
Thought Paper: Spamware

Email Address Harvesting Tools and Anonymous Bulk Emailing Software

Introduction: What is spamware?

Spam works because it is such a low-cost, high-reach endeavor. For very little investment and effort, spammers can reach millions of potential customers, and just 100 responses out of 10 million can turn them a profit. Recently, the *Pew Internet & American Life Project* reported that seven percent of Americans have purchased something through an unsolicited email. Because spamming can be so lucrative, spammers have grown wealthy and have become a market unto themselves. And, as with any new market there is often great opportunity. In fact, software writers in Eastern Europe, Russia, Southeast Asia, and elsewhere have developed tools that enable spammers to spam more effectively. We refer to these tools as “spamware.”

Spammers need two things: a list of email addresses to send their junk mail to and a way to do it anonymously.

Once spammers have prepared their junk email in such a way that it conveys their message and is set to bypass as many spam filters as possible, they need two things: a list of email addresses to send their junk mail to and a way to do it anonymously. To accomplish these goals they utilize two types of tools – one that enables them to collect or harvest email addresses and another that allows them to send their bulk email anonymously. This MX Logic Thought Paper will specifically review *Email Address Harvesting Tools* and *Anonymous Bulk Emailing Software* in order to provide basic knowledge email users can use to be better prepared in the fight against spam.

Email Address Harvesting Tools

Sophisticated spammers no longer rely on others to provide email addresses for them. Instead, they want the freshest email addresses available and even targeted lists of addresses that only email address harvesting tools can provide. These spammers, therefore, use email address harvesting tools designed specifically to collect email addresses from the Internet by combing websites or by launching directory harvest attacks on specific domains.

While many amateur spammers may still buy email addresses off the Web, professional spammers utilize ready-made email harvesting tools that have been customized for them by enterprising software developers – likely spammers themselves – looking to share in the wealth spammers create.

Two of the most common email collection tools are the Atomic Email Hunter and the Power Email Harvester.

Two of the most common email collection tools are the *Atomic Email Hunter* and the *Power Email Harvester*. Anyone can download trial versions of these tools, or buy fully-functional versions with a credit card, wire transfer, check, or even e-gold. It takes just a few minutes to configure the tools and to quickly begin collecting hundreds of emails per minute.

These tools harvest email addresses through a few different methods:

1. **Directory Harvest Attacks**—Email address harvesting tools can be used to launch directory harvest attacks (DHAs). DHAs are a way of checking a domain for valid email address by automatically generating and sending addresses at random and seeing which ones return a valid SMTP response (*See Figure 1*). These attacks can be launched in two forms by spammers on domains of their choice:
 - **Brute force sequence attacks**, which try possible combinations of letters (e.g. aaa@targetdomain.com, aab@targetdomain.com, aac@targetdomain.com, etc.).
 - **Dictionary mashing attacks**, which try possible combinations of names (e.g. robertsmith@targetdomain.com, robsmith@targetdomain.com, bobsmith@targetdomain.com, etc.).

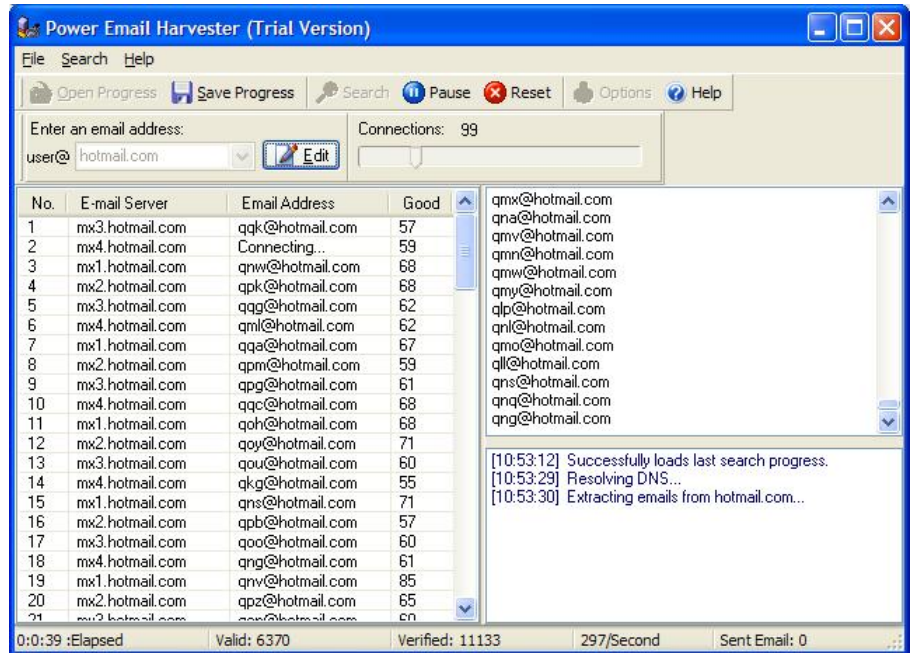


Figure 1— Power Email Harvester performing a Directory Harvest Attack.

