

Kolnos Solution Brief

Kolnos Eagleye

Fraud Detection



Abstract

As technology continues to improve, it opens the possibility for attacks never before possible. An attacker can exploit unprotected systems to commit fraud and crime by combining these new technologies. One such crime being committed is credit card fraud. However, unlike traditional techniques employed to commit this crime, unscrupulous individuals are taking advantage of the Internet's power to utilize a new technique—brute force attacks to *guess* credit card numbers.

Credit Card Theft

You might call it the least creative way to steal credit card numbers—but it works, and it's costing some merchants thousands of dollars. Computer criminals have taken to running thousands of small charges—as low as a nickel and dime—through merchant accounts, picking credit cards numbers at random. Most are declined. But the few that are authorized mean the criminal has struck gold. The criminal proceeds to charge high-priced items with the card or sell it in a criminal underground.

Several capabilities are now possible which make this primitive attack possible. The attackers are employing *botnets*—a collection of computers across the Internet—to perform this attack on a massive scale. The computers are broken into and commandeered to perform any task the attacker wishes. The botnet herder then commands the drone computers—tens of thousands at a time—to guess credit card numbers. The widespread adoption of broadband Internet access has brought this attack to fruition.

Merchants are faced with the problem of paying for each attempted credit card authorization. In some cases, the credit card issuers are threatening to cancel the merchant's account which would cripple virtually any business today.



Kolnos Eagleye

Kolnos Eagleye is a revolutionary security product for **identity verification** and **automated attack detection**.

Eagleye adds an entirely new security layer to a website for identity verification. Eagleye continuously and unobtrusively monitors the behavior of website visitors to ensure their identity. Unlike authentication which typically occurs only once per session, Eagleye monitors each visitor throughout their session, validating and ensuring their identity every step of the way.

Eagleye's security layer complements a website's existing security infrastructure, it does not contend with or compromise it.

Eagleye combines behavioral analysis with environmental and situational awareness. Behavior cannot be stolen, *phished*, or duplicated. Behavior is also unique to each individual yet is never identical, even for the same individual.

Visitors with suspicious or fraudulent activity are challenged or blocked from the system.

Eagleye integrates seamlessly into existing web applications and it works entirely in the background so web site visitors and customers don't incur any additional responsibility or burden.

Eagleye on Card Theft

Eagleye's patent-pending **automated attack detection** offers unprecedented protection against credit card fraud. By analyzing the behavior of each website visitor, be it a visit by a human or through an automated process, Eagleye can detect an intruder, impostor, or attacker *before* fraud has been committed.

Traditional analysis has depended solely on server data while Eagleye utilizes the client side to provide more comprehensive information. Furthermore, Eagleye takes a revolutionary step by incorporating behavioral analysis into the fraud detection process—the *human touch*. This is key to effectively differentiating between legitimate users and hostile automated attacks.

A botnet typically consists of many unrelated machines which are running similar processes. Collections of tens and hundreds of thousands of machines are known to exist. Each machine, or drone, attempts to carry out a transaction on the merchant's website in an attempt to verify the validity of a random credit card number.

Security products which rely on environmental factors are handicapped since the data they receive comes from the infected drones and thus is easily crafted to avoid suspicion. Another disadvantage is that these solutions are limited to comparing data from different sessions of the same visitor. Eagleye's automated attack detection does not rely purely on environmental factors. Eagleye analyzes the sessions of all visitors to the merchant's website. Without employing Eagleye's automated attack detection, fraudulent activity based on environmental data can only be discerned after an individual has engaged in multiple visits to the merchant's website. With Eagleye once any of the computers in the botnet collection visit the merchant's website any other visit from any member of the botnet is subject to detection.



Environmental information such as IP addresses, device IDs, operating systems, and browser versions can provide helpful information for the initial screening for fraudulent activity. Basing fraud detection on environmental analysis by itself however is not an effective means of detecting fraud. Hackers can easily modify the presentation of the environmental data. Information such as IP addresses, for example, that might normally be meaningful are actually of limited use.

EagleEye places most significance on an analysis of the visitor—website interaction. This is termed the visitor behavior and can be analyzed independent of environmental factors. In a botnet attack various participating computers will have different environmental factors but their behaviors will have a similar pattern. EagleEye is able to recognize this behavior as fraudulent activity.

EagleEye combines behavioral analysis with consideration of the client and server environmental factors to provide an effective detection and deterrent against automated credit card theft.

Conclusion

Credit card fraud has returned once again. This time, unscrupulous people are leveraging several facets of the Internet to commit this crime. Hackers are commandeering tens of thousands of personal computers and using the resulting army of computing power to carry out brute force attacks on unprotected web sites.

The methods employed by today's hackers involve the introduction of sophisticated Trojans and other malware onto vulnerable personal computers. The users of the infected computer are unaware that their computer may be participating in an attack aimed at securing valid credit card numbers.

To address this new threat a product that takes a new approach to fraud detection must be employed. The old approaches to fraud detection have been addressed and rendered ineffective by the current hacker organizations.

EagleEye represents a new approach in fraud detection and one that is not easily circumvented. The use of EagleEye effectively identifies illegitimate users and allows the website to prevent fraud before it ever occurs.



Kolnos

Kolnos Systems, Inc.

www.KolnosSystems.com