Global Information Assurance Certification Paper

An Incident Response Preparation Policy for Virus Outbreaks

By Thomas Kline

GSEC Practical version 1.3 option 1
May 29, 2002

Abstract

This practical is an implementation and response plan for virus outbreaks. Part of the planning includes defining the ne twork infrastructure and entry points that a virus can enter the corporate network. Best practices include a multi -layered defense strategy of anti-virus products. Each layer is described and an explanation of what protection measures can be placed is discussed. It defines procedures that the Anti -virus Administrator is to use to monitor for virus activity. Specific tasks are used to guide the administrator during a virus outbreak. This includes a decision flow chart to determine what actions are required. Explained are the duties of the call -out coordinator to notify company employees on what is occurring and what is required of them to prevent the increased spread of the virus. The end user is given a "best practices" guideline for emails received. A follow up meeting is used to improve current policies and procedures.

Introduction

New viruses and worms are constantly evolving and being introduced into the Internet. While virus detection and protection programs work relatively well if a signature or identity file has been developed and deployed, they only work if they are updated as they become available. During the hysteresis or lag time between a new strain of virus release on the Internet and the update of signatures can be hours or days. In a global company operation, virus detection and monitoring is required 24 x 7. There must be procedures in place to protect the company during this vulnerable time period. How does the IT Department handle response during this critical time period? What actions or me thods can be deployed to insure virus containment? Following the Six Stages of Incident Handling, (Preparation, Identification, Containment, Eradication, and Recovery), my company has created specific plans of action that will be described in this practical, that can be put to immediate use to protect the network infrastructure in any global company.

In the last twelve months, the corporate view of an anti -virus program has gone from annoying, but tolerated, to an essential program. My company struggled t hrough a minor outbreak of the "I Love You virus", skipped the damage of Code Red because software patches were in place, and struggled again when Nimda hit. A rough draft of a response procedure was in place when the Goner virus entered the company network. We were able to shutdown the email system within seven minutes of notice that an outbreak had occurred. At that point one machine had managed to infect nine other workstations out of a total of twelve hundred workstations. It was only through the polic y that a major disaster was averted. Symantec released a signature about eight hours later and we were able to push the virus signature out to workstations and clean the infected workstations.

Our email system was down and caused loss of revenue, but it was minor compared to what would have happened if the email servers had not been stopped. CERT's 'Overview of Attack Trends' notes that, "…the biggest impact of these worms is that their propagation effectively creates a denial of service…" [1]

Comment:

The most critical time period is the delay or hysteresis of a new virus being released on the Internet and the creation of a signature detection file by anti-virus companies. This practical focuses on this time period when no signatures are available. What has been done is to set up a series of monitoring procedures to protect during hysteresis and polices to react to virus outbreaks.

While new applications are being developed and security holes patched, our company still requires an immediate reactive policy to handle unforeseen incidents. Since this company uses the Symantec suite of anti-virus tools, examples will be given pertaining to Norton Anti-virus.

Preparation: Network Infrastructure Background

The network cannot be protected if the paths into the network are not known. It is important that a logical map of all avenues are documented and also the processes that use the paths. This also helps with policy on what systems are running and where. For example, only MS Exchange servers should be running smtp services. Since a number of worms create their own smtp mail daemon, periodic inventory of services would expose this kind of problem. A historic document of services should be kept.

Points of Entry: Avenues of data flow

Internet email - Anti-virus email gateway scanner, for both inbound and outbound internet email.
Internal email - Anti-virus for MS Exchange servers.
FTP services - Antivirus for servers
Web services (http traffic through a firewall, web hosted email) - handled by desktop anti-virus or Content Vectoring Protocol (CVP)
VPN - desktop and server anti-virus
Dialup access - Host computer runs desktop anti-virus.
Server to server - Server anti-virus
Server to workstation - Server and desktop anti-virus.
External Media - desktop anti-virus.

Multiple Levels of Defense

"It has become necessary to move beyond single-tier desktop anti-virus solutions to solutions that encompass servers as well as email and Web gateways. One of

the reasons for this, especially on email or SMTP gateways, is that newer threats leverage the power, speed, and connectivity of the Internet to spread payload into consumer and corporate environments by combining email transport and social engineering." [ii]

The Internet Email Gateway (Symantec's Norton Gateway Services, NAVGW) server checks all incoming and outgoing Internet email for viruses and worms. It is configured to send email alerts to Anti-virus Administrators. This application is very good at detecting and cleaning known viruses. Since the focus of this practical is hysteresis, the time between a virus creation and detection signature, the NAVGW blocking feature is also used extensively. Configuration allows for the blocking of subject lines and file extensions. One subject line that is blocked is "Snowhite and the Seven Dwarves" which is characteristic of the W95.Hybris virus. While an anti-virus signature is available for this virus, it is annoying and possibly embarrassing to employees. Mathias Thurman writes, " One way to deal with this problem at the e-mail gateways is to block all incoming attachments with executable extensions such as .exe, .com, or .vbs." [iii] Other file attachments blocked include .pif, .lnk, .vcd, .bat, and .scr. The newer viruses typically will be sent through an attachment.

