THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET

BOT ATTACKS | 2019

UNIVERSITY OF BALTIMORE

CHEQ

INTRODUCTION TO THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET SERIES

The internet has heralded an economic revolution. The internet economy of the G20 countries alone is worth more than $4.2 trillion representing 5.3% of their total GDP. However, as Tim Berners Lee, the father of the internet has put it: "While the web has created opportunity, given marginalized groups a voice, and made our daily lives easier, **it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit.**"

In a series of reports, we reveal the monetary cost caused by bad actors on the internet. CHEQ has commissioned economist, Professor Roberto Cavazos at the University of Baltimore, to undertake the first-ever in-depth economic analysis of the full scale of internet harm. For the first time, using economic analysis, statistical & data analysis, we measure the global economic price paid by businesses and society due to problems including ad fraud, online bullying, and fake news.

OPPORTUNISTIC BOTS AND DDOS ATTACKS

In this study, we calculate the economic costs of damage done by global bot attacks. Our analysis centers on day-to-day bot attacks affecting online businesses, in which opportunistic bots looking for small-scale weaknesses. This affects classified sites, ecommerce, and ticketing portals in particular.
This study excludes ad fraud – caused by bots – covered in detail in a previous report in this series.

Nor does this report look at highly coordinated cyber-attacks targeted at specific entities – often government-sponsored. These latter attacks with menacing names have individually created eye watering economic costs – such as Notpetya (estimated global economic cost of $10 billion in total damages, according to a White House assessment), or the WannaCry attack ($4 billion in damages).
This analysis also excludes data breaches, ransomware, piracy, targeted government attacks, identity theft, malware and phishing.

INTRODUCTION TO THE BOT ECONOMY

Bots account for approximately 45% of all web traffic[1]. Other sources note that bots account for up to 54% of web traffic. Many of these bots, as is well known, automate legitimate functions on the web such as web crawling, updating sports scores and weather, and a host of other things which make the web easier to use. Bots are also beneficial – for instance by 2023 bots will handle e-commerce transactions of over $100 billion.[2] However, approximately 40% of bots are malicious.

These bots automate tasks that are far from benign – including account hijacking, web scraping, stealing financial data and a host of other illicit activities.[3]
To pull off a DDoS attack, hackers enslave computers and create a network of bots (or botnet) working simultaneously to send large amounts of network traffic to a server.
In numerous black markets, cybercriminals advertise their services for attacking an unprotected website ranges from $50 to $100, while an attack on a protected site can go for $400 or more.

[1] What'cha Goin to do when the bad bots come for you? Matt Toomey, Aberdeen Research, April 11, 2017.
[2] Don Alaimo, Retail Dive, July 5, 2018.
[4] Ibid.

