



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

GIAC Advanced Incident Handling & Hacker Exploits (GCIH)

A Practical Assignment for Online Beta Program, Option 1

SHOCKWAVE Virus / W32.Prolin Worm

By: Kurt Eric Steiner
March 02, 2001

Executive Summary

During the late night hours of December 4th, 2000 our organization received the first e-mail message containing the SHOCKWAVE worm attached. This recent strain of W32 Prolin worm roused users with the enticing subject line: "A great SHOCKWAVE flash movie". The message body further prodded "Check out this new flash movie that I downloaded just now... It's Great, Bye". The attachment masqueraded as a real SHOCKWAVE Flash movie file.

SHOCKWAVE is a minor combination of both malicious code and denial of service attacks. SHOCKWAVE is an e-mail worm that is propagated by Microsoft Outlook. The worm itself is coded in the Visual Basic 6 and compiled as an executable named "CREATIVE.EXE". It carries the icon of a SHOCKWAVE Media Player application, however it is not. The SHOCKWAVE virus/worm causes minor system damage. Because of the volume of email it generates, it can become a denial of service (DOS) attack.

The SHOCKWAVE virus is another variant of the W32.Prolin virus worm that arrives in a victim's Inbox as an attached executable that masquerades as a SHOCKWAVE Flash movie. Once initiated by the victim it sends itself out twice to all entries found in the Microsoft Outlook Address Book. At execution the worm copies itself to the Windows Startup folder as "Creative.exe", which causes the worm to be executed whenever Windows boots. "Creative" then moves all the .jpg, .mp3 and .zip files in the hard drive to the C:\root directory and the filenames of these files are appended with the text "Change at least now to LINUX".

Our anti-virus signatures were dated 27 November 2000 which did not detect the virus. At 8:00 on December 5th, the updated November 30th signature files were acquired from our vendor and pushed to the network via a coordinated multi team effort. We did find that some workstations were not properly configured in order to allow updating themselves with the new anti-virus software signature at user sign on. Another fix for

this was quickly pushed to the system administrators so all workstations could properly update themselves.

As a whole, our enterprise Microsoft Exchange mail servers handled the increased load on the network which was induced by some users either succumbing to the rouse or being extremely ignorant or negligent in their workstation use.

One Microsoft Exchange mail sever was allegedly infected. It was noted that many workstations in the domain had not been updated to the current standard system configuration. Post recovery investigation discovered that many users who did initialize the worms' payload had been absent on extensive travel. In their absence the worm was received in their inbox before this particular node of our network had updated the automatic anti-virus scanning file executables. These users ignored multiple splash screen warnings at the sign-on, which warned them of this virus. They blatantly or ignorantly then executed the attachment which again released another cycle of the payload.

Both system administrators and users must be able to actively verify dates of virus definitions. Users must be educated on how they can quickly verify definitions dates on their workstation. They must continually be educated about viruses and their effects that normally don't arrive conveniently during business hours. Anti-Virus programs must receive timely signature updates for them to be effective. Final lesson learned, an Anti-Virus program is only as good as it's last updated signature on the latest implemented approved standard image.

Phase 1: Preparation

ENTERPRISE

Preparation work at our organization began over two years ago when we launched our Computer Incident Response Team (CIRT). The CIRT established itself as the emergent point of contact for any computer incident via 24/7 e-mail, web link and phone. The CIRT periodically publishes timely Information Systems Security Bulletins which are distributed to all Point of Presence (PoP) personnel, System Managers and Information Systems Security Officers (ISSO). These are passed down further to the users as need arises via local area network (LAN) "net sends". These bulletins provide usable discussion of the nature of incident at hand and include solutions to fully eradicate the problem or temporarily patch until a more permanent fix is offered.

