Stratecast | FROST & SULLIVAN

March 3, 2017

Advancing to Bot Management and Security

Credential Stuffing Becomes Top Concern

Stratecast Analysis by

Chris Rodriguez

Stratecast Perspectives & Insight for Executives (SPIE)—Special Publication

Volume 17, Number 7

Advancing to Bot Management and Security
Credential Stuffing Becomes Top Concern

Introduction[1]

The cybersecurity industry is characterized by one immutable constant: guaranteed change. Threat actors utilize a technique that works until security practitioners become aware and adjust their defenses. Then, threat actors simply adapt new techniques until the security industry makes its next adjustment. The constant cat and mouse game has proven to be challenging for customers of cybersecurity solutions; and many widely publicized security breaches suggest that this strategy is waning in effectiveness.

By contrast, a strategy to disarm threat actors of their most valuable tools represents an opportunity to rebalance the playing field and to regain the advantage from hackers. The focus on one such tool, the bot, has grown in popularity in recent years. The term "bot" simply refers to an automated online program. A bot's programmability to perform a wide range of tasks in an automated manner makes it a "must-have" in many hackers' tool boxes. A massive collection of coordinated bots is called a botnet, and can provide attackers with formidable computing and bandwidth resources. Bots were first developed years ago, but have recently emerged as a game changer for both defender and adversary.

Bots can be used for activities that range from malicious, illegal, or fraudulent, to activities that are more ambiguous or even benign or helpful. The effort to figure out which bots represent true, noteworthy threats can prove to be an arduous, multi-step process. Bot detection and management is an emerging market, with vendors such as Akamai, Distil Networks, Imperva, Perimeter X, and Shape Security offering solutions that perform crucial parts of the process.

But the bot arena is also marked by a high degree of technical change. As security vendors become more proficient at detecting bots, threat actors instinctively pour more resources into adding detection evasion and other advanced capabilities that make their bots more difficult to detect or control.

Naturally, the most advanced bots are used primarily for profitable activities such as data theft and account takeover. One such exploit trend is the use of credential stuffing, wherein attackers try stolen sets of credentials against a range of popular websites, based on the hope that the victim has used the same combination of credentials on multiple websites. The automated nature of a bot makes the process of brute-force checking of millions of unique credentials quite an efficient and lucrative practice. **For attackers, it's simply a numbers game; a 1% success rate of 1 billion attempts will result in 10 million breaches.**

The urgency of the bot problem is mounting—particularly when viewed through the lens of credential stuffing and account takeover. Billions of unique credentials have been stolen in recent

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- Akamai – Pawan Bajaj, Product Line Director, Cloud Security Business Unit
- Distil Networks – Jaweed Metz, Director of Product Marketing

Please note that the insights and opinions expressed in this assessment are those of Stratecast, and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

years, evidenced by the massive breach of 1.5 billion accounts at Yahoo alone.[2] Overall, this exploit trend demonstrates that the pattern of escalation has followed its expected course with bot security as well. The pressure is now on security vendors to advance from bot detection and response to full bot management and security.

Defining Bot Solutions

As discussed in previous SPIEs, the need for bot detection, management, and security has grown precipitously in recent years.[3] The market's response to the growing bot problem can be categorized by the different tiers of response offered. Early and basic bot solutions started with bot detection, and evolved to bot management. Bot management solutions are now poised to advance to full bot management and security. These various types of bot solutions are defined as follows.

Bot Detection—Is It a Bot?

Bot detection is considered a preliminary step in the entire bot lifecycle process. Bot detection is simply the answer to the question: "Is this a human user or a bot?" This decision point is an important one that enables further analysis, categorization, and response. There are many techniques used to identify a bot, some of which are more effective than others. Simple cookie checks can be done in a completely transparent manner; whereas, Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), while more definitive, is highly intrusive and inconvenient for users. But on its own, bot detection is limited and, without any effective counter measures, provides little value other than alerting the IT organization about the bot problem.

