

Closed Window

How Failsafe Enhancements Dramatically Limit Opportunities for Malware Armies and Other Targeted Attacks

Abstract

Damballa's enhanced Failsafe appliances give enterprise organizations the ability to identify targeted attacks in real-time, when they first become active. This new technology delivers:

- Faster, more definitive identification of malware and malware updates, even without signature-based malware identification and analysis
- Faster, more detailed information on malware activity and communications, as they occur
- The ability to stop low-flow and sleeper malware that evades network and behavior-based defenses
- Improved remediation via insight into exactly what's being changed on a compromised host

Deployment of Damballa's advanced In-The-Cloud technology within a Failsafe appliance is a fast, unobtrusive way for businesses to significantly improve their ability to identify previously undiscovered or newly emergent targeted attacks, with a simplified deployment that operates with very little overhead or impact on normal network operations.

Introduction

Something's happening on the network. It's not an attack, at least in the traditional sense. It's clearly not authorized, either. But there's nothing actually wrong about it, at least on the surface...

The grey area between definitively malicious and absolutely allowable is notoriously difficult for network security to manage. And yet, it is essential to know exactly what's happening and what it means when a clear-cut identification isn't possible. Without this information, security policy has only two choices:

- Allow suspicious activity to continue, based on the belief that it's better to be lenient and not restrict legitimate business communications
- Block anything that isn't explicitly allowed, even if it means interrupting normal online operations

For many organizations, the only option is to provide as full a range of services and the highest degree of user access as possible, and then hope that other layers of defense will catch anything that slips through.

Targeted attacks rely on this preference for convenience to compromise enterprise assets, even when sophisticated Defense-in-Depth (DiD) security solutions are in place. By operating in this grey area between the obviously good and the definitely bad, organized online criminal organizations can infiltrate and compromise a wide range of corporate assets.

Three gaps represent particularly difficult challenges for traditional network security infrastructure:

Zero-Day Gap – The time window between when a new type of targeted attack becomes available and when signature- or behavior-based defenses can respond

Network Noise Gap – The time necessary to differentiate a random attack from a targeted attack directed specifically at that organization

Compromise of One Gap – The time required to find a very small, very focused attack aimed at a narrowly defined, high-value target

In the Zero-Day Gap, targeted attack malware can update itself as often as every 30 minutes. Even the best signature-based security solutions require hours-to-days to decode new attacks and provide a safe, reliable update. This time lag means that enterprise networks are perpetually open to so-called Zero-Day threats, in which the malware can operate with impunity before a defense can be put into place.

In the Network Noise Gap, enterprise organizations are unable to understand which attacks are random and which ones are focused and malicious. Anti-virus and intrusion prevention systems are the most effective in dealing with random attacks. Targeted attacks are different. These attacks are often backed by organized criminal organizations, and they represent a persistent, stealthy threat that must be met with a different, immediate and appropriate response.

Finally, the Compromise of One Gap illustrates how popular conceptions of online threats can be misleading. While very large BotArmies such as the Storm and Kraken get all the headlines, the most damaging threats often come from very small malware armies seeking very specific internal resources. These virtual needles in the online haystack are very hard to find, which makes them particularly damaging.

Enterprise organizations need the ability to determine the actual intent and risk that arises when suspicious but unconfirmed activity occurs on corporate networks. Damballa's technology delivers exactly this level of insight, supplementing traditional DiD deployments by removing real-time uncertainty in tracking previously undiscovered or newly emerging targeted attacks.

Real-Time Information – Really

The current state of the art for malware analysis is to take a sample from “in the wild,” then run that code on a virtual machine to see what it tries to do. Of course, it’s a constant challenge to find the most recent version of targeted attack malware – especially since the code typically changes easily and often. As a result, this type of light, sampling-based analysis can lead to generalized insight into a class of malware, but not a detailed history of ongoing changes made to compromised hosts or record of ongoing attack activity.

