APWG Phishing Attack Trends: Latest Report

Presenter: Gao Mosweu

But… What is Phishing?

Phishing is a criminal mechanism employing both ***social engineering*** and ***technical subterfuge*** to steal consumers' personal identity data &financial account credentials.

Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords.

Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

-- Definition by APWG

Summary of Report

The APWG Phishing Activity Trends show that the number of phishing attacks increased dramatically during the 2015 holiday season.

It seems phishers found the retail sector potentially the most lucrative market and targeted this market with a barrage of phishing scams in December 2015,

These hunters and gatherers gather from the Retail / Service sector during this season while during the rest of the year, they ***gather*** from Internet Service Providers (ISPs) as the most-targeted industry sector.

There was also a major increase in Potentially Unwanted Programs: Programs that are installed without the user's consent, as part of bundles with other software. Some of these programs are malicious, or do not reveal what sensitive data they collect about the user.

Summary contd…

Belize and the United States topped the list of countries that hosted phishing sites.

USA remained the top country hosting phishing-based Trojans and downloaders during the last quarter of 2015.

The number of brands targeted by phishing remained constant throughout 2015, although new companies and institutions were always being targeted.

In Q4 2015, 14 million new malware samples were captured.

Methodolody and Data Sets

APWG tracks and reports the number of :

- unique phishing reports (**email campaigns**) received,
- **unique phishing sites** found.
- **number of unique phishing websites:** This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination.)
- **crimeware instances** (unique software applications as determined by MD5 hash of the crimeware sample),
- **unique sites that are distributing crimeware** (typically via browser drive-by exploits).
- Statistics on rogue anti-virus software, desktop infection rates, and related topics.

Highlights

Statistical Highlights for 1st – 3rd Quarters 2015

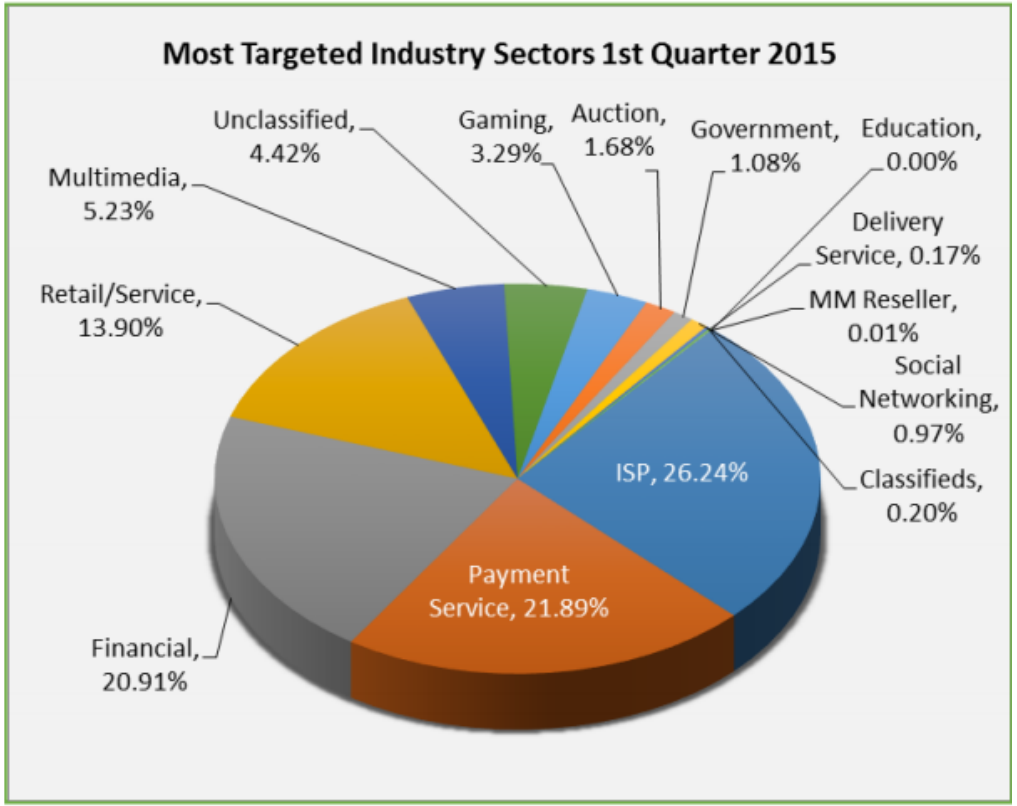
	Jan	Feb	Mar	April	May	June	July	Aug	Sept
Number of unique phishing websites detected	31,064	34,749	70,534	85,803	90,060	77,144	87,564	88,976	64,600
Number of unique phishing e-mail reports (campaigns) received	49,608	55,795	115,808	142,099	149,616	125,757	142,155	146,439	106,421
Number of brands targeted by phishing campaigns	420	438	421	393	404	420	434	442	402
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA	USA	USA	Belize
Contain some form of target name in URL	60.4%	67.4%	76.8%	69.2%	65.0%	73.1%	76.1%	76.8%	81.3%
Percentage of sites not using port 80	0.60%	1.56%	1.46%	2.19%	2.55%	2.73%	3.49%	3.68%	2.73%

