Phishing Activity Trends Report

1st Quarter 2016

APWG

Unifying the

Global Response

To Cybercrime

January – March 2016

Published May 23, 2016

Phishing Activity Trends Report, 1st Quarter 2016

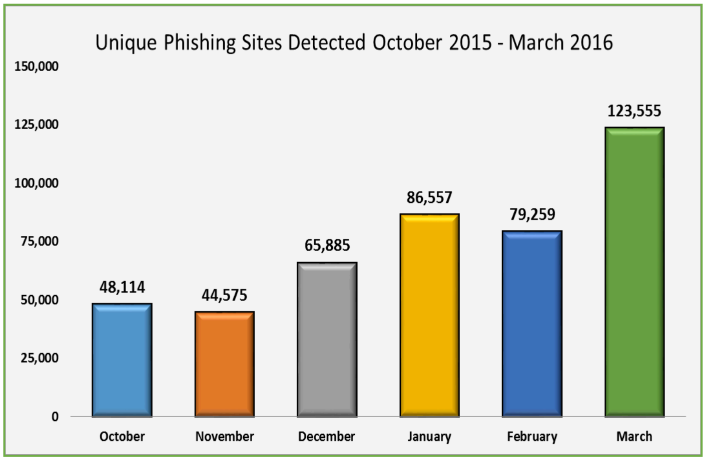
Phishing Report Scope

The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

Phishing Defined

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

Phishers Ramp Up into 2016 With Major Increase in Attacks



Phishing attacks rose in the Christmas 2015 season, and have continued to climb in the new year.

1st Quarter 2016 Phishing Activity Trends Summary

- The number of phishing websites observed by APWG increased 250% from the last quarter of 2015 through the first quarter of 2016. [p. 4]
- The Retail/Service sector remained the most-targeted industry sector during the first quarter of 2016, with 42.71% of attacks. [p. 7]
- The number of brands targeted by phishers in the first quarter remained constant – ranging from 406 to 431 brands each month. [p. 6]
- The United States continued its position at top on the list of nations hosting phishing websites. [p. 7]
- In Q1 2016, 20 million new malware samples were captured. [p. 8]
- The world's most-infected countries are led by China, where 57.24% of computers are infected, followed by Taiwan (49.15%) and Turkey at 42.52%. [p. 8]

Table of Contents

Phishing Activity Trends Report
1st Quarter 2016
www.apwg.org • info@apwg.org

Methodology and Instrumented Data Sets

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG tracks and reports the number of unique phishing reports (email campaigns) it receives, in addition to the number of unique phishing sites found. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report e-mails as those found in a given month that have the same subject line in the e-mail.