Clearly, knowledge of attack CnC is important. However, real-time insight into the actual commands passing between an attack’s controller and the malware operating on compromised systems is even more valuable in terms of delivering the information enterprise organizations need to stop targeted attacks.

Damballa’s In-The-Cloud security technology delivers real-time visibility into unexpected activity or unusual network behavior. This new approach to managing Internet-based threats operates transparently on the network and protects without signatures. The end result is immediate visibility into emerging threats and attacks, including the ability to act with confidence, even before the malware or the CnC behind an attack can be fully determined.

Damballa works by listening to the actual CnC communications stream between a targeted attack’s controller and internal compromised systems. By doing so, Damballa can deliver much faster analysis of targeted attacks **right now**, without having to wait until malware can be captured, isolated and run within a virtual machine.

Damballa’s enhanced level of protection is an ideal solution to the problem presented by the rapid rate at which targeted attack malware evolves. The malware itself doesn’t need to be identified in order to recognize that malicious activity is taking place. With that in mind, Damballa’s solutions work even with merely suspicious network activity. Protection begins as soon as controller-to-malware commands are intercepted by the Failsafe appliance.

Better yet, protection need not rely on understanding the nature or content within targeted attack CnC communications – just that the connections happen. The detail comes from observing how, where and when communications take place, which also extends protection to encrypted communications flows.

This higher level of protection begins by redirecting suspicious activity into a specialized, carefully isolated network segment. The decision to redirect traffic comes from monitoring internal DNS requests for suspicious CnC domains. The actual malware involved does not need to be identified.

This redirection is essentially transparent to the user. In addition, neither the malware nor the attack controller can tell that the CnC has been infiltrated. The process kicks in

automatically when abnormal DNS lookups are detected by a Failsafe appliance. Additional triggers include:

- Evidence of known targeted attack behavior
- Communications over non-standard ports
- Communications denied by the firewall
- Communications typical of bot/Trojan malware behavior

The analysis process is all but transparent to end users. If the suspicious communication turns out to be benign, all the end user sees is a request to refresh his/her Web browser. However, automated malicious communications are quickly isolated, no matter how “low and slow”. Once again, the key is Failsafe’s ability to focus on the signaling mechanism between malware and CnC. Any inappropriate session will trigger monitoring, even for malware that communicates as rarely as once a week.

The appliance’s interaction with network traffic flow is scalable, based on each client’s individualized needs. Deeper analysis reveals more targeted threats. However, typical use has almost no impact on normal network traffic while still providing sufficient visibility to detect nearly all active targeted attacks.

What Is It – and What Is It Doing?

Most security solutions provide excellent information on what has happened. This historical approach appeals to security vendors for a number of reasons. First, it’s much easier to understand an event after it is past. All the forensic data is available for analysis, and there’s no urgency to stop an active attack. Second, log data hopefully provides sufficient feedback to make it easier to prevent future compromises.

This model works well for viruses, Trojans and hacker intrusions, in which the attack vectors evolved relatively slowly. Even Zero-Day attacks, once the initial barrage had passed by, could be dealt with by learning from the attack and sealing off the vulnerabilities. But targeted attacks completely change this equation, which is why Damballa has developed technology that lets clients understand ***exactly what the targeted attack is doing, at the precise time that the attack takes place***. This real-time insight into actual threat activity, at the time that CnC communications occur, provides a critical advantage for identifying active compromises and stopping them from damaging or stealing key corporate assets.

Here’s how it works. Traditional malware analysis examines malware for a period of time, and then stops. The assumption is that the malware code is static, or that all useful information has already been gained. Virtual machines are very useful in this regard.

Damballa's technology runs in perpetuity. As a result, it can see how targeted attack malware evolves over time, and do so without the controller of a malware army realizing that the attack network itself has been compromised.

