Global Information Assurance Certification Paper

Defending Against the Next Deadly Virus
Chris Geffel
December 20, 2000

It's coming. We don't know when or how, but there is no doubt that it will arrive. It will spread faster than anything before it. It will cause more damage than anything in history. It's the next wave of computer viruses. And we have to be ready for it.

While viruses are not a new phenomenon (they've been around almost as long as the computer), the new trend in virus technology is alarming. What used to take weeks or months to spread to a few machines, is now taking hours to propagate globally. In the past two years alone, estimated damage from virus outbreaks has risen from $1.5 Billion in 1997 to $10.6 Billion in 2000.

The birthrate, or the speed that it takes to spread a virus, is also on the rise. In 1999, it is estimated that approximately 250,000 computers were infected with the Melissa virus. A year later, the I Love You virus spread to 55 million computers, infecting approximately 5% of these systems.

The number of viruses has also dramatically increased in the last few years. In 1993, it was estimated that there were approximately 2,300 known viruses. Today, there are well over 65,000.

What is causing this explosion in growth?
Growth can be attributed to automation. Operating Systems and the applications that run on them are becoming easier to use than ever, and are being delivered with a plethora of new features. The average user will never use most of these improvements, so why do vendors bother including them? That answer is easy – marketing. It is generally accepted that the product with the most features is the better product.

Ubiquity is another reason for the explosion in virus growth. As we depend more and more on the Internet as a major means of communication, the Internet will infiltrate more of our lives. We will see more devices that are capable of communicating on the Internet, giving all of us 24x7 access. Imagine that someday your oven may be infected with a virus.

What used to be a problem in the workplace is now starting to make its way into the home. There is already a rapid growth in DSL, cable modem, or other high-bandwidth, always-on connections. It's frightening to think that even today, most home users are not protected. Computer system vendors are pre-installing anti-virus on new computers, but how many are configured to automatically update? How many home users are able or willing to go through the update process?

Virus writing has become easier, too. What used to take savvy programming knowledge can be done in seconds with tools created for this specific task. Each generation of virus

programmers are learning from the generation before them, and correcting the mistakes made in the past.

Paddling upstream.
Anti-virus vendors are having a tough time keeping up with updates to combat viruses. This is especially true with polymorphic viruses - those that change its internal structure or its encryption techniques to evade detection. In the case of the Melissa and I Love You viruses, it was days before the major software vendors had correct updates available. This left plenty of time for these viruses to continue on their destructive paths. The lack of quick turnaround of updates caused many system administrators with only one choice – to shutdown their mail gateways until correct and comprehensive updates were made available. This caused significant loss due to being unable to conduct business.

The smart virus?
The next generation of viruses will also be intelligent. They will no longer need user intervention to deploy their payloads. As operating systems become more automatic and user friendly, they will execute more code in the background, out of site of the user. This will give virus writers more flexibility in their code, and allow them easier methods of injecting their code.

Have we learned from the past?
The next generation will also be network aware. History has not yet taught us a lesson. In 1988, the Morris Worm was released on the Internet. In a matter of days, thousands of computers were rendered useless because of the Morris Worm. There were no attachments in e-mail, there was no user intervention required. The Worm exploited various weaknesses that caused the Worm to automatically propagate to the next computer. In the future, we will see more viruses and worms that behave like the Morris Worm. These viruses may also be aimed directly at infrastructure devices like routers and switches, leaving portions of the Internet crippled.

How can we defend ourselves?
So, what do we need to combat the future generations of viruses? Well, since we don't truly know what the next deadly virus will be, it's a little unclear how best to protect ourselves. However, there are some long-term objectives that can be met that will help us become better prepared when a violent outbreak occurs.

First, the Anti-Virus software vendors need to create a better method of detecting viruses. Currently, most anti-virus programs search for unique signatures in code that identifies them as a virus. While until today this has been a satisfactory method, it is a slow method of scanning. The anti-virus companies should incorporate heuristical scanning as their primary method of scanning. Heuristic scans look for patterns that look virus-like, without scanning the actual content. While this does create a large number of false positives, patterns found that match the set criteria can be handed down to a secondary engine for a comprehensive scan.

Second, the anti-virus software vendors should work together to create a common approach to anti-virus software. They should create an interoperable standard for the writing of anti-virus filters. This will create a global community of support technicians that can collaborate on a cure. This will increase the speed of which new pattern files can be written and distributed. This new standard will also help those organizations that wish to create their own filters, or wish to only look for relevant patterns.

Because viruses will become more intelligent and complicated, it will be more difficult to distinguish between anomalous network activity and a virus. This will blur the boundary between the two, and they will become known as a single entity. Some vendors like Symantec and Network Associates are already preparing their products for this merger. They are marketing both Anti-Virus and Personal Firewall software as one. In most cases these products are installed separately, however it is conceivable that the next major release will merge the two.

Next, the infrastructure device vendors should work with the anti-virus companies to put anti-virus on the infrastructure devices. There has been a lot of talk lately about putting intrusion detection on switches. Intrusion detections systems have traditionally been unable to protect from attack, capable of only alerting when an attack has been detected. Although this is primarily to overcome a technological limitation, the idea of having this type of defense directly on these devices would significantly increase the value of intrusion detection systems.

Conclusion

In the past ten years, there has been an explosion in virus technology. New viruses are more complex than in previous years, with deadlier results. There is no indication that this trend will stop any time soon.

As these viruses become more network aware and intelligent, they will become more like a network anomaly, blurring the boundary between these attacks. Combating these new viruses is becoming more difficult with the current technology in place. Because we are combating an unknown enemy, we do know when the next attack will come, and we are put at a disadvantage trying to defend against this new wave. New methods of detecting viruses will have to be created. The community of security experts must push software vendors to design new, open standards for updating anti-virus software. This will decrease the time it takes to distribute these updates, thereby eradicating viruses early in their lifespan, limiting the damages caused. We can also incorporate scanning techniques in infrastructure devices that historically have not served this purpose, increasing the depth of protection.

References

Chess, David. "The Future of Viruses on the Internet." October 1997 URL: http://www.research.ibm.com/antivirus/SciPapers/Chess/Future.html (9 Dec. 2000)

White, Steve R. "Virus Bulletin 2010: A Retrospective." URL: http://www.research.ibm.com/antivirus/SciPapers/Retrospective.htm (9 Dec. 2000)

Zetter, Kim "Viruses: The Next Generation." PC Magazine December 2000. Pg. 191

Network Associates "The McAfee AVERT Virus Information Library." URL: http://vil.nai.com/vil/default.asp (5 Dec. 2000)

Various. "The Intrusion Detection FAQ." SANS Institute. URL: http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm (19 Dec. 2000)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event