VBSim

Symantec Computer Virus/Worm
Simulation System

Version 1.2

Contents

About VBSim 3
Simulating the spread of malware 3
Understanding the VBSim interface 4
Demonstrating infections 5
Setting corporation parameters 6
  Email checks per day 7
  % of attachments detached 7
  Average number of emails received per day, per person 7
  Average emails with attachments sent per week, per person 7
  Average recipients per email 8
  % of emails sent outside the corporation 8
  % of emails sent outside the workgroup 8
  % of shared drives in the corporation 8
  Average number of system reboots per day 8
  ALL CORPORATION mailing list 8
How viruses and worms spread 9
  Concept 9
  Melissa 9
  ExploreZip 10

About VBSim

The VBSim program is a malware simulation that demonstrates how a computer virus or worm spreads inside and between corporations. The simulation relies upon user-specified parameters, probability functions, and random numbers to model the corporate environment. Because it is a simulation, different outcomes and different infection patterns are generated each time the program runs. The infection patterns can vary widely from one run of the program to another.

Although the parameters that have been chosen and the mathematical models used within the simulation are not perfect, they do model the gross behavior of computer viruses and worms. Because this is a simulation governed entirely by random processes, its behavior may not always conform to your expectations. Over many runs of the simulation, however, trends and behaviors will emerge.

VBSim was first demonstrated at the 1999 Virus Bulletin conference in Vancouver, Canada. The Symantec AntiVirus Research Center continues to update and work with models such as VBSim to help advance antivirus research. If you have any comments or questions, please send them to Carey Nachenberg (cnachenberg@symantec.com).

Simulating the spread of malware

The VBSim program uses a very simple *Monte Carlo* simulation method to mimic the spread of malware inside the corporation. VBSim does not provide a 100% realistic simulation of how viruses and worms spread; rather, it gives a general idea of how quickly these threats might spread in a corporation. Given the vastly complex corporate environment, a truly realistic simulation is virtually impossible. Consequently, a small number of parameters that characterize those aspects of corporation that make it possible for computer viruses and worms to spread govern the simulation. See *Overview of Corporate Parameters* below for a description of each parameter.

The simulation models two different hypothetical corporations, each with its own corporate profile and policy. With two corporations, the speed at which a computer virus/worm spreads from one corporation to another can be demonstrated. VBSim users can alter the corporate parameters from the user interface, including the capability to increase or decrease the interaction between the corporations.

Each corporation in this simulation is comprised of roughly 500 workstations categorized both by their *sub-net* and by their *workgroup*. A sub-net is a cluster of machines that are all visible to each other on the network (for example, visible in the Windows Network Neighborhood). Workgroups are organizations based on functional groups such as Finance, R&D, Sales, and so on.

