Global Information Assurance Certification Paper

Virus Hoaxes to Virus Reality: Social Engineering and Malware Propagation

Charlotte Blackmer
SANS GIAC Security Essentials (GSEC)
Version 1.4b, Option 1
January 21, 2004

Overview

"Social engineering" in the inbox is no new concept to any email administrator who has had to deal with a proliferation of chain letters and virus hoaxes, but the additional threat of a malicious payload (and compromises in system availability and integrity) increases the stakes. As awareness about fast-spreading mass-mailer worms has increased and technical defenses have evolved, malware writers have started employing heavier-hitting social engineering tactics, especially impersonation of a trusted authority, to ensure that their mail gets noticed and their attachments get opened. Two recent mass-mailer worms, MiMail.A and Swen (aka Gibe) faked authority convincingly and otherwise improved upon previous hoax and malware attention-getting efforts. Their wide distribution and thus "success" in malware and hoax terms means that the tactics will be repeated in the future. In order to prevent or contain incidents successfully, administrators must look beyond purely technical solutions; a well-thought-out user policy and education program is an increasingly important part of a "defense in depth" strategy.

Some Social Engineering Basics

"Social engineering," in its broadest forms, has probably been around as long as there have been people living in groups. In the computer security world, it generally refers to attempts to trick people into performing some act that compromises computer security (e.g., reveal account info, grant access, install a backdoor or other malware that allows the social engineer to gather info).[1] Notorious (and now reformed) cracker Kevin Mitnick was not alone among social engineering experts when he said that it was easier to manipulate people than technology as a means of gaining access.[2]

Most forms of social engineering (SE for short) play on trust,[3] commonly impersonating someone with at least a plausible "need to know" (a coworker) or

[1] Gragg, David. "A Multi-Level Defense against Social Engineering." Page 4. SANS Reading Room, December 2002. URL: http://www.sans.org/rr/papers/51/920.pdf
[2] From a BBC Online interview cited by Radha Gulati in "The Threat of Social Engineering and Your Defense Against It." SANS Reading Room, 2003. URL: http://www.sans.org/rr/papers/51/1232.pdf
[3] Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." Security Focus Online, December 18.2001. URL: http://www.securityfocus.com/infocus/1527 and Gragg, page 5.

a figure of authority. Social engineers then either work on exploiting the target's desire to be helpful[4] (this is especially true with helpdesks, who are paid to be helpful) or their conditioning to respond to authority[5], with or without explicit threats. This is known in SE circles as creating a "strong affect," which is a psychological term for a strong emotional trigger.[6] Almost everyone who has worked in systems support has his/her stories of those who have screamed abuse or threatened (implicitly or explicitly) to use their authority (or report "up the chain") to get their request serviced, and most company helpdesks have their "VVIP" (Very, Very Important People) lists -- lists of people whose requests must be attended to Right Away. This can easily be exploited by the potential social engineer; obtaining the likely VVIP names has never been difficult (switchboards were usually happy to oblige) and is even easier in this era of company web pages.

Social Engineering in Action: Chain Letters and Virus Hoaxes

Chain letters were annoying to many even before the Internet was a gleam in DARPA's eye.[7] Similarly, "urban legends" have been around scaring (and annoying) people for a long time. With the proliferation and ease of use of low-cost electronic mail, however, their circulation has exploded. Very little actual cost and effort is required to send the message along.

Not long after email became a feature in many American workplaces, the virus hoax chain letter (a sub genre of the hoax or urban legend phenomenon) became widespread. (US-DOE CIAC documents email virus hoaxes back to 1988,[8] but relatively few people had email then.) "Good Times"[9] was first spotted in December of 1994 and threatened to wipe out the computer of anyone who merely read a message with a particular subject, and then forward itself as if by magic. It did spread like wildfire through the world … manually forwarded by thousands of frightened people who wanted to be helpful and prevent this from happening to others. (This was, of course, years before malware exploited security flaws in Microsoft software to do the mailing itself.)

