Use offense to inform defense.
Find flaws before the bad guys do.

GIAC Advanced Incident Handling and Hacker Exploits

Practical Assignment for SNAP

Material submitted by John J. Gerber
Attended: Orlando SANS 2000
Date Submitted: June 15, 2000

Contents

Executive Summary

On May 4th, 2000 at 7:45am, our organization received the first e-mail message with the ILOVEYOU virus attached. ILOVEYOU is a Visual Basic Script that comes in an e-mail attachment. It acts as a virus compromising the integrity of the workstations on the infected Windows machines. It also acts as a network worm resulting in a denial of service. Because of the volume of email it generates, it can saturate network bandwidth and disable mail servers.

The ILOVEYOU virus will destroy files and replicate itself by manipulating files and causing e-mails containing the script to be mailed electronically to others users. The virus began proliferating in the Far East at approximately 3:00am EST on May 4th, 2000. See Appendix for the ILOVEYOU virus timeline. Based on our company policy, in order to stop the proliferation of the virus, we shutdown our Microsoft Exchange server by 8:05am.

While the ILOVEYOU script only affected mail server and a limited number of individual workstation, it ended up costing the company approximately 230 man-hours. Twelve employees had their workstations infected, costing each employee a full day work. In order to inform employees throughout the facility about the virus and what steps were being taken to eradicate the virus, an assembly was called. The assembly cost the 112 employees, one hour each. The three members of the computer incident response team (CIRT) spent approximately 11 hours each working on the incident. Normal business operations were disrupted for the day and it is difficult to estimate productivity loss due to the Microsoft Exchange server being unavailable.

The organization did save money by having effective incident handling procedures in place. The incident was dealt with in a timely manner, containing the problem before most employees had the opportunity to become infected. Management, having been part of our efforts to develop the policies, was well educated on the risks of opening attachments. This allowed management to avoid avoided having their machines infected.

The incident did reveal a few shortcomings in our organization's readiness in handling such a denial of service attack. The CIRT had to contain the situation by shutting down the mail server. A virus filtering software package on our mail server would have allowed the CIRT team the ability to deal with the virus while mail operations continued.

Our organization needs to invest more time and the money in educating our employees. With limited resources, efforts have been focused on securing our systems and networks against attacks. Employees need to be educated concerning the role they may inadvertently play in disrupting the organizations services and compromising the systems. With better education, we could have avoided the infected PCs and the assembly meeting, saving 200 man-hours.

What follows is a description of the ILOVEYOU virus attack, our organization's security preparations prior to the script, how our CIRT dealt with the attack, and finishes with what lessons were learned.

Phase 1: Preparation

Preparation work at our organization began after I attended my first SANS conference in December 1999. While we did have a few policies in place, security policies had grown out of existing physical security policies. Policies dealing with computers were lacking or were not properly focused. Most of the preparation work this past year has been on non-denial of service attacks. The ILOVEYOU virus provided a valuable opportunity for our organization to analyze how the CIRT handled preparation, identification, containment, eradication, recovery, and finally what lessons were learned. Below is a description of the preparation work done in securing our systems.

We have had a policy on the presumption of privacy for many years. It outlines that electronic mail stored on company servers is the property of the company. It also states:

> *Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign.*

Each user must sign a statement agreeing that they understand the policy and will abide by it. See Appendix for documents entitled "Computer User Security Agreement" and "Rules of Behavior". Warning banners have been posted since December 27, 1999 on all our systems (UNIX, VAX, and Windows machines). The warning banners are included in the Appendix.

Our organization has also setup up a network intrusion detection system using Shadow, for monitoring and analyzing the network traffic. We have setup a syslog server along with a time server in order to pull the log files together for better system wide monitoring. We use programs like Swatch for looking for specific signatures and reacting appropriately. We get additional logs from such programs as TCP Wrapper and Psionic Portsentry. We also monitor our firewall and router logs.

Vulnerability assessment is done regularly. Against our network we run vulnerability scanners such as SAINT (Security Administrator's Integrated Network Tool) and Nessus. We run port scanners using Nmap. We run Firewalk against our firewalls.

In configuring our systems, we have gone through Hal Pomeranz course and the course notes on "Building Bastion Hosts with Solaris". We have followed the SANS Institute survival guide, "Solaris Security: Step-by-Step" and "Windows NT Security: Step-by-Step." The courses at SANS have helped us design our ACLs for the perimeter routers and the rules for our firewalls. We back up the systems regularly and keep up on patches

for the various operating systems. We do rotate out a set of backup tapes to an offsite location. Both locally and offsite, the backup tapes are kept in a secure location.

We have developed management support for our organization's incident handling capability. We have the political support, though funding support is lagging behind. Hopefully this should change in the upcoming fiscal budget. For the remaining quarter, funding is more limited and focused on training and certification of our technical personnel. Political support has been gained by collecting articles, cases of break-ins and other incidents, and information gathered through log files.

