Global Information Assurance Certification Paper

GIAC Advanced Incident Handling and Hacker Exploits

Practical Assignment For Online Beta Program

Option 1 – Illustrate an Incident

VBS.PLAN.A Attack on Regional Bank (An Interview)

Loras R. Even

Executive Summary:
This paper will illustrate an incident involving a macro virus attack at a large regional banking client of ours. I will attempt to describe the incident using the "six stages of incident handling" discussed in the course. I will also attempt to compare actions taken by our response team to "Best Practices" as suggested in the training material. I was not personally involved with the incident so I interviewed one of our response team members from our firm that was part of the team that responded to the client's urgent requests for help.

The incident occurred on November 17th, 2000 at approximately 4:30 PM CST. Sam, the response team member I interviewed, was at a gathering the firm sponsored to celebrate our groups first quarters results. Sam received a call on his cell-phone from the banks network administrator and the network administrator indicated that they weren't sure but they thought they might have a virus. Sam proceeded to ask for more information and after a short time realized that the bank had indeed experienced an attack. Sam called one of the other team members (John) and arranged to have them meet him at the bank.

Sam and John arrived at the bank at approximately 6:30 PM. They were able to help the client recover from the attack and put the mail service back in operation by approximately 11:30 PM the same evening.

Sam indicated that he returned to the clients facility the following Monday morning to help recover files from backups that were needed to replace corrupted files that were not discovered during the initial cleanup.

Sam was able to identify the following costs attributed to the incident:

Consulting fees:	$ 2,550
Client Downtime:	$ 8,500
Total Direct Costs:	$ 11,050

Due to valid and daily Full Backups, no files were lost as a result of the attack which helped to minimize the costs of the incident.

Preparation:

Description: Preparation in regards to incident handling simply means that a firm has prepared itself to handle or deal with incidents as they occur. Excellent preparation may even make incidents less likely! Items included in a good preparation include: Policies, People, Data, Software/Hardware, Communications, Supplies, Transportation, Space, Power and other Environmental Controls, Documentation.

Unfortunately, our firm does not have an established formal policy to handle incidents but according to Sam, we do have somewhat of an informal approach to incident handling. All of the consultants share information regarding new threats to their client's

security (both virus and firewall related) as they discover them though reading journals or if they are forwarded information from outside agencies and organizations.

Members of our firm that may be called to handle an incident are normally some of our most senior consultants. Sam explained that the reason for using only senior consultants for incidents is that they are operating specific experts, as such, the expectation is that they understand fully the implications of their actions and also understand the risk of an attack on the system.

We need to formal incident response teams with identified roles. This would help ensure that we eliminate as many mistakes as possible in incident handling and that all consultants adhere as close as possible to the six stages of incident handling.

Sam has been one of the lead consultants in the Microsoft NT group for several years. As one of our response team members, Sam has taken care to be as prepared as possible to respond to incidents as they occur and has taken the time to develop a Toolkit to facilitate handling incidents when they occur.

Sam's personal incident handling Toolkit consists of the following items:

1. Antivirus Software CD's
    a. Sam has found through experience that networks normally are installed with anti-virus software. After installation, however, the network administrators often have reduced the virus protection levels by changing the initial anti-virus configuration or even removing the virus protection software altogether. Most explanations for changing or removing the anti-virus software seem to be from attempts at optimizing performance or troubleshooting network problems; similar to firewall creep.
    b. The software CD's ensure that a team member will be able to re-install the anti-virus software if it is missing or at least be able to restore installation defaults by re-installing the software.
2. Recent Virus update files (On CD's)
    a. The live update found in many major anti-virus software vendors products has often been disabled or removed for one reason or another and the incident response team will need ready access to recent update files. Also, during the containment stage of the incident, access to the internet or network may have been removed from the affected workstations or servers. A CD again provides quick access to updated files.
3. Backup software CD's and bootable floppy
    a. Sometimes a server or workstation can be so damaged by file corruption that Sam likes to carry bootable floppies (write protected) from which he can then access backup software to restore needed files.
4. *I feel that an external Parallel connected CD/RW, spare IDE drive or possibly a tape drive would be a valuable resource as well.*
    a. *As discussed in the following containment section, often we may want to make a backup of the affected system to save as evidence or to recreate the*

situation. This would provide Sam with the capability of making this backup.