Hoaxes, since they have no technical payload, rely on the recipients for their propagation and are thus an excellent place to see social engineering techniques in action.[10] Many "debunking" sites have specifics of various hoaxes, but, as

---

[4] Gragg, page 5.
[5] Gragg, page 9.
[6] Gragg, page 6.
[7] Watrous, Donald. "Chain Letters" (last update 12/30/03). URL: http://www.cs.rutgers.edu/~watrous/chain-letters.html
[8] US-DOE Computer Incident Advisory Capability (CIAC). "History of Virus Hoaxes." CIAC Hoaxbusters site. URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#history
[9] US-DOE CIAC. "Good Times." CIAC Hoaxbusters site. URL: http://hoaxbusters.ciac.org/HBMalCode.shtml#goodtimes
[10] Coffman, Charles. "Gotcha! Virus and E-mail Hoaxes." SANS Reading Room, January 3, 2003. URL: http://www.sans.org/rr/papers/19/871.pdf

CIAC notes, most hoaxes contain technical sounding language (the more technical, the better to deceive the target) and all rely on credibility by association. As with chain letters, the virus hoaxes can be broken into three basic parts: a hook (to get the reader interested – in virus hoaxes, it's usually the "Virus Alert" subject); a threat (to stimulate "strong affect"); and a request (that keeps the chain going).[11]

While virus hoaxes do not contain malicious code, they can create non-imaginary computer problems; a user may be instructed to remove a system file, email servers get jammed, and overworked systems support staff must calm hysterical users. (As merely one example, my Exchange environment was unusable for some hours once when someone dutifully forwarded a hoax to everyone in the 12,000+ user address book, as instructed by the message, and others "helpfully" replied to all that it was a hoax.)

"Good Times" was widely derided (the "Bad Times" parody got fairly widely spread in response[12]) and is not much in circulation these days, but its descendants are still spotted frequently. Some hoaxes invoke antivirus companies as the "authoritative" source for the horrible news that "THERE IS NO REMEDY!!!!!." CNN and other news organizations also get their names taken in vain. Many hoaxes follow the same cookie-cutter formula, only changing the "authorities" and the information (or techno-babble) about the dire computer consequences involved. Some hoaxes have been modernized to include web site addresses for the authorities falsely invoked. Of course they are counting on people clicking "forward" and not stopping to fire up a browser. (Sometimes people who fall for the hoax decide to "help" by providing those – without checking it out themselves, of course.)

Case Study: "Good Times" for Hoaxers

The original "Good Times" hoax is as good an example as any of how virus hoaxes evolved quickly to become more "authoritative" using the rapid-distribution medium of Internet email.

The first variant of the hoax[13] more or less said "Beware of a mail message titled 'Good Times.'" After it circulated (and CIAC issued a bulletin identifying it as a hoax), someone took the original concept (a fake warning about a message titled "Good Times") and decided to make the warning more authoritative:

> The FCC released a warning last Wednesday concerning a matter of major importance to any regular user of the InterNet. Apparently, a new computer virus has been engineered by a user of America

[11] US-DOE CIAC. "How to recognize a hoax." CIAC Hoaxbusters site. URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html#what
[12] Yamamura, Motoaki. "Bad Times." Symantec Security Response. URL: http://www.symantec.com/avcenter/venc/data/badtimes-hoax.html
[13] US-DOE CIAC. "Good Times."

```
Online that is unparalleled in its destructive capability.  Other,
more well-known viruses such as Stoned, Airwolf, and Michaelangelo
pale in comparison to the prospects of this newest creation by a
warped mentality.
```

The "full faith and credit" of a Federal agency is invoked as the source, and "credibility by association" is also gained by using names of previously widely publicized viruses.

An even later version of the hoax increased the technical jargon content,[14] playing on most people's general ignorance of what was going on inside the computer, and lending credibility by "precise" language ("nth-complexity infinite binary loop").

"Credibility by association" was also gained by the wide list of forwarded addresses, especially when computer professionals (or those working for prestigious companies such as IBM, even if in non-technical positions) were taken in and forwarded the message with their "authoritative" email addresses and/or titles. (The latter contributed towards what Rob Rosenberger, another pioneer in virus hoax debunking, calls "False Authority Syndrome"[15]. Anyone with a vaguely computer-related job was presumed an expert.) My personal observation during the early days of internet email coming into widespread use was that many new email users quite willingly suspended disbelief for anything they received in the new, exciting, high tech medium of e-mail, thus providing a fertile ground for hoaxers. The medium itself loaned credibility, as it were.

