Joint Solution Brief

Gigamon and Stealth Security Detect and Mitigate Automated Attacks and Unwanted Traffic

The Challenge

By using syntactically correct Web, mobile, and API requests, automated attacks can evade detection by traditional security solutions like IDS/IPS or Web application firewalls.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, Stealth Security tackles the malicious automation problem, helping companies to prevent and reduce customer account takeover and on-line fraud, damage to brand reputation and user experience, and costs associated with high-user drop off rates.

Joint Solution Benefits

- Detect and mitigate automated attacks and unwanted traffic in real-time
- Enhanced visibility and easy access to traffic from physical and virtual networks through the GigaSECURE Security Delivery Platform
- Stealth Security leverages the GigaSECURE platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- The GigaSECURE platform accelerates processing throughput by effectively filtering and distributing relevant traffic from across the network to the Stealth Security solution

Introduction

As Web, mobile, and API applications become ubiquitous channels for business, nearly every company is at an increased risk of large-volume automated attacks. In fact, many businesses are already losing millions of dollars as of result of automated attacks.

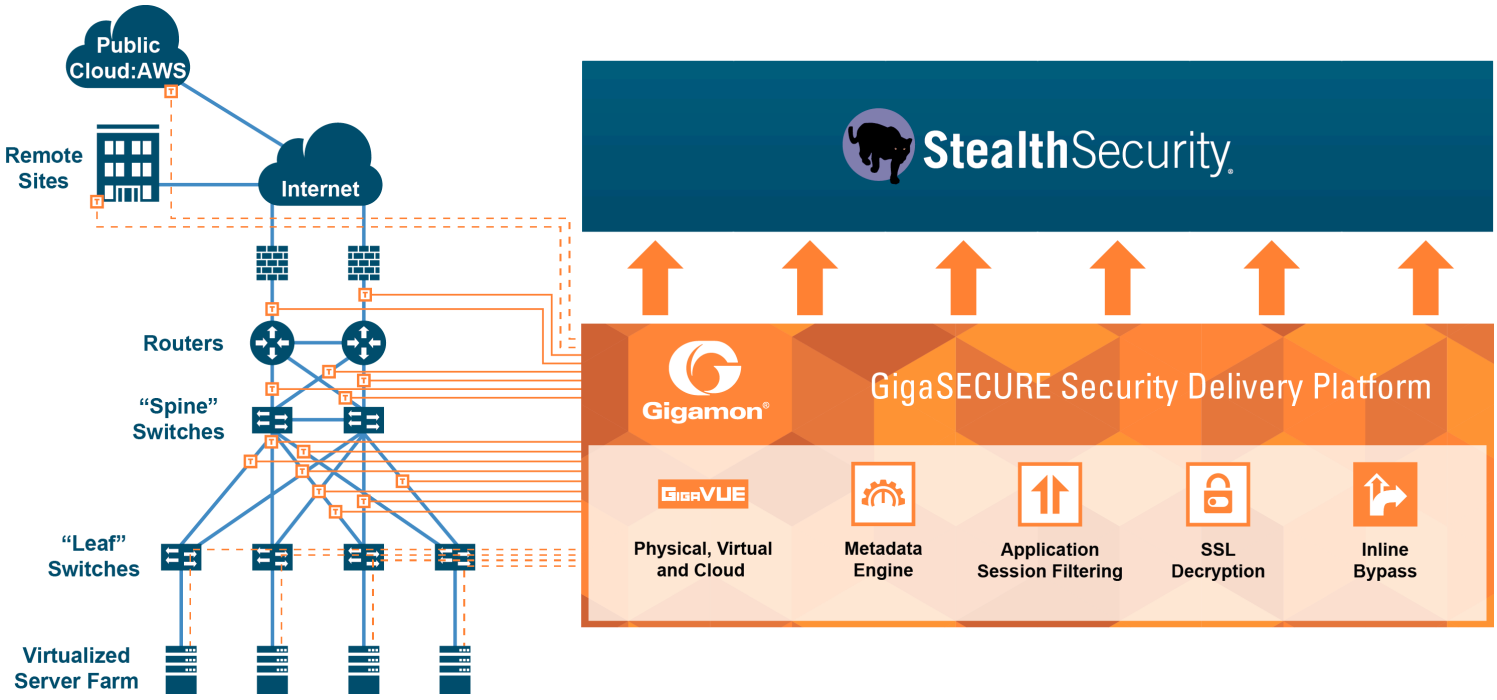
Using widely available, sophisticated black-market tools such as SentryMBA, AccessDiver, Hitman, Vertex, and AIO Checker, attackers can easily test millions of user IDs and passwords downloaded from the Internet. They tend to target Web, mobile, and even API flows—whatever the channel of least resistance—to compromise and/or create fake customer accounts, as well as perform other unauthorized activities. Their intent? Anything from validating sets of leaked user credentials to creating bulk accounts, resetting passwords, automating account/site scraping, and stealing money, goods, services, or personally identifiable information (PII).

Unfortunately, automated attacks can easily evade detection and mitigation because they use syntactically correct Web, mobile, and API requests. In other words, they do not exploit any vulnerability in the application stack and, therefore, do not trip any alerts in traditional security solutions like IDS/IPS or Web application firewalls.

The Gigamon and Stealth Security Joint Solution

Stealth Security provides a solution for companies whose core business depends upon the confidentiality, integrity, and availability of on-line customer data. For these companies, leaving any channel vulnerable to automated attacks that lead to customer account takeover, fake account creation, or theft of PII is an unacceptable level of risk.

Integrated with the Gigamon GigaSECURE Security Delivery Platform, Stealth Security provides the first solution to use real-time network traffic analysis, behavioral analytics, machine learning, and artificial intelligence technologies to dynamically adapt to the latest attack patterns for accurate detection and mitigation of automated attacks—with no effect on legitimate user traffic.



The Stealth Security solution is quick to deploy through containers, requires no application or Web integration, and is invisibile to attackers. In addition to detecting and mitigating automated attacks, the solution can detect legitimate business automation and assist companies in taking precautionary actions like:

- **Whitelisting** partners, aggregators, and merchants to focus on malicious automation
- **Blocking legitimate automation** from using Web and mobile endpoints
- **Limiting legitimate automation** to certain designated API endpoints
- **Restricting time-of-day use** of business automation to reduce impact on real customers during peak business hours
- **Implementing quotas** for business automation per aggregator, merchant, and partner

With real-time visibility of legitimate business automation, companies can rightsize their application infrastructures by provisioning based on legitimate traffic volumes.

GigaSECURE Security Delivery Platform features that augment the value of Stealth Security technology deployments include:

Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers network traffic—in the format required—to the Stealth Security platform. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to Stealth Security solution so that traffic can be monitored and analyzed together.

Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single application tool can manage, the GigaSECURE platform can split the flow across multiple tools, while keeping sessions together and instance numbers can be incrementally grown by adding new devices to those already connected.

Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to the Stealth Security solution so it only analyzes traffic that provides security value.

Learn More

For more information on Stealth Security and Gigamon solutions, contact:

StealthSecurity
www.stealthsec.com

Gigamon®
www.gigamon.com

3216-01 03/17