imperva

DATASHEET

The Business Impact from Bots Across Departments

Attack Type: **Scraping**

STAKEHOLDER			
C-SUITE	**MARKETING/PR**	**IT OPS / NOC**	**FRAUD, RISK, LEGAL**
• Customer and revenue loss from malicious competitor tactics, like out-pricing • Loss of business which depends on unique content • Loss of investments in proprietary and unique user generated content	• Bot traffic is skewing decision making metrics • Decrease in conversion rates • Duplicate content damages SEO rankings • Automated traffic has a negative effect on customer experience (e.g. slowdowns and brownouts)	• Impact to performance, availability, and reliability • Increased storage, compute, and network OpEx	• Scraping of sensitive information and risk of further fraudulent activities • Noncompliance with data privacy regulations

Attack Type: **Account Takeover**

STAKEHOLDER			
C-SUITE	**MARKETING/PR**	**IT OPS / NOC**	**FRAUD, RISK, LEGAL**
• High cost dealing with account takeover • Reputation damage affecting customer churn and the bottom line • Revenue loss • Increased support costs	• Direct impact on brand loyalty. Customers need to spend their time unlocking accounts, dealing with fraudulent charges, updating CC info because their data has been stolen etc. This leads to customer frustration, damaging the brand, increasing churn • Reputation damage that requires time and effort to fix • Negative PR	• Impact to performance, availability, and reliability • Increased storage, compute, and network OpEx • Effort responding to bot problem removes teams from other tasks that could be revenue generating • Additional operational overheads to handle bot problems	• Theft of senstive personal information, credit card data, loytalty points etc. • Risk of noncompliance with data privacy regulations • Some countries require reporting of account takeover attacks, resulting in extra legal fees • Accounts may be used for money laundering

Copyright © 2021 Imperva. All rights reserved

Attack Type: **Fake Account Creation**

STAKEHOLDER			
C-SUITE	**MARKETING/PR**	**IT OPS / NOC**	**FRAUD, RISK, LEGAL**
• Revenue loss to fraudulent activities • Brand and reputational damage • Diversion of key resources from revenue generation to dealing with bots creating fake accounts	• Bot traffic is skewing decision making metrics • Increased marketing costs everytime a new account is created • Spam in sites causing a reduced user experience • Reputation damage	• Impact to performance, availability, and reliability • Increased storage, computational, and network OpEx • Effort responding to bot problem removes teams from other more productive and revenue generating tasks • Additional operational overheads to handle bot problems	• Fraudulent purchases can occur using fake accounts, creating additional work for the fraud team • Accounts may be used for money laundering

Copyright © 2021 Imperva. All rights reserved

Attack Type: **Carding**

STAKEHOLDER			
C-SUITE	**MARKETING/PR**	**IT OPS / NOC**	**FRAUD, RISK, LEGAL**
• Reputation damage affecting customer churn and the bottom line • Increased credit card processing fees/ chargeback fees/ tarnished reputation with credit card processors • Increased customer service costs of processing fraudulent chargebacks	• Reputation damage that requires time and effort to fix • May negatively impact conversion rates due to trust issues with credit card companies that requiring added verification	• Impact to performance, availability, and reliability • Increased storage, computational, and network OpEx • Effort responding to bot problem removes teams from other more productive and revenue generating tasks • Additional operational overheads to handle bot problems	• Fraudulent purchases needing investigation • Damages the fraud score of the business • Risk of noncompliance with online transcation regulations

Copyright © 2021 Imperva. All rights reserved

Attack Type: **Inventory Hoarding/Scalping**

STAKEHOLDER			
C-SUITE	**MARKETING/PR**	**IT OPS / NOC**	**FRAUD, RISK, LEGAL**
• Reputation damage affecting customer churn and the bottom line • Revenue loss as customers move on to other retailer selling the same goods • Revenue loss due to lower average basket value (ABV) – bots target a single product while consumers tend to purchase additional items	• Brand damage: consumers identify a brand as one whose product launches are plagued with bots and "are not worth their time" • Brand loyalty: customers go to competitors selling the same goods • Automated traffic has a negative effect on customer experience (e.g. slowdowns and brownouts) • Lower conversion rates	• Impact to performance, availability, and reliability • Increased storage, computational, and network OpEx	• Precious time and resources spent on verifying the validity of purchases to combat fraud

Copyright © 2021 Imperva. All rights reserved