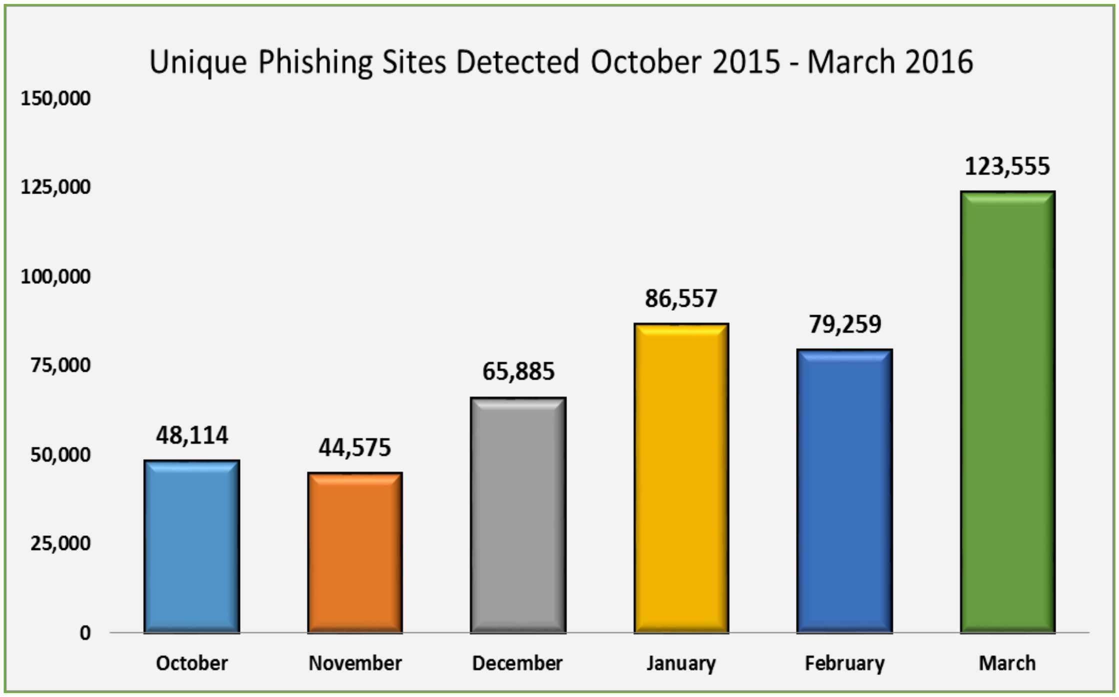
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample), as well as unique sites that are distributing crimeware (typically via browser drive-by exploits). The *APWG Phishing Activity Trends Report* also includes statistics on rogue anti-virus software, desktop infection rates, and related topics.

Statistical Highlights for 1st Quarter 2016

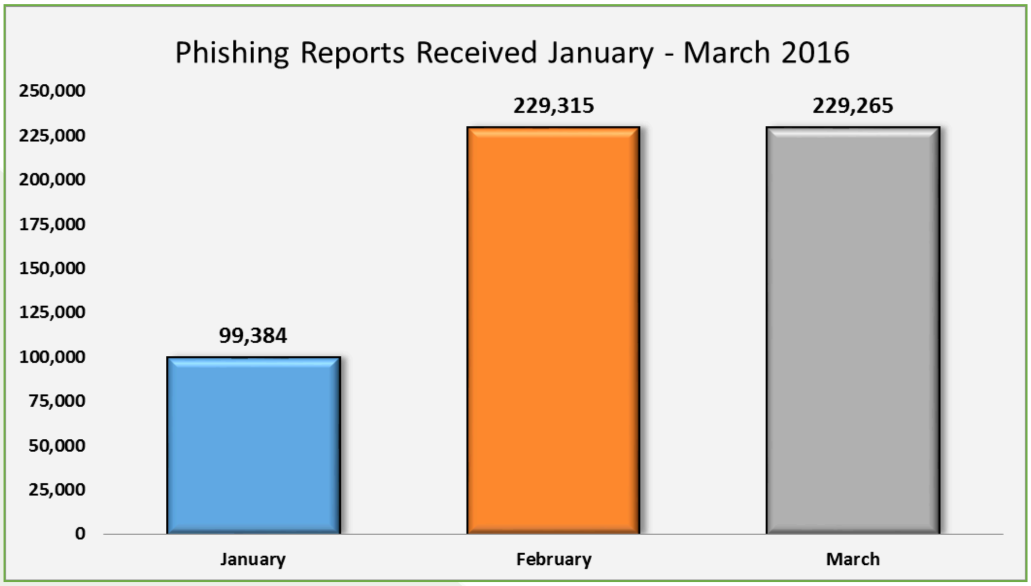
	January	February	March
Number of unique phishing websites detected	86,557	79,259	123,555
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	99,384	229,315	229,265
Number of brands targeted by phishing campaigns	431	406	418
Country hosting the most phishing websites	USA	USA	USA
Phishing URL contains some form of target name	59.39%	54.60%	55.13%
Percentage of sites not using port 80	5.95%	5.25%	4.26%

Phishing E-mail Reports and Phishing Site Trends – 1st Quarter 2016

The total number of unique phishing websites observed in Q1 was 289,371. The number observed per month rose steadily from the 48,114 detected in October 2015 to the 123,555 detected in March 2016 – a 250 percent increase over six months. The increase in December 2015 was expected, since there is usually a spate of spamming and online fraud during the holiday shopping season. The continuing increase into 2016 is cause for concern.

