[redacted]

July 16, 2015 9:31 AM

[redacted]M3AAWG's Operation Safety-Net Helps Business and Government Leaders Understand Global Online Security Best Practices

---

June 9 Press Release

M3AAWG 34th General Meeting - Dublin, Ireland, June 9, 2015 –

Operation Safety-Net, available today, is a cooperative global effort by industry and government experts outlining the online threats currently facing the world along with the proven best practices to mitigate them. The report was jointly developed by the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the London Action Plan (LAP), and describes the latest recommendations to protect users and networks from illicit Internet, mobile and telephony attacks.

"This tool doesn't just describe today's threats. It also provides straightforward recommended best practices for governments, businesses, educators and other members of the Internet and mobile industry to join in the fight against these threats. The report, an easy-to-read synopsis of the current risk environment, was a global collaborative effort from the front line community that fights spam, malware, phishing, hacking and related hazards," said Manon Bombardier, a LAP secretariat member and Chief Compliance and Enforcement Officer at the Canadian Radio-television and Telecommunications Commission (www.crtc.gc.ca).

The international community collaboratively developed the report in a public-private partnership led by Andre Leduc, Industry Canada manager of the National Anti-spam Coordinating Body. Industry experts from M3AAWG, LAP and other organizations, such as CAUCE (Coalition Against Unsolicited Commercial Email) and the APWG (Anti-Phishing Working Group), also contributed.

Written in plain language, Operation Safety-Net focuses on five areas and their related best practices. Some examples of the proven industry practices to combat these threats include:

1. Malware and Botnets

Among the most serious threats to the Internet economy, malware and bots can alter their characteristics so that even anti-abuse experts are not able to detect them.
Following industry best practices, the report encourages Internet Service Providers to notify customers of bots on their systems and also recommends the blocking of port 25.

2. Phishing and Social Engineering

Phishing schemes are going after increasingly more valuable data and high-value targets.
Among the industry best practices to curtain fraud from phishing, the report recommends prompt breach reporting.

3. Internet Protocol and Domain Name System (DNS) Exploits

The worse DNS exploits involve bad actors redirecting Internet traffic to fake versions of popular websites.
The report supports the worldwide deployment of DNSSEC (DNS Security) and recommends keeping DNS software updated.

4. Mobile, Voice over IP (VoIP) and Telephony Threats

Robocall scams are becoming more severe and new technology is also contributing to a growing number of Telephony Denial of Service (TDoS) attacks.
The report recommends the development of international threat information exchanges and developing facilities to report these newly emerging schemes.

5. Hosting and Cloud Threats

Online and mobile threats exploiting hosting and cloud services include spam, spamvertising, phishing, hacked websites, DDoS (Distributed Denial of Service) and other attacks.
The report suggests possibly implementing hardware-based intrusion detection systems (IDS) and software-based security scans and firewalls.

M3AAWG Chairman Michael Adkins said, "Operation Safety-Net isn't just for network or operational professionals. It aggregates the anti-abuse industry's global experience in identifying and curtailing current threats to help non-technical executives understand and manage online risk in their organizations."

Operation Safety-Net updates the initial "Best Practices to Address Online and Mobile Threats" report issued jointly by M3AAWG and LAP in 2012 to the OECD (The Organisation for Economic Co-operation and Development). The new report released today has been rewritten to provide more depth on threats resulting from converging technologies, the development of new mobile attack vectors, and rapidly mutating malware. For example, Operation Safety-Net addresses nefarious activities such as hijacked cloud and hosting services, VoIP "swatting" attacks that can disable emergency services switchboards, and new techniques for inserting spyware onto computers and mobile devices.

John Levine, president of CAUCE, said, "We are particularly delighted to see that the groundbreaking work accomplished in the 2012 version of this report has not been allowed to languish, given the worldwide and positive acceptance of the initial document. The global anti-abuse community coming together and creating an opportunity to review, refresh and renew this important toolkit is a remarkable milestone."

Operation Safety-Net is available on the websites of several organizations including in the Best Practices section of the M3AAWG website at https://www.M3AAWG.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_BPs2015-06.pdf and on the LAP website at http://www.londonactionplan.org/reports-stats.

About the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is where the industry comes together to work against bots, malware, spam, viruses, denial-of-service attacks and other online exploitation. M3AAWG (www.M3AAWG.org) represents more than one billion mailboxes from some of the largest network operators worldwide. It leverages the depth and experience of its global membership to tackle abuse on existing networks and new emerging services through technology, collaboration and public policy. It also works to educate global policy makers on the technical and operational issues related to online abuse and messaging. Headquartered in San Francisco, Calif., M3AAWG is driven by market needs and supported by major network operators and messaging providers.

About the London Action Plan (LAP)

The LAP (www.londonactionplan.org) is a 45-member organization drawn from governments, law enforcement agencies, academia and industry, and includes participants from Asia, Africa, North America and Europe that focus on fighting spam and online threats to consumers. The LAP promotes international enforcement cooperation and addresses spam related problems, such as online fraud and deception, phishing, and dissemination of viruses and has expanded its mandate to include additional threats, including malware, SMS spam and Do-Not-Call. The LAP coordinates joint enforcement activities, and enhances the technical skills of its members through regular teleconferences and an annual meeting.

Media Contact: Linda Marcus, APR, +1-714-974-6356 (U.S. Pacific), LMarcus@astra.cc, Astra Communications

M3AAWG Board of Directors: AT&T (NYSE: T); CenturyLink (NYSE: CTL); Cloudmark, Inc.; Comcast (NASDAQ: CMCSA); Constant Contact (NASDAQ: CTCT); Cox Communications; Damballa, Inc.; Facebook; Google; LinkedIn; Listrak; Mailchimp; Message Systems; Orange (NYSE and Euronext: ORA); OVH; PayPal; Return Path; Time Warner Cable; Verizon Communications; and Yahoo! Inc.

M3AAWG Full Members: 1&1 Internet AG; Adobe Systems Inc.; AOL; Campaign Monitor Pty.; Cisco Systems, Inc.; CloudFlare; Dyn; iContact/Vocus; Internet Initiative Japan (IIJ, NASDAQ: IIJI); Litmus; McAfee Inc.; Microsoft Corp.; Mimecast; Nominum, Inc.; Oracle Marketing Cloud; Proofpoint; Rackspace; Spamhaus; Sprint; Symantec and Twitter.

A complete member list is available at https://www.M3AAWG.org/about/roster.

+ + +

D. Reed Freeman | WilmerHale
[redacted]

Follow our Cybersecurity, Privacy and Communications Group on Twitter @WHCyberPrivacy

Please consider the environment before printing this email.