iovation
A TransUnion® Company

SOLUTION BRIEF

Fighting Fraud From Botnet Attacks

Using device intelligence to defeat fraud threats from botnets

The Botnet Battleground

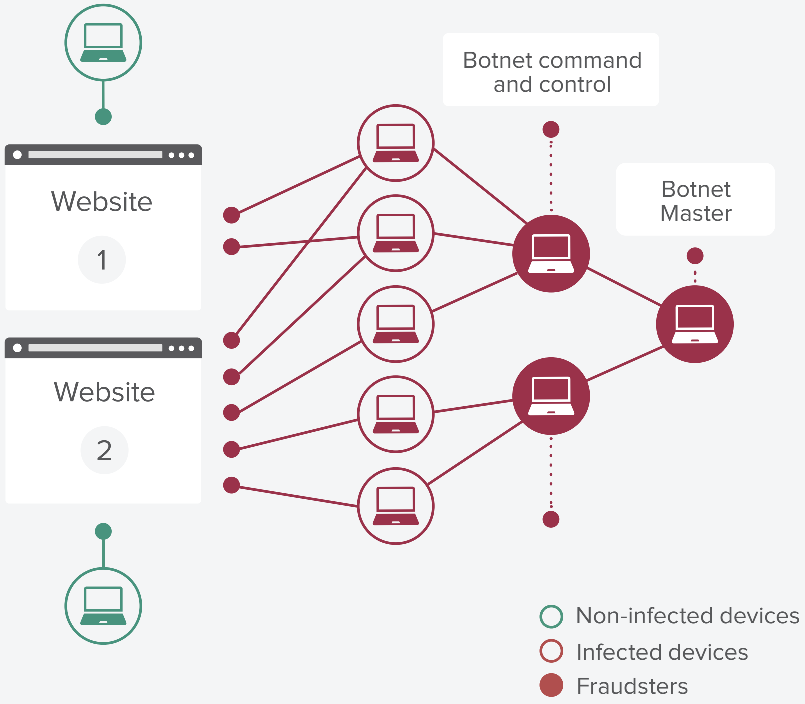
A botnet is an interconnected network of computers that have been infected with malware without the user's knowledge. Usually controlled by cybercriminals, botnets have been used for nuisance spam and distributed denial-of-service (DDoS) attacks, which are most often characterized by fast and furious network traffic targeting a specific server. Manufacturers of network firewalls and DDoS mitigation service providers rely on these high traffic volumes to help block botnet attacks.

In recent years, botnet attacks have become increasingly insidious. The SpyEye malware program alone, for example, has been used to steal from individual's bank accounts, resulting in hundreds of millions of dollars in losses to bank institutions. Instead of relying on a quick and aggressive approach for spam or DDoS purposes, today's botnet attacks are often stealing personally identifiable information (PII) in order to commit financial fraud. Through credential stuffing attacks, botnets have exploited billions of breached login credentials over the last decade to commit real fraud through account takeover.

Within the emerging trends uncovered in iovation's 2019 Gambling Report, cybercriminals are also using bot attacks to create a distraction while they perpetrate other fraudulent activity, which often goes undetected because of the focus on the larger scale attack.

A Typical Botnet Attack

A typical botnet attack involves a device serving as the botnet master, perhaps located in a high-risk geographic region or using a high-risk ISP. Using multiple command and control computers, the botnet malware spreads to other unsuspecting users' devices. Traditional high-velocity botnet attacks can often be stopped with a combination of firewall configuration and third-party packet scrubbing services, but the new slow botnet attacks make it more difficult for the website firewalls to distinguish botnet traffic from legitimate traffic.



Being that fraudsters are in the business of evading detection, they have shifted how botnets are leveraged. They are keenly aware that high traffic velocity is used to detect botnet attacks, so they respond by slowing transactions down. What's more, they know that using devices from risky geographic regions or IP addresses raises flags, and that using the same device for a long period of time could result in that device ending up on a watchlist.

Taking a signature-based or behavior-based approach to detecting a single node (infected PC) on a botnet is ineffective by itself. Botnet attacks are designed to commit online fraud with the appearance of normal, regular traffic, making them nearly impossible to detect.

A Three-Pronged Approach

As botnets get smarter, more pervasive, and more cunning, our strategies need to evolve. The old strategy of finding a bot based on a specific malware signature needs to give way to a three-pronged approach that involves multiple solutions in a layered defense strategy:

- **Detect & Prevent Fraud Caused by Botnet Attacks:** Track internet botnet activity, considering both recency and intensity of previous attacks, to provide contextual risk analysis. In combination with the device and session insight, detect the riskiness of the transaction and provide immediate alerts on account or credential compromises
- **Stop Bots at the Front Door:** Leverage strong multifactor authentication with adaptive insight when a transaction appears compromised to prevent payloads from being deposited
- **Protect Customer Touchpoints:** Monitor all your network transaction and end user interaction touchpoints through a unified system, rather than staking out key locations at firewalls