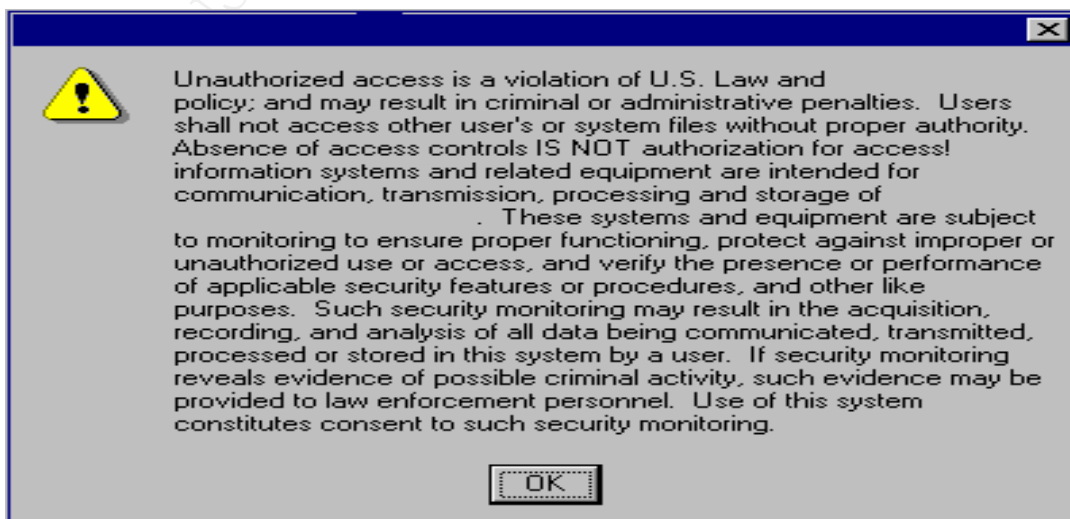
All Internet accessible servers are required to be placed in an authorized configuration and then be maintained by Internet PoPs unless a wavier is granted. The granting of these waivers is rare. The CIRT and PoPs periodically conduct vulnerability testing. All perimeter router logs are regularly monitored. All internal backbone routers are monitored. Firewalls and Intrusion Detection Equipment have been located at each Pop.

The enterprise architecture is divided in separate geographical areas that domain trust relationships do not cross. This horizontal containment helps to curtail some types of attacks. As with most organizations the exception to this architectural design is that of e-mail. The network is encrypted. Each workstation checks anti-virus signature files and updates them if needed at user logon. Users are reminded to log out each business day so up to date system back ups may be maintained and any emergent pushes can be afforded. Configuration management is tight using one standard image throughout the enterprise with minimal wavered alternative images. Each updated configuration is highly published and distributed to all levels of system management.

All our Internet mail is received by one of two Simple Mail Transfer Protocol (SMTP) gateways. SMTP is the standard email protocol of the Internet. These gateways are load balanced and can perform fail over should one of them goes down for any reason. When a message is received by a gateway, it is first run through a crude Perl Script. This strips off the obviously malicious payloads and is our way of developing ad hoc solutions when our anti-virus vendor doesn't have a solution readily developed.

The email then gets forwarded to another SMTP gateway that has "Auntie-Virus" software product loaded on it. This product looks at every attachment and screens for viruses and is more thorough than the Perl script. If "Auntie-Virus" finds an infected attachment it will strip off the payload plus forward the email message minus the attachment along to employees. In addition it copies this action to the Internet Mail Administrator and our CIRT. This is why some employees will sometimes get 'virus' e-mail that contains no attachments. Once the email is finished being processing by "Auntie-Virus" it is forwarded to our Microsoft Exchange mail servers for further processing.

Information Security Briefings are mandated upon each employee's initial user access, upon job reassignment/relocation and annual updates for all personnel. Each user must read, review and sign an extensive user agreement which receives frequent updates and improvement as required. Each user who logs onto the network is greeted with a warning banner indicating their activities may be monitored and they will be held accountable for any violations thereof. It stresses no privacy should be assumed by the user.



User awareness training is currently growing using a variety of proactive techniques. Newsletters are being published in some geographical areas and shared with other Information Systems Security Officers (ISSO) in other locals. Intranet web pages for CIRT information have been built and advertised. Additional domain specific Company Intranet web pages by various ISSOs and system managers have been promulgated to further enhance user awareness and training. ISSO's are provided the opportunity for annual training like that offered at System Administration, Networks and Security (SANS) conferences and the online Global Incident Analysis Center (GIAC) program. Some take advantage of this while others decline.

Written Information System Security policy is extremely out of date. Several updates to this policy have been attempted but have died in the bureaucratic approval process. Yet another attempt is currently underway to at least promulgate a quick change to the existing policy with hopes of a major over haul and future streamlining of the current one. Our extensive user friendly information security briefing form helps to temporarily alleviate this shortfall.