Ghost would have been an excellent tool to have used for this incident as it would have been able to create a bit-by-bit (forensic) copy of the disk drive that could have been copied and saved to a CDR or other media.

Identification:

Description: Basically, identification means being able to notice and alert others early enough to minimize damage. Key areas that need to be addressed to ensure that identification occurs soon enough are educating users what signs to look for that may indicate an incident has occurred and who in the organization they need to contact or alert.

When Sam and John arrived on site, they again spoke with the network administrator and the victim 'Bank President' that first noticed that something seemed to be wrong.

The president and the network administrator both agreed that an email on the presidents system had been opened with the subject line of "US PRESIDENT AND FBI SECRETS =PLEASE VISIT =>(HTTP://WWW.2600.COM)<=". When the email was opened by the president, he immediately noticed a lot of action on his workstation (disk lite was on solid) and it didn't seem to respond to mouse clicks and menu options. He immediately called the network administrator and they recommended that the workstation be removed from the network. The network administrator walked into the computer room and noticed that the mail server (Microsoft Exchange) was extremely busy and reported a high processor utilization as reported by Task Manager.

Sam and John, both veterans of email based attacks, both felt that the bank had indeed been attacked by a email based virus. Inspection of the Microsoft Exchange server indicated that it was still operating at approximately 100% processor utilization which confirmed that the email was indeed under attack.

After Sam arrived on site, he visited the sarc.com Internet site and performed a search on the subject line which indicated that the virus was called VBS.PLAN and would require some cleanup before the mail server could be cleaned up.

Containment:

Description: Basically, containment means isolating the virus or malicious code to systems already affected. You do not want to spread it further into the organizations systems. You also want to keep a copy of the systems in their current attacked state for forensic purposes. This phase is very similar to crime scene handling used by law enforcement officials.

Initial containment attempts by the banks personnel included:

1. Disconnecting the president's workstation from the rest of the internal LAN.
    a. This was performed in an attempt to prevent the virus from attacking other devices on the network.

       I agree with this action as at that time they were not sure if the virus could propagate to additional network resources. It could have been possible for the virus to attack data shares, online databases and other resources.

2. Disconnecting the Firewall from the Internet
    a. The network administrator was concerned that they may be sending mail to many other business partners through their Internet connection so it was decided that the external interface to the firewall be disconnected.

       Again, I agree with this action. They do not host any internal Internet services other than SMTP so there was little concern that there would be an impact to customers attempting to connect. SMTP generally will retry several times to resend mail to an unavailable server so mail will still get to them when the connection is restored.

3. Log users out of outlook.
    a. The bank used a central Microsoft Exchange server for four (4) remote locations in addition to the main location. Users were asked to log out of outlook immediately and to notify the network administrator immediately if they had received an email with the subject line of "US PRESIDENT AND FBI SECRETS =PLEASE VISIT >(HTTP://WWW.2600.COM)<=".

       Again, good action. Contain the virus to resources already affected.

       Resources used to communicate the message to users were:
        i. Public Address system at the main location
        ii. Series of phone calls to the responsible branch manager for each remote location.

       I agreed with the communication channels used. Often, I've seen fortune 100 sized organizations attempt to send an email to warn users not to open particular emails they may have previously received.

When Sam and John arrived, they had a short meeting with the network administrator to review what they already knew about the virus. Sam and John then did some initial reviews of the president's workstation and performed a short inspection of the exchange server to note the number of outgoing messages from both the external and internal sides. They noticed that over 2,500 messages were queued with the subject line of "US PRESIDENT AND FBI SECRETS =PLEASE VISIT >(HTTP://WWW.2600.COM)<=".

The network administrator "shadowed" Sam and John during their work, ensuring that the local system owners were kept up-to-date as to information discovered and progress.

They decided to immediately "shutdown" the exchange server through the "services" icon in the Control panel. One of the CD's in their toolkit had a significantly newer virus signature file than the one on the presidents workstation. They stopped the service, renamed the older signature file to *.old and copied the new version to the workstation. The service was restarted and then they performed a manual sweep of the workstation. The virus software immediately recognized the virus "VBS.PLAN" and began to prompt them as to what action they wanted the software to perform. They halted work on the workstation at that point.

I feel they should have attempted if possible to make backups of the presidents contaminated system to save as evidence and to possibly use to re-create the system if needed during the eradication step. In discussing this with Sam, it seemed as though they were in more of a headlong rush to correct the problem and lacked the resources to make a backup.