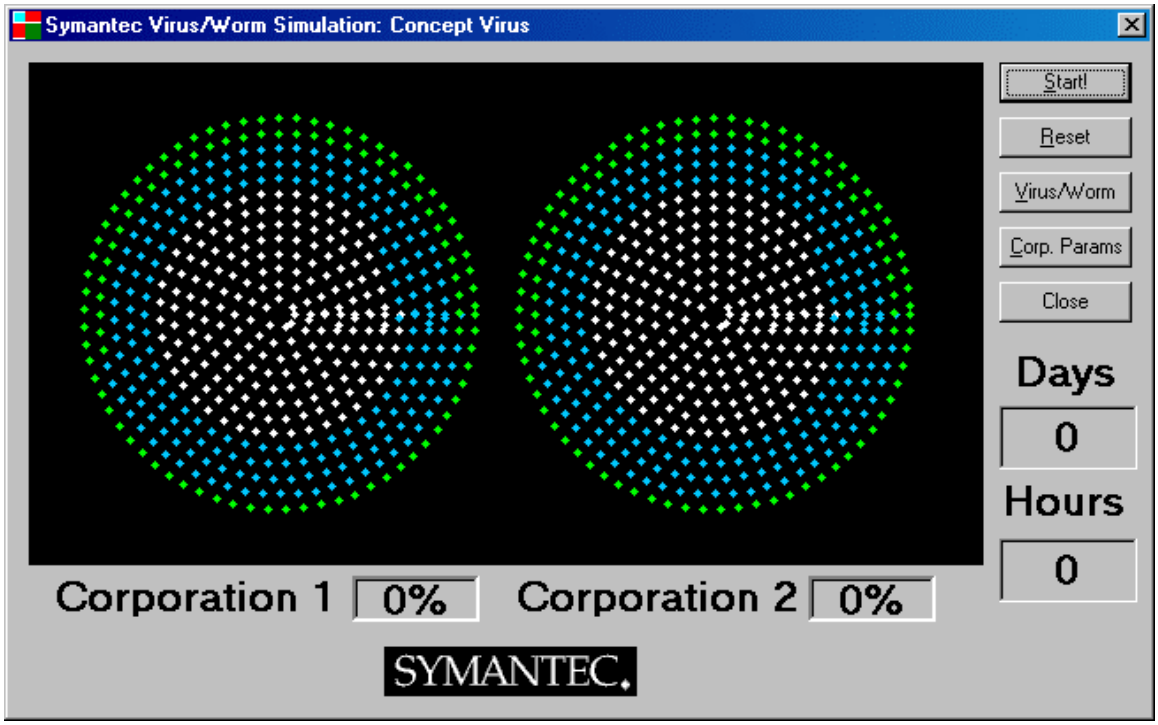
- **Sub-nets:** Machines in the simulation within the same sub-net can use peer-to-peer (shared-drive) networking to communicate with each other. Machines in separate sub-nets cannot easily obtain access to each other. For example, the sub-net grouping parameter has an impact on how the ExploreZip worm spreads in the corporation. This worm spreads, in part, by copying itself to shared disk drives. The size of the sub-net, and consequently the number of machines that can be accessed by one another, clearly affects how quickly a worm can spread.
- **Workgroups:** Each workstation in the simulation also has membership in a corporate workgroup. The simulation assumes that people in the same workgroup exchange information more frequently than they exchange information between different workgroups. This permits modeling of how quickly a computer virus spreads among workers in the same group as well as to the rest of the corporation. For the simulation, the frequency parameters can be changed.

In the simulation, each sub-net is comprised of 200 workstations resulting in three sub-nets per corporation. Similarly, there are 200 machines per workgroup resulting in three workgroups per corporation. Each workgroup is isolated on its own sub-net. The sub-nets and workgroup size parameters cannot be modified in this initial VBSim version.

The simulation also assumes that either no antivirus software is used in the corporation or that the existing antivirus software is unable to identify the virus/worm infection (for example, the corporation is being attacked by a new strain).

Understanding the VBSim interface

The main simulation screen appears at the start of the simulation. The two large circles represent two hypothetical corporations. Each corporation contains hundreds of dots, which represent workstations within the corporation. A dot's color (white, blue, or green) identifies the workgroup to which the computer belongs (for example, white could be Sales, blue could be Finance, and green could be R&D). As the simulation runs, the white, blue, and green dots change to red to indicate active viral infections.



The main simulation dialog contains three other key elements:

- The top of the dialog, "Symantec Virus/Worm Simulation: Concept Virus," indicates which computer virus/worm is being simulated. The program can run simulations with the Concept virus (the first macro virus), the Melissa virus/worm, and the ExploreZip worm.

- The bottom of the dialog displays the percentage of infected machines in Corporation 1 and Corporation 2.

- The right side of the main simulation dialog displays the number of simulated hours and days that have passed. The simulation is slightly unrealistic in that it assumes that workers in both corporations work 24 hours per day, seven days per week. Each and every computer on the network is assumed to be in use throughout the day. The simulation has no notion of down time, such as 9 to 5 work hours or lunch breaks.

The five command buttons can be used at any time:

Button	Description
Start!	Starts the simulation. Once the simulation begins, the button changes to Stop!, which can be used to pause the simulation. The simulation can be started and stopped at will.
Reset	Resets the simulation for a new run.
Virus/Worm	Specifies which virus/worm to run for the simulation. Clicking this button displays the Virus/Worm selection dialog where you can specify Concept, Melissa, or ExploreZip. You can also select how many initial infections to place in the corporation. Once you select a virus/worm and click OK, the simulation is reset just as if you clicked the Reset button from the main simulation screen. You can then click Start! to re-start the simulation with the new parameters.
Corp. Params	Specifies the corporate parameters for each of the two corporations in the simulation. These parameters are described in detail in *Corporate Parameters*.
Close	Ends the simulation and closes the program.

