back human user-initiated activity.

Host-based solutions also require that end users and administrators determine which alerts are actually malware versus false positives and then know what to do if the malware has been positively identified. It often takes a security specialist to eradicate a compromise successfully, and the compromised system usually must be pulled from service while remediation takes place.

Other vendors feature flow-based anomaly identification systems that seek traffic patterns within the enterprise that may indicate the presence and location of a compromise. Unfortunately, attackers are smart. A single bot might only send out a few spam emails or a handful of packets. While not much in isolation, this activity, combined with similar actions from hundreds of thousands of other bots on tens of thousands of disparate networks, results a tremendously large attack.

Another network-based approach attempts to identify attacks by elevating signature-based solutions to specific gateways and aggregation points on internal networks. While this approach does allow for some analysis of network traffic that isn't possible on a host-by-host basis, it remains subject to the same limitations of any signature-based product, and provides no information whatsoever on targeted attack activity outside the network perimeter.

By contrast, an Internet-based approach means that activity can be detected before it reaches the network perimeter. In addition, the attack itself can be identified and its intent determined with precision. This extra information is critical in determining the severity of the threat and the best course of remediation.

Conclusion

Organized online criminal organization's intimate knowledge of signature- and network-based security solutions – and how to defeat them – is a fact of life that security managers, network administrators and senior technical management are rapidly being forced to accept. Even worse, security solutions that attempt to stop targeted attacks at the host or LAN segment level have proven themselves to be something less than cost-effective.

Damballa recognizes that the only way to truly combat targeted threats such as BotArmies is to know where the bad guys are and how they operate. That means building the technology and infrastructure necessary to track malware and bot activity anywhere it exists, anywhere across the Internet.

Targeted attacks are a multi-network problem that spans corporate network perimeters, national borders and law enforcement jurisdictions. Damballa is the only security solution that takes this multi-network approach. This unique ability to identify, isolate and protect against threats such as BotArmies across the breadth of the Internet provides a much more functional, practical solution. These tightly interrelated technologies represent a cost-effective means to understand the risks that targeted attacks represent, uncover even well-hidden compromises and implement planned mitigation and remediation strategies.

About Damballa, Inc.

Damballa protects businesses from 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 (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation 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.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo and Harvester. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.