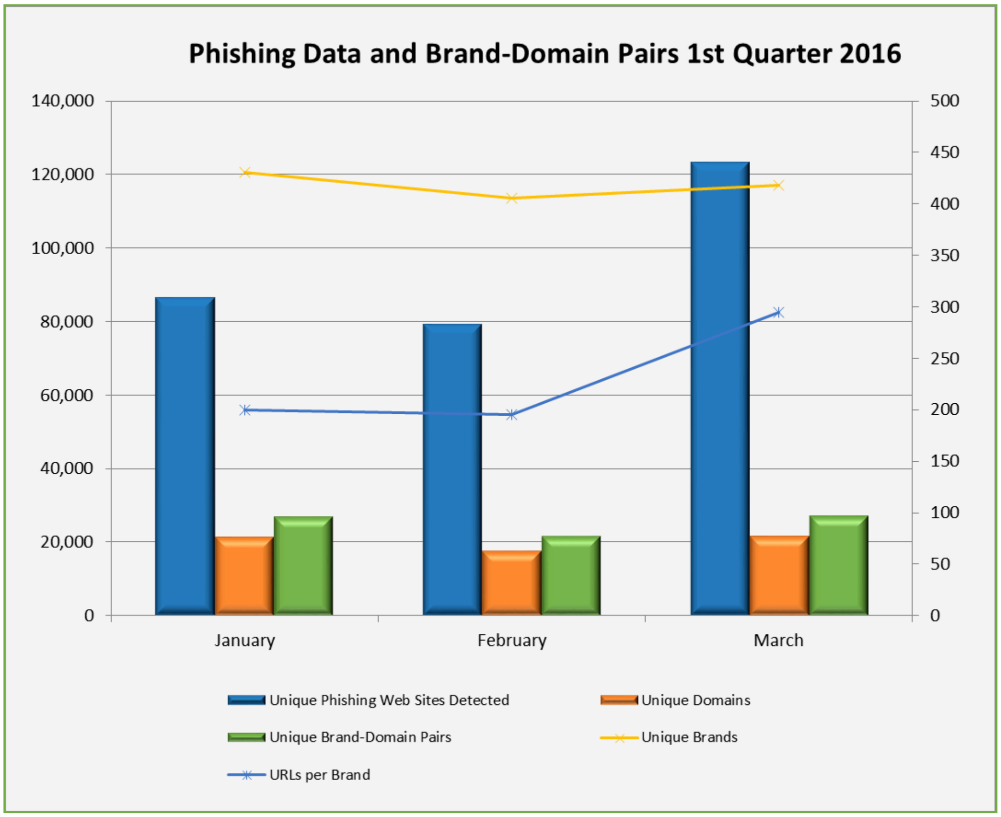


The number of unique phishing reports submitted to APWG during Q4 was 557,964. The number of unique phishing reports submitted to APWG saw a notable increase of nearly 130,000 from January to March:



Brand-Domain Pairs Measurement – 1st Quarter 2016

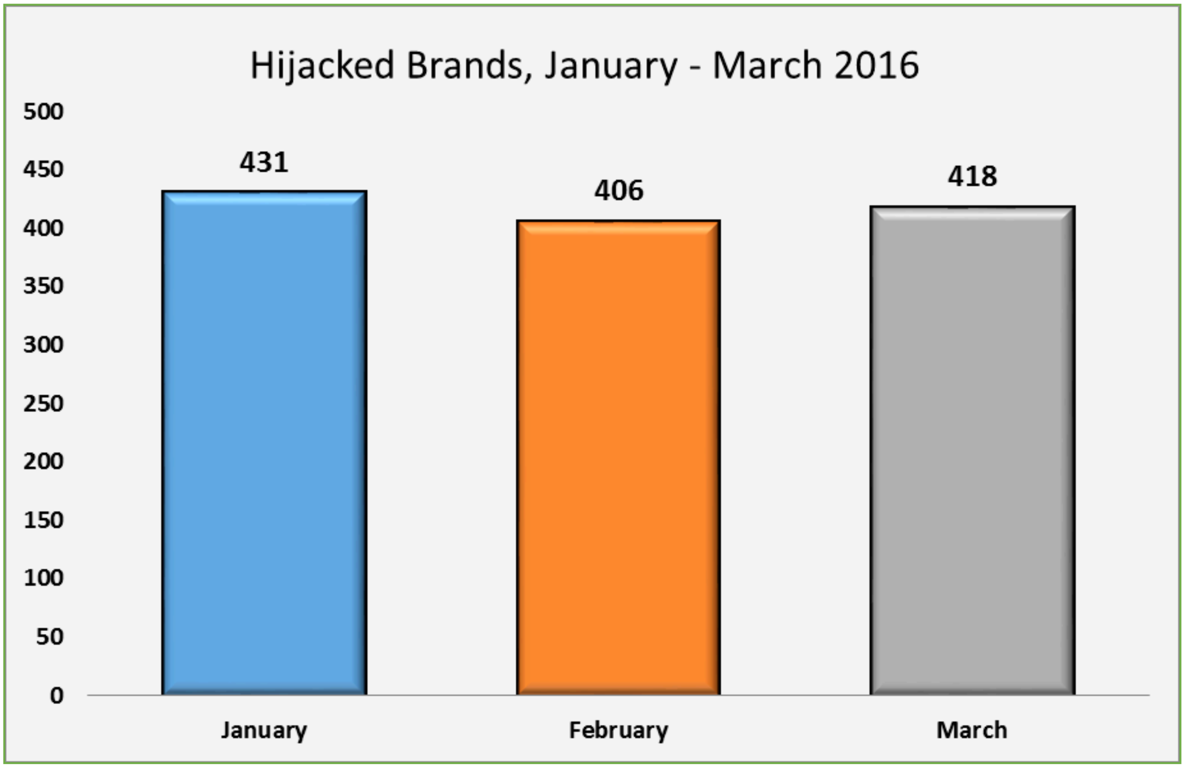
The following chart combines statistics based on brands phished, unique domains, unique domain/brand pairs, and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. (*Example*: if several URLs are targeting a brand – but are hosted on the same domain – this brand/domain pair would be counted as one instead of several.) *Forensic utility* of this metric: If the number of unique URLs is greater than the number of brand/domain pairs, it indicates many URLs are being hosted on the same domain to target the same brand. Knowing how many URLs occur with each domain indicates the approximate number of attacking domains a brand-holding victim needs to locate and neutralize. Since phishing-prevention technologies (like browser and e-mail blocking) require the full URL in order to prevent over-blocking, it is useful to understand the general number of unique URLs that occur per domain.



	January	February	March
Number of Unique Phishing Web Sites Detected	86,557	79,259	123,555
Unique Domains	21,131	17,438	21,394
Unique Brand-Domain Pairs	26,789	21,476	26,968
Unique Brands	431	406	418
URLs Per Brand	200	195	295