Demonstrating infections

This section describes how to use the VBSim simulation tool to observe the spread of the Concept virus, the Melissa virus/worm, or ExploreZip worm.

To start the Concept simulation:

1 Double-click the VBSim icon.

2 In the introduction dialog, click **OK**.

When the main screen displays, the program is ready to simulate the **Concept** macro virus.

3 Click **Start!** to begin the simulation.

By default, the simulation introduces a single infection into Corporation 1. This is represented by a single red dot amongst the white, green, and blue dots. As the simulation continues, more dots change to red to show the spread of infection to new machines. The virus may or may not spread to the second corporation, depending on the random nature of the simulation.

After about eight simulated days, click Stop! and examine the results (this should take about 40 seconds). The simulation displays the percentage (%) of machines infected in the corporation.

The Concept virus should spread to a fairly small number of machines in this timeframe, given the default simulation parameters. Typically, the total number of infected machines in either corporation is less than 5%. The Concept simulation demonstrates that computer viruses spread relatively slowly.

To start the ExploreZip simulation:

1 In the main screen, click **Virus/Worm**.

2 In the Virus/Worm selection dialog, select the **ExploreZip** worm.

3 Click **OK** to close the Virus/Worm selection dialog.

4 In the main screen, click **Start!** to begin a new simulation with the ExploreZip worm.

This simulation shows how rapidly a computer worm can spread in a corporation and that the ExploreZip worm spreads much more rapidly than the Concept virus.

After about two days of simulation (about 10-20 seconds), click Stop! to pause the simulation. In most cases, a majority of the computers are infected in both corporations by this time.

To start the Melissa simulation:

1 In the main screen, click **Virus/Worm**.

2 In the Virus/Worm selection dialog, select the **Melissa** virus/worm.

3 Click **OK** to close the Virus/Worm dialog.

4 In the main screen, click **Start!** to begin a new simulation with the Melissa virus/worm.

With the default corporate parameters, Corporation 1 does not have an ALL CORPORATION mailing list. An ALL CORPORATION mailing list is an address in the corporate address book that allows a user (or a worm) to send an email to everyone in the company (for example, "All Symantec" or "All Whammydyne"). In contrast, Corporation 2 does have an ALL CORPORATION mailing list.

Why is this important? Computer worms like Melissa spread by sending themselves to addresses in your corporate email directory. If your email directory has an address that can be used to send an email to everyone in the corporation, Melissa can spread extremely rapidly to the entire organization. During the simulation, watch how quickly Melissa spreads in each respective corporation. Clearly, disabling ALL CORPORATION mailing lists is an important policy decision to consider because it can dramatically decrease the susceptibility of your corporation to Melissa and similar threats.

The Melissa simulation demonstrates that computer worms spread orders of magnitude faster than computer viruses in a highly connected environment and that automated, immune system-like technologies are critical to battle fast spreading infections. Existing antivirus methods that work in human timeframes will fail to contain such worms.

