TABLE OF CONTENTS

Introduction ................................................................. 03
Research Overview ....................................................... 04
Top 100 Chinese Brands .............................................. 05
Takeaways ................................................................. 06
About ..................................................................... 07
INTRODUCTION

As part of our ongoing research into DMARC adoption, we dove head-first into the top 100 most valuable Chinese brands to understand exactly how they use email authentication, including Domain-based Message Authentication, Reporting and Conformance (DMARC), to provide customers and employees a minimum level of protection from phishing attacks. DMARC is a sender-published policy for messages that fail authentication.

The total Chinese retail market was nearly $5 trillion in 2016, and by 2020, China will account for about 60% of global e-commerce. China has more than 500 million middle-class consumers who have catapulted the 24-hour shopping holiday, Singles Day (11.11), into the highest-grossing online shopping event on Earth ($25.3 billion in 2017).

A 2017 study from the Anti-Phishing Working Group reported an average of 443 brands per month were targeted for phishing attacks in the first half of 2017, up from 413 per month during the same period in the previous year. These attacks are a threat to brand trust, as 91% of all cyber attacks begin with a phishing email.

How do phishing attacks that spoof institutions impact consumer trust in their brand? A study from Cloudmark revealed that 42% of consumers are less likely to do business with a company following receipt of a suspicious message purporting to be from that brand.

According to a survey recently published by Black Hat Asia¹, Asian security professionals use much of their security budgets on targeted attacks (31%) and phishing and social engineering threats (21%). These same experts (38%) pinpoint end-users as the weakest link in their defense.

RESEARCH OVERVIEW

On February 13, 2018, 250ok performed an analysis of 307 of the top-level domains owned by the top 100 most valuable Chinese brands, looking exclusively for published DMARC records.

It is worth noting a meaningful number of companies likely use a subdomain for some of their messaging (e.g., “250ok.com” is a root domain; “pages.250ok.com” is a subdomain). However, leaving the root domain unauthenticated is an open invitation for spoofing, phishing, and mail forgery.

A published record at the root domain will protect the entirety of the domain, including any potential subdomain as they will automatically inherit the DMARC records from the root, if there is not already a separately configured policy. It is also possible to publish different policies for individual subdomains at either the subdomain level or at the root domain with a defined “sp=” policy.
TOP 100 CHINESE BRANDS

DMARC Adoption

FIGURE 1
DMARC Adoption Among Top 100 Chinese Brands

Legend
n=307 domains

- Domains w/ No DMARC
- None Policy - good
- Quarantine Policy - better
- Reject Policy - best
TAKEAWAYS

The review of DMARC adoption among top Chinese brands reveals they are significantly less likely to deploy DMARC records for their domains (4.6%) than other industry verticals like top US and EU e-retailers (11.3%), or top-performing SaaS 1000 businesses (35%).

As predominantly online Chinese businesses like Alibaba and JD.com work to expand globally, their email authentication practices, which include the use of DMARC, play a significant role in their ability to deliver both transactional (e.g., password resets, shipping receipts, customer service correspondence) and promotional (e.g., sales offers, shopping cart abandonment reminders) email messages to consumers outside China.

With the number of computer systems in China appearing to host botnets, ranking second in the world for spreading infections and first for spam volume, according to the Composite Blocking List, having proper authentication and DMARC policies in place will help prevent misuse of domains owned by top brands.

With the number of computer systems in China appearing to host botnets, ranking second in the world for spreading infections and first for spam volume, having proper authentication and DMARC policies in place will help prevent misuse of domains owned by top brands.

² Source: https://www.abuseat.org/statistics.html, as of February 2018
ABOUT

Matthew Vernhout (CIPP/C)
Director of Privacy, 250ok

Matthew Vernhout is the Director of Privacy at 250ok and is a Certified International Privacy Professional (Canada) with nearly two decades of experience in email marketing. He actively shares his expertise on industry trends, serving as director at large of the Coalition Against Unsolicited Commercial Email (CAUCE), chair of The Email Experience Council’s (EEC) Advocacy Subcommittee, and senior administrator of the Email Marketing Gurus group. He is a trusted industry thought-leader, speaking frequently at email marketing and technology conferences around the globe, and maintaining his celebrated blog, EmailKarma.net. Matthew has contributed to several benchmark publications during his career including *DMARC Adoptions Among e-Retailers*, *The EEC's Global Email Marketing Compliance Guide*, *The Impact of CASL on Email Marketing*, and more.

250ok focuses on advanced email analytics, insight and deliverability technology to power a large and growing number of enterprise email programs ranging from clients like Pinterest, eHarmony, and Furniture Row who depend on 250ok to cut through big data noise and provide actionable, real-time analytics to maximize email performance.

For more information, visit 250ok.com.