



# DefensePro Whitepaper

Fighting Cybercrime: Rethinking Application Security

By Ron Meyran



## Table of Contents

Introduction.....	3
The Changing Threat Landscape.....	3
Organized Crime.....	3
Botnets – The Rise Of The Giants.....	4
From Vulnerable Code To Vulnerable Service.....	4
Where Current Network-security Tools Fail.....	6
Radware DefensePro: A Real-time IPS Against Real-time Attacks.....	6
Absolute Immunity With DefensePro.....	6
How DefensePro Real-time Signature Protection Works.....	7
On Demand IPS Scalability.....	8
Summary: The Business Value.....	8

## Introduction

The motivation of hackers has changed from gaining fame to financial gain. Large-scale worm outbreaks have been replaced by application-vulnerability exploits and dedicated malware that is owned, controlled, and operated by well-organized, financially motivated attackers. Cyber crime activities employ a new level of network attacks, which go undetected by standard network-security tools.

This paper discusses the changing threat landscape and why standard network-security tools fail to protect online businesses from emerging threats. It then describes Radware DefensePro real-time Intrusion Prevention System (IPS) solution and value proposition.

## The Changing Threat Landscape

### Organized Crime

Cyber criminals have discovered that data theft, Internet-based fraud, and extortion can be extremely lucrative. Much of this activity is driven by sprawling networks of compromised PCs, or bots controlled by criminal groups. The Internet has become saturated with botnets designed to efficiently spew spam, spread malicious software, harvest sensitive data, and launch distributed denial of service (DDoS) attacks.

Organized crime groups have jumped on this money-making bandwagon and employ malicious computer hackers to build, maintain, and operate the bot crimeware. The bot software spreads by means of a multitude of propagation vectors: When innocent user access compromises legitimate Web sites, via mail spam, P2P-file-sharing programs, and more. In most cases, the victims are unaware of the fact that their computer has been infected by the malware code and has essentially been recruited into a botnet.

The bot malware offers a wide variety of “services”: Network attacks such as DDoS floods, HTTP page floods, and brute force; information harvesting, such as local usernames and passwords or license keys, network scanning and application scanning; and more.

