Adrian Hughes, 123RFa

Although spam filtering and blocking is helpful for the end user, it doesn't stop the production of spam. KnujOn strikes spam at the source.

BY BOB BRUEN AND GARTH BRUEN

Unsolicited electronic material is more than just an annoyance. In 2004, Ferris Research Inc. estimated that spam costs US organizations more than US$ 10 billion dollars per year in manpower, software expenses, and lost productivity [1]. In addition, affected systems can suffer from a distributed loss of bandwidth and occasional server failures, not to mention the risk of virus infection and the dangers of phishing expeditions.

Citizens, consumers, politicians, law enforcement agencies, and security professionals come together with KnujOn [2] to expose Internet spammers. KnujOn (which is "No Junk" spelled backwards) is an online service that sorts junk mail, compiles information on spammers, and attempts to identify domain names associated with spam activity.

According to the website, KnujOn has helped shut down over 200,000 junk email sites. Law enforcement organizations use KnujOn's extensive spam database to search for illegal activities, and many corporations use KnujOn's services to protect their brands. For instance, a drug company or a bank can use KnujOn's services to chase down knock-off products and services that illegally infringe on registered trademarks. The participants who send their junk mail into KnujOn also benefit by shutting down spam sites and reducing the volume (and effectiveness) of spam on their own networks.

How KnujOn Works

The Internet Corporation for Assigned Names and Numbers (ICANN) delegates the name assignment within the generic top-level domains such as *.com*, *.net*, *.edu* to separate organizations called registries. Registrars such as VeriSign are given authority to hand out domain names, and they subcontract part of the business to resellers that range from Yahoo to hosting providers and local ISPs. Every piece in the chain is governed by policy documents, such as the RAA (Registrar Accreditation Agreement), Acceptable Use, and Memorandum of Understanding. The policy world for the Internet is complex and not well designed (see Figure 1). Numerous channels are available to bad actors for infiltration and participation.

Through this chain of contractual arrangements, ICANN maintains an agreement with all domain name registrars that states that the information provided by a registrant must be accurate; if not, the registrar must notify the registrant of the need for a correction. If the information is not corrected, the domain name is suspended.

Although the sending address in a spam message is almost always fake, spammers still use registered domain names all the time for fake web pages, cross-site scripting, and other nefarious purposes. To avoid detection, these cyber criminals often provide false information in domain registration forms. By tracing down the domain names used by spammers, KnujOn uncovers false information and compiles data on suspicious activities. This information then becomes evidence for an official complaint filed with ICANN to suspend the spammer's use of the name.

KnujOn offers several alternatives for a user (called a client) who wishes to participate [3]. A general membership is free for any user who wants to forward junk mail to the project. For US$ 27 per year, the user receives a bit more individual attention, with a personal reporting address and regular status reports. Numerous participants have contributed freeware to help with various mail clients that will collect spam and email it to a client's unique address. For instance, The Thunderbird mail client has a KnujOn add-on [4]. Users also can FTP their spam to a general KnujOn address.

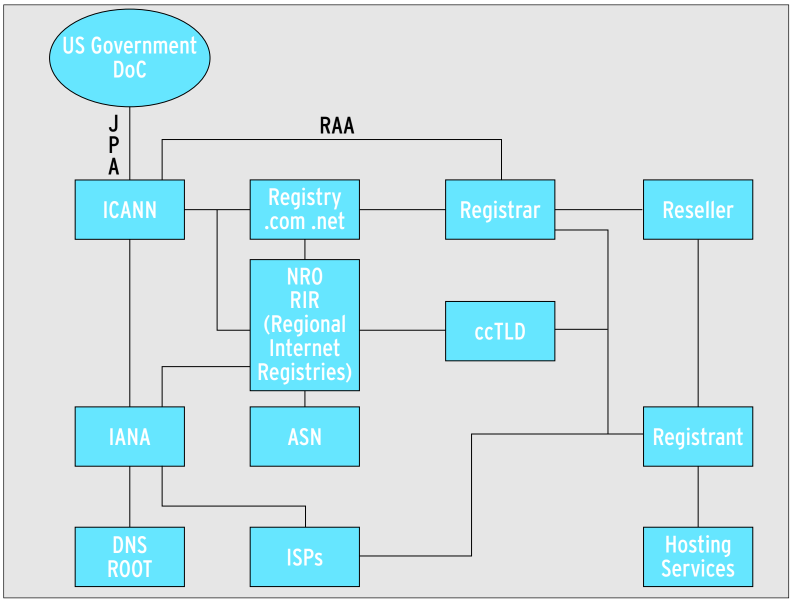

Figure 1: The Internet is a complex set of organizations, relationships, and policies.