Highlights

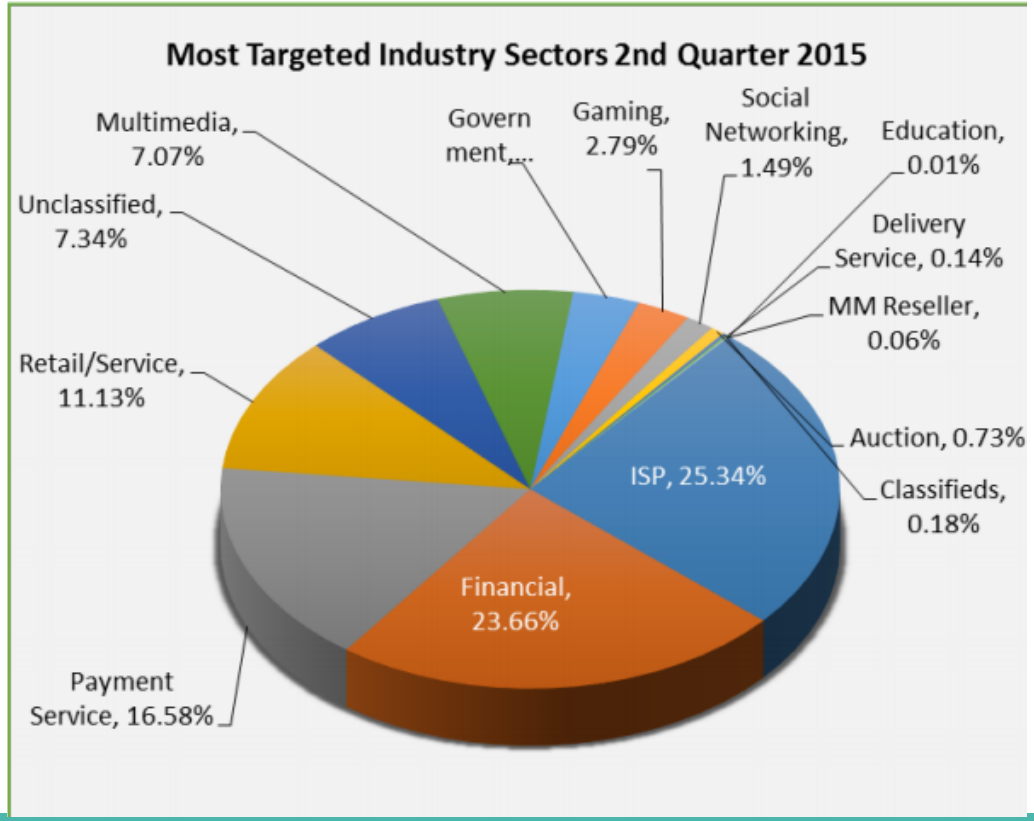
Statistical Highlights for 4th Quarter 2015

	October	November	December
Number of unique phishing websites detected	48,114	44,575	65,885
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	194,499	105,233	80,548
Number of brands targeted by phishing campaigns	391	408	406
Country hosting the most phishing websites	Belize	USA	USA
Phishing URL contains some form of target name	78.51%	72.61%	52.3%
Percentage of sites not using port 80	2.91%	3.98%	7.50%