Many vendors offer bot detection as part of their core solutions, ranging from distributed denial-of-service (DDoS) mitigation and Web application firewall (WAF) protections, to network intrusion prevention systems (IPS) and anti-spam. These ingrained bot detection capabilities are useful for their product's primary purposes; but their narrow focus on specific bot types cannot be considered a comprehensive view of the bot environment. A Web-based, bot-centric solution is required to accurately and broadly identify bots.

Bot Management—What Kind of Bot Is It?

Bot management presumes and builds upon the ability to perform broad detection of all types of bots, including bots that are desirable, benign, or otherwise ambiguous. Next, bot management performs analysis and categorization of bots. Essentially, after answering the question, "is it a bot?"—the next logical question is, "what kind of bot is it?" This step is not trivial: there are many types of bots, such as Web crawlers, ticket scalpers, inventory hoarders, price scrapers, spammers, malware bots, DDoS bots, ad-fraud bots, and others.

Every IT organization has a different risk posture for each of these kinds of bots, so a firm understanding of the bot environment is a critical function. This step also includes an ongoing process of assessment and reassessment of the bot environment, as bot owners can and do update their bots' missions and capabilities on a frequent basis.

---

[2] *Important Security Information for Yahoo Users,* Yahoo, Dec. 14, 2016, available here.

[3] Stratecast, SPIE 15-42, *Bots to the Future: The Emerging Market for Bot Management Solutions* (2015); and SPIE 14-32, *The Forgotten Barometer: Bot Detection as an Integral Security Technology* (2014)

Importantly, bot management must include the ability to provide granular, customizable controls. Bots come in a wide range of flavors, and customer tastes vary to an equally diverse degree. Bots that are unwanted in some IT organizations may not be a concern for others. Therefore, any bot management solution should offer a range of responses that allow customers to take action as they best see fit. Some of these options include:

- Allow – Allow the bot to perform its activity unimpeded. This option is sensible for benign or desirable bots such as Web indexers and partners.
- Throttle – Allow the bot to perform its activity, with varying degrees of limitations; useful for bots that are acceptable in their intent but unacceptable or overly aggressive in their methods (e.g., an excessive search engine crawl rate).
- Redirect – Direct the bot to an alternate origin or API; especially useful for directing partners to optimized or specialized resources.
- Block – Block a malicious bot outright. However, this option signals bot owners to modify their strategy, and retry.
- Serve alternate content – Send stale or intentionally false information to unwanted and malicious bots, to provide misinformation or to avoid alerting the bot owner.

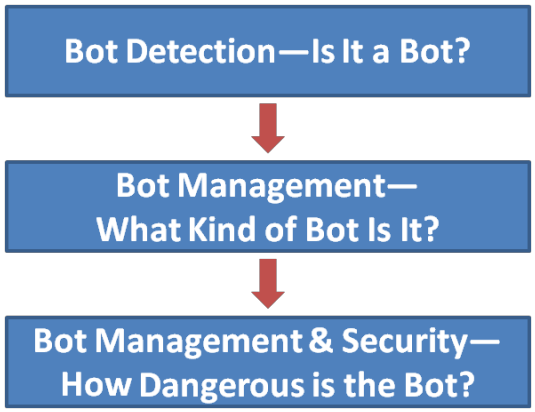
Notably, bot management serves both a security function and a business optimization function. The same bot management controls used to respond to unwanted bots can enable businesses to prioritize the beneficial bots that connect online businesses to customers and partners.

Bot Management and Security—How Dangerous is the Bot?

Threat actors have adjusted their bots to evade known defenses, and to perform more profitable attacks, such as credential stuffing. As a result, there is a pressing need to close the security gaps in bot management solutions. The concept of bot management and security builds on the broad detection, categorization, and control of bots offered with "management"; but also indicates the ability to detect the most sophisticated bots, including bots designed to evade detection, bots that conceal their true purpose, and bots designed to gain illicit access or steal data.

