2013 A YEAR IN REVIEW

January 2014

PHISHING 2013: A LOOK BACK

2013 has proven to be yet another record year in the number of phishing attacks launched globally. With nearly 450,000 attacks and record estimated losses of over USD $5.9 billion (using APWG's average uptime of 44:39 hours), phishing remains an ominous threat to consumers and businesses around the world. Compared to 2012, we only saw a slight increase – about 1% - in the total number of attacks, but did see an all-time peak in October with over 62,000 unique attacks identified in a single month.

Noticeable attack methods this year included the Bouncer attack that filtered incoming victims based on a unique URL parameter values. Not having the “right” parameter value would send the unwitting users to a standard 404-page. The laser-precision attack theme repeated several times during the year with variations on the filtering element including basic...
geo-IP filtering. The motives behind such kits are mainly commercial: selling credentials has become a commodity in the underground. A commoditized marketplace drives vendors to provide more value for money, and high-quality, precision lists provide just that.

Abundant tools and offerings flourished in the underground. For example, email bombers and mass mailers are readily available to make the lives of phishers and would-be-phishers easier. And if you are not sure how to go about mass mailing/spamming, a tutorial is not far away.

A free tutorial on mass-mailing techniques being offered freely in the underground.

A more sinister post we came across offered a tutorial—and a free tool—on how to spear-phish individuals working at specific organizations.

Jigsaw: a script-based tool to enumerate employee information for spear-phishing attacks.

Comparisons Year over Year

Last year, we witnessed a 160% increase over 2011 signifying a record year in phishing volumes. While we did not expect the 2012 record to be broken, 2013 seems to have done just that, even though just a slight increase of about one percent.
Examining phishing trends on a quarterly basis shows that 2013 saw a constant growth in phishing volumes throughout the year as opposed to the expected decline in Q4.

**PHISHING BY GEOGRAPHY**

The country most targeted, unsurprisingly, was the U.S., suffering over 60% of worldwide phishing volumes. Throughout the year, the U.S. was most targeted with the most significant volume coming in October when it saw 80% of global phishing attacks that month.

The top 10 countries targeted by phishing in 2013 were:

1. United States
2. United Kingdom
3. Germany
4. India
5. South Africa
6. Canada
7. Netherlands
8. Colombia
9. Australia
10. Brazil

**Regional Breakdown**

When looking at phishing volumes across the different geo-regions, North America (including the U.S. and Canada) was the most targeted, followed by EMEA (including the UK) with 26% of global phishing volumes. The following regional breakdown (excluding North America) shows the top three countries targeted in each region and their estimated global losses from phishing in 2013:

**Regional Breakdown: Europe, Middle East and Africa (Emea)**

The top three countries and their estimated losses for phishing in EMEA are as follows:

1. United Kingdom, 31% of phishing volume, total estimated losses = $467 million
2. Germany, 25% of phishing volume, total estimated losses = $386 million
3. South Africa, 15% of phishing volume, total estimated losses = $222 million
Regional Breakdown: Asia Pacific, Japan and Oceania

The top three countries and their estimated losses for phishing in the Asia Pacific region are as follows.

1. India, 54% of phishing volume, total estimated losses = $225 million
2. Australia, 21% of phishing volume, total estimated losses = $87 million
3. China, 14% of phishing volume, total estimated losses = $59 million

Regional Breakdown: Latin America

The top three countries and their estimated losses for phishing in Latin America are as follows.

1. Colombia, 43% of phishing volume, total estimated losses = $95 million
2. Brazil, 39% of phishing volume, total estimated losses = $86 million
3. Mexico, 8% of phishing volume, total estimated losses = $19 million

2014 PHISHING FORECAST

Phishing, the cybercrime equivalent of pickpocketing, is a crime that is easily committed with very little cost to the attacker: cheap (criminal) hosting services—offered mostly on-top of hijacked websites—are abundantly available. If spamming 500,000 email addresses only sets you back a mere $65, it is no surprise that phishing attack volumes are not dropping.

Looking forward into 2014, we expect to see:

- Phishing volumes will not drop considerably, though we may see a slight decline. The decline will be mainly due to growing adoption of email authentication, namely DMARC, which together with tighter policy should help in the reduction of phishing emails received by end users. However, wider global adoption (into LATAM and APJ) still plays a major factor in the battle against phishing.

- Big data analytics and broader intelligence collection will lead to faster detection and quicker mitigation, resulting in lower financial losses. With the millions of spam messages traversing the internet on a daily basis, separating the wheat from the chaff has become far more challenging. Advancements in phishing techniques and methods also serve to add a layer of complexity when it comes to detection. Deploying analytics into the detection process provides a way to see though the noise and get to the phish faster. Coupled with broader intelligence collection, attacks may be prevented before they are launched.

- Greater end user awareness will serve to reduce losses. Cyber awareness has become a mainstream conversation topic—people are becoming more aware of the dangers in the digital world. More awareness translates directly into fewer losses.