Since the exchange server was "shutdown" they reconnected the external interface to the firewall and used the Internet connection to attach to Sarc.com and search for information regarding the virus. Using sarc.com they were able to find and print the enclosed information on VBS.PLAN. The information includes steps required to successfully eradicate the virus from affected systems.

Eradication:

Description: Eradication simply means safely removing the malicious code, virus or correcting the systems affected by the incident. This phase can be the most difficult and time consuming when dealing with a virus.

Sam and John felt that when they reached the point where it was time to remove the malicious virus they were well armed with the information needed to make the fixes needed. The information provided by sarc.com included a step-by-step removal process. They did not attempt to make backups of either the exchange server or of the Microsoft NT Primary Domain Controller (PDC) as they felt it wasn't needed.

I feel this was a mistake; they destroyed potential evidence and eliminated the possibility of possibly restoring the system to the point where they began if something in the eradication process caused the entire operating system to become corrupt. Sam and I discussed this and he has agreed it may have been best to take the time to make a backup; especially since each server had it's own tape drive and backup software.

The first thing they did was update the anti-virus signature file on the exchange server, and the PDC, the presidents workstation already had the updated file on it from work performed in the containment step. They then ran the scan on the president's workstation in "auto" mode. They did not make notes about the number of affected files on the

workstation. They have run Norton's anti virus many times so they felt they new where to look for the files that could not be corrected and didn't see a need to be too concerned about the files that had been corrected.

After the scan was completed, they:

1. Deleted all quarantined files (Those that could not be fixed).
2. Used regedit to delete registry entries made by the virus.
3. Deleted files created in the Windows directory by the virus.
4. Restored clipart that could not be fixed from the Microsoft Office CD.
5. Deleted all *.VBS files.
6. Verified that logos.sys had not been modified.
7. Searched system for any hidden *.MP3 or *.MP2 files.

Best practice would have been to take the time to document ALL of the above information rather than race through it. Often, when we feel too comfortable with corrective actions is when we are most prone to overlook an important message from the system.

Next, they deleted ALL of the messages from the exchange server queues with the subject line of "US PRESIDENT AND FBI SECRETS =PLEASE VISIT >(HTTP://WWW.2600.COM)<=". I asked Sam why they didn't just let the virus software handle the corrections. The reasons behind the deletions were:

- They wanted to make sure that NO MORE emails of this type were forwarded from the organization.
- Most of the messages were queued sequentially, making it relatively easy to perform mass deletions.
- He and John felt that the virus scans would perform faster if they had less messages for it to correct.

I'm not an exchange expert so at first I was surprised that they manually deleted the messages in the queues. Sam indicated that it took 30 – 60 minutes to make the deletions. I think that it was the correct decision to delete the messages.

Then they performed Full auto scans on both the PDC and exchange servers. Again, they didn't document the number of files affected but Sam seemed to remember over that over 2,000 files on the PDC were reported as being infected. The scans took a couple of hours for each server due to the extremely large volume sizes, numbers of files and size of the exchange database.

After the scan was completed, they:

1. Deleted all quarantined files (Those that could not be fixed).
2. Used regedit to delete to look registry entries made by the virus.
3. Deleted files created in the Windows directory by the virus.
4. Restored clipart that could not be fixed from the Microsoft Office CD.
5. Deleted all *.VBS files.

6. Verified that logos.sys had not been modified.
7. Searched system for any hidden *.MP3 or *.MP2 files.

Again, best practice would have been to take the time to document ALL of the above information rather than race through it. Sam indicated, however, that this would have added several hours to the process and they were asked to attempt to keep the costs to a minimum by the client. In retrospect, the client may not have minded the extra time if they realized the potential value of the backup.

Now that both servers were "clean", Sam and John were ready to tackle all of the workstations. Luckily, the client ran LanDesk, which allowed them to push the updated signature file to all LAN connected workstations and then "force" an entire anti-virus sweep of all workstations connected to the LAN. This provided an efficient means of checking for the existence of any more copies of the virus that may exist on the workstations themselves.

As Sam and John were discussing the progress with the network administrator, it was brought to their attention that there were also a handful of laptops that were not connected to the LAN. The updated signature file was first copied from the toolkit CD to the laptops. The an auto scan was initiated.

After the scan was completed, they:

1. Deleted all quarantined files (Those that could not be fixed).
2. Used regedit to delete registry entries made by the virus.
3. Deleted files created in the Windows directory by the virus.
4. Restored clipart that could not be fixed from the Microsoft Office CD.
5. Deleted all *.VBS files.
6. Verified that logos.sys had not been modified.