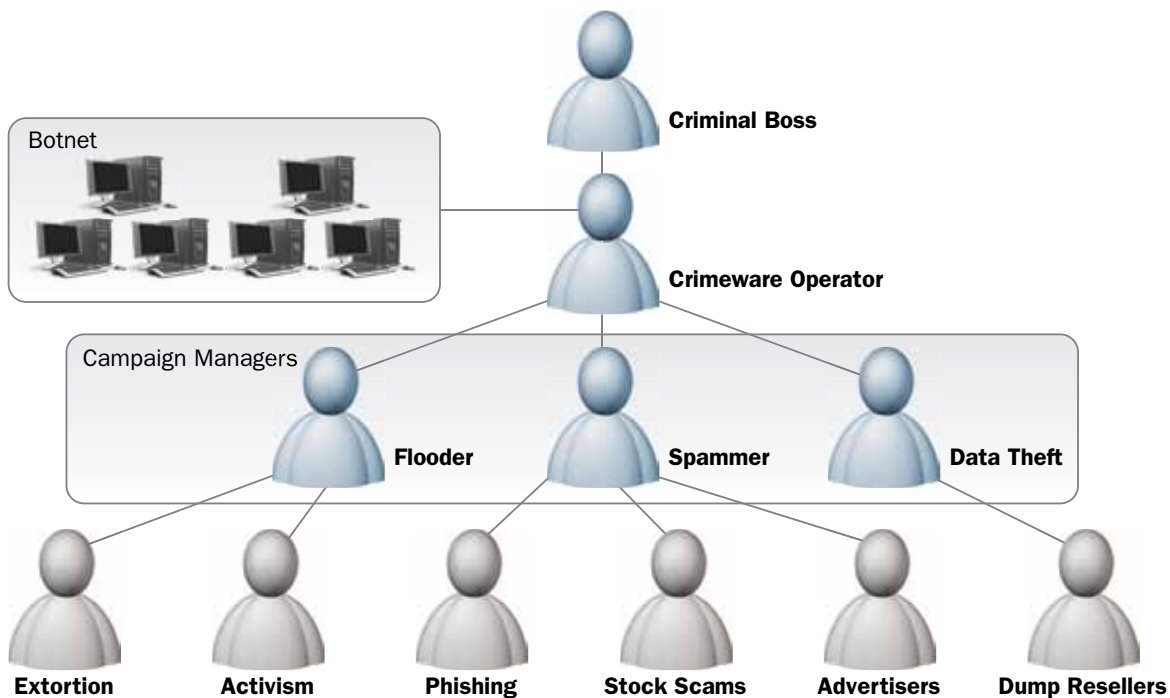


Figure 1: Cyber Crime Organizational Chart

Figure 1 depicts a typical food chain of a cyber crime organization. The crimeware operator (essentially the malicious hacker) possesses the power of the bot. Campaign managers are the next level of the criminal organization. They are “employees,” who offer cyber-crime services for a fee – flooding, spamming, data theft, and more. The “clients” negotiate prices for the services provided by campaign managers and deploy them for malicious activities, including extortion or hacktivism<sup>1</sup> using DDoS flooding, phishing, stock scams and advertising using spamming, and dump reselling<sup>2</sup> using data theft.

## Botnets – the rise of the giants

Network attacks based on the power of multiple compromised computers appeared as early as 1998 (GTBot), which used the IRC channel for the bot code download and for Command and Control (C&C).

In the past two years, we have seen evidence of several disturbing improvements in the capabilities of botnets:

- **Giant botnets.** The Storm Botnet became famous as early as 2007. It tricked innocent users into opening e-mail with interesting pictures. This essentially installed the bot code on the victim’s machine. More than 11 million computers were recruited into Storm Botnet, though it is not the biggest one. Since Storm Botnet, bigger botnets have appeared; Kraken, Srizbi, Rustock, and Cutwail are a few. Botnets are measured by the number of spam e-mails they can send out a day. Kraken can send 9 billion e-mails a day. Srizbi can send 60 billion e-mails a day. Of course, this is only to rank botnets; they offer services, from DDoS flooding up to information harvesting.
- **Stealthier C&C Channels.** Botnets moved from IRC, which is based on clear text commands, to P2P applications. This raised the level of botnet sophistication. There is no central server that can be shut down, nor can the commands be detected using signature detection technology, as typically, P2P applications encrypt their content.

Botnets have the power to put businesses under siege. Organized cyber crime has already proven its effect over the last year, through attacks such as those on Estonia<sup>3</sup>, and recently, the DDoS attack on Georgia that overloaded and effectively shut down Georgian servers. These attacks were well organized, and they demonstrated the great power of controlled cyber attacks. Their power is even greater when the attacks use new methods such as the non-vulnerability attack against online services and users.

## From vulnerable code to vulnerable service

Traditional network security practices have focused on the research of application-software code, finding flaws in the code that can lead to a security breach exploited by hackers – and patching it. The flaws are referred to as vulnerabilities. When hackers discover a vulnerability before software and security vendors do, they can launch a zero-minute attack, exploiting the newly discovered and unpatched vulnerability. This protection is about locating vulnerable application code and issuing a patch for it. Software updates and patches, anti-virus updates, and Intrusion Prevention System signature updates all are about protecting vulnerable code.

This new attack method allows attackers to integrate well with legitimate forms of communications and comply with all application rules, passing below the radar of existing network security

<sup>1</sup> Hacktivism: Computer attacks launched with political motivation. These attacks typically involve defacing or shutting down Web sites.

<sup>2</sup> You can buy “fresh dump” credit card numbers with PINs starting at \$20 each – up to \$100 for a platinum card.

