iZOOlogic

iZOOlogic Limited
Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

Case Study: High Volume Phishing Response – Africa’s Largest Bank

Introduction

This case study details the high volume of phishing targeting Africa's largest bank and how iZOOlogic has worked with the bank to combat the high speed threats.

Background

Phishing remains the mainstay of cybercrime and attacks against banks. Phishing remains relevant due to its emerging sophistication and social engineering.

Phishing results in direct financial losses, often in real time, as well as reputational damage. Phishing can now leverage other vectors such as malware, and through social media can take the form of a multi-faceted and blended attack.

iZOOlogic's long standing client is the largest bank in Africa - a transnational bank with operations in more than a dozen countries. The bank suffers many nefarious type of fraud and cybercrime, and is the target of thousands of phishing sites.

The bank suffers not only from a high volume of phishing sites but also from varied phishing techniques.

Types of Phishing targeting the bank

1. Traditional or Classic Phishing uses email, or other messaging to send a URL within the message, directing victims to the phishing site. The message looks like it is from the genuine source, often the "from" address is a spoof of the bank's domain, and messaging presents the user with a call to action. The phishing site is a direct copy of the bank's login page, that is being hosted on a hacked/compromised website, often a WordPress or Joomla site.

Over time, these sites have become more sophisticated, appearing genuine, with real time functions allowing the criminal to attempt to direct funds from unsuspecting customers.

2. Domain Phishing, or Domain Spoofing - this type of phishing is where attackers register a domain that's very similar to the bank to take advantage of users. These domains can also be used to send unsolicited emails, also designed to acquire personal and financial information from customers.

3. Vishing, or Voice Phishing - leverages unsolicited phone calls, where the attackers pretend to be a representative of the bank and attempt to acquire sensitive and personal information.

4. SMiShing - this type of phishing deals with SMS/text based messages sent with the intent to acquire information, or distribute the phishing URL.

5. Search Engine Phishing - is a type of phishing that optimizes a fake website by maximizing the searchable terms for crawlers, forcing parties to visit it instead of legitimate ones.

6. Spear Phishing - this is a more complex and dangerous type of phishing, as this is a form that is specifically directed towards a certain party (for example senior executive of the bank), with research done on said party, usually through social engineering.

7. Whaling - similar to Spear Phishing, this is directed towards a specific party, namely the bank's employees or Executives. Often the email is sent to the bank's corporate Users and leverages the bank's domain in the spoofed header.

8. Injected Phishing - this is a type of attack that inserts code into a vulnerable site, designed to return input values on that specific webpage.

9. URL Phishing — this is a type of phishing that takes advantage of URLs and inserts these to elements used in day-to-day browsing, such as buttons, pop-ups, images and the like. Attacks also leverage abbreviated URLs, or TinyURLs, where links or URLs of specific pages are shortened to reflect that of the phishing page.

In working closely with Africa's largest bank over a number of years we have been able to observe the patterns and the emergence of trends in this threatscape. This intelligence has allowed us to employ a variety of techniques and solutions to combat this fraud.

Challenges

Some of the issues and challenges we encountered during the influx of phishing attacks targeting the bank are as follows:

- High volumes of phishing sites that are hosted simultaneously or over a short time frame, such as **Fast Flux** and **Rock Phishing** types of attacks.
- Phishing sites that block the bank's and iZOOlogic's IP from viewing the content.
- Phishing sites that are hosted in countries with a problematic jurisdiction.
- Phishing sites hosted on "bullet-proof" hosts, or webhosts that are suspected to be in collaboration with the criminals, or are deliberately uncooperative.
- Phishing sites with multiple and changing redirects.
- Phishing sites that deliberately mask most detection technologies.
- Phishing sites distributed via SMS/text messaging from within the country.
- Attacks that may leverage some personal information that is likely to have originated from an inside source.

How has iZOOlogic combatted these problems?

- iZOOlogic has deployed different types of technologies to identify phishing sites as they go live—hence providing a pro-active detection.
- iZOOlogic has worked with the bank to employ a series of services to identify real time phishing and provide **phishing intelligence** enabling the bank to block/suspend accounts prior to account take over.
- iZOOlogic GSOC has leveraged relationships with many third parties around the world, such as webhost, registrars, CERT teams, ISPs, law enforcement, enabling the fastest time for the incident response.
- As a long term partner to the bank, the teams at iZOOlogic have gained a unique perspective into the types of phishing activity targeting the bank, hence are well placed for future attacks.
- An Incident Response can scale up quickly during times of heightened attack, allowing us to respond to hundreds of simultaneous attacks.

Conclusion

The effects of phishing on the bank are significant, causing direct financial losses, brand reputational damage, as well as causing major disruptions in the operations of a business.

Whilst iZOOlogic has been providing services to the bank for more than 7 years— we have seen many emerging techniques and types of attacks, that has allowed us to develop and tailor our platform and response to provide a bespoke solution to the bank.

iZOOlogic

iZOOlogic protects the world's leading organisations, across Banking, Finance, and Government.

The iZOOlogic platform provides real time Threat Intelligence and a seamless Global Security Response.

iZOOlogic helps organisation's manage Digital and Reputational Risks, and to reduce fraud and revenue losses.

To learn more, visit www.izoologic.com or ***Contact Us***

HQ / EMEA OFFICE

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com

US OFFICE

Level 1, 444 Castro Street
Mountain View, California,
USA
+1 650 396 3352
sales@izoologic.com
www.izoologic.com

APAC OFFICE

Suite 18, Level 27, Rialto Tower
Collins Street, Melbourne, 3000,
AUSTRALIA
+61 3 9088 0338
sales@izoologic.com
www.izoologic.com

iZOOlabs / GSOC

Level 30, The Leadenhall Building,
122 Leadenhall Street, EC3V 4AB
City of London, UNITED KINGDOM
+44 20 3734 2726
info@izoologic.com
www.izoologic.com