Searched system for any hidden *.MP3 or *.MP2 files.

As a final step before starting the mail services on the exchange server, Sam and John decided to install the email virus scanner on the exchange server itself. Apparently, during the initial installation of the LAN, virus protection was put only on the workstations *(The client already had a copy of the email virus scanner on location, it wasn't installed!!).* This put the burden of virus detection and eradication of email attached viruses on the workstations. They felt that it would be better to have the exchange server handle the mail virus detection and eradication directly on the exchange server for the following major reasons:

1. It would help to minimize the problem of a user disabling their virus protection either intentionally or accidentally.
2. It would clean the incoming mail at the source into the LAN (The exchange server is also an SMTP server) rather than pushing contaminated mail to the clients.
3. The mail server virus scanner used (Norton Antivirus for Exchange Version 2.0) includes three levels of virus protection by even temporarily expanding attached PKZip files to attempt to identify viruses.

4. Logging can be set so that better history is kept of email attached virus incidents.

I agree with this step as it helps to build a more secure defense against future virus caused incidents. Sam felt that the virus might not have been installed initially due to concern about resource limitations on the exchange server. Careful monitoring since the installation of the scanner has indicated that the resource utilization of the scanner varies, but users have noticed no degradation in performance.

Recovery:

Description: Recovery can be as simple as restarting a server or service and validating that the systems are operating as they should (baselines are great for this!). Sometimes, depending on the severity of the incident, systems may need to be restored from backup media.

Recovery of the system after the above steps was pretty straightforward for Sam and John. They started the mail services on the exchange server and then verified that the mail server was sending and receiving mail both internally and externally. Sam and John had a few users send each other mail internally and then Sam and John dialed up and external mail account through a ISP and sent mail to the internal users. The internal mail users replied to the messages Sam and John had sent. Once Sam and John logged into their ISP accounts and verified receipt of the replies they felt comfortable that the exchange server was working.

They also checked the event logs (error) on both servers to check for any error events that may have been created. Noting that none were present, they felt all was well and decided to discuss the situation with the network administrator. The network administrator felt that things were running smooth as well (They had tested a full range of applications while Sam and John were testing mail).

I think that Sam and John should have developed a more through test, especially application test baseline as they had to return the next Monday and restore clipart files on the server for an application that the network administrator had not run. The network administrator panicked when users had trouble-locating clipart Monday as the network administrator thought that the virus was removing them again!

Follow-up/Lessons Learned:

Description: This phase is easy to skip if you are not careful as we all get busy but it is critical to the continuing efforts to improve our incident preparation. In most cases, there should almost always be an opportunity to review what happened, what was done to correct the problem and what can we do better next time.

Sam indicated that the client and network administrator learned quite a bit from the incident and Sam felt he learned a little from stepping through the interview process as well, especially information contained in the italicized parts of this document.

Some definitive areas of lessons learned as indicated by Sam were:

1. The virus signature files definitely need to be updated. The main cause of the incident was that the signature file of the presidents workstation was not updated, it was several months old. With the rush of copy-cat Visual Basic viruses, it has become more important than ever to keep the signatures up-to-date. The client indicated that they had been manually updating the signatures on workstations when they had an opportunity, sometimes they sent an email explaining to users how to update their signature file.

   Sam demonstrated that since they already had LanDesk, they could use that product to essentially "push" the updates to clients on a regular basis. I agree that this method of updating the signature files provides a better method of ensuring that updates occur.

2. Educate users! It seems that with all of the press in the news about email related viruses you wouldn't need to remind them not to open email messages with questionable subject lines but this incident is proof that the need is still there.

