Global Information Assurance Certification Paper

ILOVEYOU Virus Incident Response

1.0 Executive Summary

On May 4, 2000, the ILOVEYOU virus was released into the wild. This document describes a formal incident handling process, and describes how this process was used to resolve problems caused by the LoveLetter virus.

The ILOVEYOU Virus

This virus is also known as Love.Letter, Love Bug, and similar names.

It has the subject of "ILOVEYOU," with the text "kindly check the attached LOVELETTER coming from me."

The attachment is named LOVE-LETTER-FOR-YOU.TXT.vbs

If opened, the attachment executes a Visual Basic script which spreads the virus to users in each address book, attempts to send communications through Internet Relay Chat, and searches for specific types of files, then infects them

Organizational Structure:

The organization described in this paper is one of many this is primarily known by its acronym. For purposes of sanitation, it is known here as AGENCY.

AGENCY is a government agency. Information Technology tasks have been outsourced to a civilian contractor.

The MIS Department is responsible for day-to-day IT Operations. It is comprised of several functional groups. Only the relevant groups are described here:

- Help Desk – First line of customer support. Installs software, trains users, and resolves user issues.
- NOC (Network Operations Center) – Second line of customer support. Provides network administration functions.
- Network Operations – System administrators and third line of support.

The Security Department is responsible for all security issues at AGENCY. It is also comprised of several groups. Only one group is involved in Information Security:

- INFOSEC – Accredit systems, establish security policies, monitor systems, and respond to incidents.

2.0 The Incident Handling Process

The formal incident handling process consists of six discrete steps:

- **Preparation** – This step involves general preparation, policies, planning, procedures and system hardening used to prepare for incidents. After initial preparation, procedures get continually refined as incidents occur, through the "Lessons Learned" phase.
- **Identification** – This is the stage at which an incident is declared, staff is alerted, and initial response begins.
- **Containment** – Once an incident is declared, the incident handling team must move to confirm the events, contain the damage, and coordinate actions with appropriate other parties.
- **Eradication** – During the eradication phase, the specific cause of the incident must be identified, and vulnerabilities corrected. Defenses must be improved, and monitoring systems updated to watch for the new attack signature.
- **Recovery** – Once the vulnerability is identified and remedied, the compromised systems should be prepared to resume production status. A base-lined, clean system that has been installed from scratch is preferred, but not always possible. At AGENCY, the decision to restore operations is made by the Director's Office or an appointed working committee.
- **Lessons Learned** – After the systems have been restored to normal operations, an "Incident Report" is required to close out the incident. This after-action report seeks to reach consensus about what occurred, conduct a review of actions, identify lessons learned, and send recommendations to management. The team then implements approved actions.

This document will describe how this process was followed for the ILOVEYOU virus. In addition to these steps, the following sections were attached:

- **Assessment Details** – Tools used to respond to the virus incident. Although a "jump bag" is not used at AGENCY, its equivalent, the test bed network, will be covered in detail.
- **System Backups** – The process used to perform normal system backups will be described.
- **Summary of Evidence** – Evidence gathered is summarized in this section.
- **Innovations specific to AGENCY** – In discussions with other organizations, it became clear that some of the tools, practices, and techniques utilized here are not in general use elsewhere. This attachment summarizes those innovations.

3.0 Preparation

AGENCY has had a formal incident handling organization for many years. As a result, many aspects of the preparation stage have been well entrenched at the organization, and security is part of the corporate culture.

Policies – User Notification

User briefing

Upon assignment to AGENCY, users are required to undergo a security briefing outlining system policies and security practices. Proper behaviors to avoid virus infection, including responsibilities for workstation backups, and keeping anti-virus signatures up-to-date, are stressed.

Warning Banners

Warning banners are present at all system logins on all systems. All workstations are created from a master hard drive, which is pre-configured with appropriate software and warning banners. All servers are similarly pre-configured.

All systems must be accredited prior to deployment. Presence of the warning banner is a checklist item on the system accreditation worksheet.

A slightly modified version of the DOD computer systems warning banner is used, after input from the FBI, legal counsel, and upper management.

Policies – Organizational approach to incident handling.

All staff is authorized to take all actions necessary to contain an incident, up to and including shutting down all network connections.

If a system, network, or device shutdown occurs for security reasons, only the Director's Office or their Security Advisory Committee can re-authorize the equipment to be re-activated.

