



# CyberHunter

## Malware Web Crawler Technology

### Version 2.0

Last Modified on: March 10, 2009



CyberDefender Corporation

617 West 7th Street, Suite 401 Los Angeles, CA 90017

[www.CyberDefender.com](http://www.CyberDefender.com) | Phone: (213) 689-8631

**Proprietary and Confidential:** This document is proprietary and confidential information of CyberDefender Corp., and is covered by copyright and trade secret protection. Unauthorized adaptation, distribution, use, or display is prohibited and may be subject to civil and criminal penalties. Disclosure to others is prohibited.

© 2009 CyberDefender Corp. All rights reserved.

## Contents

1 Overview .....	3
2 Current threat landscape .....	3
3 CyberHunter in action .....	4
4 CyberHunter key benefits .....	4
5 CyberHunter commercial benefits .....	5
6 CyberHunter main functions .....	5
7 Summary .....	6
8 References .....	6
9 CyberDefender anti malware network on cloud computing patent application .....	6

## 1 Overview

CyberHunter is a next generation web crawling technology that proactively crawls targeted locations on the internet and identifies malware as well as phishing attacks. The CyberHunter web crawler is central in CyberDefender's efforts to provide zero hour protection to its own users and other commercial websites. The CyberDefender earlyNETWORK™ 2.0 consisting of the Threat Protection Network 2.0 and the Secure Peer Network 2.0 Technology platforms is a next generation cloud computing solution for protecting users from malware and phishing. By leveraging the power of cloud computing and the secure peer, CyberDefender is able to rapidly respond to new threats and provide a higher level of protection.

The Threat Protection Network 2.0 has multiple components including:

- Phishing Protection
- Virus and malware file protection
- Malware URL protection
- Proactive web crawling of internet based threats provided by **CyberHunter**.

## 2 Current Threat Landscape

*Malware Inflection point:*

Since 2007 the volume of new malware files has been growing exponentially and it has become difficult to counter these with the traditional tools available to security companies as reported by the Washington Post<sup>(1)</sup> on its security blog.

*Quick Response Time:*

The major reason malware attacks spread so quickly is the large gap in the response time between the attacks first identified and the user's receipt of mitigating patterns. This lag is responsible for many corporate and personal users infection of malware that could have been stopped in the first few critical hours. The early and accurate detection of zero day threats is critical to today's enterprises and home users.