THE $10 BILLION BOT PROBLEM

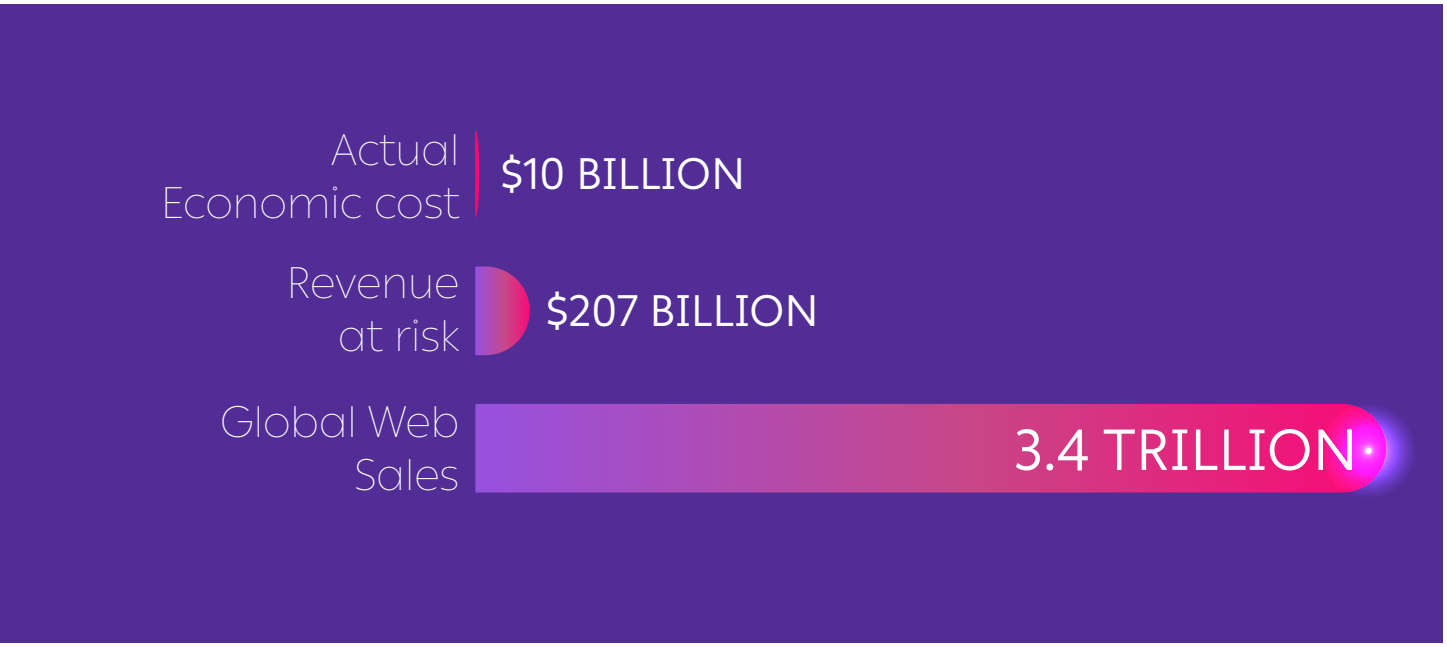
"Opportunistic" bots are engaged in continuous automated abuse and are looking for any small-scale weaknesses to exploit in attacks. This can include but is not limited to:

- Classifieds sites, with competitors stealing listings by scraping content affecting the traffic and revenues
- eCommerce attacks, where bots try to steal price information in real-time and use it as a competitive intelligence
- Bots racking up fake transactions
- Bots faking reviews, which damage products and brands
- Hurting ticketing sites through denial of inventory, spinning, and scalping, scraping seat map inventory, fan account takeover, and fraud.

CALCULATING THE COSTS

Our estimation mode for calculating the direct cost of such opportunistic bots is straightforward and intuitive. Total global web sales will amount to a staggering $3.4 trillion in 2019. Of this, it is accepted that around (6%), or a pot of $207.18 billion of global revenue, is at risk from bots in 2019. However, there is little probability of all this business revenue at risk being lost. It is reasonable to assume that anywhere from 1% to 5% of the revenue at risk will be lost in a given year.

Based on the current level of attacks our research and industry insider estimates, we consider a loss of 5% of this revenue at risk as highly realistic, creating losses of $10 Billion, through direct impact on global business revenue.
The multiplicity of businesses, variability in security and bot mitigation losses will vary. The business sector, size, sophistication, location and a host of other factors may, in fact, generate higher rates of revenue at risk and losses.