Our policy on incident handling is being reworked based on the information gained at SANS. Our organization requires more of a decentralized, distributed organization in incident response. Within our company, our CIRTs are distributes among several locations and levels within the company. This allows us to specialize the teams in the needs of its local constituency. We do maintain a centralized computer security activity team, but they more acts to log incidents and facilitate communications among the lower-level teams. The centralized CIRT coordinate contacts with investigative agencies and the press.

Within our organization, we have setup a team to review and develop our policies. We have identified qualified people to act as the On Site Incident Handling Team at the various locations and as part of the Command Decision Team. We have established a primary point of contact (POC) along with backup for the POC. We have chosen individuals who are very capable of disseminate information to the public and senior management.

Our organization has created a call list and appropriate methods for informing people quickly. In addition to work and home phone numbers, members of our CIRT have been issued alphanumeric pagers, which allow informative messages to be sent out both via e-mail and the web. Members of the CIRTs are expected to have their pagers and the contact information with them at all times.

Our organization has worked on developing an operations handbook. The handbook contains procedures that the members will follow and refer to in daily activities. The handbook is an evolving document changing as the members gain experience and benefits from lessons learned. We have had it reviewed by our company's legal advisors.

The operations handbook contains:

- Staffing information - contacts, telephone numbers, FAX numbers, pager numbers
- Hotline Use - numbers, on-call lists
- Constituency Communications - procedures for receiving and sending information
- Incident Reports - incident identification forms, incident survey forms, incident containment forms, and incident eradication forms
- Computer Equipment – administration policies, configurations, procedures
- Administrative Procedures – expense reports, travel, security clearances

- Contacts within investigative agencies
- Dealing with media – press reports, clearance process
- Vendor Contacts

We have also developed a jump bag for each incident handler. The jump bags include the following:

- Tape recorder with extra tapes and batteries
- CDs with core binaries of our organizations operating systems
- CDs with forensic software
- Fresh tapes for backing ups
- Windows resource kit
- Operations handbook
- Corporate phonebook

Administrator passwords to every system are accessible on site at the different locations. Passwords are kept in sealed, signed, and labeled envelopes locked in a fireproof safe. It is the responsibility of the system administrators to ensure the passwords are kept up to date. Our training exercises allow us to test the company's readiness.

Education of users is not currently in an organized manner. We have set up an information repository on our intranet. Information kept in the repository include:

- Alert archive
- Description of the CIRT and related information
- Security policies
- Procedures for reporting suspected problems or incidents
- Self-help information
- Information about current threats, such as viruses or software vulnerabilities

We have worked on developing interfaces with other CIRTs and law enforcement agencies. We have met with representatives from the local FBI branch.

Phase 2: Identification

The initial ILOVEYYOU script was attached to an e-mail that was received from one of our employees at 7:45am. The employee opened the attachment, and people across our organization began to receive e-mails shortly afterwards. Minutes after receiving the e-mail, other users began to open the attachment causing a high volume of e-mail traffic to be generated.

I was the initial person on site. The high number of e-mails being sent with subject line "I LOVE YOU" alerted me to the problem. I contacted, via his pager, our POC, Denny, in order to alert him of the problem. The worm nature of the ILOVEYOU virus was very

observable. The Microsoft Exchange server queue and log files confirmed that our mailer was flooded with email messages. Our network monitored demonstrated the increase in traffic.

I wanted to get a better idea of the scope of the incident. I saved the attachment to a floppy, and then viewed the virus from a machine not hooked up on the network. We have a few machines setup for testing code in relation to our security efforts. Viewing the attachment revealed that the script went beyond bombarding mail servers. I quickly saw the virus was making modifications to files and the script was accessing the Internet via WWW and e-mail.

I now had a good idea of not only the existence of an incident, but the scope. Further details about what the script was doing would be learned later.

At 7:55am, I was on the phone with Denny. He was on his way in and would inform upper management. I quickly updated Denny on what occurred, and we agreed on an initial course of action. Our computer incident response team would consist of Denny, Carroll, and myself.

Phase 3: Containment

Based on policy setup for dealing with viruses, I knew I needed to first contain, clean, and deny access. I began by shutting down the Microsoft Exchange server. The server was down by 8:05am. Fortunately, the virus hit before the majority of employees had time to access their mail. We wanted to avoid the virus getting out of our organization. Our servers are located in a secure room, so I was able to get right to work without having to clear the area.

While shutting down the mail server, Carroll arrived. I briefed Carroll on what was occurring. After shutting down the mail server, from 8:05am until 8:15am, I disabled inbound RAS connections and Web access to email.

Carroll began work on getting a building wide announcement informing the employees that our organization was dealing with a virus, people should not open up any attachments, and the Microsoft Exchange server would be down until further notice. Those who had accessed the attachment were instructed to disconnect their machines from the network. The announcement was made at 8:23am. At this point, I began to fill out incident identification forms (see Appendix). Carroll began work to ensure the infected people were disconnected from the network. I pulled from the mail logs a list of the infected machines. By 8:30am, messages were posted at each of the entrances informing the reader of the virus. Between 8:30am and 8:45am, I finished filling out the incident survey form and the incident containment form (see Appendix).