All users can report a suspected incident by calling the HELPDESK.

Upon a user's report, or upon detecting suspicious activity themselves, Help Desk personnel will immediately notify INFOSEC.

INFOSEC personnel are responsible for monitoring the network, and may declare an incident based on events seen.

MIS personnel monitor their own systems and log files, and may similarly declare incidents.

Incident Handling Team Organization

The incident handling team is created from a core team which responds to most calls, an ad hoc group of appropriate operations support staff, and management.

The core team includes security personnel from both the MIS and INFOSEC groups.

The ad hoc team is formed of the appropriate system administrators or Help Desk staff, as required.

The management team consists of both contract and government managers, and is authorized to make high-level decisions about the network.

Upon declaration of an incident, most team members will report to a designated command post. This command post is permanently established in the INFOSEC area, because it is centrally located, and can be dedicated to security issues on demand.

All system administrators, managers, team leads, and senior help desk personnel are equipped with cell phones and call lists. The call lists are kept with their security badges.

Jump bags

AGENCY teams are primarily in a fixed location, and therefore do not carry jump bags. However, two separate areas are equipped as stand-alone networks specifically for incident response and system recovery. These areas are equipped with power supplies, battery backup, and are near CD libraries with copies of all system software. The test networks can be flexibly reconfigured to be standalone, attach to the internal network, or attach to an external network (separate ISP).

Other stand-alone networks are pre-positioned near servers in the event they need to be taken off-line. Spare hubs are liberally available to system administrators for testing, isolation during system builds, and other projects.

The test bed networks are co-located with spare equipment with modular parts from the production equipment. If it is necessary to rebuild a system, it is usually possible to recreate it from a mastered hard drive more quickly than from tape backup. Procedures exist to create replacement systems for any one host, without destroying or touching the original system.

Team members carry a cell phone and call list with them at all ties. Some are equipped with two-way pagers that permit them to send and receive e-mail. All cell phones are capable of receiving text messages via Internet mail.

4.0 Identification

On Thursday, May 4, 2000, the LoveLetter virus infected AGENCY. Following is an excerpt of the consolidated incident response log report created during the Lessons Learned stage. Source files included system logs, phone system records, individual record keeping, and group consensus.

```
04 MAY 2000

0624L   AGENCY received its first copy of the Love Letter e-mail.

0659L   First infected e-mail opened by a user.

0700L   Simultaneously, NOC, INFOSEC, and HELPDESK staffs note e-mail
        activity indicative of an e-mail virus.  The Deputy Helpdesk
        manager was the only manager on duty at the time, and
        immediately declared an incident, starting the notification
        process.
```

The Help Desk has minimal staff onsite at 0700 hours local time. The staff that was present quickly noted large numbers identical messages coming from the same user, all with the same attachment. This was immediately recognized as an e-mail virus.

The manager on duty was notified, and she rapidly determined that an incident was occurring. She began preparing an AGENCY-DIST notification in e-mail, and delegated one of her staff to start calling the call tree.

Simultaneously, the NOC staff, the second-line Network Operations staff, and INFOSEC began receiving messages on their cell phones. A mail group containing the Internet addresses of their cell phones and pagers had been created at the top of all user address books. Most of this staff was either still at home, or already committed to the morning rush hour.

This staff also began calling the Help Desk, which was the hub of operations at 0700.

```
0702L   First AGENCY-DIST message launched from Help Desk, alerting
        users to the unusual message, and requesting that they refrain
        from opening it.

0705L   Help Desk analyst reaches NOC staff, and notifies them of the
        incident.  NOC was confirming the incident, and also proceeds
        down their call tree.

0710L   NOC fails to reach Exchange Administrator and Network Manager.
        Other NOC staff were beginning to call in, due to the cell phone
        messages left by the virus.  Backup Exchange Administrator was
        reached at home, and begins investigating.

0714L   INFOSEC Office reached by Help Desk, and started its call tree.
```

0715L	NOC successfully reaches primary Exchange Administrator. Both primary and backup Exchange Administrators begin working together from home, and begin crafting an e-mail block based on the subject of the message.
0720L	Help Desk manager updated by NOC that Exchange Administrators were reacting to the situation.
0724L	First AGENCY-DIST message received by AGENCY users.

During the declaration of the incident, fifteen minutes passed before mail administrators are beginning to react to the situation. It took another ten minutes to confirm the incident and attempt a local block.