Evolution of Malware Propagation

Deception has long been a part of malware propagation. Back in the old BBS days, the files would masquerade as utilities or games, or attach themselves to legitimate programs. As email, PC networks, Microsoft Office (including Outlook) with its macro capabilities, and Internet Explorer software became nearly ubiquitous in business and even home environments, malware started spreading much more rapidly.[17]

---

[14] Wells, Joe. "How to Spot a Virus Hoax." IBM Antivirus Research Institute. URL: http://www.research.ibm.com/antivirus/SciPapers/Wells/HOWTOSPOT/howtospot4.html

[15] Rosenberger, Rob. "False Authority Syndrome." Vmyths.com. URL: http://www.vmyths.com/fas/fas1.cfm

[17] Peyton, Elizabeth. "Corporate Anti-Virus Protection: A Layered Approach". SANS Reading Room, August 6, 2003. URL: http://www.sans.org/rr/papers/60/1251.pdf (and personal observation at employer's, Emeryville, California)

"Melissa"[18] was a smash success in virus terms; it spread rapidly and made international headlines for days because it temporarily shut down the mail operations of companies both large (and prestigious) and small. It also changed the prevention game in an attention-getting way since the formerly false portion of the hoaxes about the message auto-forwarding itself to people in your address book/inbox became true to a large extent.

It also got the attention of a lot of malware writers. Security holes in Microsoft software that allowed some infected attachments to auto-launch without user intervention were discovered and gleefully exploited. (Most still required some sort of user action, however.) The large installed base of Microsoft software ensured better likely results based on the numbers and the percentages. Actual programming skill of some sort was no longer required due to the wide availability of "kits" on the burgeoning World Wide Web. Additionally, because Microsoft was (and still is) regarded as an evil Goliath by the hacker, cracker, and "script kiddie" communities, many David-wannabes can't resist trying to take shots. The end result was that the self-mailing worm became one of the most common virus threats to the average computer user, and they appeared with increasing frequency. Were Andy Warhol still alive, he might very well say, "On the Internet, anyone can be famous for fifteen minutes" (by writing the next worm).

Evolution in Defenses

The rapid spread of these mass-mailer viruses caused many organizations to reexamine their virus protection strategy. Before "Melissa", very few organizations scrubbed email (because it slowed delivery), and a monthly pattern file update for file servers and workstations was standard. Antivirus vendors responded to the new challenges by coming out with improved products, including quicker scanning, content management capabilities, and the ability to rapidly deploy updates. Many organizations purchased a gateway machine that checked and removed ("scrubbed") viruses before they hit the main e-mail system. The extremely rapid spread (counted in hours) of new variants also caused more and more sites to drop all attachments with suspect extensions (such as .vbs) at their gateway. This ensured systems availability even if the antivirus pattern update lagged slightly behind the virus' arrival.

Microsoft, which had a laissez-faire attitude towards security in the beginning, released product updates that had better inherent security (such as Outlook 2000 SP2, which would not execute files with certain extensions) and became much more security-conscious and proactive in "spreading the word." In addition, the mainstream news media (not just the specialized computer press), especially their Web-based news sites, became "part of the solution" by covering major

[18] Symantec Corporation. "Melissa." Symantec Security Response. URL: http://securityresponse.symantec.com/avcenter/venc/data/w97m.melissa.a.html

virus outbreaks as news stories. This had the beneficial effect of increasing awareness outside the technical community.

And after numerous rounds of mass-mailer worms, even some of the proudly computer-illiterate started getting the idea that it wasn't a good idea to open up a file unless you were specifically expecting one. A married-with-children middle-aged woman who was not interested in tennis might suspect a problem if someone sent her a picture of Anna Kournikova or his "Sexy Wife" (the latter would be doubly suspicious if from a female sender), just as her husband might be suspicious if he started getting "I love you" letters from his golf buddies. They might be as likely to phone the sender and say, "Do you have a virus?" (or something ruder) as to open up the file.

