Global Information Assurance Certification Paper

Case Study: 'I Love You' Virus & the $500,000 day!

By Michael G. Harrison

January 31, 2001

Introduction:

What you are about to read is a true story about how one organization got caught with their proverbial pants down. The names have been changed to protect the innocent and the idiotic. Anyone in the business of securing networks, hardware, software, applications and data in general, understands that the following true story could happen to any organization. The 'ILOVEYOU' virus has played tricks on its victims for almost a year. Yet, with Valentine's Day fast approaching, the opportunity exists for this virus to play cupid again.

Computer users simply have not learned their lessons. Even though virus software signature files, created to combat the virus, have been around since June, many users would still be the weak link in a corporate structure. According to research published by IDC this week, more than a third (37 percent) of business e-mail users would still open the attachment of an e-mail titled "ILOVEYOU' -- the same message used in e-mails infected with the Love Bug.[1] The following incident involving the aforementioned virus is real.

Facts of the Incident:

In mid November, 2000, a particular State government entity known as the Agency for Bad Decisions or ABD for short, was victimized by a variant of the well established, well traveled "ILOVEYOU" virus. I know what you are thinking, after nearly six months after the first outbreak, **how** did this government agency fall victim to its illegitimate viral cousin. A combination of events and bad decisions allowed this agency to become another casualty of information warfare. First a little background to help the average reader know what exactly went wrong. Later, some helpful hints to minimize your chances of infection, as well as protect yourself and your corporation.

First of all, what happened on the day of impact was not the real crime. The real crime occurred months prior to the viral infection. As it turned out, this agency, with users in excess of 10,000 and servers numbering in the hundreds, had made the calculated blunder of not using virus protection. Sure they had some licenses for McAfee or Norton or whatever. But they did not secure anti-virus protection to every user and machine, especially the mail server. The money that was "saved" by not spending it on anti-viral licenses for each individual workstation, was used on something else more glitzy. And of the protection that they did have, an updated **.dat** did not stay current per the industry.

Anti-virus companies, which profit when people and companies pay for precautions, have long cautioned that existing patches and anti-virus software can prevent much of the lingering threat of known viruses such as the Love bug.2 When this hole was reported to the top brass of Agency BD, the common response was simply, why would anyone want to screw around with us? After all, it's not like we are rocket scientists protecting sensitive government secrets.

What I speak of next should be the preface for the fictitious book "Virus Protection for Dummies". Here are the main ingredients to the blunder: Microsoft Windows NT Operating system, Novell Groupwise, Microsoft Outlook Express and one user. Now that I established the fact that there was minimal protection for the Agency, let's just see how it all went astray.

The user received an e-mail on November 7th, 2000 to his Microsoft Outlook Express mail account, from a known third party. This user also uses Novell Groupwise for his Agency e-mail on his desktop. The e-mail contained a message in the subject field that read, **" US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (HTTP://WWW.2600.COM)."** The e-mail also contained an attachment that possessed a randomly created 4-8 character string; whereas every even numbered character was a vowel. The extension on the attachment was **jpg.vbs**. Standard protocol for the Agency's e-mail policy is to not open any attachments from parties unknown. But this user felt that he could trust the sender. Unfortunately, what transpired in the subsequent hours became not only an infected network, but also a Distributed Denial of Service (DDOS) attack.

Electronic mail came to a screeching halt. This virus is not that different from Melissa in that it spread outrageously fast. As with Melissa, many companies' first response was to shut down e-mail systems, paralyzing operations.3 The Agency decided to do exactly that, shut down the e-mail servers and purge the post offices, thus producing a window of non-productive time statewide. Although the mail was sent to the entire Novell Groupwise address book, only a few workstations were infected. A user had to actually execute the **.vbs** attachment by double clicking on it. Thankfully, the e-mail policy worked for most places. However, one by one, the servers needed to be scrubbed to rid themselves of the message and remnants of the virus. GroupWise post offices also had to be unloaded then loaded back. So what exactly did the virus do to cause such a grandiose domino effect?

Variant Payload:

The 'ILOVEYOU' variant is capable of data manipulation and destruction. The ability to destroy data is defined directly in the virus' source code. The worm copies itself into the Windows directory as **reload.vbs** and the Windows\System directory as **Linux32.vbs** and the aforementioned 4-8 character randomly generated file ending in **.gif.vbs, .jpg.vbs or .bmp.vbs.** Then if the **Winfat32.exe** file exists, the worm randomly sets the Internet Explorer Start Page to one of the following addresses:

http://members.fortunecity.com/plancolumbia/macromedia32.zip

http://members.fortunecity.com/plancolombia/linux322.zip

http://members.fortunecity.com/plancolumbia/linux321.zip.[3]

Depending on which file is downloaded; the worm performs different actions. However, the worm utilizes MAPI calls to the Outlook Application and filters through all the addresses in the users' Outlook Express Address book. Unfortunately, in this user's Outlook Express Address book was the internal Agency Groupwise addresses. The worm began to send mail to the recipients on the Agency Address book, and from there we have our infection spreading very rapidly.

Although the payload does not render the workstation or server useless, there is significant damage to macromedia files. All **.jpg, .jpeg, .mp3, .mp2, .gif, .bmp, .vbs, .vbe, .js, .jse, .cs, .wss and .sct** are overwritten and all mapped network drives are disconnected.[4] Therefore, a webmaster might lose considerable data if the webserver becomes infected. How do you define a cost associated with hidden and overwritten files? How about lost corporate productivity?

Estimated Costs:

The hard part about analyzing actual costs of the virus is attributing the cost of worker downtime. Each worker is paid differently, thus the cost of two to three hours of non-production, is at best, estimation. After all these people are Civil Servants not rocket scientists. Lack of e-mail service constitutes a breakdown of the system. A breakdown of the system translates into lost time. The cost of lost business for such defensive actions alone could far outstrip costs attributed to previous attacks by viruses such as Melissa, which rang up an $80 million price tag. Unlike Melissa, the 'ILOVEYOU' virus has the ability to destroy data, which could drive potential costs considerably higher.[5] The virus, which originated in Manila, Philippines, is so destructive that even its suspected scripter, Onel de Guzman, could not sit in front of a computer for months due to fright.[6] Lost worker productivity is the single biggest expense in analyzing attributed costs by infection. By all estimation, the lost time for the Agency for Bad Decisions, was in excess of $250,000.00.

Additional costs increase this number to almost $500.000.00. These additional costs included the decision to **finally** purchase Norton Anti-Virus 2000 licenses for each workstation and server across the state. The price tag: $180,000.00. Add up any time spent actually filtering down these licenses, cleaning infected workstations and re-creating macromedia files that were overwritten, and this figure easily adds up to the aforementioned half a million dollars. That is tax payer dollars going to work for absolutely nothing! But this could have been avoided.

Words for the Wise:

Nearly 40% of e-mail messages coming into businesses have '***dirty***' attachments.[7] With this stated, below are some best practices defined which would significantly minimize the chance of infection:

- Use Anti-Virus software;
- Keep the virus software updated either automatically or manually;
- Design, implement, educate and enforce good corporate e-mail policies;
- Perform regular system virus scans;
- Always scan floppy disks and CDs for viruses before using them; and
- Turn off Windows Scripting Host.

I know this seems like a no-brainer, but as I stated previously, one of the causes of the infection for ABD was the fact that they did not possess anti-virus software on all workstations and servers. Additionally, the software that they did possess was not maintained properly. These two points noted above are imperative to clean computing. First of all, just utilizing the software can save personal and corporate information. There are many flavors of anti-virus software. Some virus software, like those on www.freeware.com are free, while others like McAfee and Norton come complete with all the bells and whistles. The single most important additional software to use should be anti-virus protection. Secondly, update the anti-virus software on a regular basis. Script Kiddies all work the same way. They find a hole and create a script to exploit the finding. Now that anti-virus software is on the workstation or server, keeping it current is just as imperative as the software itself.

Designing and implementing an effective e-mail policy is crucial to protecting corporate functionality. Unfortunately, what is often overlooked is the education of such a policy to the end user. All too often, when a new employee starts, corporate information may be distributed to the user, but is it really explained in detail. Usually not and the user may not fully understand the consequences of opening up e-mail attachments, especially **.vbs** attachments. Sometimes those of us in the technology sector forget about the level of competency in the workplace. Thus, proper education of policies could aid in avoiding potential, ignorant issues. Although, some people just never learn that the cute little Pokemon animation that your best friend sends you may actually be the next "I Love You" virus.[8]

Ok, the anti-virus software is on the desktop, the software is up to date and the planets are aligned. All is well with the world, right! Well if you're just loading anti-virus software for the first time, it's a good idea to let it scan your entire system. It's better to start your PC clean and free of virus problems.[9] Most of the software used for anti-virus protection contain the ability to perform automated viral scans; either at boot time or during regular intervals. Another good suggestion is to quarantine a virus if one is found. Quarantine means that the file is separated from the system. The virus is not deleted, but rather put into a **safety** zone so to speak. This is useful for forensics and identifying how the virus works.

Although nearly 85% of all known viruses are transmitted via e-mail, the old-fashioned sneaker net is still a viable entry point to the workstation or server. To minimize your chances for infection via this route, two basic rules should apply. Firstly, limit the number of users allowed on the workstation. Sounds easy, but many corporations utilize work share programs to effectively capitalize on extended work hours. Secondly, perform

a virus scan against all transportable media. Floppy disks, CDs and Zip tapes could all potentially contain viruses, which if you were only performing scans on your C:\ drive, would never be caught. Run explicit scans against any new media entering the computing environment.

Lastly, with all of the known viruses out there which exploit the vulnerabilities in Visual Basic Scripting within Windows Operating Systems, simply turn off Windows Scripting Host to limit your risk of infection.[10]

Despite all the advances in anti-virus technology, it is only as effective as the people operating them allow them to be. In the chain of computer security, human error continues to be the weakest link [11] In order to create sound protection from the evil do-ers, be smart! Never open e-mail attachments from unknown sources, be leery of ones from known sources and above all, use updated anti-virus software for all computing; whether it's e-mail or sneakernet. Protection and knowledge are the keys!

Bibliography:

1. Leyden, John "Survey: Love Letter remains seductive". The Register, February 6, 2001 2:13 p.m. PT

   http://www.securityfocus.com/news/147 (February 8, 2001)

2. Festa, Paul. "Love virus variant plagues email systems".CNET News.com. October 23, 2000, 1:10 p.m. PT

   http://india.cnet.com/news/2000/10/23/20001023m.html (December 28, 2000)

3. Festa, Paul and Wilcox, Joe. "Experts estimate damages in the billions for bug" CNET News.com. May 5, 2000

   http://news.cnet.com/news/0-1003-200-1814907.html?tag=st.ne.ni.rnbot.rn.ni (December 28, 2000)

4. Ewell, Brian. "VBS.Plan" Symantec Anti-Virus Emergency Response Team (AVERT) December 7, 2000

   http://www.symantec.com/avcenter/venc/data/vbs.plan.a.html (December 28, 2000)

5. Festa, Paul and Wilcox, Joe. "Experts estimate damages in the billions for bug" CNET News.com. May 5, 2000

http://news.cnet.com/news/0-1003-200-1814907.html?tag=st.ne.ni.rnbot.rn.ni (December 28, 2000)

6. Schmetzer, Uli " Hackers say 'love bug' was ammo in cyberwar" Chicago Tribune, February 8, 2001

   http://sns.chicagotribune.com/technology/sns-lovebug.story?coll=sns%2Dtechnology%2Dheadlines (Feb 8, 2001)

7. Festa, Paul and Wilcox, Joe. "Experts estimate damages in the billions for bug" CNET News.com. May 5, 2000

   http://news.cnet.com/news/0-1003-200-1814907.html?tag=st.ne.ni.rnbot.rn.ni (December 28, 2000)

8. De la Garza, Joel. "Five ways to protect yourself. Advice from a security a Security Expert" December 6, 2000 http://www.msnbc.com/news/496359.asp#BODY (December 28, 2000)
9. Vamosi, Robert. "Another ILOVEYOU Variant" ZDNet.com, June 9, 2000, revised October 20, 2000

   http://www.zdnet.com/zdhelp/stories/main/0,5594,2583071,00.html (December 28, 2000)

10. ibid
11. Zenkin, Denis." Protecting Your Workplace: 10 Anti-Virus Rules" Kaspersky Lab, February 5, 2001

    http://www.securityfocus.org (February 8, 2001)