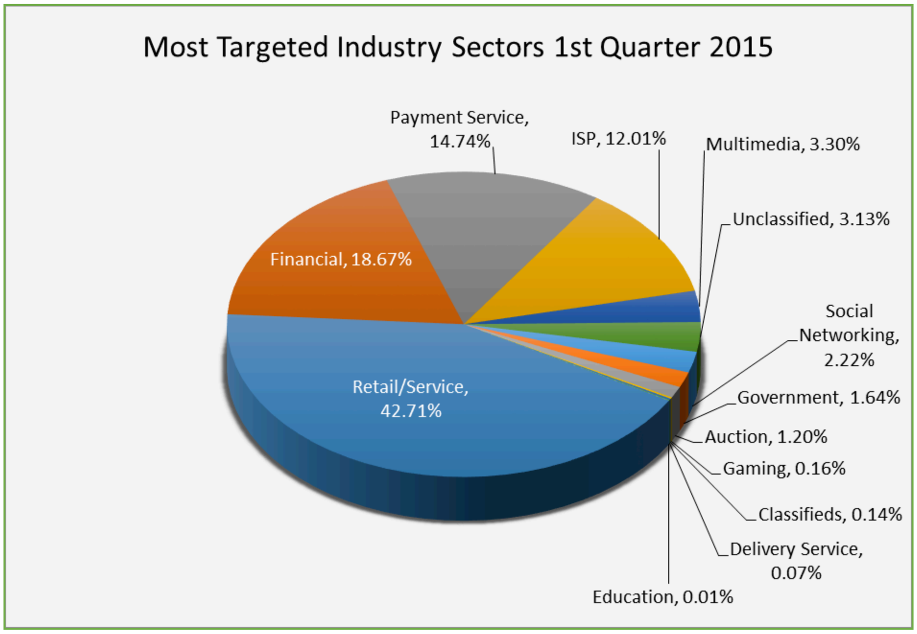
Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 1st Quarter 2016

The number of brands targeted by phishers in in the first quarter remained fairly constant – ranging from 406 to 431 brands each month. Across 2015 and into 2016, phishers targeted between 391 and 442 unique brands in any given month of that year.



Most-Targeted Industry Sectors – 4th Quarter 2015

The Retail/Service sector remained the most-targeted industry sector, with 42.71 percent of attacks, followed again by Financial Services. According to Stefanie Ellis, AntiFraud Product Marketing Manager at MarkMonitor: “MarkMonitor continues to detect a high volume of attacks targeting cloud-based or SAAS companies, driving significant increases in the Retail Service sector. Financial and Payment targets are still heavily targeted.”



Countries Hosting Phishing Sites – 1st Quarter 2016

The United States continued to top the list of the countries hosting phishing sites. Phishers often break into vulnerable web hosting networks to provision phishing sites, and the United States hosts a large number of web sites.

January		February		March	
United States	75.10%	United States	81.90%	United States	75.62%
Belize	4.79%	United	2.20%	China	4.16%
Netherlands	3.59%	Germany	2.15%	Hong Kong	3.05%
Germany	2.13%	Belgium	1.83%	Netherlands	3.02%
Belgium	1.79%	Netherlands	1.55%	Germany	2.24%
United Kingdom	1.57%	Canada	0.63%	United	1.31%
China	1.46%	Russian	0.59%	Russian	0.75%
Russian Federation	1.28%	Kazakhstan	0.56%	Italy	0.74%
Australia	0.64%	Australia	0.56%	Australia	0.71%
France	0.60%	Chile	0.52%	France	0.56%

Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned. Definition: Crimeware is code designed with the intent of collecting information on the end-user in order to steal the user's credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components, which attempt to monitor specific actions (and specific organizations, such as financial institutions, retailers, and e-commerce merchants) in order to target specific information. The most common types of information are access to financial-based websites, e-commerce sites, and web-based mail sites.

Malware Infected Countries – 4th Quarter 2015

APWG member PandaLabs started the year by detecting more than 20 million new malware samples, at an average of 227,000 a day. This is a figure slightly higher than discovered in the same quarter in 2015, where the average new samples were 225,000 a day. Trojans were the most common type of malware, as they have been for years. Ransomware is counted in the trojan category, and that kind of malware has increased markedly.

New Malware Strains in Q1	% of malware samples
Trojans	66.81%
Virus	15.98%
Worms	11.01%
Adware / Spyware	1.98%
PUPs	4.22%

Malware Infections by Type	% of malware samples
Trojans	65.89%
Virus	1.95%
Worms	3.03%
Adware / Spyware	4.01%
PUPs	25.12%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, trojans comprised 66.81 percent of the malware samples observed during the quarter, an increase from 53 percent in the fourth quarter of 2015. Most infections are also caused by trojans, in 65.89 percent of cases.

Asia and Latin America were the regions that registered the highest infection rates. The countries with the lowest infection rates are generally in Europe, with Japan also appearing in the bottom ten.

Ranking	Country	Infection Rate	Ranking	Country	Infection rate
1	China	51.35%	36	The Netherlands	26.15%
2	Turkey	48.02%	37	Denmark	25.43%
3	Taiwan	41.24%	38	Japan	24.99%
4	Ecuador	39.59%	39	Germany	23.64%
5	Guatemala	38.01%	40	United Kingdom	23.61%
6	Russia	37.98%	41	Belgium	22.87%
7	Mexico	36.32%	42	Switzerland	21.43%
8	Peru	36.02%	43	Finland	20.45%
9	Poland	35.55%	44	Norway	20.33%
10	Brazil	34.00%	45	Sweden	19.80%

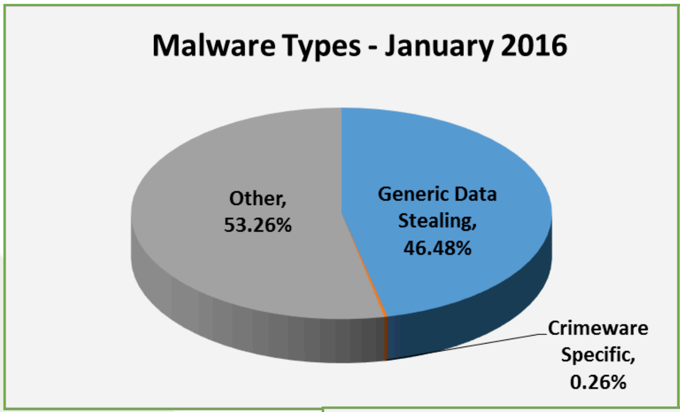
Measurement of Detected Crimeware – 4th Quarter 2015

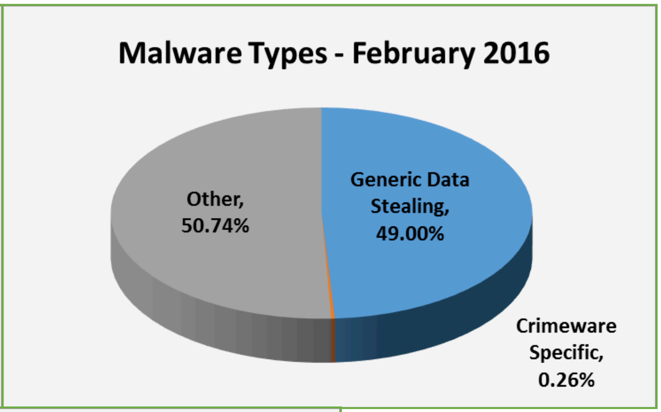
Using data contributed from APWG founding member Forcepoint regarding the proliferation of malevolent software, this metric measures proportions of three genera of malevolent code:

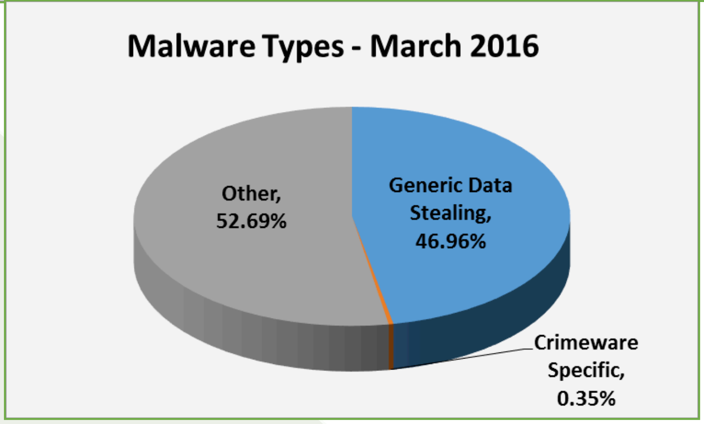
1. *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities);
2. *Data Stealing and Generic Trojans* (code designed to send information from the infected machine, control it, and open backdoors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