Once the first e-mail block was established (based on subject line), the incident handling process moved from the Identification stage to the Containment stage.

Events moved very quickly. The first AGENCY-wide e-mail notice about the message was sent at 0702, shortly after the first virus message was triggered. It took about twenty minutes for the message to be delivered. This indicated that the internal mail was already beginning to slow down from the load.

The initial responses to this incident were pre-scripted actions developed as a result of the Melissa e-mail virus, which had occurred some months earlier.

5.0 Containment

When AGENCY users were initially disconnected from external e-mail, it was accomplished by disabling certain gateways. At this point, the mail servers were still untouched.

0730L	AGENCY users were disconnected from external e-mail.
0745L	Sendmail gateways were disconnected, to enforce the mail shutdown.
0750L	NOC informed Help Desk manager of previous actions.
0800L	Trend Micro, one of the two anti-virus vendors used by AGENCY, provided new virus definitions. Trend Micro was used to protect servers. Virus scanning began immediately.
0805L	After discussion between incident handling team and mail administrators, Exchange Administrator instructed the NOC to disconnect all mail servers from the network.
0825L	After completion, NOC informed Help Desk of action.

AGENCY has a switched network topology. The backbone is configured in such a way as to allow the physical disconnection of certain classes of servers from the network. This is the equivalent of unplugging their network connections, although they remain plugged into what is now a stand-alone network.

This approach has the advantage of speed. The size and number of Exchange servers deployed at AGENCY is so large that it may take 30-45 minutes to perform a clean shutdown.

This approach also leaves the Exchange servers intact and unmodified. The servers themselves are unaware that all clients have been physically disconnected. In this case, virus scanning commenced immediately. This immediately changed the state of the drives.

The decision to immediately recover from e-mail virus attacks and not backup the systems to gather evidence was reached in advance, during the preparation stage. The reason is twofold: First, full Exchange backups currently take 14 hours to complete. It was unacceptable to wait that long before beginning recovery. Second, virus attacks are too common, and are not a prosecution priority for our legal decision-makers.

0830L	Government, contract, and other managers began arriving onsite.
0840L	Management briefings continue. All group managers were now briefed, and the command center was activated. All coordination was moved from the Help Desk to the command center.
0910L	Analysis of the virus indicates that it may spread in ways other than just the Internet. All user Internet connections were disabled.

0950L	Meeting – All team members met to compare notes, agree on preventative and restorative steps and broke at 1010L to continue action. The decision to contain and recover was confirmed by management.
1005L	All UNIX servers shutdown.
1035L	User file server, which had been infected by the virus, was shut down.
1100L	Norton anti-virus definitions received. This was tested and confirmed. An update to protect workstations was now possible.
1200L	Meeting – All team members met for a full status report. An estimate was made of the data to be scanned and the speed of the scans. It was concluded that operations would be suspended until at least Friday. A full network shutdown was ordered until that time. File servers could not be scanned because of the time requirements. A full restore of the last known good backup was ordered instead.
1400L	All hubs disconnected.
1420L	All web and file servers disconnected. All systems were now in stand-alone mode or off.
1500L	Exchange server virus scans completed. Exchange restored for internal mail operations. All attachments are being held in quarantine.
1600L	NOC began writing special procedures for operations over the weekend (i.e. how to handle customer call-ins, backups, and monitoring servers and sites.) This was required because the network topology was completely re-arranged from the normal state of affairs.
1900L	Antivirus.com listed new variant called "Brainstorm." NOC notified command center, sent out a note via AGENCY-DIST.
2000L	Symantec listed new variant called "Virus Alert!!!" Command center staff notified.
2245L	Symantec listed 2 new variants called "No Comments" and "Important! Read Carefully!!" "Important! Read Carefully!!" was identified earlier as "Brainstorm" by AntiVirus.com. NOC notified command center staff.
2130L	Full restores of file servers completed. Virus scans begun.

6.0 Eradication

The dividing line between containment and eradication is not easily defined for this incident. It typically occurs when prevention of further infection stops and elimination of the virus begins.

In this case, actions were being taken simultaneously to both contain and eradicate the virus. The clean dividing line was removed by the nature of this virus, which continued to spread initially on the file servers while the e-mail problems were being eradicated.

