Global Information Assurance Certification Paper

Computer Virology: Protection, Prevention, Identification & Containment
Jules Fiorentino
November 22, 2000

Companies large and small have increasingly started to initiate policy and programs that are geared towards a lifecycle approach to anti-virus control. It is no longer sufficient to have a singular desktop anti-virus program on all client nodes of a network to secure a network against a computer virus attack. The newer model for anti-viral control has become much more complex, including everything from firewall protection to lay-user education. Nevertheless, many companies still neglect to recognize that developers of viruses and other types of malware (Trojan Horses, etc.) are usually two-steps ahead of us, and thus fail to contribute the necessary resources required to keep their networks secure. This paper will briefly examine the different facets of good anti-virus control Protection, Prevention, Identification and Containment, incorporating models developed in microbiological studies of viral diseases by Frederick A. Murphy, and Damaris Christensen's 1999 computer article, *Beyond Virtual Vaccinations: Developing a digital immune system in bits and bytes*.

Protection and Prevention

The most simplistic network model contains a firewall, an internal mail server, and several client nodes. Years ago it was sufficient to have a network manager install anti-virus software on the clients to insulate the network against most viral attacks. Now, of course, we have anti-viral software running on each of the three components which has increased security. However, it is a false sense of security. In my experience, the biggest mistake a company can make is trusting one Anti-Virus Company for all its anti-virus needs. It is not enough to believe that one Anti-Virus Company (or scan engine or algorithm) can prevent every virus or malware from entering the company, just as we cannot rely on one vaccination for this year's Flu to prevent us from contracting the Flu next year or even a few months down the road. Rather, it is my recommendation and first-hand observation that the best networks have multiple software and scan engines actively running on each of the different components of a network to increase protection. On occasion, a definition may be up-to-date but the scan engine is not, causing a virus to inadvertently pass through one component but be detected on another. Another scenario I have observed is that one company may be privy to a new virus or variant and quick to release an update while another has not received a live sample to examine. Still another may receive a copy of the virus and release definitions that claim to detect the virus but upon further testing do not stop the virus at all. It would be foolish for a country to only build boats and believe that it is safe from every imaginable attack, so why do networks managers think that the best strategy for anti-virus defense is using one type of weapon? I believe that there should be anti-virus scanners on firewalls, DMZ, Sendmail, mail servers, and each client node. I also believe that a heterogeneous network (full of Macs, PCs and UNIX/Linux boxes) is better than a homogenous one for protecting networks against viruses and malware, although more labor intensive to troubleshoot.

It is important to have multiple anti-virus scanners on the network. That being said, it is not good to haphazardly throw every anti-virus scanner that exists on your computers. I believe that three really good scanners are better than ten mediocre ones. Evaluation and discussion of anti-virus scanners is tough, but a team should be put together to decide what criteria is important to your particular network. Rob Slade has put together an excellent essay, *Antiviral Software Evaluation FAQ*, that considers important questions that administrators should ask when looking at different scanners. Slade writes:

> The most important factor in judging an antiviral is accurate and complete detection of all possible viruses. Unfortunately, since it is proven that this is impossible, we are left with trying to determine which antiviral will detect, accurately, the most viruses that the user is likely to encounter. Complete and accurate detection, though, is the number one priority. It should never be superceded by *any* other factor in a trade-off.

The three most important criteria that I look for in an anti-virus company are as follows. Reliability: how reliable is the company and the company's definition files, and how well have they performed on benchmark tests when compared to other companies? Response Time: how quickly has a company received a live sample of a virus and turned out *reliable* definitions and\or Auto-Fixit programs to help expedite the cleanup process? Availability: If I have questions about their software or definitions or other products, how easy is it to contact or get a response from the support team? An excellent resource for any anti-virus coordinator is Virus Bulletin Online Journal. Their benchmark tests (http://www.virusbtn.com/100/vb100sum.html) against different

anti-virus software and their comparative review summaries for ITW (In The Wild) viruses is great.

Part of the difficulty network managers face today is that there is just too much work to do just to maintain the health of a network: Is my firewall up-to-date? Are my mail servers reliably delivering mail to the clients? Are the printers successfully queuing and printing? Is the web server working and the DMZ functioning properly? It is close to impossible to get everything done that needs to be done in a forty-hour work week to maintain the basic health of a network, let alone remain educated and up-to-date on every new virus and definition file and scan engine and hack. As a result, anti-virus work gets put on the back burner in place of more immediate problems.

In an ideal situation, a company should provide the funds for a full-time anti-virus coordinator and malware investigator. Truly, keeping up with the newest viruses, Trojan Horses, and other related malicious software is a full-time job. It is not enough to maintain the latest updates on every firewall, server and node on the network. An anti-virus coordinator must also be educated on how the virus works, advise network administrators about recent holes that malware can exploit, and push out definitions to each node on the network. In addition, the coordinator must also interact with the technicians who are developing and deploying new images for company computers, making sure that the anti-virus software does not decrease the operability or efficiency of the computer. For example, many times a specific feature of a scanner's auto-protect function will interrupt or completely disable a computer application. Furthermore, the coordinator must also be able to write and revise anti-virus policy, as well as put in place strategy to educate lay-users.

Now, let us imagine that we have implemented the aforementioned recommendations: a variety of anti-virus software on different network components; up-to-date definitions and scan engines on each piece of anti-virus software; and an anti-virus coordinator dedicated to understanding new virus threats and helping network administrators and technicians keep abreast of the important issues. Even with these conditions in place, the model can still fail if the lay-user is not aware and on-guard when left alone in his/her office. The fundamental core of anti-virus control is User Education. When a virus hits, such as the LoveBug, there is no defense but the Last Defense. Picture how easily this virus could have been contained if the lay-user was educated in recognizing some of the typical signs of virus behavior! After the Loveletter virus, my company began to educate clients about anti-virus control, and twice in the last four months these lay-users have successfully identified new virus strains, unidentified by anti-virus companies at the time, and contacted User Services because something "looked fishy" and they wanted us to examine the email. Of course, there will always be the user who brings in photos of the newborn on zip disk from home and infects his/her office computer because the home computer has not updated its definitions since the date of purchase from the store. However, even in the most ideal situations we can expect to be blown away by the inventiveness of the Wily Hacker.

In a short but interesting article from the Associated Press, *Virus Points to Prevention Needs*, the FBI's lead investigator on computer viruses, Michael Vatis, is interviewed about the effects of the Loveletter virus. His insights about lay-user education and old models of anti-virus control helped me understand that no matter how well-protected a network is in the eyes of an administrator, relying on what happened yesterday is not enough. He says that, "The conclusion we must draw is that this will happen again . . . Unfortunately, the existing strategy does not work. The question is, 'How do we adapt'". Indeed, adaptation is the key, and the only way to fight the next hacker's virus is to remain aware, educated, and prepared to change strategies at the first sign that something is not working.

Identification and Containment

Murphy writes in his article, *Problems in the Surveillance and Control of Viral Diseases with Special Reference to the Developing World,* that

> At one time surveillance, prevention and control seemed to represent a simple continuum -- find the disease, learn a bit about it, then set in place a prevention or control scheme to deal with it. Pasteur and Theiler felt this continuum in their bones -- they sowed the seeds for the later idea that if one pressed had enough, one could achieve regional virus elimination and even global eradication. But, along came HIV/AIDS, the ultimate case where surveillance and control have gone separate ways.

One (of the many) problems with the study of HIV is that it is constantly mutating, creating variants of itself, and changing the way in which the disease attacks the body. Within one human body there can be a myriad of

strains and mutations of HIV. Similarly, hackers are constantly developing new variants of the Loveletter virus (currently Loveletter-AS is a threat), as well as new viruses that keep network administrators laboring to keep up.

Worst case scenario, all methods fail and a new virus is identified on the network. The next step is containment. Murphy writes,

> For example, in 1991 PAHO sent some resources to Peru to deal with the first cholera introduction into the western hemisphere in 75 years. Well, a million cases later, and 7,000 deaths later, one might wish that the initial response had been more vigorous. Alas, there never is a chance to reconsider, to start over, and the public has rising expectations that disease control officials should get it right the first time.

The most important job of the anti-virus coordinator is to determine when it is time to implement damage control and disaster recovery methods. The president of the company is not going to be thrilled if the network is shut down once a week to clean the mail spools, disinfect the network, and recover lost data from backup tapes. However, if a major virus is identified and detected prior to total meltdown, I am certain that the president would prefer 2-3 hours of network downtime once a year if we could assure that it will prevent any data from being lost from the local machine.

Each company has its own set of specific anti-virus damage control procedures, so I choose to not examine one policy, in particular. Rather, it is sufficient to make note of the most general but important steps to follow after an outbreak has been identified. First, pass a generic telephone message to all users that email will be unavailable due to a virus threat and it is imperative that they do not open any email they have downloaded to their computers. Next, shutdown all incoming/outgoing mail from the internal and external servers so that users cannot spread the infection to others within the office or to the outside world. The team should then locate a sample of the virus and *carefully* examine its attributes (Subject, Message Data, Sender) for anything consistent in order to develop a script upon which a filter can be based. If the mail servers are UNIX-based, the script should be run on the mail spools to identify and quarantine the virus. If the mail servers are not UNIX-based, such as with Exchange, an NT application should be used to identify and expunge the Exchange servers. Once a sample of the virus is found, the anti-virus coordinator should get a copy of the sample to at least one anti-virus software vendor to examine and develop new definitions. Coordinate with the helpdesk troubleshooters to begin identifying which computers have been infected and begin creating lists. Continue to check with vendors until they have developed definitions to detect the virus. Once the definitions have been tested, deploy them globally. Educate the troubleshooters about the virus and how to remove it from infected computers, then send them into the field. Once the troubleshooters have informed network administration that the virus is contained in the field, it is okay to bring up the mail servers again. For the next few days, the backup tapes should be carefully monitored so that any infected files are not copied and stored on backup. Email and bulletins should be placed in mailboxes so that everyone in the company is informed of the status of the virus and the efforts being made to contain it, encouraging anyone to call or email with questions.

Conclusion

In an excellent essay about where virus trends will take us in the next decade, Steven R. White writes in his article, *Virus Bulletin 2010: A Retrospective,*

> . . . some people say that the anti-virus industry is still more reactive than proactive, waiting for problems to occur in a new viral niche before creating a solution for them . . . To be fair, it is difficult to anticipate exactly which niche will become populated with viruses, and users do not often change their behavior in the absence of a clear and present danger. Still, the stakes are increasing, and it is becoming more and more problematic to be behind in protecting new areas of the computing environment.

Indeed, the nature of virus prevention, protection, identification and containment is, for the most part, reactive rather than proactive. However anti-virus companies are becoming increasingly proactive. For example, these companies are using spiders to crawl the web and seek out malicious code and viruses rather than waiting for a virus to find them. I believe that the best model of viral control is adaptive, continually evolving to meet the attackers at the front gates of the castle. Hackers are not going to suddenly disappear. Our job is to meet their aggression with the most current defense strategies available. *"Just as water has no constant shape, there are in warfare no constant conditions. Thus, one able to win victory by modifying his tactics in accordance with the*

enemy situation may be said to be divine". -- Sun Tzu's Art Of War (500 B.C.)

Bibliography

Associated Press. "Virus Points to Prevention Needs". 7 May 2000. URL: http://www.jsonline.com/bym/tech/ap/may00/ap-love-bug-securi050700.asp (17 Nov 2000).

Christensen, Damaris. "Beyond Virtual Vaccinations: Developing a digital immune system in bits and bytes". 31 Jul 1999. URL: http://www.sciencenews.org/sn_arc99/7_31_99/bob2.htm (17 Nov 2000).

Murphy, Frederick A. "Problems in the Surveillance and Control of Viral Diseases with Special Reference to the Developing World". Fifth International Congress on the Impact of Viral Diseases in the Developing World, Johannesburg, South Africa, 9-14 July 1995. URL: http://www.uct.ac.za/microbiology/icvomurp.html (10 Nov 2000).

Slade, Rob. "Antiviral Software Evaluation FAQ". HTML release 1.01. 1996. URL: http://www.claws-and-paws.com/virus/faqs/avrevfaq.shtml (17 Nov 2000).

White, Steven R. "Virus Bulletin 2010: A Retrospective." Virus Bulletin Conference, September 2000. URL: http://www.research.ibm.com/antivirus/SciPapers/Retrospective.htm (15 Nov 2000).

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event