Since this technology focuses on changes in malware and in malware activity over time, it gives Damballa's clients insight into what an attack is trying to do, as it tries to do it. Information is available in real-time, which means that customers can make measured decisions on how best to respond to an active attack, even before the malware code has been identified or the CnC nodes have been definitively identified as malicious. In other words, Damballa takes away the ongoing window of opportunity that the organizers of targeted attacks rely upon in order to ply their craft.

Damballa provides a wide range of information for network security staff that can't be found using any other means. Basic categories include:

Drop Sites – The locations across the Internet where malware attempts to send stolen data.

Compromised Host Behavior – Detailed information on file changes, additions and deletions, file access attempts and file read attempts. In other words, the specific items that the malware was attempting to uncover.

Binary Updates – The changes in targeting and capabilities as the malware evolves over time. Damballa's technology can also force malware to take action without prompting from its master, which reveals the full capabilities of the code at any point in time.

Communications Strategy – Complete logging of CnC ports and protocols, and how these items change over time.

Packets Sent – Netflow statistics that cover all network communications.

Web Sites Visited – Detailed information on potential online account fraud or Distributed Denial of Service (DDoS) attacks originating from compromised internal assets. Damballa can connect small, under-the-radar activity with broader attacks across the Internet to confirm even small amounts of malicious activity.

Email Sent – Clear evidence of spamming activity or social engineering attacks aimed at expanding the number of malware compromised systems.

Bandwidth Utilization – Concrete measures of the cost of a targeted attack, in terms of the bandwidth consumed by malware and CnC activity.

Customized Intelligence and Improved Remediation

Damballa's In-The-Cloud innovations are easily customized for the specialized needs of each enterprise client. The goal is to automate the advantages of a full-scale

consulting engagement inside a single, easy-to-understand appliance. Clients can quickly adjust the depth of monitoring to focus on specific threats, or to increase or decrease the scope of the effort to respond to the current threat landscape.

Remediation of targeted attacks also becomes much improved due to the true real-time insight Damballa delivers. It begins with Damballa's ability to recognize targeted attacks in advance of malware or compromise identification, and then continues by measuring the actual current state of the malware, not a previous version that might bear only a faint resemblance to its current incarnation.

Next, the malware's activity can be monitored over time, which delivers detailed information into host changes. This data includes files added, changed and/or deleted, and often includes insight into modified registry keys or kernel alterations. Armed with this data, security staff can quickly determine:

- Which systems have been compromised
- Whether compromised systems need to be quarantined or remediated immediately
- Whether remediation or reimaging is the best strategy
- How best to restore normal, healthy operations

Finally, remediation strategies are tested on virtual machines. If a given set of tactics works within Damballa's test environment, then the client can confirm the tests, evaluate alternatives and then deploy a solution across the enterprise once the results have been proven successful.

Conclusion

Damballa's technological enhancements deliver significant improvements in an enterprise organization's ability to defend itself against targeted attacks. These benefits include:

- Faster identification, understanding and response to newly emergent or previously undiscovered targeted attacks
- Rapid analysis of suspicious activity, without requiring signatures or network behavior profiles
- Detailed, real-time information on changes to compromised systems
- Immediate attack disruption, including infiltration of malware armies and the issuance of false information to malware CnC nodes
- Live attack monitoring within a safe, controlled environment in order to learn more about the exact risk, intent and evolution of an attack

The key is that Damballa's technology automatically redirects suspicious activity so that it can be contained and understood – in perpetuity. This ability to recognize stealthy, targeted threats in real-time, then analyze the evolution of those threats over time is why Damballa's technology is so effective at preventing sensitive information from leaving the enterprise. Better yet, Damballa protects with minimal impact on network management, security management or end user operations. This powerful addition to any enterprise organization's security strategy is easy to install and manage, and integrates easily with existing Defense-in-Depth infrastructure. As such, it represents a powerful advance in real-time protection against previously undiscovered or newly emergent targeted attacks.

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.