ZapFraud Supports APWG Accredited Reporter Program by Identifying Scams and Scammers

Automated Multi-filtering, Machine-Generated Scam Data Enlarge Scope of Global Phishing Clearinghouse

PALO ALTO, CA – JULY 28, 2015 - The APWG announced today that counter-cybercrime start-up ZapFraud has joined the APWG Accredited Reporter Data Submission Program, leveraging its fraud detection technology to identify scam and phishing e-mails and route them systematically into APWG's global cybercrime machine-event clearinghouse. As more databases are breached, there are more attacks on people and companies because scammers have more personal consumer data to launch highly targeted scam attacks—with an estimated 10 times the yield of non-targeted attacks.

ZapFraud's founders have committed to contributing the output of its patented scam and fraud filtering system to the APWG's URL Block List (UBL) phishing report clearinghouse, which receives reports from hundreds of sources worldwide. Focused primarily on consumer protection along with brand protection, ZapFraud is the first to contribute data that will span brands and report the many and varied types of scam circulating. Thus, the clearinghouse has a broader scope of detection and reporting than current brand-specific reporting can provide.

With its new contribution to the Accredited Reporter program, ZapFraud joins the APWG Information Sharing and Analysis Organization (ISAO), the oldest and most influential ISAO focused on cybercrime events, currently distributing upward of 80 million records per day to its clearinghouse members and correspondents worldwide.

The US Department of Homeland Security (DHS), following the Feb. 13 2015 executive order of US President Barrack Obama has established ISAOs as a crucial defense against criminals, fraudsters, and government-sponsored attacks. The APWG is proud to welcome ZapFraud as an Accredited Reporter and contributor to its ISAO resources' plexus.

ZapFraud's reports will be logged in near real-time (NRT) like all inbound reports to the UBL and archived with a Confidence Factor of 90 percent, like other automated reporting schemes that are sending reports to the UBL programmatically.

"APWG welcomes the contribution of the ZapFraud system to its phishing report clearinghouse," said Peter Cassidy, Secretary General of the APWG. "The automation of fraud detection, reporting and notification is of great interest to the APWG, and should be to all stakeholders. The automation of attack has been current art for more than a decade, and given the subsequent growth in all manner of fraud and phishing schemes, there will never be enough hands in the universe to manually process and report phishing emails."

APWG established its initial URL Block List (UBL) repository in 2003 in response to the demand from industry and NGOs for a central clearinghouse to receive phishing reports from brand holders and responders, and to distribute them to developers of security software, such as

browser security toolbars and anti-virus systems, as well as to cybercrime investigators requiring first-instance notification of attacks.

"Every year, more than one out of every ten adult Americans report falling victim to scams," said Dr. Markus Jakobsson, the founder of ZapFraud, "and while only about 6% of users fall for 'traditional' scams, targeted scams fool more than 60% of the recipients."

Chief Architect of ZapFraud Bill Leddy says further, "ZapFraud believes the APWG UBL is an important component in fighting Spam and Scam. Early detection and reporting through a shared clearinghouse minimizes the chance for Internet users to be scammed. This means less profits for scammers and better protection for consumers and enterprise."

The Accredited Reporter program was established in the fall of 2014 to broaden the number of qualified contributors to the APWG's machine-event data clearinghouses across the globe in order to maximize the trans-industrial exchange of event data required to deflect, investigate and respond to cybercrime attacks.

Since 2003, responders and investigators from industry, government and NGO sectors have been routing phishing reports to the UBL to inform security applications and forensic programs, including:

- Rapid distribution of block list notifications for spam filters, browsers, anti-phishing toolbars, web filters and proxies
- Global protection of consumers and business from frauds involving commercial enterprises and brand-holders
- Prevention of users globally from downloading malicious software developed to animate a financial crime
- Prevention of users from disclosing login and password credentials
- Benchmarking efficacy against others in similar industries to determine if fraudsters are targeting them more intently
- Informing forensic databases for researchers, industrial investigators and law enforcement to better succeed in legal investigations and actions against criminals who have multiple target companies in common
- Data exchange with other members of an economy or government affected by the same threats (phishing kits, malware distribution sites, botnet C&Cs, malicious IP addresses, re-shippers, mules, etc.)

Any brand holder or responder that has cybercrime event data they want to be cleared through the UBL to alert software developers or inform investigators' forensic routines, should be participating in the Accredited Reporter program. If any brand holder wants to leverage the larger community of AV vendors, responders and investigators they'll be first and fastest to report transgressions against their brands.

The Accredited Reporter program introduces a new level of APWG membership, fees for which are waived for eligible NGOs and public-sector agencies. The data sheet and application form for

the program is available:
http://docs.apwg.org/reports/Accredited_Reporter_Intro_and_Application.pdf

Questions about the program can be addressed by APWG Engineering and APWG managers who may be contacted at reporter@apwg.org.

About the APWG

APWG is the worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership of more than 1800 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe and the Organization of American States. The APWG is also on the steering group of the Commonwealth Cybercrime Initiative of the Commonwealth of Nations. For more information, please visit http://www.antiphishing.org.

About ZapFraud

ZapFraud is the leading provider of proactive email and online scam protection services for consumers, as well as threat detection services for enterprises. ZapFraud's patent-pending scam protection service helps provide peace of mind for consumers as they face the increasing and ever-changing threat of email, social media and online phishing scammers who attempt to steal intellectual property, identity, online credentials and, ultimately, their hard-earned money. Visit https://www.zapfraud.com for more information.

Zap Fraud Media Contacts:

Suzanne Matick
Suzanne@Zapfraud-inc.com
831-479-1888

or

Natalie Beck
Natalie@Zapfraud-inc.com
602-317-5162

APWG Media Contact:

Peter Cassidy
pcassidy@apwg.org
617-669-1123