radware

How Bots Are Taking Advantage of the COVID-19 Pandemic

As the world struggles to get ahead of the coronavirus outbreak, cybercriminals have quickly adapted to take advantage of the situation, using armies of bots. Sophisticated bots accounted for 58% of bot traffic in February 2020;[1] they are a force multiplier to malicious actors who are looking to steal data, disrupt network and application services and profit from the fear, uncertainty and doubt that occur during unsettled times. They deceive conventional security solutions by disguising their identity and acting like humans. For example, they can create fake accounts on social media sites, making it easy to spread disinformation.

TOP THREATS

- FAKE NEWS
- SPREAD PHISHING AND MALWARE
- SCRAPING MEDICAL RESEARCH
- DIGITAL FRAUD
- CLEARING OUT RESPIRATORS AND SANITIZERS
- INVENTORY HOLDUPS
- SPAM
- DENIAL OF SERVICE (DoS)

During this crisis, Radware has witnessed bots being used in spreading fake news, phishing, malware, spam, digital fraud and even scraping and hoarding personal sanitation equipment. The World Health Organization (WHO) has warned of an “infodemic,” an overabundance of information — some accurate and some not — making it difficult for people to differentiate between legitimate news and misleading information.

PRIMARY TARGETS

- TRANSPORTATION
- SOCIAL MEDIA
- ADVERTISING
- E-COMMERCE
- MASS MEDIA
- HOSPITALITY

[1] https://www.radware.com/products/bot-manager/#big-bad-bot-research

EXAMPLE I – Bots Are Searching for Sanitizers and Face Masks

Here is an example of what we witnessed from a leading European e-commerce customer site that sells hand sanitizers and face masks. As coronavirus fear increased, bots ramped up their search for face masks and sanitizers as shown in Figures 1 and 2.

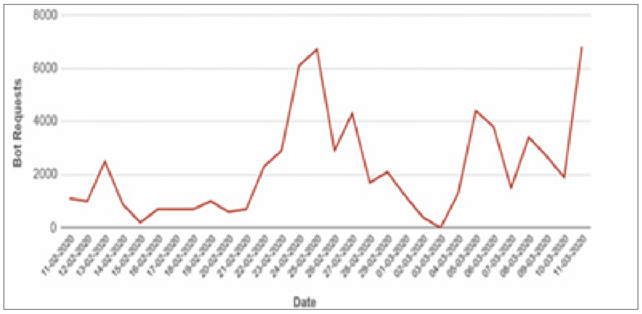

FIGURE 1: SEARCH FOR HAND SANITIZERS BY BAD BOTS.

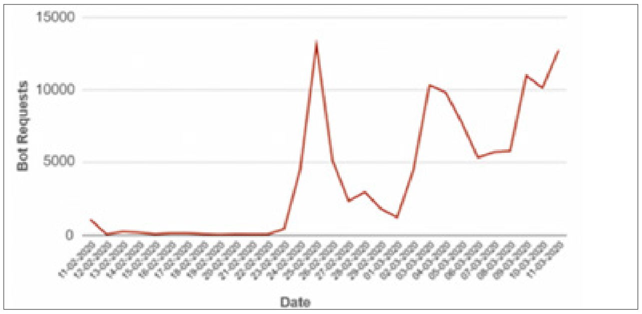

FIGURE 2: SEARCH FOR FACE MASKS BY BAD BOTS

These automated attacks could be aimed at performing denial-of-inventory attacks, hoarding these essential products to sell on the black market or even scraping product details to list similar products on malware-ridden sites to scam people.

EXAMPLE II – Bots Scraping Content and Using Fraudulent Links

Many ongoing phishing campaigns are aimed at luring people with the promise of essential or breaking news on COVID-19, enticing them to click on malicious links or open infected attachments. This is another customer case study of a renowned media site that has a section dedicated to coronavirus-related news. Figure 3 highlights how the presence of bots gradually increased on the coronavirus section of this website in February and March.