On a more positive note recent specific policy guidelines have been have been promulgated and implemented. Information covered in the guidelines emphasized the need for all employees to exercise responsible use of network bandwidth and email usage. This was promulgated company wide. Presently, there is a ray of light in gaining in intensity sight now. We hope.

Phase 2: Identification

On 30 November 2000 our anti virus vender identified the SHOCKWAVE variant of W32.Prolin.Worm and promulgated an updated their virus definitions. The initial threat assessment was that of high distribution, medium damage, and medium in the wild. Late 5 December 2000 Computerworld reported that this virus was doing little damage. Still the National Infrastructure Protection Center issued a warning that SHOCKWAVE was a medium threat do to it's "mass mailing capabilities". A few weeks later on 13 December 2000 Security Portal listed SHOCKWAVE at number one spot on their Top 20 Virus Report since "a multitude of users continued to fall victim to the promise of a great new SHOCKWAVE Flash Movie."

After SHOCKWAVE or W32.Prolin worm is executed by initiating it's payload of creative.exe it also crates a text file called messageforu.txt", which is a list of all the .jpg, .mp3 and .zip files that were changed. The following message is also seen

"Hi, guess you have got the message.
I have kept a list of files that I have infected under this.
If you are smart enough just reverse the back the process.

i could have done far better damage, i could have even
Completely wiped you hard disk.
Remember this is a warning & get it sound and clear...-
The Penguin"

The text file continues with a list of the previous locations for all the renamed files, which were moved to the C:\ directory. It also sends an email with the subject "Job Complete" and the text "Got yet another idiot" to a YAHOO mail account.

To guard against possible software and standard configuration image corruption our company does not automatically forward the vendors updated anti-virus definitions to the network. Our central configuration management team first reviews each new virus definition received from the vender on a test bed system prior to any further distributing it to the enterprise. This helps to guard against possible software and or workstation image compatibility problems.

ENTERPRISE

The method of entry is suspected to be the MS Outlook E-mail's use of a Microsoft Transport Neutral Encapsulation Format (ms-tnef), although downloading from a web based e-mail account cannot be ruled out. The ms-tnef message format allows the executable to bypass the SMTP Perl script, which quarantines all messages with executable attachments.

The executable Trojan virus employees a method where it grabs addresses from a person's inbox then sends those addresses an e-mail with the virus as an attachment. By using inbox names the rogue message has some creditability since it came from someone the victim knows therefore making it more likely to be activated.

Several employees fell victim to this rouse. One advantage for the company is that the addresses that are used are configured in SMTP format, which forces them to go out the SMTP gateway and then come back in. This allowed the Internet Mail administrator to use "Auntie-Virus" with an updated signature to strip of the executable before it re-entered into the network. Although it can at times put a heavy load on the SMTP gateway this configuration helps to limit the effectiveness of a virus.

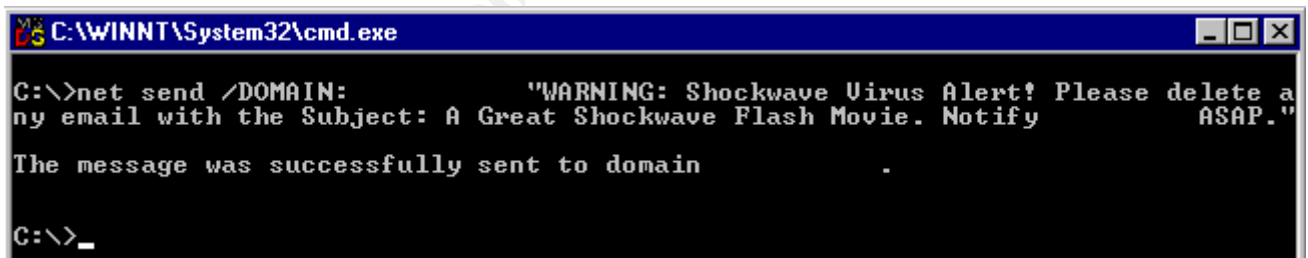
To quickly educate all employees, System managers were instructed to send out broadcast messages using Windows NT "net send" command. The Network Engineering group was able to discern a general size signature of the payload. This allowed them to pluck infected messages directly out of the SMTP Mail Queues. This combination of team effort allowed a rapid containment of the virus with only a moderate effect on the enterprise email system for approximately 12 hours. Only one domain circuit was saturated due to excessive traffic in the enterprise volume which cannot be entirely blamed on the virus but did not help the situation. No other systems reported to been overly burdened or disabled by the virus.