<sup>3</sup> See Estonia recovers from massive DDoS attack at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019725>

To bypass existing security technologies that focus on patching vulnerable code, hackers deploy application-specific attacks, which are referred to as “non-vulnerability-based attacks.” This new type of attack does not exploit any flaw in the code, and therefore, patching will not help block it. Non-vulnerability-based attacks are executed on Internet-connected services and on users. These attacks go unnoticed by existing protection technologies and can result in information theft, fraud activities, and service disruption.

So what is a non-vulnerability attack? Non-vulnerability-based threats aim to exploit weaknesses in server applications that cannot be defined as vulnerabilities. A non-vulnerability-based attack attempts to misappropriate software without vulnerability. A non-vulnerability-based attack can be typified by a sequence of legitimate events, generally not associated with unusually large traffic volume. The attack can break authentication mechanisms and scan the application for hidden confidential files. More sophisticated non-vulnerability-attack forms include well-chosen repeated sets of legitimate application requests that misuse server CPU and memory resources, thus creating a full or partial denial of service (DoS) condition in the application. This new attack method allows attackers to integrate well with legitimate forms of communications and comply with all application rules, so that in terms of traffic thresholds or known attack signatures, they will pass under the radar of existing network security technologies.

Non-vulnerability attacks do not exploit any application vulnerability (a bug in the software application). They use legitimate application services for malicious activity such as authentication defeat, information theft and denial of service.

To emphasize the difference between the traditional vulnerability-based attack (known as a zero-minute attack) and the non-vulnerability-based attack, we can say that for the first, there is always the possibility of either creating a signature (sooner or later) that represents the malicious code and that can be used to block the attack or of developing an application patch that fixes the relevant application flaw. In the case of non-vulnerability attacks, the malicious code does not exist, and therefore, there is no attack signature nor is there an application patch. Non-vulnerability-based attacks can be executed unnoticed by today's protection technologies on server applications such as financial online transaction services, and can have a severe negative impact on availability and customer/client trust.

Examples of non-vulnerability attacks:

- **Brute force attack** – used to defeat an authentication scheme by running a sequence of login attempts until successful. Each attempt is a legitimate application transaction, however, the actual threat is in the systematic use of logins until successfully guessing a username and password.
- **Web application vulnerability scanning** – scanning of a Web server for known vulnerabilities or pages left for maintenance. Hackers use this information to launch targeted attacks or break into maintenance backdoors.
- **Service flooding** – more sophisticated than the older, simple DoS/DDoS packet-based flood attacks used previously by hackers. Hackers are moving to more sophisticated non-vulnerability application flood attacks including HTTP, SIP Invite floods, etc. These types of attacks are based on a completely legitimate session-based set of requests – generated towards the victim server, exhausting CPU resources.

These are only a few examples of typical threats that rely on service misuse. Hackers use services through “legitimate” sessions, easily integrating attack traffic with real user traffic, undetectable by standard security tools. The challenge is clear: differentiating between legitimate and attack traffic.

### Where Current Network-security Tools Fail

Standard network-security solutions depend on static signature protection against known application-vulnerability exploits and rate-based protection against high-volume attacks and unknown attacks.

Static signature-protection technology, deployed by Network-IPS, firewalls, and anti-viruses, can only identify predefined attacks. This type of traditional perimeter security relies on periodic signature updates, leaving the business vulnerable to zero-minute attacks, and offers no solution against non-vulnerability-based attacks.

Rate-based technology is designed to suppress abnormal traffic patterns. This technology is deployed as means of mitigating high-volume attacks or zero-minute attacks. However, a rate-based solution does not differentiate between attack traffic and legitimate traffic. Packets and sessions, good and bad, above predefined thresholds are dropped. Rate-based technology offers no protection against lower-rate attacks (for example, brute-force attacks, low-rate malware propagation, slow network and application probes). Furthermore, rate-based technology cannot prevent improper-use scenarios where attack traffic such as an HTTP page flood appears identical to legitimate application requests as in a flash crowd.

“The nature of the most damaging attacks on businesses has changed. Financially motivated attacks don’t simply go after unpatched PCs and servers; they increasingly are using targeted malware that requires more than simple, signature-based detection.”