Notably, the focus of each term does not imply the total exclusion of the other. Bot detection implies a "management" or security response (typically a binary "block" or "allow" choice). Bot management requires detection, and provides a notable level of security protection. But the term "bot management and security" implies a high level of security efficacy and completeness. Existing bot management solutions must go beyond known bots to detect the most sophisticated and pernicious bots in use by threat actors today. Figure 1, below, shows the evolution of bot solutions.

Figure 1: Evolution of Bot Solutions



Source: Stratecast

What Bot Management and Security is Not

The "bot problem" and the concomitant need for a bot solution are expressed in different ways for each IT organization. Customers are rarely aware of a bot problem; they are typically concerned with the unwanted end effects of bots, such as fraud, spam, data breaches, or malware. As a result, there has been little consensus on what defines a bot solution.

Amidst the confusion, integrated bot-related components of adjacent network and email security technologies are often conflated with bot management solutions. Examples of integrated anti-bot capabilities that are not included in the definition of bot management and security solutions are:

- Blacklists of bot IP addresses for anti-spam purposes, or for DDoS detection and mitigation
- Bot malware signatures included with antivirus solutions
- Bot command and control detection for network defense purposes, such as through an intrusion prevention system (IPS) or IP reputation-based defenses
- General advanced threat protection solutions

Additionally, there are some basic steps that customers can take to limit their exposure to bot-related risks, ranging from basic User-Agent checks to simple cookie or Javascript challenges. Security event monitoring and analysis can uncover evidence of bot activities, as well. However, these options provide limited efficacy against more advanced bots, or fail to provide real-time protection.

Advanced Bot Threats

Bot technologies have evolved significantly over the years. Early versions of bots were simple scripts, and could be detected with tracking cookies. Tracking cookies confirm that the source is a Web browser and not a script. Yet, the next generation of bots defeated tracking cookies by emulating a browser.

To detect these bots would next require the use of Javascript micro-challenges to ensure the human-driven use of a browser. For example, bot solutions can inject Javascript challenges, such as a simple math problem using random numbers, which a bot could not execute or could only guess at. As should be expected, bot creators have adjusted their strategy to fool Javascript challenges as well.

Headless browsers, user interface and human behavior replicators, and device spoofing are all examples of bot creators adjusting their strategies and techniques.

Headless Browsers

A headless browser refers to a Web browser without a graphical user interface or other user friendly features. A headless browser has full Web browser functionality, but uses a command line interface (CLI) in place of a graphical user interface (GUI); and, therefore, requires minimal computing resources. Headless browsers are programmable, can be network command driven, and can execute Javascript.

These characteristics make the headless browser an ideal tool for bot creators that want to create bots that resemble actual Web browsers rather than scripts. Selenium, PhantomJS, and SlimerJS are some examples of headless browsers that are programmable and are popular with bot creators.

User Interface and Human Behavior Replicators

While headless browsers provide a passable imitation of a Web browser and a human user, human behavior replicator bots are able to go a step further and mimic human behaviors. This capability allows the bots to defeat any behavior-based detection technologies that may be in place.

For example, advanced bots are able to simulate user actions—in particular, replicating activities such as mouse clicks, mouse movement, accessing the sites from different landing pages, filling forms, and navigating the site in random patterns before reaching the target page. Bot capabilities vary tremendously in this category; and these advanced bots are used by the more sophisticated, dedicated adversaries against specific, high value targets.

Device Spoofing

IP address blacklisting and signatures of known bots are considered basic or entry-level detection technologies because of the inherent short-lived nature of these factors. Bots can spoof IP addresses; attackers can leverage new bots with new IP addresses, and can easily change their signature by modifying code or other attributes.