An analysis of the virus code indicated several weaknesses in the propagation method of ILOVEYOU and its copycat clones. All relied upon Visual Basic. It was believed to be only a matter of time before other esoteric executable extensions were used.

Microsoft provided a list of other executable file extensions. The server antiviral filters were set to reject all attachments with the suspect file extensions.

7.0 Recovery

```
05 MAY 2000

0500L    Scan of file servers completed.

0700L    Meeting.  Current status discussed.  Weekend plans discussed.
         Network was to be left down over the weekend, but restored for
         the day.

0745L    Updated Trend virus definitions loaded onto server.  All
         services restored.

1500L    Meeting.  Current status discussed.  Weekend plans resolved.
         Network to be restored over the weekend, and closely
         monitored.  If no further infections were detected, the
         incident would be declared closed.


08 MAY

0730L    Meeting.  Current status discussed.  Incident declared
         resolved.
```

Several other copycat viruses continued to appear, but all ended with .vbs, and were blocked by the file extension blocks.

8.0 Lessons Learned

After an incident summary is created with the consensus of the incident handling team, it became necessary to draw conclusions.

- **User awareness training had failed.** Increased awareness training had followed the Melissa virus, but the message's appeal overrode the training. Prior to mail system shutdown, the Melissa infection rate was approximately 45%. That is, 45% of the users who read the message opened the attachment. That rate was more than sufficient for Melissa to raise havoc.

  The infection rate for ILOVEYOU was nearly 100%. The relatively small number of users in the office at the time the virus hit skewed this figure. However, the message seemed to be opened by everybody who saw it. The few users who were not infected had not yet read their e-mail. This included users who should have known better, including some of the computer support staff.

- It was also soon clear that the **ILOVEYOU virus greatly increased user awareness of virus issues**. Users appeared to have acquired a healthy suspicion of all unsolicited attachments, including those sent by friends.

Due to the length of the outage, the incident handling team came under intense pressure to restore service, even as senior managers decided to err on the side of safety and remain off the air.

- **Automated systems that maintained logs were invaluable with obtaining an accurate timeline**, especially during the critical opening moments of the incident, when every minute counted. During that time, multiple individuals were reacting to the same situation, and acting in a loosely coordinated fashion. The automated logs kept by the internal phone systems, system logs, and file date/time stamps proved critical in corroborating the intrusion detection team's account.

- **Most of the Melissa countermeasures were effective.** The change to a two-vendor anti-virus model proved to be a godsend. In addition, the ability to segregate the network by type of server proved critical.

Recommendations:

- **AGENCY should consider blocking all attachments, except .zip and other acceptable compressed formats.** The intent of this measure is to ensure that all attachments are deliberately sent, and are deliberately opened.

- **More effective user training is required.** Most of the training appeared to go out the window when the message received appeared to be personal in nature. There is now user awareness beyond the capabilities of the best training program. The goal now should be to retain virus awareness at that level.

- **A conference call system should be maintained for virtual meetings.** This capability would have allowed better coordination for a distributed staff.

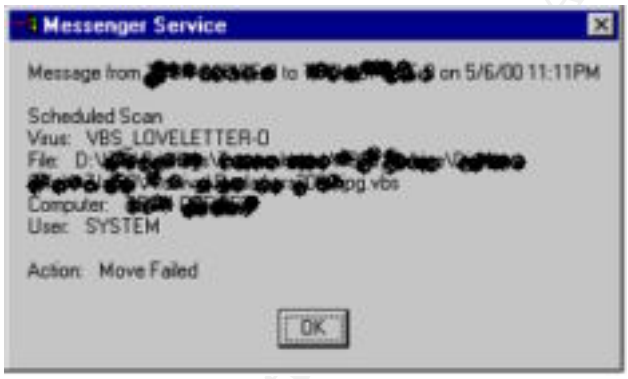
Attachment I – Assessment Details

Virus Identification:

The ILOVEYOU virus can be identified in several ways:

1. The signature of an e-mail virus is a large number of mail messages from the same person with the same attachment. This can be confirmed if other users are simultaneously sending the same message with the same attachment.
2. Nokia phones have the ability to receive text messages when sent a message through the Internet. This capability is supported by all major cell phone services. A group with the cell phone accounts of all virus response team members were included at the top of the address book. This resulting in the virus paging the team upon attack.
3. Norton AntiVirus is used to protect desktops.
4. Trend Microsystems is used to protect servers.

