I Thought We Had Virus Protection: The Mistakes that Made Us Vulnerable to the W32 SirCam Virus

Bob Green

Bob Green
GSEC Practical Assignment
Version 1.2e

I thought we had virus protection: The mistakes that made us vulnerable to the W32/SirCam@mm virus.

Background

Computer security around our office used to be pretty lax. But with the threat of systems and data compromise we realized that we needed to have more than just an old 486 running Linux acting as a firewall and a few copies of Dr. Solomon (now McAfee's VirusScan Classic) to protect ourselves.

The first step was to beef up our security against external threats with a packet filtering firewall and establishing a DMZ between our intranet and the internet. Next we selected VirusScan ASaP from McAfee to provide nearly real-time updates of virus signatures and consolidated management reporting. Finally, I was sent to the SANS Institute's Security Essentials course to become our "security expert". Of course the most important thing I learned was that "I have a lot to learn and a lot to do".

As with many SANS students, I'm sure, I came back from class knowing that there were many things I needed to do about our security, and hardly knew what to do first. Besides that my duties had not been changed, merely increased. So there I sat one fine morning when a couple of programmers came to my office. "My computer was acting kind of funny, so I re-booted it. Now I can't run any programs. And Doug re-booted his computer and got this weird message." My response, "Oh no! What do I do now?" This pointed out our first weakness.

Lack of Policy

Day one of the Security Essentials course the need for a security policy was emphasized both through example (i.e. the Randall Schwartz case) and directly in the fifth unit. Developing a security policy was to be one of my first priorities upon returning from training.

> "A security policy establishes what must be done to protect information stored on computers. **A well written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured and evaluated.**"
>
> SANS Security Essentials I (slide 5-3)

Would a security policy have kept an employee from receiving an e-mail with a virus attached, it could have. Could a well written security policy have prevented an employee from opening an attachment that contained a virus, it should have. Should a well written virus policy have guided us in our response once the virus had infected our system, it should have.

Woulda, coulda, shoulda. Let's examine the elements of a well written security policy that could have kept us out of this mess, and certainly would have lead us out of it, once we got in to it.

Anti-virus policy

An anti-virus policy would have included what files to scan (programs, documents, system files, all files), when to scan them (scheduled and/or when accessed), how often scans should be scheduled, where to execute scans (desktop, file servers, mail servers), who is responsible for scans and what to do when a virus is detected. The same questions must be answered with regard to installing anti-virus software and updating the software and signature files.

CERT recommends filtering both incoming and outgoing e-mail as part of your perimeter defense. Filtering outbound mail traffic is a matter of being a good citizen of the Internet, much like using a handkerchief when you sneeze. After we had shored up our defenses and ability to recognize the SirCam virus, we isolated one copy that seemed to come directly from a server at AOL!

> Sites can use email filtering techniques to delete messages containing subject lines known to contain the malicious code, or they can filter all attachments.
>
> Likewise, a firewall or border router can be used to stop the W32/SirCam outbound SMTP connections to mail servers outside of the local network. This filtering strategy will prevent further propagation of the worm from a particular host when the local mail configuration is not used.
>
> CERT Advisory CA-2001-22 W32/SirCam Malicious Code

There are several commercial tools available to provide e-mail filtering. A short list includes:

Mail essentials for Exchange/SMTP from GFI Software
http://www.gfisoftware.com/me/mailessentials.htm

MailMarshal from Networking Technologies
http://www.nwtechusa.com/mailmarshal.htm

Panda Antivirus for MS Exchange Server
http://www.pandasoftware.com/com/pgvi/exchange/exchange.asp

Security awareness

Malicious code writers always seem to be one step ahead of the anti-virus companies. Somebody always gets to be the first recipient of a virus or worn. For instance, had our recipient noted a few oddities in the e-mail he had received, he could have quarantined or deleted it and avoided infection. The SirCam virus has two rather unique attributes that should raise a red flag to the security aware.

As with much malicious code it arrives unexpectedly. In Protecting Yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond(1), CERT states "Before opening any attachments, be sure you know what the source of the attachment was. It is **not** enough that the mail originated from an address you recognize." Secondly, the body of the email is nebulous, it doesn't describe what is attached, and in the case of SirCam it is not very good grammar. The McAfee.com Virus Information Library lists the text as having these variations:

```
Hi! How are you?

I send you this file in order to have your advice
   I hope you can help me with the file that I send
or I hope you like the file that I send you
or This is the file with the information that your ask for

See you later, Thanks
      McAfee.com - Virus Information Library
```

I don't think my English teacher would have gone any further with the email!