Sender Line Impersonation as a Means of Circumventing Defenses

The next major landmark in malware propagation came with Klez,[19] which chose the sender address randomly based on the content of the victim's address books, thus causing aggravation for both the recipient and some innocent third party. It disguised or "morphed" the true source (Internet header-reading still being a specialist skill), so the infected person might not be aware for some time that his system was compromised. Because this trick ensured that confusion and frustration reigned (helpdesks and support staff got many aggravated calls from the innocent alleged "senders," as well as from the recipients who didn't know it had been morphed), many malware writers took note, and reprogrammed sender lines with great energy. (Indeed, among email administrators, the phenomenon became known as being "Klezzed".)

As more and more seemingly random email sent by strangers (actually mass-mailer worms) clogged up inboxes, some writers took a different approach to the "sender" trick. Choosing an address from a well-known Internet-related business was easier to program than "random" and was far more likely to get *delivered*, due to the possibility of bad addresses in cache, and *read*, since many recipients learned to trash unexpected attachments from strangers. Letters faked to come from Ebay[20], Hotmail, and other well-known companies warning the user that his/her password would expire unless a form were filled out and returned (strong affect, or attempting to panic the recipient again) became common. (Information in the form, containing credit card or other information, would be mailed back to the malware writer and used in identity theft). But some of these had a necessarily limited audience: someone who doesn't use Ebay is not going to fall for "your Ebay account is expiring," and the vendors themselves increased their publicity efforts in getting the word out about the scam (usually by prominent

[19] Trend Micro Corporation. "Worm_Klez.H." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?Vname=WORM_KLEZ.H
[20] Trend Micro Corporation. "Worm_Cayam.A." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_CAYAM.A

notices on their websites). Some writers, however, took note of what was out there and “improved” upon it.

Impersonation Case Study #1: WORM_MIMAIL.A

Worm_MiMail.A[21] forged its return address as the target's own administrator (admin@domainname is a standard address that many organizations use), and the subject line was "your account" (followed by a random string of characters designed to defeat subject line filters). That, despite the oddness of the random characters, was a "Read This Message Now" hook of the first order.

The message itself was designed to get the full and undivided attention of all its recipients, including the most jaded fun-file and/or chain-letter hater:

```
Hello there,

I would like to inform you about important information regarding
your email address. This email address will be expiring.
Please read attachment for details.

---
Best regards, Administrator
---
Attach: message.zip
```

Most people would be both surprised and panicked by this message because they have grown dependent on their email. Many dutifully double-clicked the self-extracting attachment sent by this extremely authoritative source to learn the details. Perhaps they were thinking that they were going to call and complain about such arbitrary behavior, but they wanted to see what was in the file first; perhaps not. Perhaps they just panicked and didn't stop to wonder about the odd extra characters. In any of these cases, the malware spread.

MiMail.A was cleverly constructed in more ways than one. Besides the universally applicable (but subtle – a great improvement on "the sky is falling" exclamation-point-laden virus hoax messages) message designed to create panic, forging an "internal" address ensured that it would get through many spam or content filters. The payload was in a .zip file, which many administrators were still allowing through their gateways (as opposed to .exe, .vbs, and a host of other suspect extensions), suggesting that the writer had an awareness of some standard defensive measures then current.[22] (Similarly for the odd subject line characters.) And the fact that many antivirus gateways would still deliver a mail message even if a viral attachment were "defanged" caused work for administrators even if they stopped the virus at their gateway; people who couldn't get the attachment to open called the helpdesk or wrote the administrator in a high state of panic (or dudgeon).

---

[21] Trend Micro Corporation. "Worm_MiMail.A." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMAIL.A

[22] One excellent list is Exchange MVP Martin Blackstone's "List of Danger." URL: http://www.swinc.com/resource/exch_faq_appxj.htm. Microsoft Outlook versions with extension-blocking capabilities were also commonly installed by that time, at least in many business environments.