- “Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08”  
by Greg Young, John Pescatore, Gartner  
February 2008

### Radware DefensePro: A Real-time IPS against Real-time Attacks

#### APbsolute Immunity with DefensePro

Radware’s award-winning DefensePro™ is a real-time Intrusion Prevention System (IPS) and DoS-protection device. It maintains business continuity by protecting the application infrastructure against existing and emerging network-based threats that cannot be detected by traditional IPSs – such as network- and application-resource misuse, malware spreading, authentication defeat and information theft.

DefensePro features full protection from traditional vulnerability-based attacks through proactive signature updates. This protection prevents the already known attacks including bots, trojans, worms, SSL-based attacks, and VoIP attacks.

DefensePro provides “immunity” against known and undiscovered vulnerabilities that seek to compromise the health of your application infrastructure (network bandwidth, server resources and clients activity).

Unlike market alternatives that rely on static signatures, DefensePro provides unique, behavioral-based, automatically generated real-time signatures. These signatures prevent non-vulnerability-based attacks and zero-minute attacks such as network and application floods, HTTP page floods, malware propagation, Web application hacking, brute force attacks that aim to defeat authentication schemes, and more. DefensePro does this all without blocking legitimate user traffic and with no need for human intervention.



Figure 2: APbsolute Immunity offers real-time signatures protection on top of standard vulnerability-based static signature protections

### How DefensePro real-time signature protection works

DefensePro inspects network traffic and creates baselines that represent the normal behavior of clients, servers, and networks. The behavioral-analysis engine detects abnormal patterns (network bandwidth, server resources, and client activity) and automatically creates a real-time signature that accurately mitigates the attack, using up to 20 L4-L7 header fields with AND and OR operations. All this is done with no human intervention.