Finally, the payload itself was a file with a double extension. In the windows world this is pretty unusual (though Unix users are very familiar with files that end with a .tar.gz extension pair). This combined with the other oddities should have been enough to prevent infection by and the spread of the SirCam virus.

All of these may seem pretty obvious to you and I, but not my user base. Why, because a lack of security awareness. The first day of SANS Institute Security Essentials training begins with Information Assurance Foundations, which includes an introduction to vulnerabilities. The day concludes with a review of Malicious Software (Malware). We are reminded of the threats around us through out the course. But what about the folks at home, how will they know unless they are told.

A Security Awareness policy, like any other, will answer the "who, what, and when" questions. First who is responsible for security awareness? Everyone is responsible for security, but who will turn on the light? The policy should define what type of information should be disseminated and how often. There should be an initial security briefing for all employees, and periodic refreshers. Additionally, important threat information, and possibly hoax clarification should be provided as necessary.

Incident Handling

To paraphrase the joke lists, an "Ohnosecond" is the moment between the time an incident occurs, and when you initiate a response. The ohnosecond is not the time to begin writing policies and procedures, it is the time be enact practiced procedures based on sound policy. Slide 5-24 of Security Essentials I(2) states "Good policy empowers people to do the right thing." This is perhaps never more important and never more true than during the ohnosecond. The ohnosecond is also where the principle that a good policy is readily available (ibid. 5-20). This means online and off (as a machine under attack may have to be isolated from the network).

The SANS Institute provides a model for Incident Handling, "NAS Security Incident Handling Procedures" (http://www.sans.org/newlook/resources/policies/item7.pdf). In Protecting yourself from Email-borne Viruses …(1), CERT provides an Incident Response Checklist and equally important a list of What Not to Do. The second list is perhaps more interesting than the first and is excerpted below.

"Don't necessarily deviate from your normal security practices.
Don't act on, send out, or publish unsubstantiated information. Hoax email messages will continue through the Y2K event period (and beyond - auth.), so follow existing guidance.
Don't be fooled by social engineering whether by email, telephone, or in person.
Don't assume you should turn off your computer or network equipment especially for this single event.
Don't make unnecessary changes to your hardware or software.
Don't make noticeable changes without warning your users.
Don't install hardware or software from untrusted sources.
Don't release unnecessary or excessive information to unauthorized persons or groups.
Don't respond to an intrusion by attacking.
Don't make decisions in a vacuum.
Don't be overconfident. "

http://www.cert.org/tech_tips/virusprotection.html#IV

Security Policy Templates
The SANS Institute provides a number of model policies and templates at http://www.sans.org/newlook/resources/policies/policies.htm.

Security is not the job of interns (God love them)

The McAfee Virus Information Library indicates that SirCam virus was first discovered July 17, 2001 and the risk was upgraded to High on the 23rd. So how is it that, despite using VirusScan ASaP, we were infected with SirCam on the 24th? Lacking a security policy to guide us, we assigned the task to an intern and got burned.

First, we trusted the vendor too much. The installation instructions are simple, and McAfee would manage everything else.

> "The process of distributing VirusScan ASaP to workstations is simple. When you subscribe to VirusScan ASaP, you will:
>
> ✂Receive an e-mail with a customized URL that was specifically created for your organization.
> ✂You then distribute the URL to employees within your organization via e-mail.
> ✂Each user should click on the URL for the seamless VirusScan ASaP installation to begin. That's it, implementing VirusScan ASaP is complete."
>
> VirusScan ASaP, Installing VirusScan ASaP

It can't get much easier than that. We use Netscape or StarOffice as our web/email clients. This way we avoid the many viruses that target Microsoft Outlook and Exchange Server. Installation of VirusScan ASaP required Internet Explorer to be set up as the default browser during installation, then we wanted each individual to return to either Netscape or StarOffice. So we assigned an intern to perform the task on each workstation, and thought we were now safe from viruses. We were not.

One of our systems had to be rebuilt, and when the anti-virus software was re-installed something went wrong. With no set procedure for installing the anti-virus software we are not exactly sure what went wrong. Perhaps, the software was installed with Netscape as the default browser and the installation was not exactly correct. Perhaps many things, there was no written procedure to follow, no documentation, no verification and no auditing. We just don't know what happened.

Auditing would have shown us that one of our systems was not being updated, and we could have taken remedial action at that time (according to our non-existent policy). But alas, there was not policy assigning an audit responsibility for the anti-virus software.