However, device fingerprinting has also become an important technology in the process of detecting and blocking bots. Device identification or classification takes into account a number of device attributes such as Web browser, plugins, operating system, patch levels, hardware specifications, screen size, and resolution. Once a device is determined to be compromised and acting as a bot, the device is blocked.

Device fingerprinting-based reputation is considered more reliable and "sticky," as it does not rely on superficial attributes such as User-Agent or the short-lived factors such as an IP address. But as expected, bot creators are working to spoof device attributes in order to defeat device fingerprinting protections.

Bot Security Risk Spotlight—Credential Stuffing

One particular issue related to the bot security problem is credential stuffing. Credential stuffing is the process of trying a set of stolen credentials against multiple websites, in the hope that the credentials were reused. If so, the bot owner gains access to an account, and can perform a wide range of illicit actions such as data theft, fraud, ransom, and account takeover. **While some bot**

activities border in terms of legality, ethicality, or desirability, credential stuffing is a clear case of a malicious action and intent on the part of the bot and bot owner.

Already, credential stuffing has resulted in fraudulent activities at organizations such as the UK National Lottery, where 26,500 accounts were breached through a credential stuffing attack (out of 9.5 million accounts).[4] Retailer Neiman Marcus reported a similar attack that resulted in 5,200 breached accounts nearly a year earlier.[5] As these attacks become more common, more and more businesses are demanding solutions to credential stuffing attacks.

The Conditions that Enabled the Credential Stuffing Trend

The concept of "brute force" guessing at passwords is not new. However, bots offer three key features that make brute force account breaches more feasible: 1) automation, 2) a large pool of IP addresses, and 3) advanced evasion detection techniques. Additionally, two general conditions have made credential stuffing more popular in recent years.

First, online accounts have steadily become more pervasive in day-to-day life. From work email to social media, and from banking to smoothies, there are Web sites and applications for every aspect of modern life. And users must create and memorize credentials for each of these accounts. Considering that a single person may have dozens of different accounts to keep track of, it is no surprise to discover that users are reusing credentials on multiple sites. Accordingly, once a set of credentials are stolen, savvy hackers know to try those credentials against other websites.

Next, hackers have amassed huge databases of compromised credentials over the years, as evidenced by the many security breaches in the news, where hackers steal millions of account names, passwords, and email addresses at a time. Consequently, **credential stuffing is the result of the confluence of broad global technological conditions combined with evolving hacking techniques.**

Technical Requirements for Credential Stuffing Bots

The process of credential stuffing requires the ability to automatically test a large database of known passwords against a login page. This requires certain capabilities and characteristics on the part of the attacker and their bots.

First, a large botnet is helpful, as a large number of IP addresses is more difficult for defenders to sort through and determine which connections are bots versus legitimate users. When combined with normal traffic patterns, such as attacking during standard business hours, the bots will blend in with the many different users legitimately accessing their accounts. In one known case, a botnet would use any one bot against a target only three times, before using the next bot.

Next, the attacker requires some level of obfuscation, such as changing or spoofing IP addresses, hiding behind proxies, or even using public cloud computing services to enable cycling through IP addresses. Obfuscation techniques may include some behavioral capabilities as well, such as user emulation or waiting out login attempt timers.

[4] *Camelot Statement on National Lottery Website,* Camelot Group, Dec. 3, 2016, available here

[5] *Notice of Data Breach*, Neiman Marcus Group, Jan. 29, 2016, available here

Difficulty of Credential Stuffing Detection

Credential stuffing bots can be difficult to detect, and will require more advanced bot detection technologies. For example, Javascript micro-challenges can help to block bots that emulate Web browsers. Device fingerprinting can help track bots that attempt to evade blacklists by spoofing their IP addresses. And finally, behavior-based detection systems could help to detect bots that emulate both the presence of a Web browser and human user. However, each of these capabilities is increasingly difficult to implement without a dedicated solution.