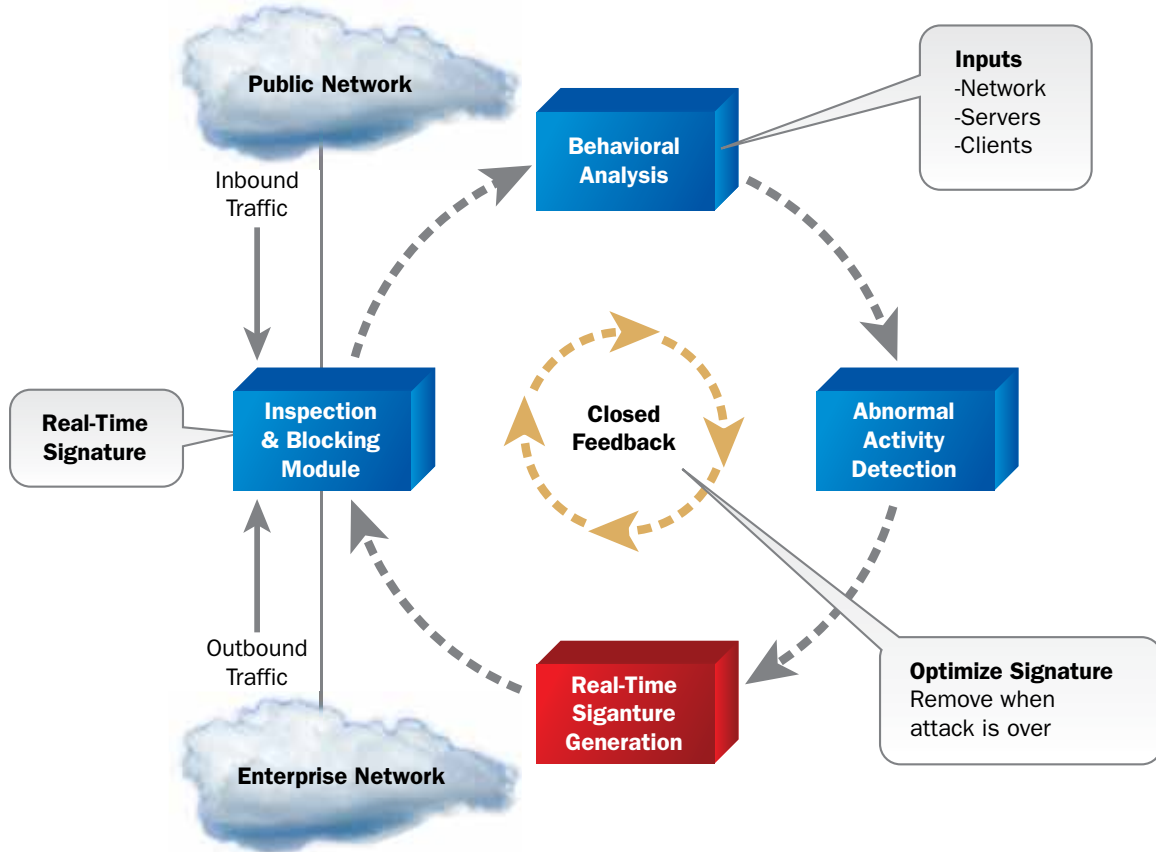


Figure 3: The APSolute Immunity Engine detects abnormal network activity and mitigates it in real-time

Once a real-time signature is created and applied, DefensePro employs a closed feedback mechanism that has the following roles:

- Refining the real-time signature for the most accurate attack mitigation
- Modifying the real-time signature if an attack pattern develops or mutates
- Removing the real-time signature once the attack is over

To understand how the real-time signature protection engine works, let's look into two cases of attack mitigation:

- **Non-vulnerability attacks.** Since these attacks do not exploit any application design flaw or bug, there is typically no signature available to counter the attack. However, since DefensePro learns traffic behavior, in the event of a non-vulnerability attack like an HTTP page flood, DefensePro is able to detect the malicious sources generating the flood as well as identify the specific Web page under attack. DefensePro then generates a real-time signature that blocks the attacker's access to the Web page under attack, while maintaining legitimate user access to the Web site.
- **Zero-minute attacks.** These attacks exploit a vulnerability for which a signature can be created to match the attack pattern. However, given the accelerated timeline under which hackers are now exploiting application bugs, vulnerability research centers lag behind in researching and creating signatures to counter these attacks. DefensePro has a distinct advantage when dealing with zero-minute threats by virtue of its real-time signature capabilities.

## On Demand IPS Scalability

Radware is the first to offer on demand IPS scalability across its line of IPS models, which range from 100 Mbps all the way up to 8Gbps. The line is complemented by Radware's set of behavioral protection products, which range from 4 Gbps up to more than 12 Gbps of throughput to offer the highest performance available. An initial deployment of an IPS can use the IPS model that supports the throughput the business requires right then. When the business grows or network bandwidth grows, the business can simply upgrade the IPS to a higher bandwidth product model by applying a software license key. No need for hardware replacement, configuration conversion, lab testing, staging or training.

The on-demand IPS scalability offers clear benefits:

- **Buying what is needed.** The business saves on CAPEX by avoiding overspending on the IPS solution when trying to size future network growth.
- **Paying as the business grows.** The business requires no forklift upgrade when the network bandwidth needs to grow. And moving to the next DefensePro model can happen with no service downtime.

## Summary: The Business Value

Radware DefensePro offers a unique value proposition for online businesses, Hosting/colo Service providers and Enterprise Datacenters:

- Maintain business Continuity of Operations (COOP) when the network is under attack by preventing emerging network attacks as well as vulnerability based attacks in real-time without blocking legitimate users.
- Support large online businesses and data center consolidation trends that require multi gigabit network security solutions
- Reduce total cost of ownership (TCO) of network security management through exclusive On-Demand-IPS approach that allows you to buy what you need and upgrade to higher bandwidth model when you need.

“Radware has done a good job... making this one of the best Attack Mitigator devices we have seen in our labs to date.”

“Overall we found the DefensePro to be a robust and capable Attack Mitigator and believe that it should be on any short list as a candidate for a mitigation solution on the network perimeter.”

- Bob Walder, NSS Labs, April 2008