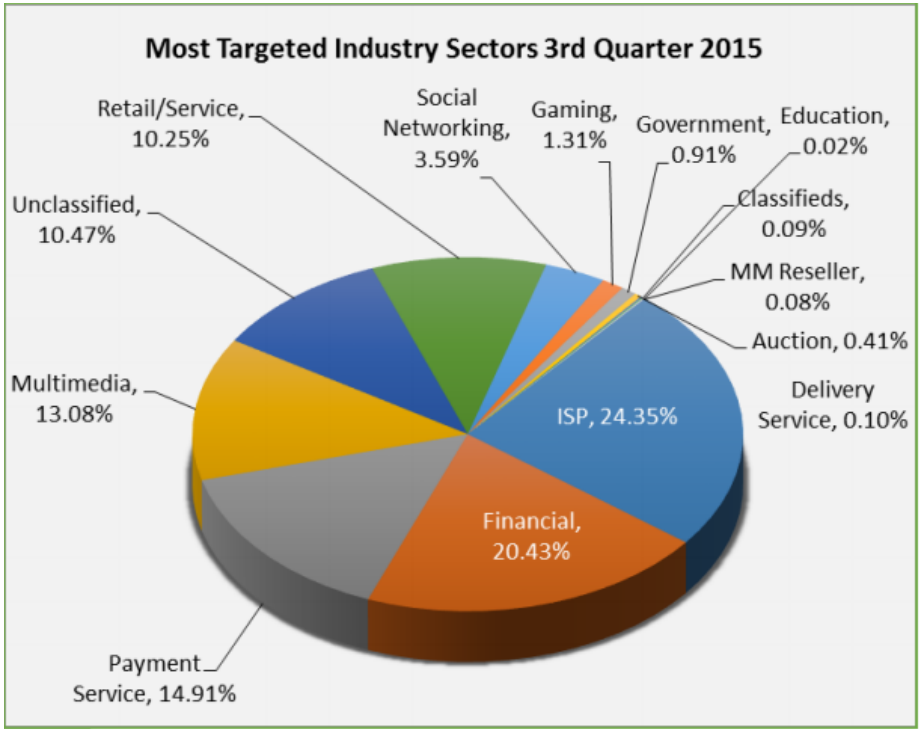
Most-Targeted Industry Sectors by Quarter

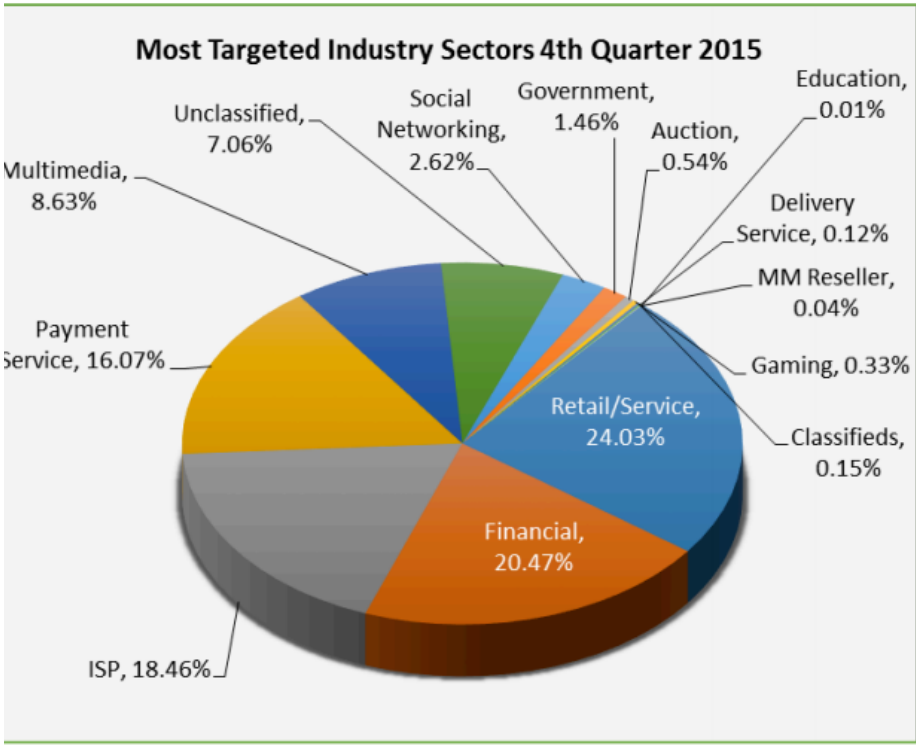


Most-Targeted Industry Sectors by Quarter contd…



Most-Targeted Industry Sectors by Quarter contd…





Countries Hosting Phishing Sites – 4th Quarter 2015

October		November		December	
Belize	42.75%	United States	50.90%	United States	83.58%
United States	42.56%	Belize	27.22%	Netherlands	1.95%
Belgium	2.58%	Europe	4.65%	United Kingdom	1.51%
Europe	2.38%	Hong Kong	4.57%	Germany	1.26%
Germany	0.99%	China	1.14%	Australia	1.12%
United Kingdom	0.81%	Canada	1.09%	Hong Kong	0.86%
Canada	0.71%	Italy	0.88%	China	0.82%
Brazil	0.63%	Germany	0.86%	France	0.73%
Hong Kong	0.60%	United Kingdom	0.81%	Russian Federation	0.60%
France	0.50%	Australia	0.76%	Ireland	0.57%

Where the “Phish” is: Infection rates

- Asia and Latin America were the regions with the highest infection rates.
- countries with the lowest infection rates are generally in Europe, with Japan also appearing in the bottom 10.