Setting corporation parameters

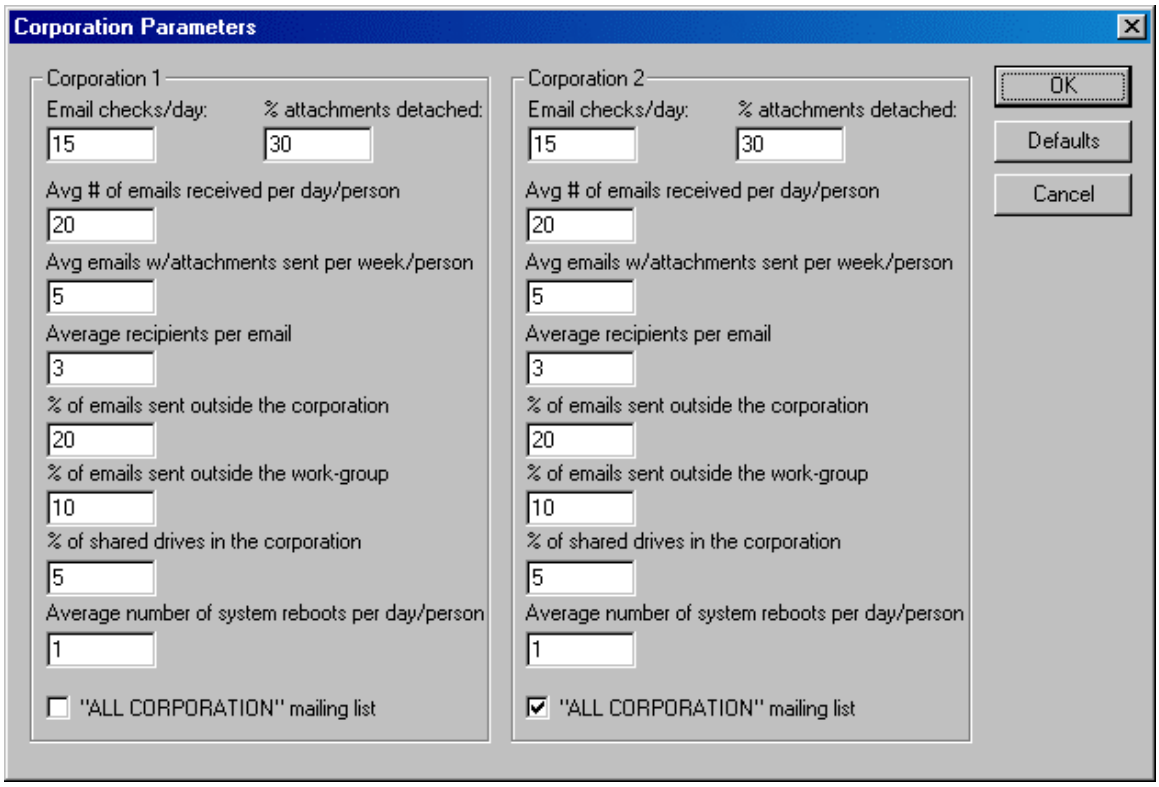
VBSim is governed by a number of parameters that describe the corporate environment. You can alter these parameters to see how a computer virus/worm spreads in other environments, which may more closely reflect your own corporation.

To change the corporation parameters:

- In the main screen, click **Corp. Params**.

To restore the original parameter settings:

- In the Corporation Parameters dialog, click **Defaults**.



Email checks per day

Specifies how many times average users checks their email inbox in a 24-hour period. This is significant because each of these email checks may result in an infection if the user receives an infected email attachment. By default, this value is set to 15, meaning that users check their email, on average, 15 times per day. Clearly, this value will be much higher for email addicts and much lower for prototypical data entry-operators.

% of attachments detached

Specifies how often users detach and view an email attachment from an email in their inbox. By default, this value is set to 30%, meaning that the average user opens about one in three attachments sent to them. Viewing an infected attachment could cause a computer virus/worm to gain control of the computer and spread to other computers. The default value was selected empirically. Most users don't have the time to detach and view all email attachments received.

Average number of emails received per day, per person

Specifies how many messages users receive on average each day (over 24 hours). This is significant because the ExploreZip worm spreads by responding to emails. If a machine is infected, every email received by a user on that machine will serve as a target for the ExploreZip worm. The actively running worm examines the user's inbox and replies to each and every email with a copy of itself. The default value of this parameter is 20 emails per day, per person. This means that on average, each user receives 20 emails per day.

Average emails with attachments sent per week, per person

Specifies how many emails a user sends each week that contain a potentially infected attachment (such as a Word for Windows document). If a user sends an infected document to a co-worker, that co-worker can become infected by the virus as well. This user-oriented parameter determines how quickly computer viruses spread in the hypothetical corporation. The default value of this parameter is five emails per week,

per person with an attachment. This means that, on average, each user send one email with a susceptible attachment per day.

Although this may seem unrealistic to some (especially power users that send many emails per day), the typical worker does not send many email attachments during the average work week. Again, this value was based on empirical observation. The simulation further assumes that once a user has launched a virus-infected file on their system, all files on the system become infected. Any subsequent emails containing attachments sent by the user from the infected machine will also be infected.

Average recipients per email

Specifies the number of recipients to whom a typical email attachment will be sent. Does the average user send email containing a Word document to one person or to twenty people? This user-oriented parameter determines how quickly computer viruses spread in the hypothetical corporation. The default value of this parameter is three recipients per email sent, which means that, on average, a user sends the attachment to three recipients.

