



CONVENIENCE



AUTOMATION



CLICK FRAUD



THINK APP SECURITY FIRST

FROM DDoS TO DIGITAL POINT OF SALE:
BOTS MEAN BUSINESS



EFFICIENCY



DDOS



WE MAKE APPS  SAFER

INTRODUCTION

Have you ever wished for an army of clones to do all your thankless tasks and chores? Well, that fantasy is becoming a reality—at least on the Internet.

And while they may not be actual clones, bots have begun doing lots of digital dirty work.

Managing your relationship with bots—good and bad—has become an inherent part of doing business in a connected world. With more than half of online traffic in 2016 initiated by autonomous programs, it's clear that bots are a driving force of technological change, and they're here to stay.¹

As bot technology, machine learning, and AI continue to evolve, so will the threats they pose. And while some bots are good, many are malicious—and the cybercriminals behind them are targeting your apps. Preparing your organization to deal with the impact of bots on your business is essential to developing a sustainable strategy that will enable you to grow as you adapt to the new bot-enabled world.

¹ <https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference>

51.8%

OF ONLINE TRAFFIC IN 2016 WAS
GENERATED BY BOTS.



THE GOOD NEWS: BOT INNOVATION IMPROVES CUSTOMER EXPERIENCE

What does it mean to be human on the Internet these days? Does it even matter whether you're interacting with an actual person or with an autonomous program? There are many scenarios where bots are there to help the average consumer do what they want to do—in a fraction of the time it would take to do it themselves.

Consider an online shopping scenario. If your customers already know exactly what they need, there is no reason for them to navigate your site to find it when a helpful bot can place the order more efficiently for them. This is already happening, all over the web.

Now think about the growing use of digital assistants, such as iOS-based Siri or an in-home version like Amazon's Alexa. These are also bots, and they're intended to make our lives easier. In exchange for the ease of automatically ordering more granola bars when you run out, people are giving up significant privacy, judging the reward of convenience to be more than worth the cost.² Consumer-facing sites that don't adapt to the new reality of a bot-centered world may see their market share eroded by those that do.

Designing an organizational strategy to manage the growing bot traffic on the Internet is essential, because

bots are getting smarter, enabled by machine learning and neural network technology. Leading tech organizations are leveraging these autonomous programs to build more resilient networks and to monitor and maintain operations, in turn making life easier for their customers. However, bots are also making life easier for attackers, fraudsters, or competitors seeking to exploit weaknesses in software and business processes.

² <https://insights.dice.com/2017/07/14/digital-assistants-greater-usage-adoption/>

³ <https://insights.dice.com/2017/07/14/digital-assistants-greater-usage-adoption/>