- 2. Target Market Keyword Searches**—Often, spammers have messages they want to bulk email to certain markets. Email address harvesting tools allow them to enter keywords describing that target market (“homeowner organization members in Memphis,” “restaurant owners,” etc.). These harvesting tools will then utilize common Web search tools like Google to search Web pages that match those search terms, and look for email addresses on those pages (See Figure 2).

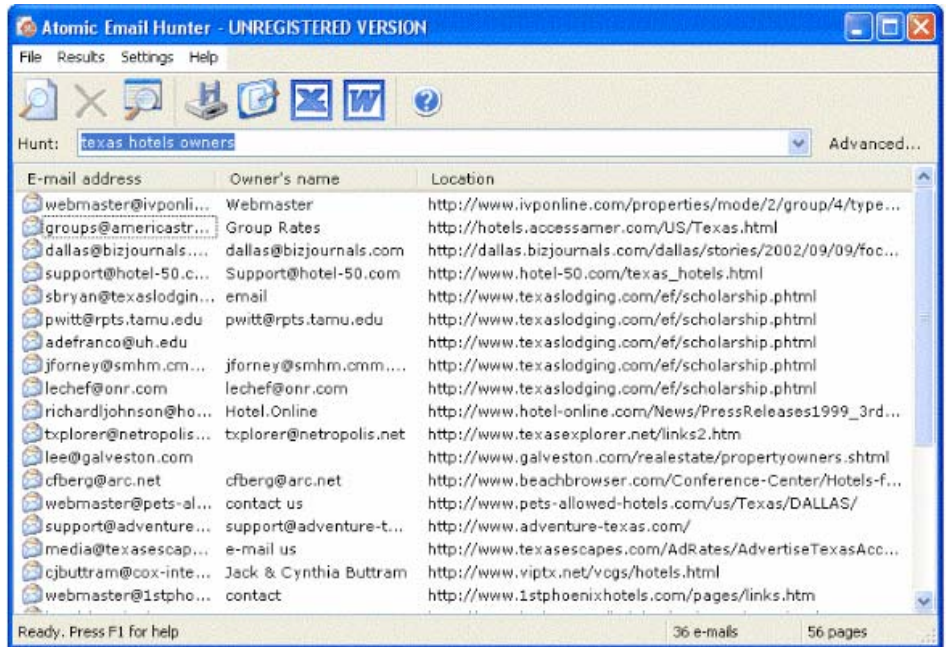


Figure 2— Atomic Email Hunter performing a targeted keyword search.

3. **Generalized Web Searches**—Finally, email address harvesting tools can also perform generalized web searches looking for email addresses, combing websites, web forums, web logs (“blogs”), and any other sites on the Web that contain email addresses.

Anonymous Bulk Emailing Software

To avoid detection, spammers need tools to help them deliver their junk email anonymously. This is a two-part process requiring technology to send the spam in bulk, and technology to make the bulk email anonymous. These technologies have been brought together in anonymous bulk emailing software.

The first aspect of this process—sending a lot of email quickly—involves a straightforward approach, generally using a multi-thread Message Transfer Agent (MTA) to send out a large number of messages in as short a timeframe as possible. The second part of the process, making sure that the email is sent anonymously (or, more specifically, that it does not point back to the spammer) involves

Spammers need tools to help them deliver their junk email anonymously.

“spoofing,” and requires sending the bulk email through unprotected servers.

Spammers are so universally reviled that if it were possible to track spam back to the source, spammers would likely be exposed to legal action or perhaps even online vigilante justice. Spammers therefore “spoo” their email addresses, either by forging a false email header so that it appears to come from a source other than the spammer, or by using unprotected email proxy servers known as “open proxies” or “open relays.” More recently, spammers have been utilizing a network of hijacked PCs on broadband connections (“BotNets”) whose owners have no idea their PCs are unwitting participants in a “zombie” spamming army.

Open relays are still the mainstay method of anonymous email distribution, so the most utilized anonymous bulk emailing software helps spammers locate and utilize these unprotected email servers.

Two of the most popular anonymous mass mailing tools are *StealthMail Master* and *Send-Safe Mail*. *StealthMail Master* (www.mailinglistmaster.com), which costs \$150 for a 30-day license, and \$700 for an annual license, is believed to be developed and distributed from Satu Mare, Romania. *Send-Safe Mail* (www.send-safe.com) costs spammers anywhere from \$50 to \$1,500 to use its range of open proxy scanning and bulk emailing services, and is believed to be developed and distributed from Moscow, Russia.