Impersonation Case Study #2: SWEN/GIBE

The person or persons responsible for Swen (aka Gibe)[23] took advantage of the weeks of publicity about the MS-Blaster/Nachi worms. Many home (and business) users who had never heard of "security patching" before had the necessity of doing so impressed upon them in quite dramatic fashion - rebooting machines, ISPs unreachable, work networks slow or just unusable. The Swen author(s) also took advantage of Microsoft's post-Code Red/Slammer security attitude; Microsoft had been very much front and center in the mainstream media and computer press immediately before and during Blaster. There had been previous viruses that had masqueraded as Microsoft security patches that had not achieved very widespread circulation for a variety of reasons, mostly because the accompanying text was poorly constructed and thus not particularly convincing, but at least partly because awareness about patching was not high in the general public before Blaster.

The sender names and subject lines of the messages that got sent were cleverly engineered, once again, to grab the attention of just about everyone. They were randomized to defeat subject-line filters,[24] but included:

From: MS Customer Service
Subject: Internet Critical Patch

From: Microsoft Security Service
Subject: Latest Security Update

From: MS Corporation Security
Subject: Newest Net Security Update

The above examples are taken from the hundreds of copies delivered to my personal mailbox. I was impressed by the "hook" caused by the faked sender and subject lines even though as a systems professional I knew full well that Microsoft never sends files except in response to a support call. Sometimes the worm would disguise itself as some sort of message delivery failure with the same payload, which is also clever since many people will open up such messages to figure out what went wrong.

Blaster/Nachi had affected many companies as well as many individuals, and was in the news for some days, so awareness that security patching was a necessity for Windows users was at a new high. Who could know better than Microsoft what was required? Who could be more authoritative? And wasn't it

[23] Trend Micro Corporation. "WORM_SWEN.A." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SWEN.A
[24] Symantec Corporation. "W32.Swen.A@mm." Symantec Security Response. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.swen.a@mm.html

nice of them to send along the information? (And, of course, the Microsoft return address would not be blocked as a sender by gateways.)

The message text itself was much, much more sophisticated than previous virus-generated or hoax email, which is usually rife with poor grammar and spelling, odd random text strings to try to defeat text filters (spam, or unsolicited bulk email, had also become a problem, so text filtering was common), and dire threats with much use of capital letters and exclamation points. The “install this now or your computer will have problems similar to Blaster” threat was only implied, and in the most business-like, professional language possible. To complete the impersonation, the letter was no doubt constructed with “watermarks” (electronic graphics) stolen from MS’ own site. According to antivirus vendor Sophos,[25] the message text itself was randomized (no doubt to defeat attempts to content-filter it at gateways; anti-spam programs had also become common in business installations), but the following[26] is one variant:

[25] Sophos Corporation. “W32.GibeF.”
URL: http://www.sophos.com/virusinfo/analyses/w32gibef.html
[26] Source for graphic: Symantec (URL above).

Microsoft

All Products | Support | Search | Microsoft.com Guide

Microsoft Home

MS User

this is the latest version of security update, the "September 2003, Cumulative Patch" update which eliminates all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express. Install now to maintain the security of your computer from these vulnerabilities. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us.

Thank you for using Microsoft products.

Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

Contact Us | Legal | TRUSTe

Only experienced PC support professionals were likely to know that 1) different patch executables are required for different Microsoft operating systems and 2) Microsoft isn't providing patch support for some of the operating systems named. As expected, many people who either hate all the chain letters or had learned the hard way to not open every "fun file" that came in their mailbox thought "This looks real, and it's a good idea" and clicked away, wishing to protect their machine.

The professional quality of the forgery was no doubt a large factor in why Swen/Gibe "succeeded" (in virus terms) where previous attempts to hijack

Microsoft's identity had failed by not achieving wide circulation. Contrast the above with the text of the "Dumaru" worm:[27]

```
From:  "Microsoft" security@microsoft.com
Subject:  Use this patch immediately  !

Message:
Dear friend , use this Internet Explorer patch now!  There are
dangerous virus in the Internet now!   More than 500.000 already
infected!
```

The above message, in text format (no watermarks), with its unbusinesslike language and poor punctuation, would not inspire confidence that it really came from Microsoft in most native English speakers.