Although this may seem unrealistic to some (especially power users that send many emails per day), the typical worker does not send many email attachments during the average workday to hundreds of users. Again, this value was based on empirical observation. The simulation further assumes that once a user has launched a virus-infected file on his or her system, all files on the system become infected. Any subsequent emails containing attachments sent by the user from the infected machine will also be infected.

% of emails sent outside the corporation

Specifies what percentage of emails are sent between corporations, instead of just inside the current corporation. This parameter affects the spread of computer viruses/worms between corporations. The default value of this parameter is 20%, meaning that 20% of all emails are sent to the partner corporation rather than inside the current corporation.

% of emails sent outside the workgroup

Specifies what percentage of emails are sent outside of the current workgroup, instead of just inside the current workgroup (for example, from R&D to Finance). This parameter affects the spread of computer viruses/worms between workgroups. The default value of this parameter is 10%, meaning that 10% of all emails sent within the corporation are sent inter-workgroup.

% of shared drives in the corporation

Specifies what percentage of computers have shared hard drives that are freely available on the corporate intranet (that is, without password protection). Machines that share hard drives are susceptible to infection by the ExploreZip worm. This worm seeks out other computers on the current sub-net and copies itself to their hard drives. Upon the next reboot, a system launches the worm and becomes infected. The default value of this parameter is 5%, meaning that 5% of all computers in the corporation have their hard drives accessible from the intranet.

Average number of system reboots per day

Specifies how often the average user reboots his or her computer on a daily basis (for whatever reason). This parameter is critical to the spread of the ExploreZip worm. This worm copies itself to the hard drive of peer-to-peer networked machines. The copy then lies dormant until the targeted machine is rebooted. Once a targeted machine has been rebooted, the worm gains control of the computer and starts spreading to other computers. The default value of this parameter is 1, meaning that each computer is rebooted an average of one time every 24 hours.

ALL CORPORATION mailing list

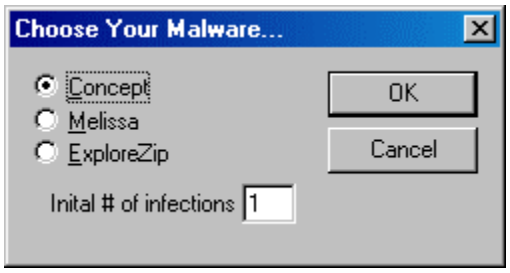
Specifies whether or not the corporation has an address book entry that allows users (or worms) to send an email to the entire corporation by addressing it to a single address. Examples of such an email address are "All sales" or "All Symantec."

How viruses and worms spread

The following sections describe how the Concept virus, the Melissa virus/worm, and the ExploreZip worm spread in the corporate environment, and how this spread is related to the corporate parameters. Each of these viruses/worms can be chosen from the Virus/Worm dialog.

To select a virus/worm and set the initial number of infections:

- In the main screen, click the **Virus/Worm** button.



Concept

The Concept virus is widely known as the first computer macro virus. This virus, which infects Word for Windows documents, spreads from computer to computer when users exchange documents via email, on floppy diskettes, or on file servers. The Concept virus spreads to each document within an infected computer that is opened in Word for Windows. The Concept virus does not, however, intentionally spread from one machine to another over the network. This behavior makes it a classical computer virus (as opposed to a worm).

The following corporate parameters directly or indirectly affect the spread of the Concept virus:

- Email checks per day: The rate at which users check their email affects how quickly they will become infected and infect other computers.
- % of attachments detached: If users have a low probability of opening attachments, they will rarely become infected. If they open virtually every attachment, they're likely to become infected as soon as they receive a virus in email.
- Average emails with attachments sent per day, per person: Every email a user sends with an attachment is a potential infection.
- Average recipients per email: The more recipients on an email, the more users that will potentially become infected.
- % of emails sent outside the corporation: This parameter affects how rapidly the virus will spread from one corporation to another.
- % of emails sent outside the workgroup: This parameter affects how rapidly the virus will spread from one workgroup to another in the current corporation.

Melissa

The Melissa virus is both a computer virus and a computer worm with two different spreading mechanisms. First, if an infected document is opened on a computer, Melissa infects that computer just as a traditional macro virus does: It spreads to other documents on the computer as they are edited or viewed by the user. If the user then shares these infected documents with someone else (via email or the file server, for example), they too will become infected. Second, when a user first opens an infected document, the worm attempts to email a copy of this infected document to the first 50 people in the user's email address book. Because of this behavior, Melissa spreads very rapidly to at least the first 50 people in the address book, but more slowly to people beyond these 50.