Malware Types

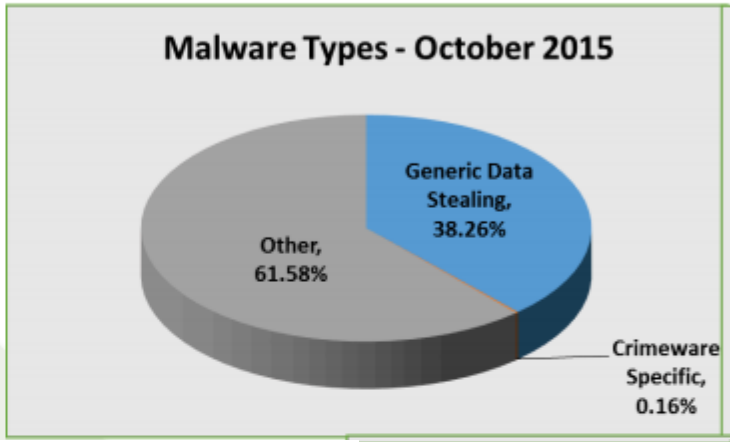
- **Crimeware** (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities);
- **Data Stealing and Generic Trojans** (code designed to send information from the infected machine, control it, and open backdoors on it); and
- Other (the remainder of malicious code commonly encountered in the field such as auto-replicating worms, dialers for telephone charge-back scams, etc.)

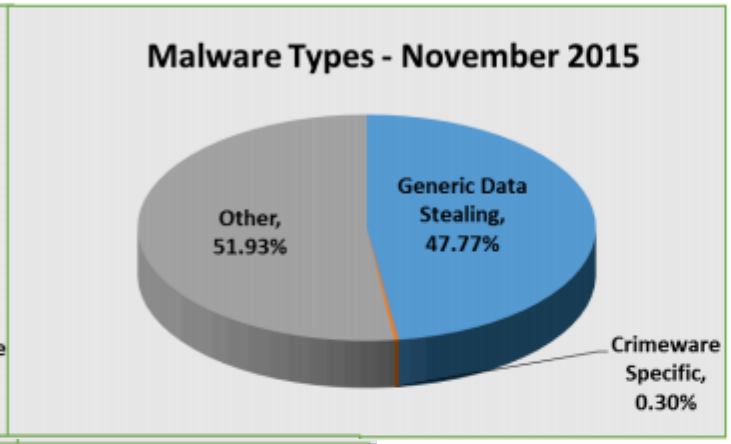
Malware Types

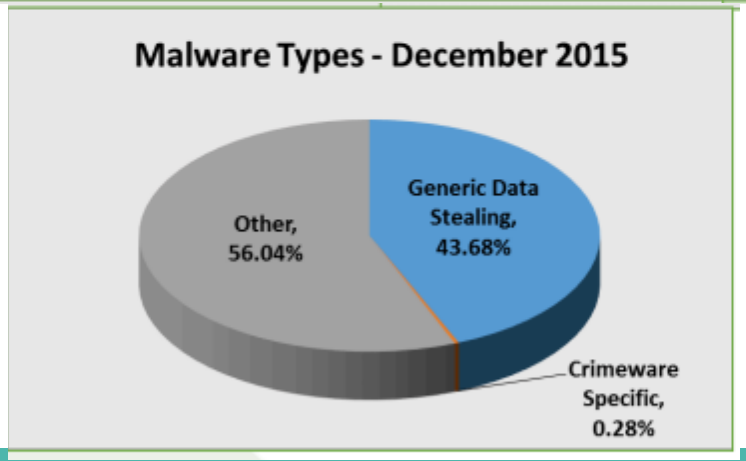
New Malware Strains in Q4	% of malware samples
Trojans	53.05%
Viruses	23.48%
Worms	13.38%
Adware/Spyware	1.83%
PUP	8.26%

Malware Infections by Type	% of malware samples
Trojans	61.28%
Viruses	2.02%
Worms	2.40%
Adware/Spyware	5.25%
PUP	29.05%

Malware Types by last Quarter 2015







THE END

Credits

APWG Phishing reports:

https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf

Photo Credits

1. www.malwarehero.com
2. http://anileweb.com/blog/new-phishing-attack-targets-gmail-users-and-others-email-web/