"Defense In Depth" – Necessary Now More Than Ever

MiMail.A and Swen/Gibe are still circulating and will by no means be the last of the "faked authority" worms. Indeed, "patch now" post-Blaster messages have appeared since Swen/Gibe was introduced; one even went back to the "virus hoax" roots by "forwarding" a message alleged to have been sent by a Microsoft customer support employee.[28] Microsoft software is still widely installed, and vulnerabilities are being exploited on an accelerated timeline.[29] As an additional factor, many corporate users have VPN or other remote access capabilities from their home machines (usually outside the company defenses) and a problem at home can quickly spread to the work environment. User education has often been neglected in the enterprise[30], but is an increasing necessity given the easy ability to impersonate a trusted sender and the additional threat posed by remote access. If users are savvy, not only will "problems at home" not become "problems at work", a level of defense will operate even in the (hopefully) rare event that the virus arrives before the antivirus vendor has released a new pattern.

A list of suggestions on how to deal with both the technical and "people" sides of the issue follows. Administrators should implement as many as feasible:

1. Virus-scanning gateways (whether a server such as Trend's Interscan, an appliance such as McAfee's Netscreen, or a firewall/IDS solution like Microsoft's ISA server) of some sort are still a necessity in all but the smallest organizations, but are not sufficient. Blocking certain classes of

---

[27] Trend Micro Corporation. "PE_DUMARU.A." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=PE_DUMARU.A

[28] Trend Micro Corporation. "Worm_Yaha.AA." URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_YAHA.AA

[29] Microsoft Corporation. "Patch Management Workshop" seminar. October 15, 2003. San Francisco, California.

[30] Peyton, page 9.

file extensions,[31] preferably at the gateway level, is a necessity in today's environment. As MiMail.A showed, even attachment blocking by class is not 100% effective. Content management capability that can block specific file names or message text is an important adjunct to the "scrubber" or email virus gateway. Gateways should also be able to update their patterns from the Internet, because fast-spreading worms often arrive in the middle of the night when the organization may be unstaffed.

2. Organizations should have antivirus software on internal workstations, mail servers, and file servers as well as on the "scrubber" to catch anything that may get through to the inside.

3. Administrators and the Helpdesk (first response) should be on antivirus vendor mailing lists for incident outbreak notices.

4. The organization should have an easy (and preferably automatic) means of distributing antivirus pattern updates and new security patches throughout the company, and an easy way for administrators to tell which machines have fallen behind or are not running antivirus software at all so they can be visited before there is a problem.[32]

5. Users should be instructed to turn off "preview" if they are using Outlook, and should have more-recent versions of Outlook with built-in security features installed.

6. The organization should have a clearly formulated and enforced policy about use of personal email accounts (e.g. Hotmail, AOL, Earthlink) from business machines. Many ISPs shift the burden of antivirus to individual users, which means that work machines can become infected if infected personal mail is read on them. Proxying HTTP mail through the "scrubber" and ensuring that all workstations update pattern definitions automatically and rapidly will go a long way to mitigate any problems if "outside" account access is allowed.

7. With the increasing use of VPN and other remote-access solutions, clear rules must be communicated (and enforced) as to which remote access solutions are permitted and requirements for keeping antivirus, patching, and personal firewalls up to date on home systems. Home users should be encouraged or even required to have a modern operating system that supports "automatic updates," and to enable this feature.

---

[31] Blackstone, Martin. "List of Danger." URL: http://www.swinc.com/resource/exch_faq_appxj.htm

[32] Cisco Systems is working with several major antivirus vendors on a product (the Cisco Network Admissions Control program) that will quarantine machines not at a pre-set patch and antivirus pattern level. Press release URL: http://newsroom.cisco.com/dlls/prod_111803d.html

8. Similarly, a clear policy should be articulated about use of instant messenger and peer-to-peer file sharing programs within the organization, and any technical means possible (firewall blocks, policy scripts, etc.) should be implemented to block unauthorized program use. The firewall may also be used to prevent rogue SMTP mailers from sending mail outside the organization.