⁴ <https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home/>



91%

OF PEOPLE WITH DIGITAL ASSISTANTS SAY IT WILL MAKE THEM MORE LIKELY TO BUY ADDITIONAL CONNECTED DEVICES.³

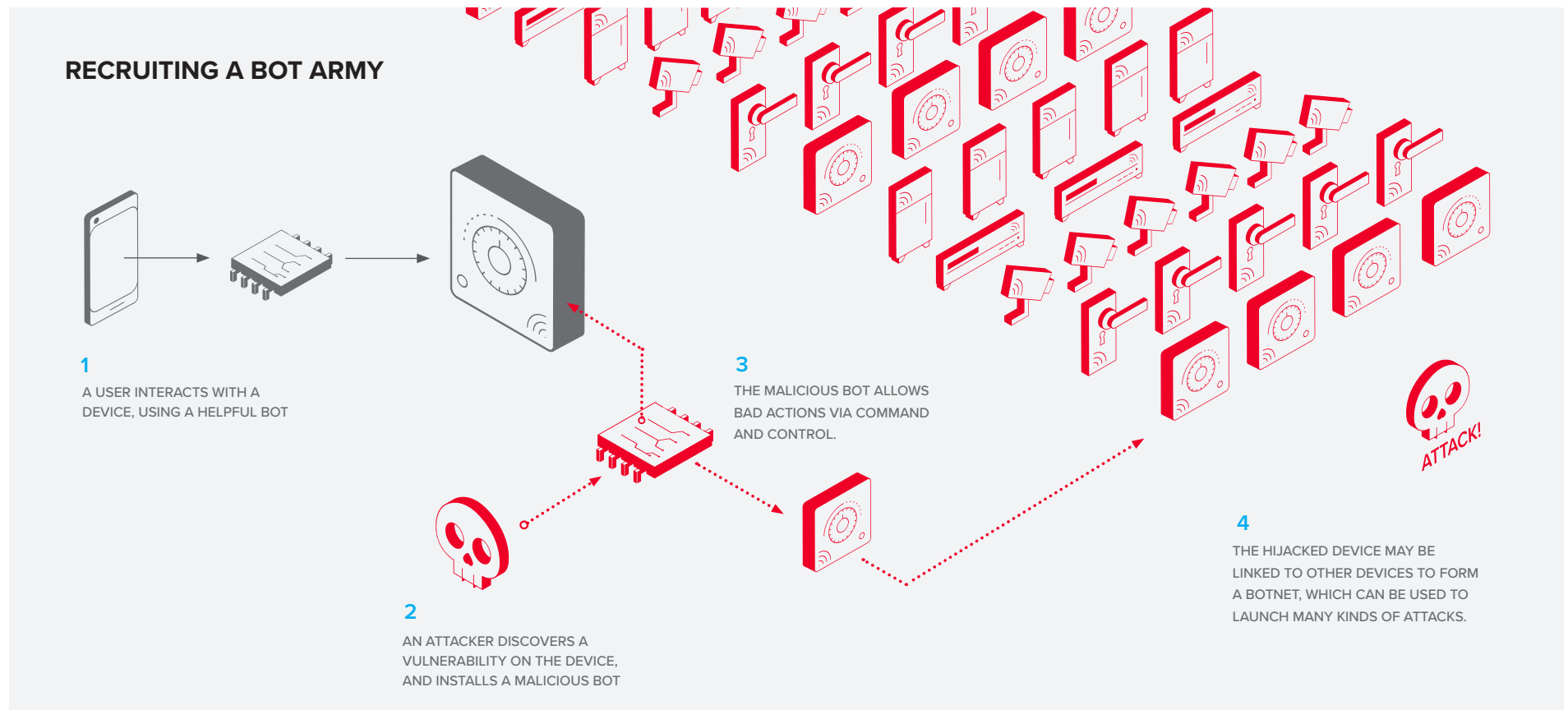
70%

70% OF PEOPLE WITH A DEDICATED HOME ASSISTANT LIKE ALEXA OR GOOGLE HOME HAVE HAD IT FOR LESS THAN A YEAR.⁴

THE BAD NEWS: BOT INNOVATION ENABLES CYBERCRIME

Just like any useful tool, bots can be co-opted by attackers to optimize their criminal activity.

The threats being faced are constantly evolving—driven by a growing list of motivations, including direct consumer fraud, IP theft, long-tail profiteering, political ends, or petty personal grudges—and bots are doing the dirty work.





JUST LIKE ANY USEFUL TOOL,
BOTS CAN BE CO-OPTED BY
ATTACKERS TO OPTIMIZE THEIR
CRIMINAL ACTIVITY.



DDOS ATTACKS

DDoS for hire is both lucrative and highly accessible. Launching an hour-long DDoS attack using a cloud service can cost as little as four dollars,⁵ which is much less than the cost of mitigating it. This kind of DDoS attack can be used by criminals who then demand a ransom to turn it off, or potentially by your competitors looking to interfere with your business and capture a greater share of the market. The rise of IoT botnets like Mirai means that criminals can easily outclass the defenses of most legitimate organizations.⁶



INTELLECTUAL PROPERTY THEFT

Cybercriminals also use bots to duplicate proprietary information and data, which can then be parsed for intellectual property such as videos or PDFs of printed materials, email addresses or usernames that are sometimes hidden in web code. They also target logos or graphics, which could help an attacker design a realistic phishing site, thus degrading your brand and company reputation—as well as hurting your customer relationships.



RESOURCE HOARDING (AND RESALE)

Bots are the perfect tools for ticket scalpers, helping them easily scoop up large numbers of tickets to popular events, which they can then resell at a premium. There are also automated agents like the All-in-One sneaker bot being used by scalpers vying to get their hands on the latest pair of limited-edition Yeezys—and then offering them to sneakerheads at exorbitant prices.⁷



COMPETITIVE INTELLIGENCE

With goods like airline tickets, hotel rooms, and other travel-related items where costs can fluctuate rapidly, bots can glean information from other providers to drive prices down and create a competitive advantage in the marketplace.

