

Re: RFC: virus handling

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-02/0018.html>

From: Jeremy Mates (jmates_at_sial.org)

Date: 01/28/04

Date: Wed, 28 Jan 2004 10:07:44 -0800

To: bugtraq@securityfocus.com

* Thomas Zehetbauer <thomasz@hostmaster.org>
> *To allow filtering of these messages they should always carry the text*
> *'possible virus found' in the subject optionally extended by the name of*
> *the virus or the test conducted (eg. heuristics).*

I prefer the term 'malware' instead, to avoid the various worm/virus/
trojan horse/Microsoft Windows distinctions that can be made.

The 'possible virus found' statement might actually work for some
English speakers where the malware in question was not forged from some
other system not under the control of the recipient in question.

Personally, I prefer discarding all malware, and would love to see e-
mail forwarding break in favor of Sender Permitted From (SPF):

<http://spf.pobox.com/>

> *The notification should never include the original message sent as*
> *otherwise it may send the worm/virus to a previously unaffected third*
> *party or re-infect a system that has already been cleaned.*

Without even the full message headers to figure out where the message
originated from?

> *It seems that this worm is trying to avoid people getting treacherous*
> *non delivery notifications by using obviously faked but otherwise*
> *plausible e-mail addresses. This may cause double bounce messages or*
> *even message loops at badly configured sites.*

Some sites configure their e-mail systems this way to prevent 'RCPT TO'
scans from revealing all valid e-mail addresses. Others may use
forwarding services, where the forwarding service has no means of
guessing what addresses the site in question allows.

> *Virus filters should therefore be designed and implemented before*
> *checking the legitimacy of the intended recipient. This would also*

Re: RFC: virus handling

SecurityFocus Bugtraq: Re: RFC: virus handling

- > *avoid helping the virus spread by bouncing it to a previously*
- > *unaffected third party.*

What, instead of a quick 'EHLO, MAIL FROM, RCPT TO, User unknown' a site instead has to accept every message, scan it for known malware, and then figure out what to do? I do hope this is not what you are recommending.

- > *Providers should provide an adequately stuffed abuse role account to*
- > *allow the affected users beeing notified. To ease efficiency messages*
- > *sent there should include the IP address, the exact time and date of*
- > *the incident and the name of the virus on the subject line.*

Which name of the malware? Worm.SCO.A? MyDoom? Other? What if the IP address turns out to be a e-mail relay? Where does one find the original infected Microsoft system without the full message headers? What if the mailing list stripped out the previous headers? What if the malware starts forging the received headers?

- > *Additionally providers should provide e-mail aliases for the IP*
- > *addresses of their customers (eg. customer at 127.0.0.1 can be reached*
- > *via 127.0.0.1@provider.com) or a web interface with similiar*
- > *functionality. The latter should be provided when dynamically assigned*
- > *IP addresses are used for which an additional timestamp is required.*

Expensive and hard if not impossible to implement at larger sites. Would be prone to spamming, and false notifications about e-mail relays that are not yet catching the latest in malware. And downright useless if the user does not know or care what their Windows system is doing, is on vacation, or whose open wireless network is letting someone else release malware to the Internet.

- > *Providers should grant their customers some grace period to clean*
- > *their infection and should thereafter be disconnected entirely or*
- > *filtered based on protocol (eg. outgoing SMTP) or content (eg.*
- > *transparent smarthost with virus scanner) until they testify that they*
- > *have cleaned their system.*

Others null route infected hosts first (thereby stopping the flow of malware) instead of waiting. This allows one to close off any open wireless networks one does not otherwise have the policital clout to properly disable:

1. Install Microsoft Windows on a laptop.
2. Infect said system with various malware.
3. Connect to open wireless network.
4. Wait for Network Operations to close wireless network port down.

SecurityFocus Bugtraq: Re: RFC: virus handling

- application/pgp-signature attachment: stored