DOMAIN X

The initial emails containing the SHOCKWAVE attachment arrived at our organization during the late night hours of December 4th, 2000. It is believed that the initial receipt of this mail was received via an employee in another one of our affiliated domains linked by a business to business intranet using Microsoft (MS) Outlook rich text message that employs MS Transport Neutral Encapsulation Format (MS-TNEF). The attachment was opened and the payload launched causing a high volume of email traffic to be generated throughout the network enterprise.

During the early dawn hours of December 5th a few emergent notification emails from various valid trusted company information system sources were made in response to the initial late night receipts of the virus as employees shuffled into work.

At 8:03 another notification from a trusted company source was distributed to all system administrators instructing them to immediately conduct a "net send" in each of their respective domains to warn all employees of this vulnerability. This included explicit easily to understood directions on how to quickly conduct this event. It included a bit map example to use as a template of what the command should look like. This helped to guard against creating any additional confusion during this event. In addition, it helped to eliminate any possible mistakes made in a potentially stressful situation among those junior less experienced or new system administrators.



```
C:\WINNT\System32\cmd.exe

C:\>net send /DOMAIN: "WARNING: Shockwave Virus Alert! Please delete any email with the Subject: A Great Shockwave Flash Movie. Notify ASAP."

The message was successfully sent to domain .

C:\>_
```

At 8:16 a different trusted originator again repeated these instructions.

DOMAIN Y

Domain Y promulgated an all user notification bulletin advising all users to be cautious of the holiday theme viruses and videos. The notification stressed not downloading or forwarding any of those cute holiday programs. It covered various items including the potential of the SHOCKWAVE virus on parts of the network. It warned of the details of SHOCKWAVE, explained how to identify it and then to properly delete it if a user should encounter it first hand. They also sent informative splash screens via "net send".

A few days later several employees who had been traveling returned to their respective offices in Domain Y. These returning users logged in, ignored the detailed splash screen warnings pertaining to the SHOCKWAVE virus that had been sent via "net send". These users proceeded into their email accounts and when seeing the enticements to check out a cool video clicked on the creative.exe attachment. At one location while an ISSO was on the phone with a system manager discussing the procedures to help combat the situation another employee logged on right next to the system administrator. This individual quickly proceeded to click through all the splash screens and launched the cool movie! The system administrator quickly shut down the workstation but the payload had already done its damage. One Microsoft Exchange sever in that domain received over an estimated 100,000 copies of SHOCKWAVE emails.

Phase 3: Containment

ENTERPRISE

At 8:37 am our CIRT issued an Information Systems Security Bulletin (ISSB) to inform all system administrators and security personnel of the new virus/worm vulnerability. The ISSB provided a full discussion of the virus. The alert notified that appropriate anti-virus signature files had been pushed to all sites. It repeatedly informed all system managers to quickly alert and educate their users via "net send" broadcast command and for users to be aware of the SHOCKWAVE VIRUS and to properly delete any occurrences of the virus and notify help desk personnel of any occurrences.

Phase 4: Eradication

The solution for eradication was ensuring that all servers and workstations configurations had been updated to the most recent one and verifying that the machines had received the updated definitions. The proper configuration and log on command files would enable the virus definitions to be updated as each user logged in.

After successfully running the updated anti-virus definitions on any infected workstation any effected files could be easily restored to their original state. The file "messageforu.txt" contained a list of the original path and file names of any maligned files. Changing the file extensions to their original state would complete this restoration process.

DOMAIN X

At 9:40 Domain X started to receive reports that some desktops were not updated to the current November 30th 2000 anti-virus definitions pushed earlier in the morning. In fact, these desktops still had anti-virus definitions dated January 5th 2000! Notification was sent to all system administrators to verify if their servers did have the new definitions.

At 9:59 the problem was isolated to that being the LOGON.CMD files on the application file sever was missing a couple of entries which were causing the individual desktops to fail in updating themselves when users signed on with each new session. At 10:40 the enterprise's central quality assurance configuration management team sent details confirming the proper set up of the recent change of workstations being able to automatically update themselves upon each user logon. By 11:31 the application servers in Domain X were updated and tested and all system administrators were notified of the required changes to get their desktops to update.