Accoring to Carl Leonard, Principal Security Analyst at Forcepoint: "The onslaught from ransomware has not abated in 2016. Ransomware authors exhibited a willingness to change their scare tactics and algorithms in Q1 2016 as they sought to scam end-users. The Jigsaw ransomware displayed imagery from a horror film to its victims and gave them an exceptionally short payment deadline – just one hour to pay the criminals or have their files deleted."

"Malware authors were also able to adjust their algorithms in an attempt to keep under the radar. The authors of the Locky ransomware changed their Domain Generation Algorithm in less than five days in order to reach out to a new set of command-and-control domains. The takeaway is clear – ransomware authors are more determined and aggressive in 2016. End-users should be aware of the danger and take preventative measures."


Malware Types - January 2016


Malware Types - February 2016


Malware Types - March 2016

Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

The United States remained the top country hosting phishing-based Trojans and downloaders during the three-month period. The United States uses a notable percentage of the world's IP addresses and hosts a significant percentage of the world's web sites.

January		February		March	
United States	77.73%	United States	71.50%	United States	62.36%
China	5.00%	Iceland	4.91%	China	13.71%
Rep. of Korea	3.41%	United Kingdom	3.50%	Iceland	3.28%
Germany	2.27%	Canada	2.80%	Russian Federation	1.93%
Iceland	1.82%	France	2.80%	United Kingdom	1.74%
Netherlands	1.82%	Russian Federation	2.34%	Canada	1.74%
Russian Federation	1.14%	Germany	2.10%	Germany	1.74%
France	1.14%	Italy	1.17%	Netherlands	1.74%
Canada	0.91%	Netherlands	0.93%	France	1.16%
Ukraine	0.45%	Turkey	0.93%	Turkey	0.97%

APWG Phishing Activity Trends Report Contributors

iThreat Cyber Group

iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.

IID

An Infoblox company, IID is a US-based provider of technology and services that help organizations secure their Internet presence.

MarkMonitor

MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PANDA SECURITY

Panda Security's mission is to keep our customers' information and IT assets safe from security threats, providing the most effective protection with minimum resource consumption.

FORCEPOINT POWERED BY Raytheon

Forcepoint brings a fresh approach to address the constantly evolving cybersecurity challenges and regulatory requirements facing businesses and government agencies.

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282 or foy@apwg.org. For media inquiries related to the content of this report, please contact APWG Secretary General Peter Cassidy at 617.669.1123; Te Smith of MarkMonitor at 831.818.1267 or Te.Smith@markmonitor.com; Luis Corrons of Panda at lcorrons@pandasoftware.es; Carl Leonard at Forcepoint CLeonard@forcepoint.com

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a 501(c)6 not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to qualified financial institutions, retailers, ISPs, solutions providers, the law enforcement community, government agencies, multi-lateral treaty organizations, and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG. APWG's first meeting was in November 2003 in San Francisco, and it was incorporated in 2004 as an independent corporation controlled by its board of directors, its executives and its steering committee. Because electronic crime is a sensitive subject, APWG maintains a policy of confidentiality of member organizations.

Websites of APWG include its main site <http://www.antiphishing.org>; the *STOP. THINK. CONNECT.* Messaging Convention public awareness program <http://www.stopthinkconnect.org> , the APWG's research website <http://www.ecrimeresearch.org>, and the APWG's European chapter < http://www.apwg.eu>. These serve as resources about the problem of phishing and electronic frauds perpetrated against Internet users – and resources for countering these threats.

Analysis by Greg Aaron, iThreat Cyber Group; editing by Ronnie Manning, Mynt Public Relations.