The list goes on. From malware distribution to click fraud, bots are being used by cybercriminals to make money, which has left traditional fraud investigators attempting to cope with an entirely new front in their battle against fraudulent transactions.⁸

⁵ <https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/>

⁶ <https://f5.com/labs/articles/threat-intelligence/ddos/ddos-newest-minions-iot-devices-v1-22426>

⁷ <https://www.cnn.com/2017/05/13/adidas-yeezy-collectors-sneakerheads-using-bots.html>

⁸ <https://krebsonsecurity.com/tag/bot-ad-fraud/>

OPTIMIZING BUSINESS INTELLIGENCE IN THE AGE OF BOTS

With an understanding of the opportunities and threats posed by these digital mercenaries, it's essential for any organization to delve deeper and analyze the ratio of bots to humans interacting with their sites and applications. While this may require an investment in tools and services that have the requisite intelligence to identify and distinguish bot and human traffic, it will give you a good idea of how much money you're spending servicing the requests of other machines. Implementing tools such as web application firewalls (WAFs) that offer advanced bot management capabilities can help alleviate costs associated with serving bots.



However, overly aggressive bot deflection could have a negative impact on your customers' ability to interact with your services. If they have to spend a lot of time and effort proving that they are human, they may leave in frustration and try their luck with your competitor.

Also, failing to facilitate "good" bots like digital assistants and search engine indexers for Google, Bing, etc., could result in your services not being available or visible to potential customers.

Keep in mind that successful bot management will result in some level of impact to your site statistics (like page views), and data mining will likely look somewhat different—but be more accurate—since you will be blocking some traffic. However, being aware and prepared for these changes will help give you the confidence that you're still serving your human customers.

HOW BOTS AFFECT YOUR CURRENT SECURITY STRATEGY

With the explosion of autonomous programs on the Internet—both malicious and benign—it may be necessary to rethink existing strategies for keeping applications and data safe.

While traditional IP intelligence and reputation-based filtering can help, these technologies may need to evolve to keep pace with smarter and smarter bots. Looking forward, the business community should consider alternatives to IP reputation—including evaluating longer-term reputation associated with cryptographically verifiable identities—to better facilitate bot detection and management.

Advances in AI technology mean that bots could begin using applications the way humans do, which could

hinder efforts to identify them based on behavioral traits such as session and workflow profiling. Some bots are even human enabled, meaning they can outsource certain types of tasks (like solving CAPTCHA challenges) to humans when those tasks are too difficult for them.

ADVANCES IN AI TECHNOLOGY MEAN THAT BOTS COULD BEGIN USING APPLICATIONS THE WAY HUMANS DO.

Command-and-control systems are evolving, too. Cybercriminals have begun employing steganography techniques to relay commands hidden within images posted to public forums and social networks, a process that makes bot-enabled malware traffic very difficult or even impossible to detect. Consider the novel (but probably already imitated) case of hackers testing a piece of malware and hiding their commands in comments on Britney Spears's Instagram account.⁷


⁷ <http://gizmodo.com/russian-hackers-testing-malware-with-britney-spears-in-1795912325>

SECURITY NOW: **FIGHTING THE BOT BATTLE ON MANY FRONTS**

If blocking all bots is not an option, how can you best distinguish between different kinds of bots—and block the malicious ones from causing damage to your business?

There are no silver bullets that make it easy to comprehensively deal with the bot challenge, but an intelligence-enabled, defense-in-depth strategy can go a long way toward facilitating the good bots—while mitigating the effects of malicious bots on your organization. Here are some steps you can take.

1. Use identity and reputation to help classify and prioritize bot vs. human traffic.
2. Bot “acceptable use” policies could make it easier to interact with and service the benign bots, as well as manage their impact on your services.
3. Review and bolster business process to more efficiently deal with fraud-related problems, making your organization more secure, and, hopefully, encouraging fraudsters to move on to easier targets.
4. Employ actionable threat intelligence to determine the likelihood of being attacked, and prioritize your response.
5. Deploy a full-featured, flexible WAF to reduce and block unwanted traffic with capabilities such as proactive bot defense, headless browser detection, form and field-level encryption, layer 7 DoS mitigation, input sanitization, and behavioral analysis.
6. Use traffic management tools that employ machine learning such as your WAF to quickly build and implement mitigations that help you address new and evolving threats.



EMPLOY ACTIONABLE THREAT
INTELLIGENCE TO DETERMINE
THE LIKELIHOOD OF BEING
ATTACKED, AND PRIORITIZE
YOUR RESPONSE.

It's clear that bots are changing life as we know it online. And while it's tempting to concentrate on the multitude of malicious bots roaming the Internet, organizations should also be mindful of the opportunities these autonomous programs present. By developing a comprehensive, flexible strategy to address the impact of bots on your business, you can protect your applications and your data while preparing your organization for sustained growth.

For more information about application protection, visit f5.com/security.

THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business—but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.

Learn more about application security at the [AppProtectLibrary](#).



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.

Any other products, services, or company names referenced herein may be trademarks of the irrespctive owners with no endorsement or affiliation, expressed or implied, claimed by F5. EBOOK-SEC-16993358 1017