While the vendor supplies an automatic signature update feature, the signatures are typically only updated once a week, or in the case of fast spreading virus, more often. This schedule was considered by IT as not frequent enough to keep systems free from viruses. As a result a script was created to check for signatures on a more frequent basis and download and install the signature. Symantec posts signatures almost on a daily basis for manual download, but it is not incorporated into their LiveUpdate feature or is a part of extended maintenance.

A rudimentary vbs script adapted from Symantec's cgetter script [iv] shows how to automate the update process. The format of Symantec's virus signature files are mmddx86.exe. The first section of the script creates this file name using the current date. The next section creates a text file that contains the ftp commands that will be executed. Finally, the signature file is extracted silently and updates the signatures of the virus application.

```
myDate = Date()
myDay = day(myDate)
myMonth = month(myDate)
If len(myDay) = 1 then myDay = "0" & myDay
If len(myMonth) = 1 then myMonth = "0" & myMonth
myFileName = myMonth & myDay & "x86.exe"

set myFSO = CreateObject("Scripting.FileSystemObject")
Set filetxt = myFSO.CreateTextFile("c:\ftp.txt", True)
filetxt.WriteLine("open ftp.symantec.com")
filetxt.WriteLine("anonymous")
filetxt.WriteLine("tom.kline@idc-ch2m.com")
```

```
filetxt.WriteLine("lcd c:\")
filetxt.WriteLine("cd /public/english_us_canada/antivirus_definitions/norton_antivirus")
filetxt.WriteLine("bin")
filetxt.WriteLine("get " & myFileName)
filetxt.WriteLine("bye")
filetxt.Close


Set myObj=CreateObject("WScript.Shell")
myObj.Run "cmd /c ftp.exe -i -s:ftp.txt"
WScript.sleep(120000)

path = myFSO.GetAbsolutePathName("c:\" & myFileName)
If myFSO.FileExists(path) Then
        myObj.Run "cmd /c " & myFileName & " /Q"
End If
```

All Email Servers have Symantec Anti -virus installed. The newest version of NAV for Exchange, version 3 (NAV AVF), allows extensive filtering of email by subject line, domain source, attachments, and file content. One problem with this robust feature is that it cannot block attachments from a specific source, while allowing attachments to pass through from other sources. This is significant where blocking Internet email attachments and allowing internal email attachments is not possible, but desirable, as NAV for Exchange Version 3 will quarantine blocked attachments, but NAV for Email Gateways (NAVGW) will not quarantine blocked attachments. NAVGW doesn't allow a mode of recovery for valid attachments.

All workstations have Symantec Anti -virus installed and are maintained through Symantec's' System Center (SSC) which gives a hierarchical view of servers and workstations. In addition, the Alert Management System (AMS) is configured to report any virus activities on workstations and servers. The SSC also has a visual alarm feature to help the Anti -virus Administrator detect problems. There are also a number of laptops that employees use during travel. While they have been instructed to run Symantec's LiveUpdate manually while they are traveling, one can never be certain that signature updates happen. Once an employee logs into the company network, Norton Anti -virus checks in with the parent server for new signatures and con figuration settings. While Symantec licensing allows the distribution of Norton Anti -virus for any workstation attaching to the company network, including an employee's home computer, it was determined that too much administrative work was required in the installation of the application. Also, there was not a guarantee that the employee would remove the software when leaving the company. So that avenue remains a problem within this company's infrastructure.

Anti-virus Administrator Responsibility List

An Anti-virus Administrator Responsibility List was created so that each IT person

would know what was required of them. This included:

1. Anti-virus Administrator Coverage Responsibilities.
2. Decision Flow Chart - Taking appropriate action based on a decision flow chart that was created to facilitate response
3. Call out list and Announcement Template
4. Anti-virus Policy of Internet Email Attachments.
5. End user guidelines - Email security best practices for employees.