   Upon detection of a virus, the following alert was generated:



5. Two primary web sites were used to identify new variants of the ILOVEYOU virus.
   - http://www.symantec.com/avcenter/index.html
   - http://www.antivirus.com/vinfo/

User Notification:

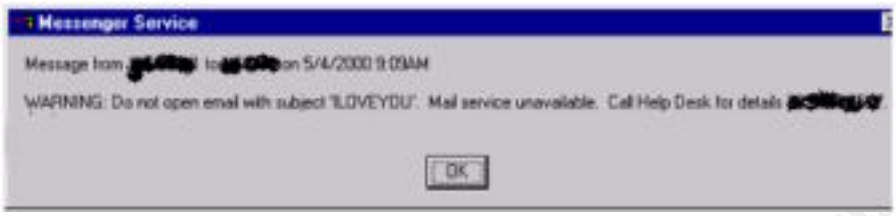
Communications with the end user community had to be maintained while the e-mail system was inoperative. This was accomplished in several ways:

1. The NT NET SEND command.

   From an MSDOS command prompt, type:

```
C:\ NET SEND * "WARNING: Do not open email with subject
'ILOVEYOU.' Mail service unavailable. Call Help Desk for details.
***-***-****"
```

This results in the following notice to all users:



2. Pre-printed generic notices to post on all user entrances and in elevators. These notices are kept in stock and deployed by Help Desk staff immediately after a network shutdown is required.
3. Voice mail broadcasts through the phone system. While not as effective as e-mail broadcasts, voice mail broadcasts will be heard eventually by everybody with a voice mail box.

Isolated Workspace:

A pre-designed test bed network was available for use, but was not required for this incident. This test bed includes the following equipment:

- Switched hub – used to attach multiple pieces of equipment, when performance is a factor.
- Shared hub – primarily used when a packet sniffer is required to analyze traffic.
- Laptops – Configured as Linux, NT, or dual-booted, laptops are issued to all support personnel.
- Spare equipment – Parts are used to replace damaged or destroyed equipment.
- Servers – spare servers identical to those deployed are available for rapid recovery without touching the original compromised systems.
- Uninterruptible Power Supplies, to reduce risk of loss during a critical recovery.
- Network access to both the internal network and an external network. This must be changed in the wiring closet – the change is easily made by trained staff, can't be made by accident, and prevents being connected to both simultaneously. The default setting is a standalone network.
- CD Library – includes all original operating systems and commercial programs.
- Hard drives – some of the critical systems are mastered onto hard drives, with minor changes to customize them for a specific task. This practice permits rapid deployment with minimal restores (which are slower and can potentially re-introduce compromised files.) Hard drive masters are created from scratch.
- Sniffer, intrusion detection systems, and system scanners are available to assess systems prior to rollout.

Modular Network Design:

The network is designed such that certain critical systems can be isolated onto a stand-alone network with ease. This allows rapid disconnection when required. Typical devices that might be configured in this way include:

- Firewall
- File Server
- Mail Server
- Scheduling Server

Each stand-alone network should have a server with a tape device (for backup and recovery) and a printer attached.

The modular network may be accomplished in several ways:

1. Attach all like servers to a switched hub, then attach the high-speed uplink port on that hub to the backbone. If disconnection is required, disconnect the uplink. This has the fastest disconnection time, but may serve as a potential bottleneck.
2. Leave a stand-alone hub near the servers. If disconnection is required, move the network cable from the normal network hub to the stand-alone. This requires more equipment and is messy. Hubs are relatively cheap, however, and this works.
3. Use a Virtual Local Area Network (VLAN) to define two ports per server. Both ports should be next to each other, near the server. One of the VLANs should connect the system to the main network; the other should be stand-alone. Each server can therefore be easily made stand-alone or connected as required.

The choice of which method to use will vary depending upon the circumstances and the budget.

Attachment II – System Backups

File system backups are a critical part of day-to-day IT operations. After backups are complete, the tapes are rotated off-site on a regular schedule. Tapes are recycled every month.

Backup Equipment

NT backups at AGENCY are very straightforward. NT Backup software is used for file and Exchange servers. Backups are performed to DLT tape drives.

File Servers

The affected file servers were running on NT Server 4.0, and are on a weekly backup schedule. That is, a full backup is scheduled once a week, and a differential backup is performed every other day.

