Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

AVOIDING THE WHACK-A-MOLE ANTI-PHISHING TACTIC

By: Douglas Otis, Advanced Threats Researcher

Imagine playing a whack-a-mole game where the mole moves to a different hole in the amount of time it takes one to raise and lower a mallet. Instead of just six holes, however, there are millions.

Few would want to play such a game. People would rightfully conclude that random attempts to hit the mole would improve their chances. With so many holes, the mole will proceed unabated, except in the rare cases that it does get hit. Stopping phishing attempts is similar to playing such a game.

Only a small amount of time lapses for reputations to accumulate and propagate. To help deal with this, ADSP, an extension of DKIM, allows Author Domains to make assertions about whether they would use DKIM to sign all of their outbound email messages or not. This provides recipients an immediate basis to decide whether to reject an unsigned email message or not.

Normally, an email message is accepted after checks are made against the sources' reputation. As in the whack-a-mole game, the amount of time given for one to react with a mallet is comparable to the amount of time allotted for reputations to accumulate then propagate. To help deal with this, Author Domain Signing Practices (ADSP), an extension of DomainKeys Identified Mail (DKIM), allows Author Domains to make assertions about whether they use DKIM to sign all of their outbound email messages or not. This provides recipients an immediate basis to decide whether to reject an unsigned email message or not. Unfortunately, simply asserting all messages are signed prove inadequate since there are many cases wherein third-party services invalidate signatures. To overcome doubts about whether unsigned email messages—messages that may have been modified by third-party services—should be rejected or not, the assertion "discardable" was created.

Although discardable assertions convinced many email servers to refuse noncompliant messages, others took this as permission to accept then discard the said messages. This created a problem for mailing lists that represent a third-party service that normally invalidates DKIM signatures. Mailing lists will accept properly signed messages but in the process of flattening and of providing related links and subject line tags, the DKIM signature added by the author's domain is invalidated. The mailing list then has trouble delivering messages for Author Domains making the ADSP assertion discardable when recipients rightfully refuse messages. For some, when the mailing list determines that there are delivery issues for a particular subscriber, the subscription is made inactive.

Rather than unsubscribing those who reject noncompliant discardable messages, the Author Domain that makes this assertion and sends messages to the list needs to be excluded instead. This forgives those who decline unsigned discardable messages and instead holds those sending them responsible. Domains making the ADSP discardable assertion are then advised to send their messages using subdomains that do not make problematic ADSP assertions.

TREND MICRO

Unfortunately, using different domains to differentiate practices will result in increased phishing, which draws into question the entire ADSP effort. Phishing will increase because recipients will become confused. They will not know what to trust and will not understand the significance of URI hierarchy but instead will see a profusion of similar domains. This means that whenever a domain wishes to utilize this type of third-party service, their only alternative is to use more domains or subdomains to differentiate their practices. Doing so then allows any unsigned source to send messages on their behalf using any of their unprotected domains.

The TPA-Label scheme could proactively contain the phishing problem without employing more domains. It represents a specific authorization strategy using a single DNS transaction that is checked whenever a noncompliant message is encountered. The authorization is based on hashed labels.

It would be better to proactively contain the phishing problem without employing more domains. The TPA-Label proposal allows just that to happen. All Internet service providers (ISPs) should do what many already do with respect to verifying control over different *From* email address domains. At this time, it is not practical for ISPs to impose restrictive ADSP practices that would negatively affect the usefulness of their services.

However, let's say that one of their customers wishes to protect messages related to their small office/home office (SOHO) online flower shop business by using an ISP's DKIM service.

To do so, they make the ADSP assertion *dkim=all tpa-sig;* for their domain *soho-flower.com* even though the virtual private server (VPS) running their online business does not offer customer-specific DKIM signing. As suggested, they want to utilize their ISP's DKIM signing account that receives messages for *soho-flower@isp.com.* Before the ISP allows them to send messages whose sender (*From* field) is not *soho-flower@isp.com,* a ping-back must confirm access to the different *owner@soho-flower.com* email address.

The *L* scope requires the authorized domain to include its List-ID header field. This additional header field enables message sorting of sources into their own folders, a tactic that offers protection from look-alike domains.

The *L* scope requires the authorized domain to include its List-ID header field. This additional header field enables message sorting of sources into their own folders, a tactic that offers protection from look-alike domains. To send messages in conjunction with *owner@soho-flower.com* using the ISP to send to the *florist-list@example.net,* the *soho-flower.com* domain must publish a TPA-Label with an *F* scope for the ISP's DKIM domain and a TPA-Label with an *L* scope for the mailing list domain. Any number of third-party services could be added in the same fashion. This scheme does not expect the ISP or the mailing list to change its process or the recipients to know which subdomains are trustworthy and which are not.

The TPA-Label scheme represents a specific authorization strategy using a single Domain Naming System (DNS) transaction that is checked whenever a noncompliant message is encountered. The authorization is based on hashed labels. If *soho-flower.com* wishes to subscribe to a secret mailing list that does not advertise the signing domain used, the TPA-Label scheme would only offer authorization to message recipients. The SHA-1 hash size makes guessing this name impractical.

Also, the job of publishing the list of TPA-Label authorized domains can be delegated to a different entity such as a small business consortium for the local region. A draft of this proposal can be found at http://tools.ietf.org/id/draft-otis-dkim-tpa-label-05.html.