Denny arrived at 8:45am and took over as lead handler of the incident. I updated him on what had occurred up to that point. I also provided him with the incident notebook

containing the incident forms that had been filled out. Carroll, Denny, and I continued to work on the incident. Management announced a building wide meeting to occur at 10:00am in order to update the employees. We were to meet with management to update them at 9:45am.

Between 9:00am till 9:30am, Carroll, referencing the incident contact list, called our information service provider along with two computer CIRTs outside our organization. His mission was to gather information on what they were experiencing. Our centralized CIRT was alerted. Being located on the West coast, they were unaware of the virus. The team on the East coast was also dealing with the problem.

From 9:00am until 9:10am, I took a more in depth look at the script. We needed to determine the risk of continuing operations. The ILOVEYOU virus is a Visual Basic Script (VBS). It is a macro virus consisting of code that is embedded in an e-mail attachment. It will destroy files and replicate itself by manipulating files and causing e-mails containing the script to be mailed electronically to others users. It can also be classified as a worm in that it propagates itself through networks.

The ILOVEYOU script will send itself to all recipients found in a user's Microsoft Outlook address book. The script will work for e-mail programs other than MS Outlook (such as Lotus Notes). The only part that does not work is the propagation via e-mail. The script targets Windows 98 and Windows 2000 operating systems by default and Windows NT 4 and Windows 95 if a VBS host engine is installed. It is limited to users of the Microsoft Windows operating system. It does not have a limit on the number of recipients, so it spreads to every address book entry.

The e-mail carries a Visual Basic Script with the subject "I LOVE YOU" and a message that says, "kindly check the attached LOVELETTER coming from me." The attachment is named "LOVE-LETTER-FOR-YOU.TXT.vbs."

The ILOVEYOU script has the potential to overload mail servers due to the volume of mail sent out automatically. The ILOVEYOU script also sets the default page of Internet Explorer to get the copy of WinFAT32.EXE and WIN_BUGFIX.exe. It sets registry entries so that MSKernel32.vbs, Win32DLL.vbs and WIN-BUGSFIX.EXE execute on start up. It installs a program that steals passwords. This program becomes active when the recipient opens Internet Explorer and reboots the computer. The ILOVE YOU script searches through all the subdirectories on local and attached network drives overwriting files with the extensions .JPG, .JPEG, .VBS, .VBE, .JS, .JSE, .CSS, .WSH, .SCT, .HTA, .MP3, .MP2 with the ILOVEYOU script while adding a .VBS extension to all these files.

A method to remove the virus is included in the Appendix. Most popular virus detection programs now carry eradication capabilities. The virus hit so quickly on May 4th, the signatures/updates to the virus software did not exist until the middle of the day.

Based on what we learned about the virus, we choose to lock the accounts of the people who had been infected. Denny had all the account locked by 9:15am.

From 9:15am until 9:30am, I searched the Internet for additional information on the virus. Information from the Internet revealed that the virus was launched internationally. At 9:15am, Denny went to talk with the original person within our organization who opened the attachment. By 9:30am, Denny contacted the site that initiated the e-mail to our organization. We knew the company, and they were also dealing with the virus/worm.

At 9:35am I initiated a backup on one of the infected PCs. From my jump bag, I used my burned in CD to load my own critical binaries. I set up the system paths to run from them. Then I was ready to make a backup of the system. I wanted to follow the procedure outlined in our incident handling policy even though it was pretty certain that the evidence we collected would not be involved in prosecution of the originator. I initiated a backup using the Symantec Norton Ghost software. This allowed me to make a backup of the image of the disk.

At 9:40am, Carroll, Denny, and I met to discuss our various experiences. We were comfortable that the virus was contained within our organization, and eradication could occur. At 9:45am, we met with management and updated them. From 10:00am until 10:45am Denny and Carroll met with the employees and answered questions. I stayed with the backups, and searched the Internet for additional information.

At 10:50am, Carroll contacted our information service provider, and the CIRTs he had been in contact with earlier. Denny and I did additional searches of the Internet and began looking at the major anti-virus software sights to see if they were providing information and eradication techniques.

At 11:15am, we examined our network intrusion detection system, router, and firewall log files to see if any unusual traffic was being generated either entering or exiting our network. We did not see anything out of the ordinary.

The pizza arrived around 11:30am; compliments of management. It was a good opportunity to discuss where we were and our future steps in eradicating the virus.

Phase 4: Eradication

By noon, we had detailed information on how the ILOVEYOU script operated. Having the script to examine provided us the opportunity to confirm outside analysis of the script.

At 12:40pm, Denny began working at clearing out e-mail attachments that contained the ILOVEYOU script. He searched and deleted all VBS files on the Windows NT servers.

We would have to wait until later in the afternoon before gaining access to the anti-virus software. While the anti-virus software companies were beginning to come out with eradication software, their sights were being hit so heavily as to not be accessible.

At 2:10pm, we received a floppy disk with an anti-virus software program. We choose to try it on one of the infected PCs. At 2:35pm, we received a report outlining the manual method for removing the virus (see Appendix). This allowed us to compare the results of the anti-virus software to the steps outlined in the manual method. We held off using the anti-virus software in mass until we were able to compare the results. The anti-virus software completed at 3:30pm. By this time, we had another anti-virus software program available to us. We ran the second anti-virus program against the machine.