Exchange Servers

Exchange is run on a separate backup, using an Exchange-aware version of NT Backup. Exchange is on a daily backup schedule. That is, a full backup is run every night. This is because Exchange data is effectively kept in a single file per server. Either all the data on a server is backed up, or none is.

Microsoft does have a mechanism for doing incremental backups on an Exchange database, but it proved to be unreliable.

Exchange backups take approximately 14 hours to complete.

Recovery

Due to the early morning nature of the ILOVEYOU virus incident, few file server changes were actually made legitimately by the user community. This meant that the data from the last full backup was still current.

Some of the files modified by the virus were not saved, but were destroyed. This meant that the most prudent course of action was to restore files destroyed by the virus. Unfortunately, one of the users affected by the virus had system administration privileges over one of the file servers. The entire file server had to be restored from backup.

Other file servers were isolated in time to prevent damage, and were either completely undamaged, or required only minor directory restorations.

NT Backup uses a graphical command interface. Restoring the files was as simple as selecting the RESTORE button, and choosing a destination. Restorations were uneventful.

Attachment III – Summary of Evidence

In the event evidence collection is required, the INFOSEC team assembled an evidence collection kit. This kit is used by incident response teams as required, and is maintained in the INFOSEC office space (also the command center.)

This kit consists of tape, permanent markers, a memo card with evidence-handling guidelines, and plastic bags. Evidence is collected into the bags, and sealed with the tape. The tape is then marked with the date, time, location, signature of the witness, and stored in a safe cleared for classified materials. The evidence bags are then registered with the INFOSEC manager. Access to the safe is available only through the INFOSEC manager and his deputy.

This event did not generate any evidence. The moment to collect the evidence would have been prior to attempting repair of the virus. This was not done because of the time required to backup the data files. Full Exchange backups take 14 hours to complete. The decision was made in advance not to perform this backup when responding to e-mail viruses.

Other information was collected, but was not maintained at a level for legal proceedings.

- 25 staff members had participated in the incident to one degree or another. Raw incident notes and briefs were gathered by INFOSEC and used to collate an overall timeline.
- Use of the file and mail servers was lost for nearly 25 hours, as measured by the NOC logs. Over 200 man-hours of effort were spent responding to this incident, as measured by officially submitted timesheets and status reports.

Attachment IV – Innovations Specific to AGENCY

In discussions with other organizations, it became clear that some of the techniques used by the AGENCY were not in wide use elsewhere.

1. **Have the virus page the staff.** The first global mail group listed (alphabetically) in the e-mail system includes all pagers and cell phones of the support staff. The user community does not use this group normally. However, e-mail viruses will automatically send to all members of the user's address book, including the virus response group. In e-mail viruses, early notification and action is critical. The virus effectively pages the support staff when the system is infected.
2. **Use pre-designed test beds in lieu of a jump kit.** Obviously, this may not be possible in many environments. The problem with portable equipment is that it must be portable. Ready replacements for all server parts are available at several pre-positioned locations within the Agency. Only cell phones and contact lists need be carried with each response team member. The test bed networks are much more flexible than a jump kit.
3. **Critical segments of the network are designed to be self-contained, for easy disconnection.** Pulling the Internet plug, separating the file servers, separating the mail servers, and otherwise isolating certain internal systems can be accomplished with minor physical changes. This permits, for example, the Exchange servers to be completely disconnected by pulling a single cable. The topology allows for much faster response than shutting down multiple individual systems, and leaves the systems in a state ready for recovery.
4. **The Agency subscribes to two separate antiviral engines.** The major vendors develop anti-virus signatures independently. Some signatures are more effective than others, and some are developed faster than others. By incorporating two separate anti-virus engines into the network, there is a better chance of catching a virus. When new viruses hit, it allows the network to become operational much sooner. One virus engine is used for to protect all desktops; the other is use for server-based scanning and detection.
5. **All .vbs attachments were blocked.** The Agency consulted with Microsoft, and was provided a list of all executable extensions. These were blocked as well. This measure prevented the copycats from infecting the organization.
6. **The Agency is considering blocking all attachments except .zip.** This would prevent users from automatically opening messages. By deliberately opening attachments, the users would have to make a specific decision to expose themselves to the risks. This may not have stopped users from opening the LOVELETTER file, but it would have prevented users from spreading it.