### 3 CyberHunter in Action

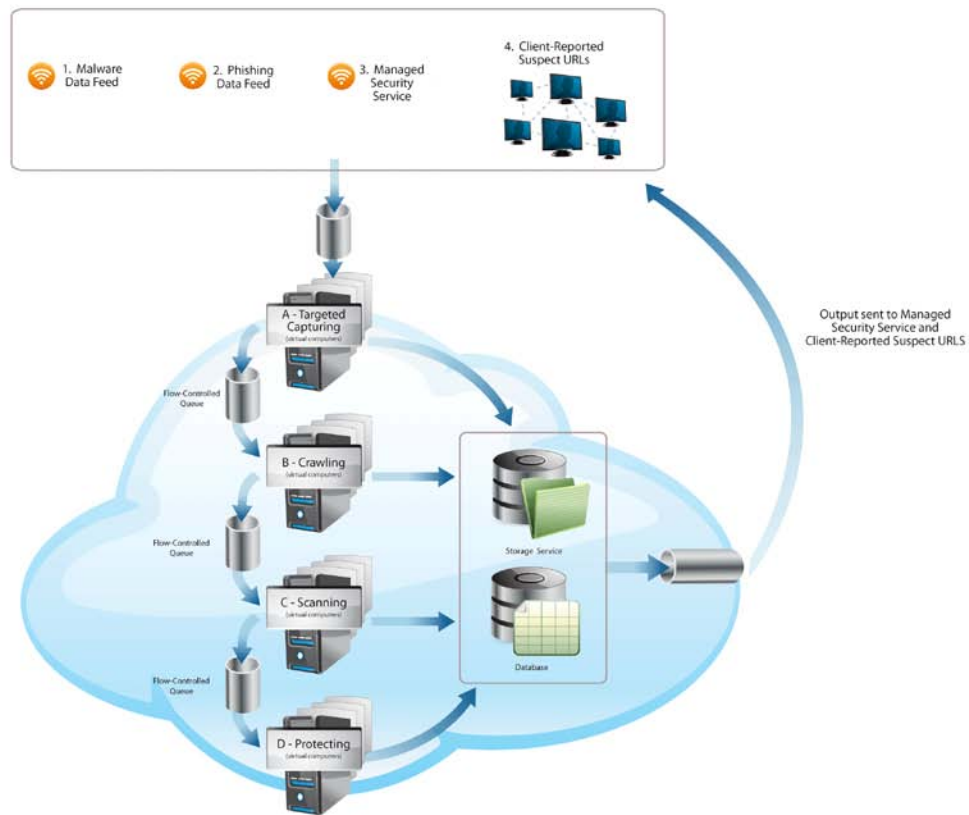


Figure 1

### 4 CyberHunter Key Benefits

- Multi-source data feed: Malware and phishing URLs are aggregated from different sources to be crawled.
- Targeted crawling: The crawler uses a pre-validated set of suspicious or malware URLs as seed.
- User feedback: CyberHunter uses suspicious data feedback from the users. All reported suspicious phishing URLs are crawled as part of the Targeted Capturing.
- Multiplier effect: Once a malware URL has been identified, other URLs linked to the domain are also crawled for malware.
- Leveraging cloud computing to offer scalability: CyberHunter databases are capable of dynamically scaling “in the cloud” to meet increased processing demands for threats.
- Real Time monitoring: Ability to proactively monitor websites on an ongoing basis.

- Frequency of attacks: In the future CyberHunter will track the frequency and prevalence malware files found to alert a new malware attack.

## 5 CyberHunter Commercial Benefits

- The ability to reduce the cost of updates to its users by continuing to expand its cloud threat databases populated by CyberHunter.
- Managed Security Service to monitor specific domains in real time for domain hi-jacking and malicious user posted content

## 6 CyberHunter Main Functions

### a. *Targeted Capturing:*

CyberHunter will first capture specific targets to crawl since the internet as a whole is too large in today's day and age to be crawled in its entirety. The preparatory capturing module is multi-source oriented. It can feed domains from specific locations such as banking / ecommerce and, major software download service sites. It can also feed domains and URLs from verified Anti-malware research entities.

The targeted capturing module sends this multi-source feed to be crawled from cloud databases. The module also throttles the number of URLs that are in the queue to be crawled as well as re-crawled.

### b. *Crawling*

The crawl function spiders through the URLs pro-actively to find linked URLs and identify executable files that are to be scanned.

### c. *Scanning*

The scanning function scans executable files and identifies malware. It uses both behavioral analysis as well as signature based detections. The download URLs and domains are then blacklisted.

### d. *Protecting*

After scanning, the new threat data is added into cloud-hosted threat databases (virus, phishing, malware host pages) and are used for 'Protecting' for CyberDefender users.

## 7 Summary

To counter the new phenomenon of fast growing disposable phishing attacks and one time malware infections "*the time to update*" is the major drawback in traditional systems. CyberHunter addresses this by leveraging cloud computing and a pro-active approach in scanning web pages.

## 8 References

- (1) ([http://voices.washingtonpost.com/securityfix/2008/06/redefining\\_antivirus\\_software.html](http://voices.washingtonpost.com/securityfix/2008/06/redefining_antivirus_software.html))

## 9 CyberDefender anti malware network on cloud platform patent application

CyberDefender has already filed a USPTO patent application number 61,221,477 which is titled "System and method for operating an anti-malware network on a cloud computing platform."