Advancing from Bot Management to Bot Security

Currently, bot management and bot security solutions can be acquired separately; but in reality, these are two sides of the same coin. Businesses that identify bot-related threats on their Web assets will almost certainly face a wide range of non-security-related bot challenges as well. Businesses with bot challenges may gain a valuable level of protection from bot management solutions, but remain vulnerable to advanced bot problems such as credential stuffing.

As a result, the security industry faces pressure to deliver complete bot lifecycle management and security solutions. The addition of behavioral analysis and machine learning, explained next, can be used to distinguish complete bot management and security solutions from bot management solutions (lacking comprehensive security capabilities).

Behavioral Analysis

Behavior-based detection, or behavioral analysis, is required to detect the most advanced bots that are capable of appearing, even if superficially, as a human user. Behavior-based detection includes the ability to perform inspection and analysis of websites, devices and their communications, and user interactions, in order to identify suspicious behavior or signs of programming.

Behavioral analysis may refer to the ability to monitor for site-specific factors (e.g., traversal rate) that can be used to identify bots. Device-specific behaviors may be useful as well. For example, communications to known command and control (C&C) systems, communications that appear to be covert, and communications that follow an unusual, non-human pattern, may indicate a bot.

Behavioral analysis also includes the ability to monitor user behaviors and interactions, identifying and analyzing activities such as mouse movement, mouse hover, mouse clicks, context clicks, landing page, page dwell time, site navigation, and level of interaction. With mobile devices, data from sensors such as the accelerometer or gyroscope may come into play, in the effort to identify human behavior. The technology is still developing, but existing solutions have been able to identify obvious bot activities. This technology must continue to evolve, as bot owners will certainly work to improve their user behavior emulation capabilities.

Machine Learning

The term "machine learning" has become very popular in the security industry. **Machine learning provides the algorithms and mathematical models needed to compare the many factors that must be taken into account when performing behavioral analysis.** For example, machine learning algorithms may leverage queuing theory models and probability distributions to determine what constitutes a "normal pattern" of arrival times; and can factor in other considerations (e.g., time of day, IP reputation, or region of origination). Similar algorithms and models may be necessary

to detect more complex user behavior simulator bots by determining what defines smooth (versus erratic) mouse movement, what actions indicate human intent, how much time is too little time for an action to be a human action, and other human indicators.

In the 2015 report titled *Bots to the Future: The Emerging Market for Bot Management Solutions,* Frost & Sullivan noted that "the use of advanced security analytics and big data to identify and track bots may even enable the possibility of 'predictive security', on a long enough time scale." This predication is coming true, primarily out of necessity. In the case of credential stuffing, multiple bots, all from different IP addresses, or using spoofed IP addresses, are used in rotation to try a number of credential sets. A Web asset owner will require the ability to detect not just one bot, or even the bot that presents the immediate threat, but at some point will need to determine the likelihood that the next log-in attempt will be human or not.

Stratecast
The Last Word

Businesses all around the world are realizing that bot management is a necessary component in a complete Web property management practice. Bot management provides benefits of optimization and performance improvements, as well as an important level of security.

However, in recent years, bots have emerged as a true security threat. Advanced bots are designed to evade defenses and commit costly criminal activities—with credential stuffing being the most recent and highly visible example. Indeed, while customers often express their "bot problems" in non-security-related terms such as performance degradations, skewed analytics, or end user complaints, bots are frequently, and increasingly, tied to questions of cybersecurity and fraud prevention.

The bot management market continues to develop at a frantic pace, in response to the evolution of bots and bot-related threats. But the market's development must be guided by an important foundational principle: the unbreakable connection between bot management and bot security. A complete Bot Management & Security solution inevitably includes protection against the most advanced and sophisticated bots. As such, vendors must endeavor to deliver holistic solutions; and customers must know to ask for them.

Chris Rodriguez

Senior Industry Analyst – Information & Network Security

Frost & Sullivan

chris.rodriguez@frost.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.