The key to anonymous bulk emailing is to mask the origination point of the email.

The key to anonymous bulk emailing is to mask the origination point of the email. *StealthMail Master* allows spammers to search for open proxies they can then use to send their email anonymously. *Send-Safe Mail* provides a menu of services allowing spammers to use open proxies detected by *Send-Safe Mail*, or to provide their own open proxies and just use *Send-Safe Mail* to do the actual bulk emailing. Because open relays may not be open for long once an administrator realizes the server is insecure, spammers cannot rely on old lists of these open proxies. Sophisticated spammers are constantly updating their lists of unprotected email servers. *StealthMail Master* and *Send-Safe Mail* enable spammers to find open proxies in real time. Because of the services they provide to spammers, these tools may violate the 2003 US CAN-SPAM act under a provision that institutes criminal liability for conspirators, aiders, and abettors of spammers.

SCANNING FOR OPEN PROXIES

StealthMail Master is an industrial-strength bulk emailing tool, utilizing multiple concurrent connections for sending out high volumes of email, and lists of open proxies to send that email anonymously. Right before a spammer is ready to begin a bulk email campaign, they can

use StealthMail Master to search and download a list of open proxies, to learn whether or not these proxies are “good” (i.e. unprotected) and determine their connection speed (See Figure 3). It even comes with a service that updates the software with new proxies or open relays automatically.

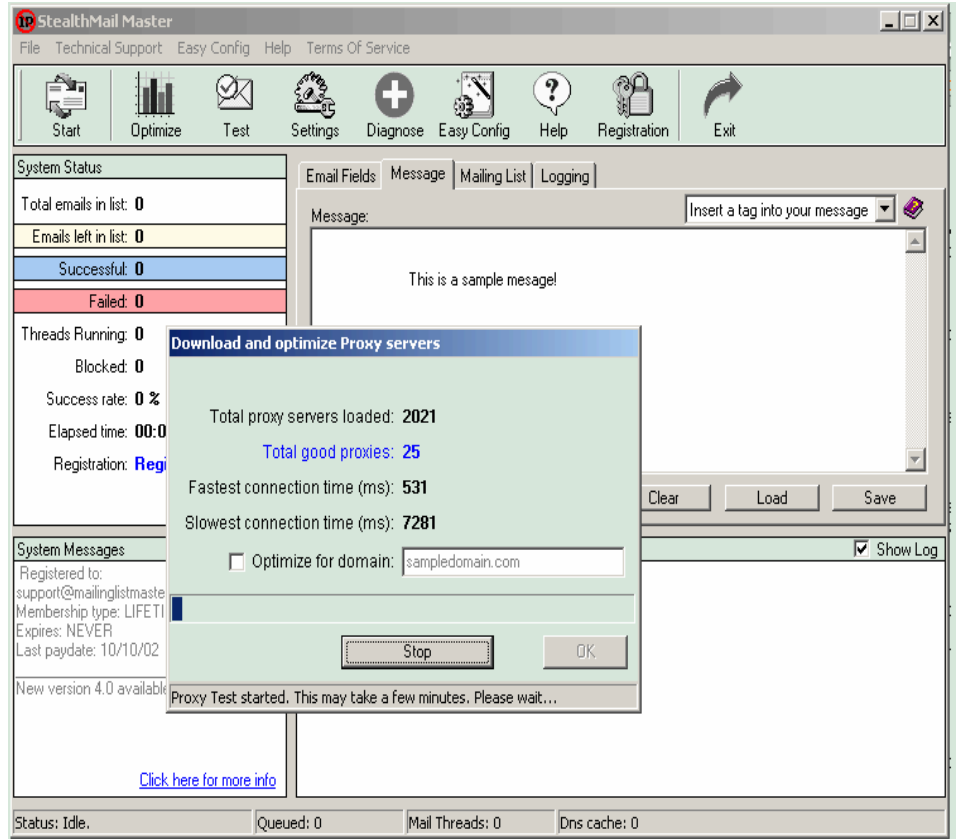


Figure 3—StealthMail Master searching for open proxies

Similarly, Send-Safe Mail enables spammers to send anonymous email in bulk. Send-Safe Mail also gives spammers the option to use their own list of open proxies, or to use open proxies detected by Send-Safe Mail. Spammers who want to use Send-Safe Mail to detect open proxies can use the Send-Safe Proxy Scanner – by simply entering a range of IP addresses within which they want to scan for unprotected email servers (See Figure 4). Should the spammer already have their own list of open proxies, they can use a stand-alone version of Send-Safe Mail for bulk emailing without the proxy scanning service.