9. The organization should have a "do not forward chain letters through company email" policy, and should also tell staff to forward all warnings about computer viruses to IT/computer security for validation.

10. General information about computer viruses, computer security, and types of messages to consider suspicious (as a hoax or a virus) aimed towards a general audience should be included in employee training materials and publicized on internal web sites. Links to "hoax busting" or "urban legend" sites such as http://hoaxbusters.ciac.org/ and/or www.urbanlegends.com, to Microsoft's "How to keep your computer safe"[33] (or a similar site), and to the company's antivirus vendor should be prominent. Information about policies as per above should also be here. The materials should include some information on "best practices" for doing a scam/virus/hoax "reality check" (see Appendix A for an example) to increase user awareness that they are an important part of keeping their own email flowing freely. The materials should prominently include text that says something like "Please contact (the Helpdesk) if you have any virus-related questions" (with a mail-to link in online versions).

11. If any of the above policy/education steps are newly implemented, a "VVIP" within the organization -- such as the company president, CEO, director of information systems -- should be the one to announce it via company email, thus lending his/her authority to the enterprise. If these policies have been in place for a while, annual or semi-annual reminders (possibly including sign-off on a form) are useful.

12. The organization should have an incident response plan ironed out, including paper copies of phone numbers and other key information for important staff members and vendors, and a draft of an email message to be sent out during virus outbreaks. This message should be sent out during major publicized virus/worm events even if the company's defenses are catching the problem as a user education tool. (See a sample letter in Appendix B.[34]) As a caution in writing these messages, because different

---

[33] URL: http://www.microsoft.com/security/protect/ (available from the MS home page). As an additional note, I heard Kevin Mitnick recommend the same three steps during an interview broadcast on NPR's "The California Report" (URL: http://www.kqed.org/calreport) in early 2003.

[34] Gullett, Chris. "Computer Virus Policy, Training, Software Protection and Incident Response for the Medium-Sized Organization: A How-To Guide." SANS Reading Room, July 30, 2001. URL: http://www.sans.org/rr/papers/36/35.pdf

vendors often give the same virus different names, it's useful to put them all in the message ("also known as …"). This will cut down on confusion because users are likely to get bulletins from their correspondents (who may use a different antivirus program) during outbreaks.

Summary

Viruses, hoaxes, and defenses are constantly evolving in response to each other. As word gets out about various types of scams, threats, and hoaxes, and technical defenses get more sophisticated, malware writers will try to find new "people" angles to get "their" attachment opened. Technical means of trying to keep viruses out of the organization are still paramount; however, the increased impersonation of authority as a "hook" means that administrators cannot neglect the "people factor" and user education as part of their "defense in depth".

APPENDIX A: Sample list of tips on recognizing emailed scams, hoaxes, and viruses

[Author's note: This is my original work; however, it has been inspired by similar lists on many reputable sites, including:

CIAC Hoaxbusters: http://hoaxbusters.ciac.org/
Vmyths.com: http://vmyths.com/
IBM Security Research (link may wrap):
http://www.research.ibm.com/antivirus/SciPapers/Wells/HOWTOSPOT/howtospot4.html

Feel free to modify appropriately for internal, non-commercial use in your organization.]

Following is a "reality check" list for determining whether unexpected mail may be a hoax, a scam, or a virus. For specifics of widely circulating hoaxes, scams, and viruses, there are many resources available on the web; you should bookmark a good antivirus site (we use Trend Micro at the office, www.trendmicro.com) and a good "hoax busting" or "urban legend" site such as CIAC Hoaxbusters (http://hoaxbusters.ciac.org/) or Snopes (www.snopes.com). This is not meant to be a substitute for keeping your antivirus, security patches, and personal firewall (at home) up to date, but may save you trouble or panic.

Please do not use company email to forward any sort of chain letter. Virus-related messages you receive from outside sources should be validated against a reliable antivirus or hoax awareness site (as below) or sent to the Computer Helpdesk either by email at "Computer Helpdesk" or by telephone (ext. 4357 – HELP). Do not forward them, except to the Helpdesk for validation.

- If you're not expecting an attachment from someone you know … be very, very suspicious. Consider saving it to disk and scanning it first. Ask the person if s/he meant to send you something. If you get an attached file from someone you have never heard of… don't open it.

- Any message about "a new virus" should be checked out on antivirus vendor sites and with reliable news services such as CNN. Due to the fast-spreading nature of many real

viruses/worms, real problems WILL be reported, and antivirus vendors will probably have the update by the time you check their sites.

- The truth of **any** message that mentions an announcement or promotion by a well-known company such as IBM, Microsoft, or Disney can be verified by visiting that company's Web site and checking the news or announcements section.

- If the message offers you something for (almost) nothing, it's almost always a hoax or a scam. Pyramid scheme chain letters ("Turn $5 into $50,000") are illegal, Bill Gates and Outback Steakhouse can't track your forwarded mail and wouldn't give you money or a free dinner if they could, and those people pretending to be refugee heirs to some vast African fortune are scammers working out of Internet cafes in Lagos. Legitimate "Internet promotions" will be advertised on the company's web site, not through mega-forwarded email.

- If you receive an unsolicited "fix file" claiming to be from Microsoft or some other computer vendor, DON'T INSTALL IT. This is almost certainly a virus. Microsoft never sends out unsolicited attachments and the same is true for most vendors. It is trivially easy to "spoof" a return email address. Many vendors will PGP sign their messages. Be careful about clicking through web links provided in non-PGP signed messages claiming to be from some company since some malware writers write mail with "URL redirects" to take you to a site they control instead.

- Poor grammar, bad spelling, LOTS OF CAPITAL LETTERS, and too many exclamation points are hallmarks of hoax and virus letters. Be very suspicious, even if your best friend sent it to you.

- Any message that has odd random characters in the subject line (such as XGBHIQ) is almost certainly spam or a virus. Delete it.

- If you get several odd messages with the same subject in short order, it might be a virus. Proceed with extreme caution, especially if your email program shows there is an attachment.

- If the message claims to be from your administrator (here at work, Ebay, your bank, et cetera) and insists that you open up an attachment to confirm account details, it is almost certainly either a scam or a virus, especially if they claim the account is expiring. DON'T OPEN IT. Legitimate businesses don't work that way. Call customer support if you have questions.

APPENDIX B: Sample Incident Notification Letter

[Editorial comments in brackets]

From: Security Team
To: All Employees
Re: Computer Virus Advisory – "MiMail.A"

[Quick summary and "We're getting it" – this is a basic hook, when combined with the subject line:]

Late last night (our time) a new mass-mailer worm, "MiMail.A," started circulating around the Internet. Our Email gateway is blocking the infected files but you still may get messages (with an attachment saying that the infected file has been removed) in your Inbox.

[Some more specific information:]

The message arrives with the subject “your account” followed by six random letters (e.g. XBYZGA). It forges a return address of admin@<sitenameremoved>. Please delete all messages like this unread. If you opened one up to learn that “we” were expiring your account, please be assured that we did not send the message and we are not doing anything to your account. (As a side note, any message asking you to open up an attachment to confirm account information is likely to be a scam or a virus. Legitimate businesses have other ways of asking you this information.)

[Info about requested user followup actions – “you’re a part of it too”:]

Please ensure that your workstation antivirus is up to date (Trend pattern should be 676 or up) and be sure to update your home antivirus immediately, before you open up your personal mail or dial in to our network. Please note that many ISPs do not virus scan mail so similar messages in your home email might be infected.

[Further resources]

For more information about the virus, please consult the Trend Micro webpage at:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMAIL.A

As always, please call the Helpdesk at extension 4357 if you have any virus-related questions.

APPENDIX C – Some websites with hoax information

http://ciac.hoaxbusters.org/

http://www.hoaxinfo.com/

http://www.snopes.com/

http://vil.nai.com/VIL/hoaxes.asp

http://www.symantec.com/avcenter/hoax.html

http://www.vmyths.com/

http://www.trendmicro.com/vinfo/hoaxes/hoax.asp

http://www.urbanlegends.com/

http://hoaxbusters.org/

http://antivirus.about.com/library/blenhoax.htm

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event