COMPANIES HIT BY ATTACKS

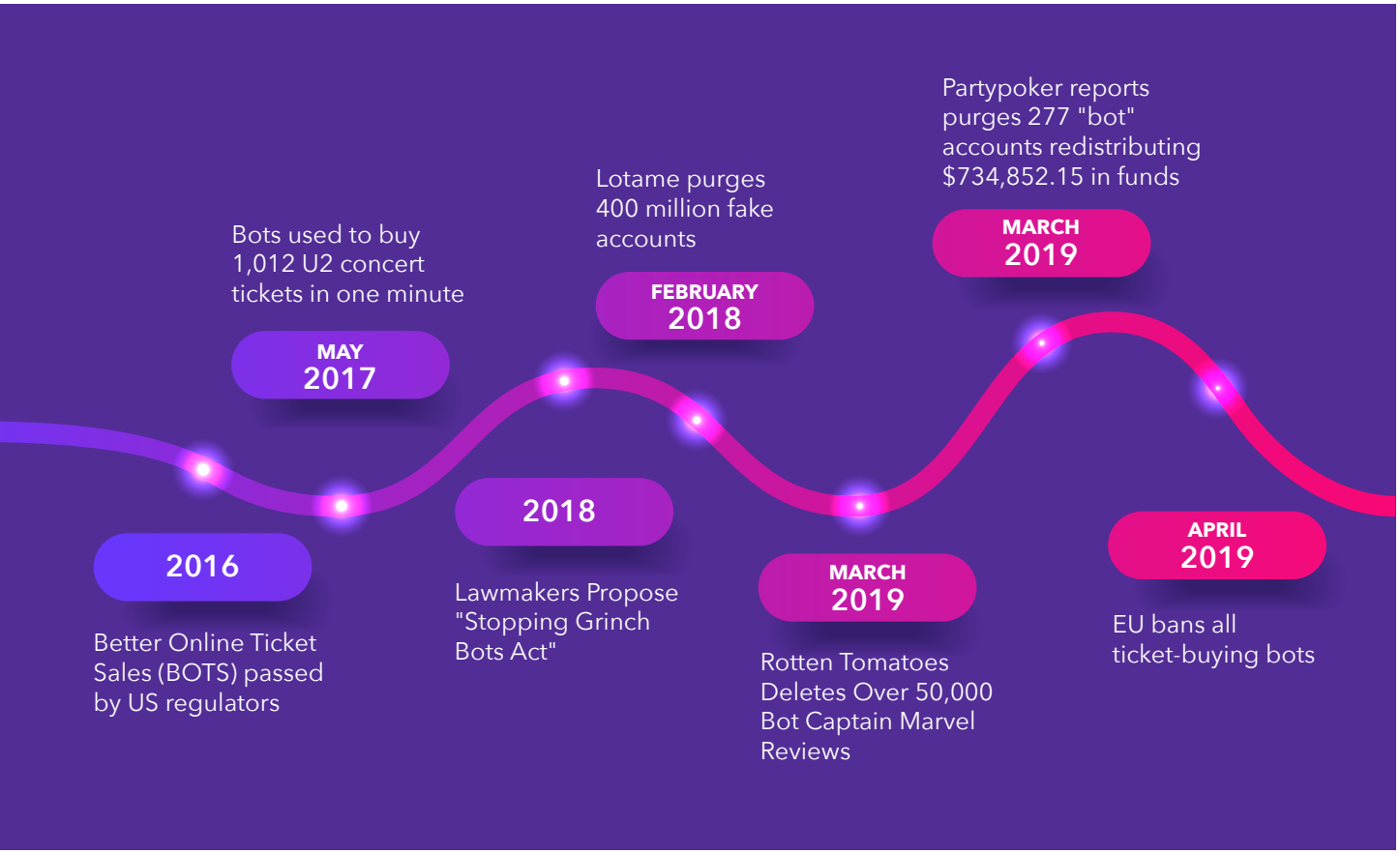
Companies – hit by such attacks – have themselves attempted to calculate their individual direct economic costs. In one lawsuit Ticketmaster acknowledged that the cost of bots "restricting other customers" use of the site through their abusive conduct, using number and letter generators to gain access to events is extremely difficult to ascertain. "The ticketing giant argued that accessing more than 1,000 pages of the site and making more than 800 reserve requests in a 24-hour period, made potentially bad actors liable for damages in the amount of twenty-five cents ($0.25) for each page request or reserve request. In total, they claimed a loss of over $5000 in a one-year period. This sits alongside their costs of "several damage assessments, designing of new security features, and diverted resources to combat defendants' unauthorized use of Ticketmaster's website and mobile platform." In another case, in October of 2018 the venerable publication "The New Oxford Review" (NOR), a magazine of Roman Catholic cultural and theological commentary, described their attack by bots. The publisher discovered in total transactions totaling $97,000. The business faced a $25,000 deficit from the attack at the same time as they hemorrhaged money waiting for their web host's schedule to clear. They explained: "$25,000 is a precious sum to us. We had been planning to use it to help fund a direct-mail and print-advertising campaign for new subscribers in the spring. But without a steady stream of new subscribers to replenish those who quit on a monthly basis, we've watched our subscriber base shrink to a critical level."