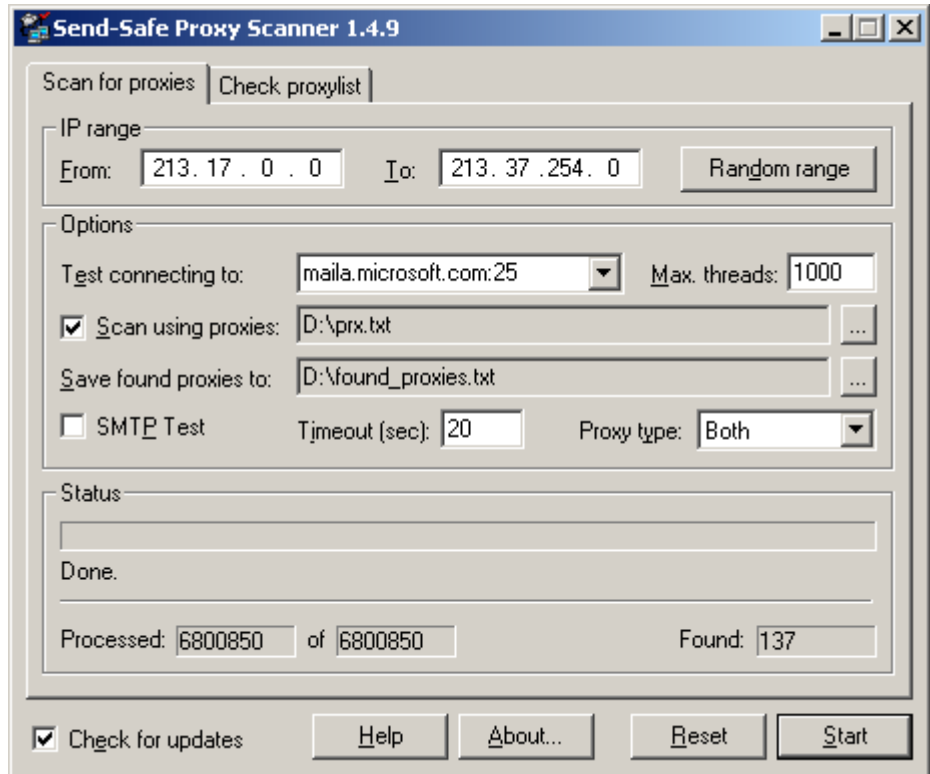


Figure 4—Send-Safe Mail Proxy Scanner

With tools like Send-Safe Mail, spammers can find the latest available unprotected email servers through which they can anonymously send their bulk email.

Once they have a new list of open proxies, spammers can begin to send their bulk mail through them. As the messages pass through these relays, their header information is altered so that they appear to have been sent from that unprotected server, and not the spammer. Before long, either because they get blacklisted or receive complaints, administrators of open proxies will realize their email servers are being used by spammers to spoof their junk email. They will secure their servers, and the spammer will no longer be able to use them. But on the Internet, new servers are always coming on line, and operating systems are constantly being changed or upgraded, so there will always be unprotected servers for spammers to use as open relays, even if only for a short time. With tools like *Send-Safe Mail*, spammers can find the latest available unprotected email servers through which they can anonymously send their bulk email.

Conclusion

Spammers have a wide variety of software tools, or spamware, that enable them to more successfully launch massive spamming campaigns – including the email address harvesting tools and anonymous bulk emailing software discussed in this paper. But, while defeating spammers will take time and involve a combination of technology solutions, legislation, and end-user education, understanding the tools spammers use is an important step in becoming better prepared for their attacks. In today's fight against spam – as when facing any threat – it is always important to know the enemy.

About MX Logic

MX Logic, Inc. provides innovative email defense solutions that ensure email protection and security for enterprises, service providers, government organizations, and resellers and their customers. Deployed as a managed service or on-premise software, the company's feature-rich solution suite is the industry's most comprehensive, flexible and easy to use.

Founded by messaging industry pioneers, MX Logic has delivered numerous industry firsts to the enterprise spam market, including becoming the first managed service provider to: leverage Bayesian Statistical Classification; provide spam beacon ("Web bug") blocking; offer quarantine management via email; provide corporate-level quarantine release reports that help reduce inappropriate email while decreasing corporate liability; and deliver a solution for tracking URL click-throughs from email to the Web, providing increased corporate control and security.

Through the company's managed service offering, MX Logic processes millions of messages per day for over 2,500 organizations, including EnCana, Hyundai Motor America, The Sports Authority, YMCA, and Service Master. In addition, MX Logic is the only email defense company to offer both a managed service and a turnkey, carrier-grade software solution for service providers. For more information, visit www.mxlogic.com.