Anti-virus Administrator Coverage Responsibilities - Monitoring:

A global company requires 24 x 7 monitoring of virus outbreaks. A team of I.T. personnel were selected to cover all time periods. Since we have offices in Asia and Europe, it was easy to have 24x7 coverage. Each IT person on the virus team is responsible to subscribe to several email lists that have virus outbreak alerts and information about new viruses. They are responsible for reading and assessing potential damage to the company. The most common path of virus infection of our company is email and so that is the focus of monitoring. Included email lists to monitor can be subscribed at:

Sophos, http://www.sophos.com/virusinfo/notifications/ [v]
Trendmicro http://www.antivirus.com/vinfo/ [vi]
McAfee http://dispatch.mcafee.com/sub.asp [vii]
Winnet magazine Security-UPDATE_Sub@list.winnetmag.com . [viii]

Other lists are security and general computer news lists:
Security Wire Digest http://infosecuritymag.bellevue.com/ [ix]
Computerworld Daily http://www.cwrld.com/nl/sub.asp [x]

In addition, email alerts are sent to the Anti-virus team from a number of internal systems. These include the Internet Email Gateway (NAVGW), Norton Anti-virus for Exchange, Exchange services, and Symantec's Norton Anti-virus Alert Management System (AMS). The Exchange email servers are configured to report excessive mail queue loads. Excessive email queues can indicate a virus outbreak and requires further investigation.

Preparation also includes making sure Anti-virus administrators have access to services pertaining to anti-virus. This also includes proper training on how anti-virus and email services run, how to stop and start services, make configuration changes, and documentation of such changes in time of an incident.

Identification and Containment

Decision Flow Chart

The decision flow chart guides the administrator on a course of planned actions and procedures. It helps to determine the severity of the virus outbreak and what measures need to be implemented. A list of managers for each area of 24x7 coverage shoul d know their responsibilities when an Anti -virus Administrator requests that a system be changed or stopped due to a virus outbreak. Sarah Scalet writes, "One of the most political parts of incident response planning -but one that can save precious time if an attack is successful - is deciding ahead of time who's in charge of incident response and which people could pull the plug on the website or network if need be." [xi]

Receive information on new virus

A. Is virus rapidly spreading through company?
    1. No - go to B.
    2. Yes - go to G.

B. Is virus rapidly spreading through the Internet?
    1. No - go to C.
    2. Yes - go to E.

C. Does Symantec have a signature file for the virus?
    1. No - go to E.
    2. Yes - go to D.

D. Is signature distributed to company servers and workstations?
    1. No - test and distribute to Internet Email Antivirus Gateway, Email server Anti -virus engine, and workstations. Notify and document change. End flow chart.
    2. Yes. End flow chart.

E. If subject line or attachment block c an be created on Internet Email Antivirus Gateway, do so and end flow chart. Other wise go to F.

F. Notify designated manager. Shutdown Internet Email Antivirus Gateway. Use template to create announcement that Internet Email is unavailable until further notice. End of flow chart.

G. Assess potential damage and speed of spread of damage. Based on criteria notify designated manager and implement shutdown of Email services. Use template to create announcement and activate call out procedure. End flow chart .

Call out List

Call out Coordinator

This list if to be used in the event of a massive virus outbreak that would cripple the

company. Whomever is assigned this duty will be responsible to distribute information to all of the company. An information announcement template will be provided to the call out coordinator to use to disseminate the information. This information also includes updates, further action required, and end of the incident.

It is the responsibility of the contacted person to convey t he information to local users. This could be in the form of an overhead intercom announcement. Other methods of contact include: email (if system is not down), phone, or fax. A list of offices and sites checklist is to be compiled to make sure the entire company is notified. At the call out coordinator's discretion, he may assign call out areas down flow of his position. Example: A Dublin, Ireland contact can be assigned to distribute information to all European offices and sites.

Announcement Template

This template was created to make sure that all pertinent information was relayed properly. It is amazing how often information is distorted from one person to the next. It has been found that users have enough information overload, so the idea is to keep the announcement short. At the end of the sheet, a detailed explanation is given for I.T. and for those users interested in learning more about the situation.

Critical Virus Alert

The company is experiencing a <name of virus> outbreak. This virus is spreading through <avenue of infection> (Internet email, internal email, web access, workstation software, server software, specific application, Instant Messaging).

As a result, < avenue of infection> is shutdown. To help stop the spread of this virus, please <End user action required > (log off email, save your work, don't shutdown workstation, shutdown workstation, log off network). Estimated time to normal work is <time>. Updates will be sent out periodically. Thank you for your cooperation.

This virus < b rief explanation of what virus does>.

Details: <>

.

Anti-virus Security Policy of Internet Email Attachments

In effort to insure the security of the company's network, we have enabled selective blocking of attachments at the Internet Gateway. What this means is that ANY mail destined to or coming from the Internet with an attachment of the

following types:

*.lnk, *.vbs, *.vcf, *.vcd, *.exe, *.scr, *.com, *.bat, *.

will be stripped of the attachment - with the remaining message passed on to the designated recipients. Internal messages are not impacted. These attachment types are frequently used to distribute viruses. It is common practice to block these attachments among other Corporate environments. The recipient will be notified that the attachment was stripped - the sender will get no notification (...wouldn't want to let the sender of a virus know that his payload was not delivered).