In another example, at a polar end of the internet, between Dec. 1, 2018, and March 31, 2019, gambling site, Partypoker reported confirming and closing 277 "bot" accounts while redistributing $734,852.15 in funds to affected players – stressing both the financial and administrative costs of fighting back.

REGULATORS STRIKE BACK

Regulators have sought to protect the economy and distortion of buying practices from bots. In May 2017, the New York attorney general's office took action after six companies used bots to resell hundreds of thousands of concert tickets after hiking up the prices. This followed a situation one broker using bots bought 1,012 tickets to a U2 concert at Madison Square Garden in a minute – nearly 17 tickets a second. In the cases of fashion launches, bots have been responsible for 473 million requests to purchase sneakers in a single day.

In 2016, Congress passed the Better Online Ticket Sales Act (BOTS Act) but the legislation only outlawed bots buying tickets. Senators called – around the holiday season – for a "Stopping Grinch Bots Act" making it illegal to use bots to shop online and also outlaw all reselling of items purchased by bots.



INDIRECT COSTS: LONG TERM

Direct costs refer to the direct losses and damage as a result of the situation. Indirect costs are the losses and opportunity costs imposed on society by the fact that a crime or attack is carried out. The US government has suggested that to best understand the cost of crime, estimates should consider both the financial and non-monetary effects of harm — such as the impact on quality of life, increasing fear, or indirect effects, such as change in behavior. Some researchers have concluded that crime's most costly factors stem from these less tangible effects[5].

When it comes to bot attacks, indirect costs include the loss of reputation or brand value. A survey of 300 security professionals confirms that indirect costs created a larger shock than more immediate financial loss. Discussing the most damaging effects of DDoS attacks, 78 per cent of IT professionals cited the loss of customer trust and confidence as the biggest fear, followed by intellectual property theft and malware infection.

FINAL THOUGHTS

Even a short loss of systems availability, investors doubting a company's resilience can precipitate a fall in the stock price. Bots can also damage your SEO and website reputation – through scrapers stealing content and illegally distributing it to other websites. No less damaging is the time spent mitigating such attacks. Betfred, the 4th largest bookmaker in the UK with over 10,000 employees, has said that their volume of bad bots was as high as 87% of all web traffic on some domains. Shaun Clark, Head of Infrastructure, Betfred says:
"It was a real resource drain. Even if attacks weren't successful, we had to go through our full security incident reporting compliance process. This process could involve up to 35 team members to complete. You can imagine the amount of time that took up"
It has even been suggested that bots are creating long term economic damage to competition through forming "cartels".

Maurice E. Stucke, Professor of Law at the University of Tennessee, says:
"By increasing the speed at which price changes are communicated, detecting any cheating or deviations, and punishing those deviations, algorithms can foster new forms of collusion...that are beyond the law's reach. Indirect costs also involve the complex cleaning up of the problem and the lack of trust and transparency that sectors can all too often suffer from. [6]***"***

The economic costs of bots go beyond the direct losses we have seen. The costs of business leadership headspace and energy on the issue, diverting resources from other uses such as expansion, innovation or investment in the business to fight the bots is a real long term and at present difficult to calculate cost which in our view is worthy of closer examination.

[5] https://www.gao.gov/assets/700/691895.pdf

[6] Harvard Business Review, How Pricing Bots Could Form Cartels and Make Things More Expensive