Additionally, companies often maintain an ALL CORPORATION email list, such as "All Symantec Employees." If a user (or worm) sends an email to this address entry, it will be sent to literally everyone in

the corporation. Many corporations hit by Melissa had company-wide mailing lists and Melissa spread hundreds of thousands of copies of itself in minutes.

In the simulation each corporation has roughly 500 machines. Notice that Melissa spreads to about 10% of those machines (roughly 50) rapidly, and then spreads to the other 90% more slowly. If the program simulated 5000 machines, roughly 1% of the machines would become infected rapidly (the first 50 entries in the email list) and the other 99% more slowly. The exception to this spread rate is if the corporation has an ALL CORPORATION email list allowing Melissa to spread through the entire corporation rapidly.

The following corporate parameters directly or indirectly affect the spread of the Melissa virus/worm:

- Email checks per day: The rate at which users check their email affects how quickly they will become infected and infect other computers.
- % of attachments detached: If user's have a low probability of opening attachments, they will rarely become infected. If they open virtually every attachment, as soon as they receive a virus in email, they're likely to become infected.
- Average emails with attachments sent per day, per person: Every email a user sends out with an attachment is a potential infection.
- Average recipients per email: The more recipients on an email, the more users that will potentially become infected.
- % of emails sent outside the corporation: This parameter affects how rapidly the virus will spread from one corporation to another.
- % of emails sent outside the workgroup: This parameter affects how rapidly the virus will spread from one workgroup to another in the current corporation.
- ALL CORPORATION mailing list: If the corporation has an ALL CORPORATION mailing list, Melissa can send itself to literally the entire corporation with a single infection.

ExploreZip

The ExploreZip worm spreads itself to other computers using two distinct mechanisms. First, like Melissa, ExploreZip is capable of leveraging Outlook, Outlook Express, and Exchange email programs to send itself over email. But, instead of sending itself to the first fifty users, ExploreZip sends itself (replies) to users that have recently sent email to the infected user. Second, ExploreZip also iterates through all machines that are visible on a peer-to-peer Microsoft network. The worm copies itself to accessible computers and updates a configuration file on the target computer causing the computer to launch the ExploreZip worm during the next boot-up. The worm continually searches for other peer machines to infect.

Historically, ExploreZip was difficult to eradicate from corporate networks because the moment an administrator removed the worm from a computer, another copy re-infected it. The peer-to-peer capabilities of this worm clearly underscore the vulnerability of peer-to-peer networks in the enterprise. In addition to infecting peer-to-peer networked machines, ExploreZip also deleted the contents of a variety of files from both local hard drives and the hard drives of networked peers.

In the simulation, it is assumed that an infected machine attacks other peer-to-peer networked computers on the local sub-net (with their hard drives available on the network) at a rate of 6 per minute. These machines become infected after a reboot. This parameter cannot be changed in the current simulation.

The following corporate parameters directly or indirectly affect the spread of the ExploreZip worm:

- Email checks per day: The rate at which users check their email affects how quickly they will become infected and infect other computers.
- % of attachments detached: If user's have a low probability of opening attachments, they will rarely become infected. If they open virtually every attachment, as soon as they receive a virus in email, they're likely to become infected.
- Average # of emails received per day, per person: ExploreZip, when running on a computer, will respond to every incoming email with a copy of itself. This parameter specifies how many emails the average user receives per day. This directly affects the number of copies ExploreZip sends of itself.

- Average emails with attachments sent per day, per person: Every email a user sends out with an attachment is a potential infection.
- Average recipients per email: The more recipients on an email, the more users that will potentially become infected.
- % of emails sent outside the corporation: This parameter affects how rapidly the virus will spread from one corporation to another.
- % of emails sent outside the workgroup: This parameter affects how rapidly the virus will spread from one workgroup to another in the current corporation.
- Average # of system reboots per day per person: Once ExploreZip has copied itself to another computer using its peer-to-peer technique, the target computer must be rebooted for the worm to activate. This parameter has an affect on how quickly ExploreZip can infiltrate a new computer on the peer-to-peer network.
- ALL CORPORATION mailing list: If the corporation has an ALL CORPORATION mailing list, ExploreZip can send itself to the entire corporation from a single infection.