Denny began cleaning the network drives at 3:00pm. At 3:45pm, I did a vulnerability analysis of the PC that had been cleaned up. I ran Nmap against the machine, and Nessus and Saint. No vulnerabilities were detected.

At 4:00pm, we began to visit each of the infected PCs, running the anti-virus program on each. On the network, the updated signature file was made available, and an announcement was made to all employees to run the anti-virus software with the new signature file against their disks.

At 5:30pm, I took another look at the network intrusion detection, router, and firewall log files. I then ran Nmap against our network. Everything appeared normal.

Phase 5: Recovery

Denny had been familiar with a software package, ISSCAN. ISSCAN is a utility that will eradicate the virus from an Exchanger Information Store. He had made a recommendation to management a few months before that our organization should purchase this software package. Unfortunately, he was told that money was not available at that time. At 3:30pm, Denny was informed that money would be allocated for the purchase of ISSCAN. The software allowed for 30 days free evaluation. Having already tested the software, Denny implemented the anti-virus software on the Microsoft Exchange server. He ran ISSCAN against the Microsoft Outlook Exchange Information Store.

At 6:10pm, our company's Microsoft Exchange server was brought back on line. At 6:15pm, we were testing it. By May 5th, we had examples of e-mail messages containing the virus that had been blocked by the software.

The virus had replaced a lot of files on people's hard drives and network drives. These would be restored over the next couple of days. On May 5th, the people who were infected by the virus, came to Denny to have a new passwords generated on their accounts. Their accounts remained locked until they had new passwords generated.

In the days that followed, we continued to keep a close eye on the network watching for any unusual network traffic.

Denny restored files damaged by the virus. At this point we were comfortable restoring the files using Computer Associates ARCserve software. The Windows machines are backed up nightly using this software package.

Phase 6: Lessons Learned

At 6:30pm, the CIRT met to discuss the day's activities. We discussed what had occurred.

On the positive side, the CIRT contained the problem in a timely manner. The infection was limited with no negative publicity. The incident did reveal a few shortcomings in our organization's readiness in viruses handling. While we have policy requiring the installation of anti-virus software, users became reliant on the anti-virus software to protect them. One member who opened the attachment stated that they ran it through the anti-virus software, and when no virus was found thought it was safe to open the attachment.

We discussed the ISSCAN program and how it would help in future incidents. We also discussed the need to educate employees concerning the role they may inadvertently play in disrupting the organization's services and compromising the systems. The virus also taught us that we needed take a closer look at our policies and update them. It can be argued that there is no reason for our organization to allow attachments to be sent via e-mail. We can make files available to users over our Intranet. This issue is still being discussed.

Members of our team could use additional training across platforms. While everyone took on assignments, some delays were introduced just out of not being familiar on the particular operating system. We still need to develop checklist style documents to help step members through operations under different incidents on different platforms.

Communication onsite was good mostly because the incident was relatively easy to contain. It did demonstrate how easily communication could have degraded under more stressful situation. International communication would also have helped minimize the impact of the virus. We had branches in Europe that could have informed Western branches of the situation. Our policies need further examination to ensure that they fit our company's needs. Analysis of the cost of the incident was generated and reported to management.

Backups

While information from the Internet revealed that the virus was launched internationally, we did perform a backup on one of the infected PCs. I wanted to follow the procedure outlined in our incident handling policy even though it was pretty certain that the evidence we collected would not be involved in prosecution of the originator. I initiated a backup using the Symantec Norton Ghost software to make a backup of the image of the disk.

A description of the hardware is as follows:

Hardware Manufacturer: Dell
Serial Number of CPU: 2154889570
Corporate Property Number if applicable: 000076
Operating System type/version: Windows 95
Disk Capacity (if known): 8G hard drive
Tape Unit: Hewlett Packard SureStore DAT 24x6

At this location, nightly incremental backups of the Windows machines are done using Computer Associates ARCserve products. Employee's PCs are backed up incrementally throughout the week, with full backups done Friday evening starting at 10:00pm.

No problems were encountered while backing up the employee's PC using Symantec Norton Ghost, nor were there any problems encountered restoring files using ARCserve.

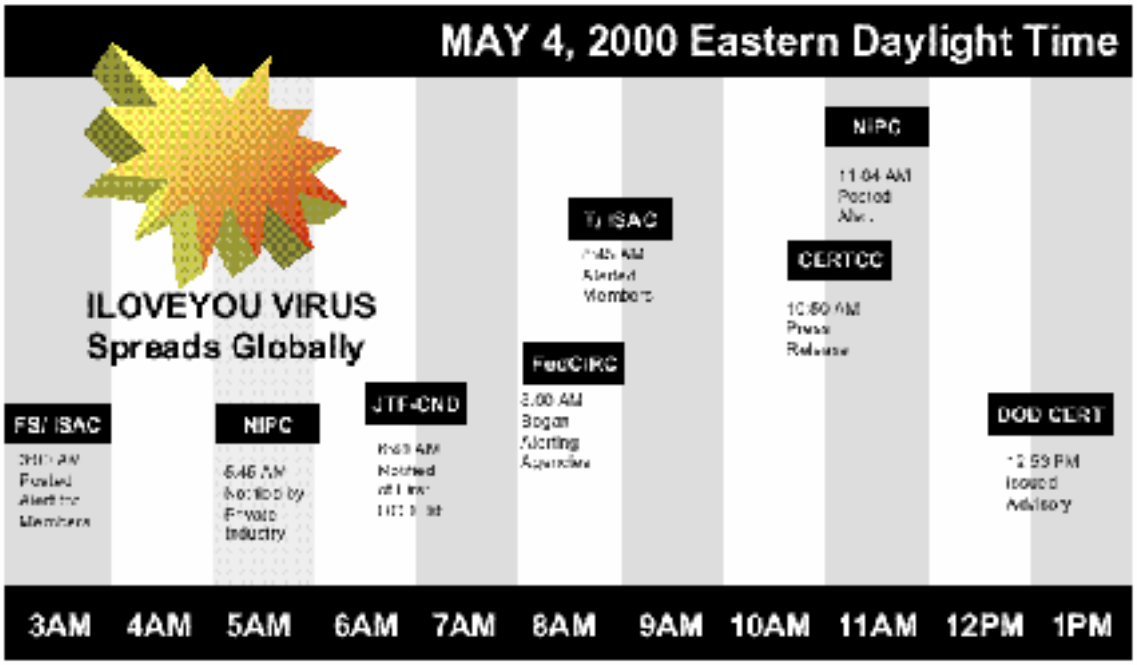
Chain of Custody

The backed up tape remained with me throughout the day. At the end of the day, before we met to discuss lessons learned, we gathered up the incident forms and notes. Denny made four copies of each. Each member of the team kept one copy. We took the tape recording each of us had, and made copies. We prepared two folders, each containing the set of notes and forms generated that day, and the tapes recordings. We provided the on site security manager, Pat, with one folder. In Pat's folder we also included the Symantec Norton Ghost backup tape. She provided us with a receipt inventorying each item. Pat stored that information in a safe. Denny took the second folder, which would be stored offsite.

Appendix

ILOVEYOU Virus Timeline

The following timeline was generated by the United States Accounting Office.



- The virus began proliferating during business hours in the Far East, while the United States—a 12-hour time difference away—was still sleeping. The virus spread with unprecedented speed through Asia and Europe. By the time it was 3 p.m. in Hong Kong, it was 9 a.m. in Western Europe and the impact of the virus was becoming evident.
- Meanwhile, a private sector group, the Financial Services Information Sharing and Analysis Center (FS/ ISAC), had also discovered the virus and, at approximately 3 a.m. EDT, posted an alert to its members.
- At 5:45 a.m. EDT, a representative from private industry notified the National Infrastructure Protection Center (NIPC), located at the Federal Bureau of Investigation, of the problem.
- The Department of Defense Joint Task Force for Computer Network Defense (JTF-CND), which operates a 24-hour global operation center, was first alerted that the virus had hit DOD at 6:40 a.m. EDT by one of the military services. After about an hour of analysis to determine the nature of the virus, JTF-CND began to notify the various DOD components individually.
- By 7:18 a.m. EDT, the Telecommunications Information Sharing and Analysis Center (T/ISAC) received a message that one of its major carriers was "taking severe actions to close its e-mail gateways" because of the ILOVEYOU virus.
- At 7:45 a.m. EDT—2 hours after it was first notified of the virus—the NIPC notified FedCIRC of the rapidly spreading virus, and FedCIRC began notifying senior agency officials via phone and fax.
- At 11:00 a.m. EDT, the NIPC posted a short alert paragraph on its home page warning about the ILOVEYOU virus. At about the same time, the CERT-CC sent an e-mail to the media stating that it had received over 150 reports of the virus.

Removing The ILOVEYOU Infection

The procedure for removing the is as follows:

1. Look for the following files and delete them if they exist:

   - MSKernel32.vbs in Windows\System
   - Win32DLL.vbs in Windows
   - LOVE-LETTER-FOR-YOU.TXT.vbs in Windows\System (you may also see a
   - LOVE-LETTER-FOR-YOU.HTM - delete this as well)
   - WinFAT32.EXE in Internet download (may not be there)
   - WIN-BUGSFIX.EXE in Internet download (may not be there)
   - script.ini in mIRC directory

2. Click on Start, Run and type regedit <return>. This will invoke the registry editor. Navigate to:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

   and delete the entry for MSKernel32 and delete the entry for WIN-BUGSFIX if it is there. Then navigate to:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

   and delete the entry for Win32DLL

3. Search for all *.vbs files on your system and delete them. Note that there will be a lot of files that used to have vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3 and mp2 extensions (and may now have extensions like *.jpg.vbs). Delete all of these files. Do not open them as this will cause a reinfection.

4. Start Internet Explorer. It will attempt to load a page that no longer exists. Click Stop. Then go to Tools, Internet Options and change the home page back to what you want it to be. If you do not use Internet Explorer, delete the entry that is there.

   Note that step 4 can also be accomplished by changing the registry settings for the home page at:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Start

Warning Banner

NOTICE TO USERS

This is a <Department Name> computer system and is the property of <Company Name>. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, <Department Name>, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or <Department Name> personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Computer User Security Agreement

The <Policy Reference Number> made security programs for all <Company Name> departments mandatory for computer systems which process sensitive unclassified information. As a computer user at the <Department Name>, it is your responsibility to protect the computing resources and information as required by <Company Name>. You must acknowledge your awareness, understanding, and acceptance of the following security requirements and responsibilities.

- I am aware that any computer accounts, User IDs, and/or Passwords assigned to me are to be used only by me and are not to be divulged to any other person for any reason.
- I am aware that all <Company Name> computing resources (i.e., hardware, software, and information) are for use in official duty or officially sanctioned functions and activities only.
- I am aware that activities on <Department Name> computer systems may be monitored and recorded and subject to random audit. I understand that use of the computer systems is expressed consent to such monitoring and recording.
- I am aware that I must protect all computer resident information from unauthorized access, disclosure, modification, or destruction to the best of my ability.
- I am aware that access to sensitive/proprietary information is restricted to authorized personnel only, therefore, I will not attempt to gain access to information, resources, or facilities to which I am not specifically authorized nor will I grant access to unauthorized personnel.
- I am aware that copyrighted software purchased by the <Department Name> is subject to specific license requirements. I will not copy, share, and/or transport

licensed software from or to any workstation or out of the facility without specific written permission by recognized authority.

- I am aware that I may work off site on official business, and: 1) <Company Name> will not be liable for loss, damage, theft, maintenance or repair of any privately owned equipment used; 2) no classified information may be processed off site; 3) all data created, generated, modified, etc., as a result of off site work is the property of <Company Name>.
- I am aware that working off site may involve transporting storage media (e.g., floppy diskettes, tapes, CD-ROM, etc.) in and out of the facility which introduces an increased risk to <Department Name> resources (e.g., loss of data, disclosure of sensitive or proprietary information, malicious code contamination of computer systems, etc.) for which I assume full responsibility.
- I am aware of the network and dial-up capabilities for electronic transfer of software, information, and data, of the risks involved (e.g., loss of data, disclosure of sensitive or proprietary information, malicious code contamination of computer systems, etc.) and agree to accept full responsibility in the use of those capabilities, to use them only for official use, and to act only in the best interests of <Company Name>.
- I am aware that failure to comply with any of these requirements may be considered a security incident and is subject to disciplinary actions as defined in the <Company Name> Employee Handbook, Chapter XVI, Section L. I am also aware that federal laws may specify additional prosecution and/or penalties for specific security violations.

I have read the information presented above and been given an opportunity to discuss any issues with the Computer Protection Program Manager. My signature indicates my understanding of these requirements and my acceptance of the associated responsibilities.

Rules Of Behavior

<Department Name> *"RULES OF BEHAVIOR"* FOR AUTOMATED INFORMATION SYSTEM(S) USERS

Introduction

Today's information system (IS) users are far more comfortable with using ISs than they were 10 years ago. Given this increased confidence in IS users, national regulations and guidance are beginning to recognize that today's IS users must also be an integral part of protecting <Company Name> Information Systems and the information that they store, process and/or transmit.

<Policy Reference Number> covers all <Company Name> Information Systems. The key <Company Name> regulation implementing <Policy Reference Number> is Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of <Company Name> Automated Information". This appendix establishes a minimum set of controls to be included in <Company Name> automated information security programs; assigns <Company Name> departments responsibilities for the security of automated information; and links departments automated information security programs and department management control systems established in accordance with OMB Circular No. A-123. This appendix incorporates requirements of the <Policy Reference Number> and responsibilities assigned in applicable directives.

Personnel who use any <Company Name> computing resource at <Department Name> to process, store, or transmit data and information shall first read and familiarize themselves with the Principles (1 thru 8) and Responsibilities discussed below and sign an F 5310.5 (Computer Users Security Agreement). The form can be found on <Department Name>'s Intranet (Electronic Forms). A signed copy of the form will be retained by the user, and the original by the Computer Protection Program Manager's (CPPM) office. This form must be read, signed and returned to the CPPM's office before user can obtain access approval to <Department Name>'s AISs.

Principles and Responsibilities

1. Official Business Only

<Department Name> computing resources are government property funded by <Company Name> for the purpose of supporting the various programmatic and scientific research efforts needed to accomplish the company's missions. As such, these resources are to be used only for official business. Users should remember that when they use <Department Name>'s computing resources, they are acting in their employment capacity on behalf of <Department Name> and <Company Name>.

Electronic mail sent via site networks, for example, ordinarily bears site-specific identifiers in the address (e.g., <e-mail-address>). It therefore reflects on <Company Name> and <Department Name>, indicating to all who read the message that it was composed on <Company Name> equipment at a <Company Name> branch.

For these reasons, regardless of disclaimers, when you use electronic mail resources you are representing <Department Name> and <Company Name>, and you must act accordingly. Because the mail that you send and receive through the <Department Name>'s computational resources is official business by definition, there ordinarily would be no legitimate reason to use anonymous re-mailers or personally owned copies of encryption software for the transmission of your messages. Unless approved by management, any activity outside the scope of your employment, or any activity which could embarrass the organization must be avoided. (Reference Memorandum from Archer L. Durham, dated 6/25/96, "Appropriate use of the Electronic Mail System and of Employee Duty Time")

2. Monitoring, Recording and Auditing of Federal Computing Resources

Because <Department Name>'s computational resources are <Company Name> property, their use may be subject to monitoring, recording, and audits to insure the systems and networks are functioning properly, to protect against unauthorized access or use, and to ensure the confidentiality and integrity of data and information resident on the systems and networks. In addition, <Company Name> may access any user's <Company Name> provided computer system or data communications and disclose information obtained through such auditing to appropriate third parties, including law enforcement authorities. User have **NO EXPECTATION OF PRIVACY** when using <Department Name>'s computing resources or public switched networks (e.g., Internet). Use of <Departmetn Name> computing resources and network connections constitutes **EXPRESSED CONSENT** by the user to monitoring, recording, and auditing for purposes identified above. (Reference Memorandum from Ken Williams dated 6/27/97, "Policy on Use of Internet and Electronic Mail")

3. Protection of Authenticators

Information stored and processed on all <Department Name> systems must be protected from unauthorized access, disclosure, modification and destruction. The main security feature for protecting ISs is authorized user authentication, i.e., passwords. Passwords are sensitive information and should be memorized, never shared, and not written down and/or stored in desk drawers, files, etc. Passwords should be at least six characters in length, not a word found in the dictionary and for better results should contain at least one numeric character. Passwords should be changed as you feel necessary or at least every six months. Report any compromise of a password to the designated computer security personnel.

4. Avoiding the introduction of malicious code (e.g., viruses, worms, Trojan horses) into computing resources

<Department Name> users have access to electronic file exchange, news services, list servers, e-mail communications, etc. via a router link to ESNET. With the entire Internet community possible both at work and at home (through dial-up connection) the connection introduces risks to the security of <Department Name>'s computing environment. The user must maintain an acute awareness of the potential for loss or alteration of information/data, damage from importing malicious code and from possible disclosure of sensitive/proprietary information during electronic transfer. It is the users responsibility to act responsibly and in the best interests of <Department Name> when accessing the Internet.

Virus protection software must be run on all <Department Name> Information Systems at least one time each day. Software must also be used on any media brought into the user's organization. Additional protection measures include not sharing disks without first virus checking. The detection of a virus is considered a computer security incident. (See Guide to Incident Report Handling)

5. Security Incident Reporting

<Department Name> Information Systems must be adequately protected, it is each users responsibility to understand <Department Name> procedures for reporting computer security incidents, which include reporting suspected viruses or intruders. (See Guide to Incident Report Handling)

6. Marking of Media/Printouts

All AIS storage media and printouts containing unclassified sensitive information should be marked and protected in accordance with the information contained therein. For assistance in marking media/printouts containing unclassified sensitive information, contact the CPPM, the Information Security Officer, or the Classification Officer for <Department Name>.

7. Prevention of physical damage to <DEPARTMEN NAME> computing systems

It is the responsibility of <Department Name> computer users to protect computing resources from physical damage. Users should: (a) supervise and observe maintenance work being performed by outside personnel, (b) know what hardware/software belongs on/at your workstation, do not move equipment (contact qualified personnel for assistance), (c) do not leave workstation unattended without saving your work, clearing the screen, removing any data disks and logging out or disconnecting from network, or invoking the use of a screen saver with password protection, (d) eating or drinking should not be done in the immediate vicinity of the computer equipment, and (e) books, papers, boxes, etc. should not be stored on or around the air flow vents of the computer equipment.

8. Copyrighted Software

In order to protect <Department Name> (as well as users) from liability for copying or disclosing proprietary information, each user should learn what restrictions exist for the software used on their system. Commercial software is copyrighted and must be licensed for use. (Reference Chalmers Wilson Memorandum of 1/96, "Control and Handling of Copyrighted Software")

Incident Identification Form

Date Updated: _May 4, 2000_____ Page_1_of__1___ INCIDENT#: __2000541__

Your contact information:

Name: ___David Smith_____

Phone/Alt Phone: ____865-576-xxxx_____

FAX/Alt FAX: _____865-576-xxxx_____

E-mail:_____smithd@xxx.xxx_____

Type of incident (denial of Service, Espionage, Hoax, Malicious code, Unauthorized access, Unauthorized use.)