The user's spam messages arrive at KnujOn in the form of an mbox mail file. The mbox file then moves to another machine, where a series of scripts splits each mbox and decompresses any attachments, such as ZIP, TAR, and RAR files, to produce single email instances. The resulting files are renamed – because spammers do all sorts of things to file names to slow down processing – then they are moved again to client directories for the next step, which involves finding the transaction or landing site where unsuspecting users end up when they click on what appears to be a legitimate link.

Once a site is discovered, KnujOn performs checks on the information associated with the site, including a whois check, and the results are aggregated for automated bulk complaint filing with ICANN. Criminals rarely tell the truth and rarely correct faulty whois data, so the complaint often results in the suspension of the domain name.

KnujOn ran alpha tests for about 18 months with great success. People who were receiving a large amount of spam stopped receiving spam. KnujOn then moved to beta testing by opening up the process to a larger audience, again with success, but by now spammers were sending nasty-grams, and they started to evolve to protect themselves.

In July 2006, KnujOn went live. The larger number of participants required a data center with more computers and software to manage the process. For a lack of funding, the data center was made as inexpensive as possible; therefore, with a few exceptions, the computers run Linux, and the software is mainly written in Perl. A few Microsoft systems perform part of the processing, but these systems have moved to virtual machines with VirtualBox on Linux. Lucene and the Java-based Nutch are used for search engine functions. This operation would not exist without open source software.

Results

KnujOn's system for filing complaints about junk mailers worked quite well; however, ICANN initially was not prepared for the number of complaints. Their limit was about 4,000 per day, whereas KnujOn discovered upward of 10,000 inaccuracies per day. KnujOn exceeded the capacity of ICANN's compliance engine and database in early 2008. In 2009, ICANN rolled out a new complaint system, which allowed for the option of bulk complaints.

Spammers started to register large numbers of domains, so that if one domain was suspended, another could take its place. With the use of fast-flux and domain tasting, they made their operations more robust. In 2007, three registrars were responsible for 30,000,000 new domain names, mainly the five-day, free, domain-tasting types. ICANN has since stopped this practice. KnujOn also uncovered a number of loopholes in the RAA agreement signed by registrars. In early 2009, many of these loopholes were closed as amendments to the RAA.

KnujOn eventually discovered that roughly 85 to 90 percent of all spam sites are registered with 10 to 15 registrars. Brian Krebs of the Washington Post, in his Security Fix blog, published the first Top Ten Worst Registrar list in May 2008 [5], with a huge effect on the industry. When the second list was published in February 2009 [6], eight of the original members were off the list because of process improvements, lost business (the sunshine effect), breach notices from ICANN, and deaccreditation.

Conclusion

ICANN's At Large Advisory Committee (ALAC) recently invited KnujOn to become an At Large Structure (ALS), which means that KnujOn now has a formal channel of input into ICANN's policy work. KnujOn helped reveal that spam is merely a gateway to a vast assortment of criminal activities, such as phishing, illegal online pharmacies, malware, and botnets. Proper policies at all points in the Internet are critical to keeping systems safe. Transparency and whois accuracy can make a significant difference in how much of our resources are wasted by criminal behavior. ■

INFO

[1] Electronic spam: *http://www.spamlaws.com/state/ca.shtml*

[2] KnujOn: *http://www.knujon.com/*

[3] KnujOn Registration Options: *http://www.knujon.com/register.html*

[4] KnujOn Thunderbird Add-on: *https://addons.mozilla.org/en-US/thunderbird/addon/2824*

[5] "Most Spam Sites Tied to a Handful of Registrars" by Brian Krebs, *The Washington Post*, May 19, 2008: *http://voices.washingtonpost.com/securityfix/2008/05/*

[6] "Report: Most Spam Sites Tied to Just 10 Registrars" by Brian Krebs, *The Washington Post*, February 4, 2009: *http://voices.washingtonpost.com/securityfix/2009/02/*