None of the Microsoft Exchange mail servers in Domain X were burdened with an excessive or unmanageable volume of the SHOCKWAVE generated emails. No known users in the domain opened and executed the payload. There is strong user awareness in Domain X. This does not mean we can let up in our user awareness and education programs, as employee turnover for a variety of reasons is a continuous revolving door. User awareness, configuration management and effective system administration are just a few parts of an effective layered security program.

DOMAIN Y

Against the recommendation of the Enterprise management Domain Y decided to remove the mail server until all workstations could be verified to have the most up to date desktop configuration. It is believed the Microsoft Exchange server would have successfully processed the amount of traffic it had received rather than creating a large backlog to process once it was returned online. User email was out for approximately 24 hours. During that time the Microsoft Exchange server was rebuilt with and updated configuration and workstations in the Domain were verified to have the correct configuration.

Phase 5: Recovery

ENTERPRISE

Overall the network did not have any difficulties in processing the email created by SHOCKWAVE. Some Microsoft Exchange servers did work hard in processing the extra load. There were no server crashes reported.

DOMAIN X

After discovering that some servers and workstations were not properly configured to automatically process and distribute update anti-virus definitions the network system administration quickly combated the attack.

DOMAIN Y

Still no server crashed. System administrators made the call to take one Microsoft Exchange server off line after it was allegedly infected. Post event review revealed they made the assumption the server could not keep up with the load it was processing. It appears the server could have successfully processed the load.

Phase 6: Lessons Learned

Today if we generated an email with an attachment "virus.exe" and mailed it to our employees undoubtedly some users in the enterprise would still open and execute it. Constant and never ending user awareness training is a must. We must be creative in marketing this awareness in a variety of delivery methodologies. These methods must have effective user indoctrination at initial system access and continued follow up education. Users must be providing easily available information on Intranet web pages to assist in enhancing their security awareness.

In addition to continues effective user awareness, the SMTP Gateway Perl Script and Auntie-Virus cannot be used as a total crutch to prevent Internet borne viruses. They can only be used as part of a total Security Process that consists of a combination of Gateways, E-mail Servers, File Servers, and Workstations. Servers and workstations must be verified to have the proper up to date configuration changes and upgrades. Patches must be done expediently including service packs and any crucial hot patches directed by the configuration management team.

Both system administrators and users must be able to actively verify dates of virus definitions. Users must be educated on how they can quickly verify definitions dates on their workstation. They must continually be educated about viruses and their effects which normally don't arrive conveniently during business hours. Anti-Virus programs must receive timely signature updates for them to be effective. Final lesson learned, an Anti-Virus program is only as good as it's last updated signature on the latest implemented approved standard image.

Notes

The events described herein were compiled via interviews and general research. I was not on site and directly involved in this event; however, I normally work directly with Domain X. In order to effectively sanitize all information contained in this report many details were either left out completely or generalized in order to meet my companies' sanitation standards and for general readability.

References

1. "Computer Security Incident Response, Step by Step Guide", Version 1.5, The SANS Institute, 1998.
2. SANS GIAC Report 13 December 2000 "The Funky Worm"
URL: <http://www.sans.org/y2k/121300-1000.htm>
3. Symantec "W32.Prolin.Worm"
URL: <http://www.symantec.com/avcenter/venc/data/w32.prolin.worm.html>
4. Security Portal "W32 Prolin"
URL: <http://securityportal.com/research/virus/profiles/w32prolin.html>
5. Security Portal "Top 20 Virus Report", 13 December 2000
URL: http://securityportal.com/research/virus/top20_20001213.html
6. Computerworld "SHOCKWAVE Virus Appears To Do Little Damage" (5 December 2000)
URL: http://computerworld.com/cwi/stories/0,1199,NAV47_STO54734,00.html
7. National Infrastructure Protection Center "Assessment 00-061 W32/Prolin@MM Internet Worm. (5 December 2000)
URL: <http://www.nipc.gov/warnings/assessments/2000/00-061.htm>
8. Security Portal "Top 20 Virus Report" 13 December 2000
URL: http://securityportal.com/research/virus/top20_20001213.html