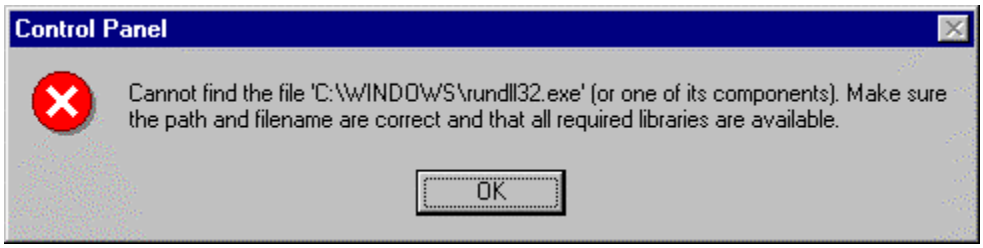
After suffering through the SirCam incident, we learned that we were not performing periodic scans of anything. According to VirusScan.ASaP, Managing Virusscan.ASaP" on demand scans must be scheduled through third-party tools. The command line has a long and fairly complex syntax. McAfee provided no instructions for setting this up, until after our incident.

Following security policies and procedures should be simple enough for interns, but creating them or working without the net of a good security policy is not.

File sharing hazards

As was mentioned earlier, another employee got a weird message when he re-booted his computer. That message is repeated below. Talk about "good news, bad news". The bad news is of course that the virus seems to be spreading, the good news is that a quick trip to McAfee's web site identified the virus as SirCam. Soon others began to report this same message and we suspected a major virus outbreak.

After applying the removal procedures to the first infected computer, we began to repair other computers that were beginning to display this message. The strange thing was that as we went to repair registry entries and file systems the errors weren't there! What was common across many of our systems was the entry "@win Recycled\SirC32.exe" in the autoexe.bat file and that the file "rundll32.exe" had been renamed "run32.exe". (Apparently SirCam failed to replace run32dll.exe with the it's self-replicating version. Either the vendor's instructions did not originally address the rundll32 issue, or we missed it in the documentation. We discovered this when trying to check the properties of My Computer yielded a message like the one above.)



So how was it that one of our systems was clearly infected by the SirCam virus, some machines merely showed symptoms of the virus, and yet others were totally clean? As we began to analyze our systems we noted that those systems showing symptoms of SirCam were those that were sharing their c: drives without protection.

In his paper Open Source File Shares: An Unexpected Business Risk(3), Jaime Carpenter demonstrates the threat to confidentiality and integrity imposed by network file shares. Sharing desktops is very common in our organization. It is faster and easier to drop a file on someone else's computer than to attach it to an email, send it out to the mail server, and await its return. All those systems sharing their c: drives made themselves open to an integrity attack on the operating system. Given SirCam's penchant for e-mailing files we were also been vulnerable to confidentiality attacks as well.

Mr. Carpenter's paper outlines several tools for scanning your internal network, and yes, suggestions for policy regarding file sharing.

The Good News

The good new comes on several fronts. First, we had the ability to isolate and eliminate the SirCam virus. Second, we have our anti-virus software properly operationalized to have us truly up to date. Third, we have improved our network infrastructure to reduce our risk of confidentiality and integrity attacks on our intranet. And finally, and perhaps most importantly, the downtime caused by firefighting this virus has raised the awareness of both management and staff, and the way for effective security policies has been prepared.

List of References

CERT Advisory CA-2001-22 W32/SirCam Malicious Code, CERT Cordination Center,
URL: http://www.cert.org/advisories/CA-2001-22.html

"McAfee.com - Virus Information Library", McAfee.com Corporation,
URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99141&

(3) Open File Shares: An Unexpected Business Risk, Jaime Carpenter,
URL: http://www.sans.org/infosecFAQ/threats/file_shares.htm

(1) Protecting Yourself from E-mail-borne Viruses and other Malicious Code During Y2K and Beyond, CERT Coordination Center, Carnegie Mellon University,

URL: http://www.cert.org/techtips/virusprotection.html

(2) SANS Security Essentials I, SANS Institute

"VirusScan ASaP, Installing VirusScan ASaP", McAfee.com Corporation,
URL: http://corporate.mcafee.com/content/virusscan_asap/installing_virusscan.asp

"VirusScan ASaP, Managing VirusScan ASaP", McAfee.com Corporation,
URL: http://corporate.mcafee.com/content/virusscan_asap/managing_virusscan.asp