__Denial of service (worm) and Malicious code (virus)_____

Location of incident:

Address: __175 Oak Ridge Turnpike_____

Building: _____ Room: ___341_____

Additional Information: _____

How was the incident detected:

_ Incident response member, John Gerber, was on site when his mailbox received___
_ a suspicious email containing the subject "I LOVE YOU" from a male colleague.__
_ Within a minute, multiple emails from other employees appeared. Examination___
_ of the Microsoft Exchange server log and queue revealed the mail server was_____
_ being bombarded with mail messages._____

Who detected the incident: __John Gerber_____

Signature: _____

When was it detected:__7:50am on May 4th, 2000_____

Incident Survey Form

Please note that one form was generated for each of the PCs infected. What follows is a sample of the multiple forms filled out.

Date Updated: _May 4, 2000_____ Page_1_of__1___ INCIDENT#: __2000541__

Location(s) of affected system(s): _Oak Ridge location, Room 257_____

Date/Time incident handlers arrived at site: __4:12pm_____

Describe affected information systems: (one form per system is recommended)

__This was a personal workstation not running any servers. On the PC, files were_____
__replaced, changes made to Internet Explorer client default home page, a password____
__stealing program was installed, and registries were modified. See attached document_
__for complete description of the ILOVEYOU virus._____

Hardware Manufacturer: _Dell_____

Serial Number of CPU: ___2154889570_____

Corporate Property Number if applicable: __000076_____

Operating System type/version: ___Windows 95_____

Disk Capacity (if known): ___8G hard drive_____

Is affected system connected to a network? YES

System Name: __censored_____

System Address: __censored_____

MAC address: ___censored_____

Is affected system connected to a modem? __No__ Phone Number: _____

Describe physical security of location of affected information system (locks, alarm systems, building access, etc.):

__The machine exist in a personal office. The building itself has security guards and__
__access is restricted to employees._____
_____
_____

Incident Containment Form

Please note that one form was generated for each of the PCs infected. What follows is a sample of the multiple forms filled out.

Date Updated: _May 4, 2000_____ Page_1_of__1___ INCIDENT#: __2000541__

Isolate affected systems:

Command Decision Team approved removal from network? __YES___

If NO, what was the reason:

_____
_____
_____

If YES, time systems were disconnected: _8:15am_____

Backup affected systems:

System backup successful for all system? ____Yes_____

Name of persons who did backup(s): ___John Gerber_____

Time backups started: ___9:35am__ completed: __10:50am____

Backup tapes turned over to: ___Pat Thomas_____

Signature: _____

Location tapes will be stored: ___Safe located in room 343_____

Incident Eradication Form

Please note that one form was generated for each of the PCs infected. What follows is a sample of the multiple forms filled out.

Date Updated: _May 4, 2000_____ Page_1_of__1___ INCIDENT#: __2000541__

Names of all persons performing forensics on affected systems(s):
__John Gerber_____

_____
_____
_____

Was the vulnerability identified? Describe:
__Yes. The vulnerability introduced was the result of the ILOVEYOU virus._____
__See attached description of the virus for a complete understanding of how the _____
__how the virus operates._____
_____

Was the validation procedure used to ensure problem was eradicated?
___Yes. We ran Nmap, Saint, and Nessus to check for any vulnerabilities after _____
___the anti-virus software reported the system clean. We also checked log files of _____
___our network intrusion detection system, firewall, and routers. _____
_____

ILOVEYOU Script

Intentionally left out. The script was causing the document to be flagged as a virus by implemented mail virus scanners. If you need to analyze the script, please make a request to the author of this report.

References

"Critical Infrastructure Protection." United States General Accounting Office, May 2000.

"Incident Handling: Step by Step, Version 1.5." The SANS Institute, 1998.

"Solaris Security: Step by Step, Version 1.0." The SANS Institute, 1999.

Wack, John P. "Establishing a Computer Security Incident Response Capability (CSIRC)." Computer Systems Laboratory, National Inistitute of Standards and Technology, November 1991.

West-Brown, Moira; Stikvoort, Don, & Kossakowski, Klaus-Peters. "Handbook for Computer Security CIRTs (CIRTs)." CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburg, PA, December 1998.

"Windows NT Security: Step by Step, Version 2.15." The SANS Insititute, July 1999.

Last Updated: June 18th, 2018

Upcoming SANS Penetration Testing

SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
Minneapolis 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
Mentor Session - SEC504	Oklahoma City, OK	Jul 10, 2018 - Sep 11, 2018	Mentor
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANSFIRE 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANSFIRE 2018 - SEC560: Network Penetration Testing and Ethical Hacking	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Community SANS Honolulu SEC560	Honolulu, HI	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pen Test Berlin 2018	Berlin, Germany	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201807,	Jul 24, 2018 - Aug 30, 2018	vLive
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
San Antonio 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - AW SEC560	Austin, TX	Aug 08, 2018 - Oct 10, 2018	Mentor
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
Northern Virginia- Alexandria 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Community SANS Ventura SEC560	Ventura, CA	Aug 13, 2018 - Aug 18, 2018	Community SANS
Community SANS Reno SEC504	Reno, NV	Aug 20, 2018 - Aug 25, 2018	Community SANS
SANS Krakow 2018	Krakow, Poland	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Prague 2018	Prague, Czech Republic	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session - SEC504	Cincinnati, OH	Aug 21, 2018 - Oct 02, 2018	Mentor