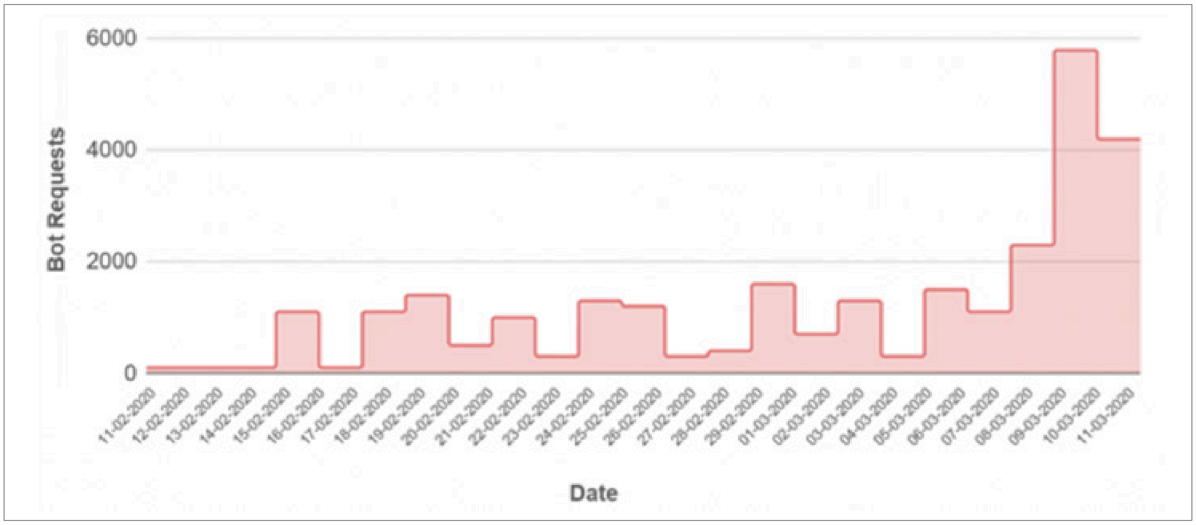

FIGURE 3: SCRAPING ATTACKS ON THE CORONAVIRUS SECTION OF A RENOWNED MEDIA SITE

Bots on this website are attempting scraping. Figure 4 highlights that as soon as an article on the coronavirus is published (blue dots), bots try to scrape it (red dots). These bots then post the scraped articles on malware-ridden websites to lure visitors in order to scam them.

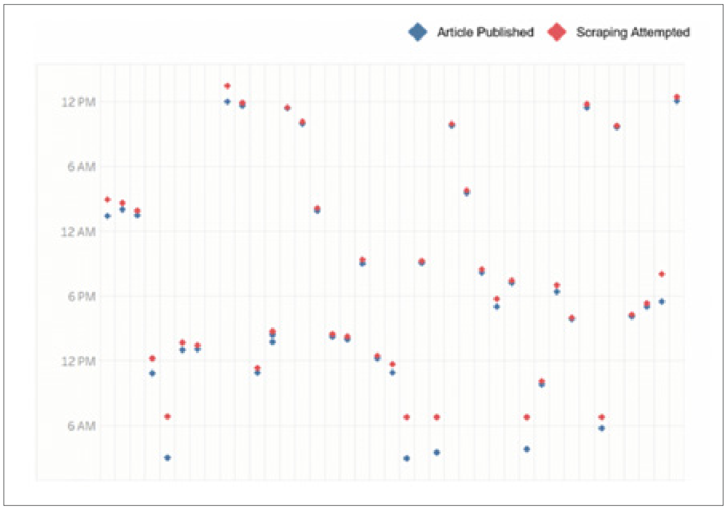

FIGURE 4: SCRAPING ATTACK ANALYSIS

KEY CONSIDERATIONS IN CHOOSING A BOT MANAGEMENT SOLUTION

1: **Intent identification:** Use behavioral analysis to determine whether the bot is legitimate or malicious.

2: **Flexible integration options:** Each business unit has a preference. Choose a solution that is a business enabler, not a showstopper.

3: **Different mitigation options:** CAPTCHAs, feeding fake data, throttle and redirects are all great ways to deceive bots.

4: **Visibility and customization:** Opt for a solution that offers granular analytics and customization.

Radware's Bot Manager is the industry's most comprehensive protection for web applications, mobile applications and application programming interfaces (APIs) from emerging generations of automated threats (bots) targeting applications and systems. This solution allows precise bot management across all channels, combining behavioral modeling for granular intent analysis, collective bot intelligence and device fingerprinting. Radware's Bot Manager protects from all forms of account takeover, denial of inventory, distributed denial of service (DDoS), card fraud, web scraping and other OWASP automated threats and helps organizations reduce expenses and increase revenue.

Feeling concerned? Radware is here to help!
Sign up now for a free assessment of bot traffic to your application.