Detecting Bots

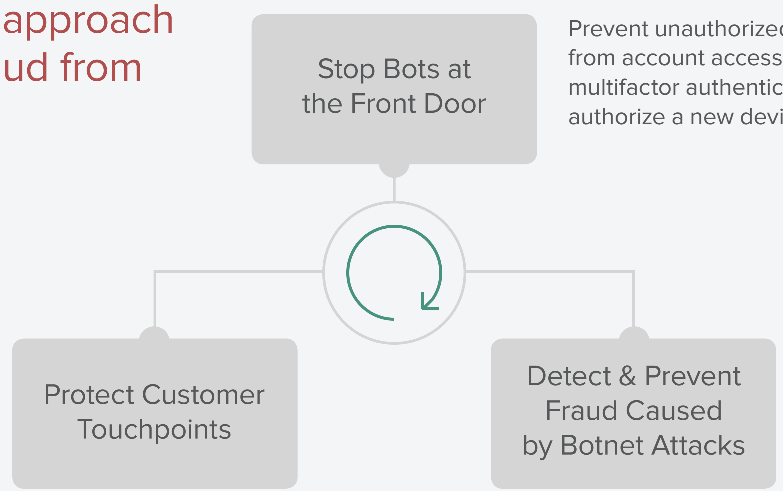
Detecting bots on specific devices is extremely difficult to accomplish without the assistance of locally installed anti-malware software. Even then, bot characteristics constantly change and are not always detected by anti-malware. Because many of the devices used are merely regular devices belonging to unsuspecting people, techniques such as relying on watchlists and geographic locations often prove ineffective.

Several indicators may signal the presence of a bot, but by no means guarantee that one exists. For example, if a mobile device has been jailbroken or rooted, then it is much easier to infect with a bot. If a particular device has accessed multiple accounts across a variety of businesses and industries, that could also be an indicator. However, in today's Internet economy, most people use the same device to access their bank accounts, favorite e-tailers, and social networking sites. This creates a challenging question: How many accounts being accessed by the same device is too many, and thus signals a potential bot?

Beyond simply detecting bots, botnet detection and prevention must extend into understanding the larger context of the fraud that is being committed through them.

iovation's FraudForce solution provides a botnet risk score based on the historical severity of botnet attacks as well as time elapsed since the last attack. Tracking network patterns and botnet activity is a powerful component of a multi-pronged strategy to combat botnets up front. Combined with our robust device intelligence consortium, iovation leverages the power of device intelligence to help stop fraud caused by botnets.

A three prong approach to stopping fraud from botnet attacks



Stop Bots at the Front Door

Prevent unauthorized devices from account access and use multifactor authentication to authorize a new device

Protect Customer Touchpoints

Any unprotected customer touchpoint creates a vulnerability for your entire online property

Detect & Prevent Fraud Caused by Botnet Attacks

Track internet botnet activity in combination with insights on the device to detect the riskiness of the transaction

Stopping Bots at the Front Door

If a compromised device attempts to access an account, additional step-up authentication can be used to verify identity or prevent access. This approach is effective for granting access to good customers with minimal friction while keeping out both fraudsters and bots relying on authorized devices.

iovation's dynamic authentication solutions play an important role in making this happen by enabling risk-based, multifactor authentication for online accounts.

Fighting Botnet Fraud with iovation

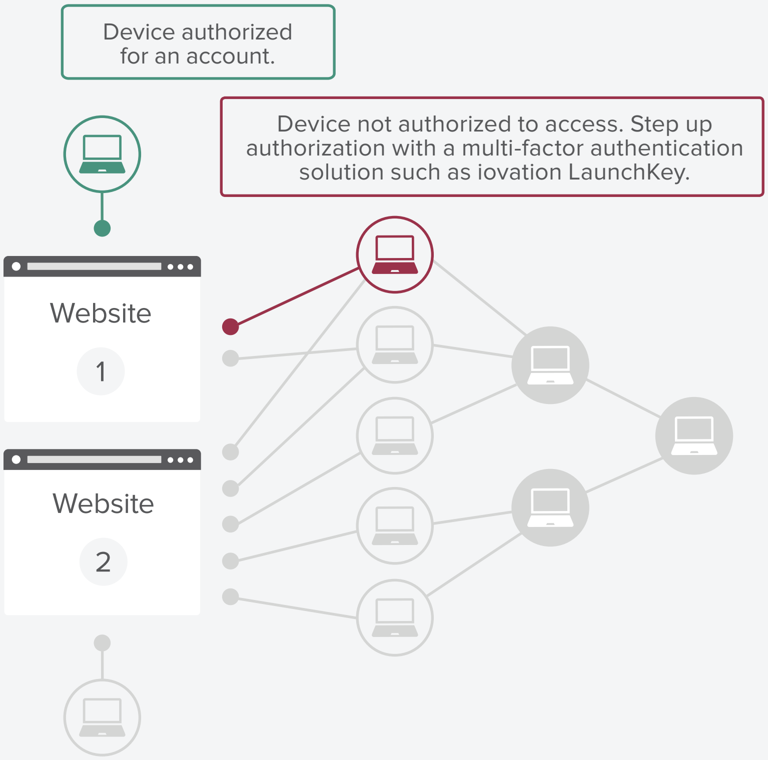
iovation is widely recognized as a leading provider of online fraud detection and prevention solutions. Many of the capabilities we offer have proven to be effective at stopping sophisticated global fraud rings. Our powerful fraud prevention capabilities have been effective against bots and human fraudsters alike with capabilities that include:

- **Global Fraud Fighting Consortium:** More than 6,000 global fraud and security analysts utilize iovation’s fraud fighting consortium. When fraud is confirmed by one of these analysts, they submit feedback to iovation in the form of a “reputation report” and label the device or associated user account with the specific type of fraud or abuse they observed. This gives the client the capability to stop subsequent transactions from that device or account while sharing this information with other global clients so they can benefit as well. Once fraud has been confirmed on a device compromised with a bot, further fraud from that device is easily recognized.
- **Botnet Risk Score:** By tracking network patterns, the botnet risk score provides a calculation based on the recency and severity of previous botnet attacks. As botnet attacks often come from the devices of unsuspecting users, this score provides a powerful component of a multi-pronged strategy to determine potential fraud correlation with a particular transaction and ultimately combat botnets up front.
- **Device and Account Associations:** To iovation, botnet fraud attacks appear as groups of related devices trying to access multiple accounts. When fraud is confirmed as coming from one of these devices, we propagate that fraud evidence to all other related devices and accounts, immediately stopping a coordinated botnet attack.
- **Prevent Delivery of Malware:** If a device is not recognized as being authorized for use with the account, then a multifactor authentication solution, such as iovation's LaunchKey, can be used to confirm with the user that the new device is authorized to access the account.
- **Advanced Behavioral Analytics and Rules:** Fraudulent botnet attacks may employ low and slow velocity to avoid velocity detection. iovation offers advanced behavioral analytics that can detect coordinated attacks in other ways. For example, we can flag when a specified number of accounts have been created or accessed by a specific device, the number of email addresses per device, the number of devices per phone number, number of accounts per device, or number of countries per device. Correlating these behaviors with the botnet score can provide valuable insight on detecting attacks.

Detect & Prevent Bots at the Front Door

Track internet botnet activity by recency and intensity through our botnet detection solution in FraudForce. In combination with insights gathered from the device, detect the riskiness of a transaction to provide an immediate alert on the account and detect potential fraud before it occurs.

Step-up authorization with a multifactor authentication solution such as iovation’s LaunchKey to prevent botnet access while allowing the good customers in.


Device authorized for an account.
Device not authorized to access. Step up authorization with a multi-factor authentication solution such as iovation LaunchKey.
Website
1
Website
2

- **Unique Velocity Rules:** Unlike traditional velocity rules that focus on the velocity of traffic for a single business, iovation's unique velocity rules track transaction velocity across our entire customer base, and across a full spectrum of industries. While low and slow botnet attacks may fly under the radar at a single business that is using other tools, iovation can spot them when the same collection of devices is seen attacking multiple businesses in a short amount of time.
- **Abnormal User Behavior Rules:** It takes a typical person a certain amount of time to fill out an online form. If an online form is filled out much more quickly than this, then it is very probable that a bot is involved and filling out the form programmatically. By utilizing iovation's black box age rule, it is easy to trigger and stop forms from being processed when they are completed in a very short amount of time. This helps stop new account fraud, and application fraud that is being driven by bots.
- **High-Risk Indicators Rules:** More and more, botnets are using tools like Tor to hide their command and control traffic. iovation gives subscribers the ability to review transactions routed through Tor exit nodes, or those coming from specific high-risk geographic regions and IP ranges.
- **Jailbroken and Rooted Devices:** A jailbroken or rooted mobile device is more prone to be infected with a bot. To address this, iovation offers rules for detecting devices that have been jailbroken or rooted to highlight the increased risk of bots or other malware.

A Balanced Fraud Prevention Approach

Botnet attacks are far more serious than the simple nuisances they once posed for businesses. They can cause significant financial losses for businesses across every major industry. Preventing online fraud demands an approach that both detects and prevents botnet attacks. With a combination of device intelligence, botnet activity tracking and multifactor authentication solutions, iovation is well positioned to help you stop all vectors of online fraud, including botnet attacks.

iovation
A TransUnion® Company

To learn more about iovation's **authentication and fraud prevention solutions**, please contact us or visit iovation.com

PORTLAND • PH +1 (503) 224-6010 • EMAIL info@iovation.com **LONDON** • PH +44 (0) 800 058 8731 • EMAIL uk@iovation.com