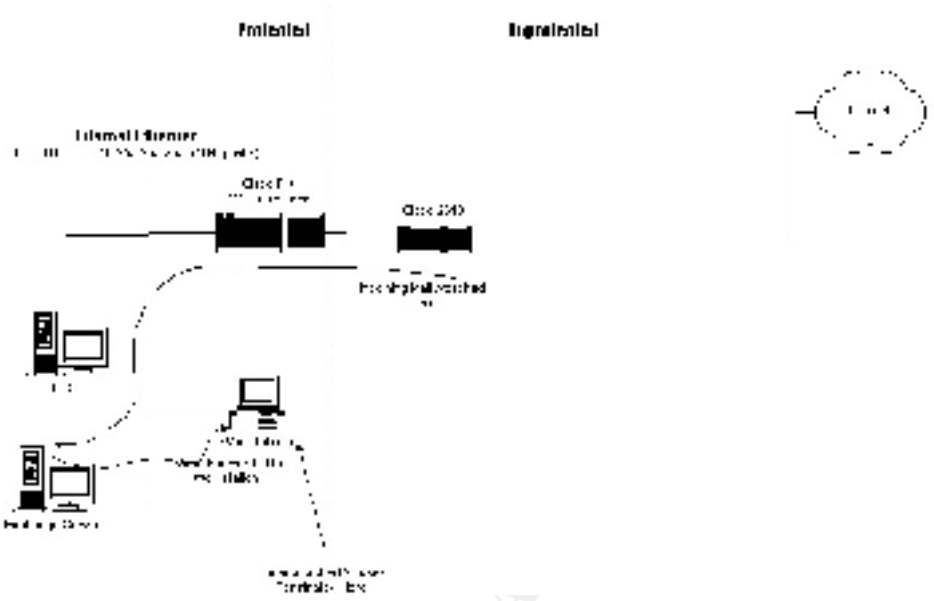
3. Unfortunately, partially due to our lack of preparation, there were really no chain of custody procedures used or any evidence saved during the incident. Volumes of evidence could have been created from an incident like this, documented and stored for future use.

   I can really see some value to better preparing our firm to handle an incident such as occurred and preparation for similar incidents is now on my todo.

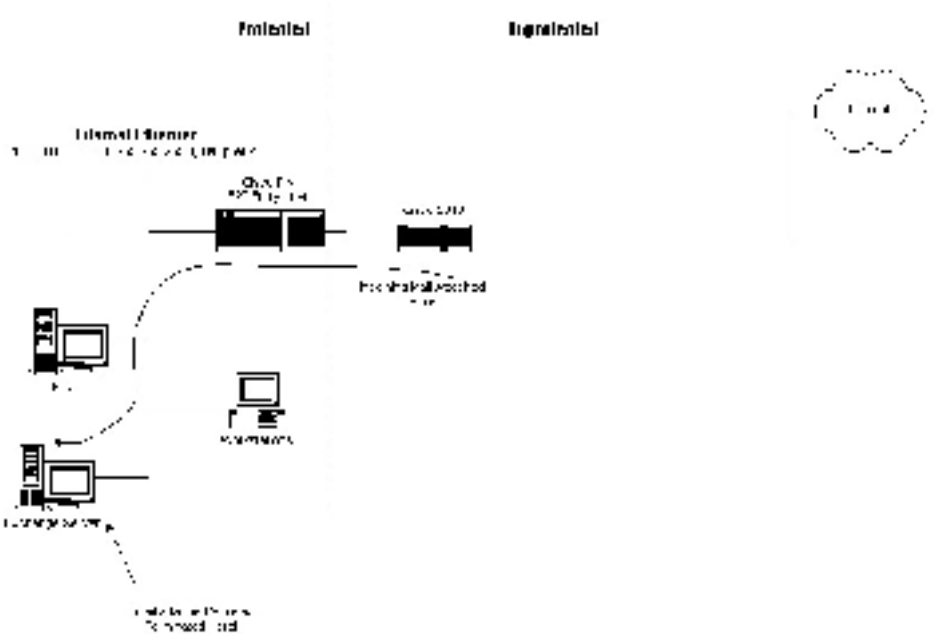
4. Email virus protection needs to be installed on the mail server. The workstation should not be left to scan the emails for viruses as the workstation is not as controlled as a server. Additionally, scanning on the server instead of the workstations can have some indirect benefits on network performance.

   Diagrams of the before and revised configurations are as follows:

Regional Bank
Original Configuration



Regional Bank
Revised Configuration



References:

The following links direct you to information regarding the vbs.plan.a cirus
http://www.symantec.com/avcenter/venc/data/vbs.plan.a.html
http://www.cai.com/virusinfo/virusalert.htm#vbsplanaworm

The following links direct you to the benefits of email server based virus protection:
http://enterprisesecurity.symantec.com/products/products.cfm?productID=12&PID=na
http://www.pandasoftware.com/

The following link identifies Virus Detection and Preventative tips:
http://dispatch.mcafee.com/virus_tips.asp?cid=1593