If you feel you need a file of the above mentioned types to be sent or received, you have two options:

- Have the sender rename the attachment to use a different extension name (e.g. program.exe --> program.ex_) and then rename the attachment upon receipt
- Use the company's FTP server to have the file(s) placed on then retrieved
- Note that zipped files are scanned and any .exe inside the zipped file will be removed. Unfortunately, there will be no notice of the blocked files.

I recognize this will cause some confusion and labor - but the cost of recovery (and potential damage) from a viral outbreak is significant. Please let me know if this policy has SIGNIFICANT impact on your company business.

Signed, IT Manager

End user guidelines - Email security best practices for employees.

Be cautious of emails from unknown sources, unsolicited email, or email with strange subject lines, and subject lines or content containing grammatical or spelling errors.

Assume that attachments from unknown sources contain viruses. Delete them without reading if possible.

Today's viruses can imitate email from a familiar sender. IF th e spelling or grammar contains errors, or the content of the email is unusual for that sender, it is advisable to check with the sender that it really was sent to you.

You can always call the Help Desk and ask them to check the email for you.

Recovery

Conducting a follow-up report or meeting is essential to preventing future outbreaks. Stephen Northcut in The SANS Institute Incident Handling Survival Guide states it best, "The primary purpose of the meeting is to improve your corporate incident handling process, not to play politics!" [xii] There will always be room for improvement in current procedures. This is an opportunity to review current policy and response procedures. Change in policy may include re-configuration of services, applying patches, or review of patch procedures Any tension within the team can be discussed and resolved. This also serves the purpose of reviewing the incident as a team. It is also useful to send out a report to the general user briefly describing the incident. This helps them understand the severity of the outbreak, any impacts it had, and an opportunity to review corporate guidelines.

Conclusion

This practical has focused on proactive monitoring and incident response to virus outbreaks. It is not intended as a complete solution, but rather a policy that satisfies immediate needs within the scope of established manpower, software, applications, and existing hardware.

Having an Incident Plan and Policy in place greatly enhances response time, coordination, understanding of responsibilities, and communication of potential problems. The procedures allow for 24 x 7 coverage of outbreaks by IT personnel during their work day, rather than forcing I.T. on a regular basis to work after normal hours. This did not discuss other areas of concern that are vital to keeping virus outbreaks to a minimum, these include: software patches, malware or pests, content scanning of http traffic, instant messaging, and protection of traveling users and employee access from home computers.

References

[i] "Overview of Attack Trends." CERT Coordination Center. URL: http://www.cert.org/archive/pdf/attack_trends.pdf

[ii] Ensuring Rapid Anti-virus Response Across the Network: From Desktops to the Gateway". Symantec. URL: http://enterprisesecurity.symantec.com/Content/featurewhitepapers.cfm?PID=9698913&EID=0

[iii] Thurman, Mathias. "Virus Attacks Can Enter Through Many Doors." Computerworld.com. 28, January 2002. URL: http://computerworld.com/securitytopics/securi ty/story/0,10801,67720,00.html

[iv] URL: http://service4.symantec.com/SUPPORT/ent - security.nsf/pfdocs/2000010708230148

[v] URL: http://www.sophos.com/virusinfo/notifications/

[vi] URL: http://www.antivirus.com/vinfo/

[vii] URL: http://dispatch.mcafee.com/sub.asp

[viii] URL: Security-UPDATE_Sub@list.winnetmag.com

[ix] URL: http://infosecuritymag.bellevue.com /

[x] URL: http://www.cwrld.com/nl/sub.asp

[xi] Scalet, Sarah D. "How to Plan for the Inevitable." 15 March 2002. URL: http://www.cio.com/archive/031502/plan.html

[xii] Northcutt, Stephen. The SANS Institute Computer Security Incident Handling Step By Step, Version 1.5. May 1998.

Greenwood, Darren. "How end users keep their networks secure." URL: http://idg.net.nz/webhome.nsf/UNID/9C1D168F56F8FAE4CC256B860077E129!opendo cument

Thrower, Woody. Prevent E -Mail Worms. Prevent Current and Future E -Mail Worms. 12 May 2000. URL: http://securityresponse.symantec.com/avcenter/security/Content/2000_05_12.html

Gordon, Sarah. Virus Bulletin. URL: http://www.commandsoftware.com/virus/ strategy.html

Lewis, Dick. "Real-World Scripting: Automate the Download of Virus Definition Files." URL: http://www.secadministrator.com/Articles/Index.cfm?ArticleID=9803

Greenwood, Darren. "The Virus War." URL: Http://idg.net.nz/webhome.nsf/UNID/6E513346EF90FBB2CC256B8600764E83!opendo cument

Last Updated: July 28th, 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 New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Sacramento SEC401	Sacramento, CA	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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS