Wisconsin Historical Society

Using Micro Focus® Secure Gateway, the Wisconsin Historical Society filtered and blocked emails containing the SoBig virus, keeping the Micro Focus GroupWise® system secure.

Solution
Thanks to Secure Gateway, “I slept pretty well last night, actually,” said Peter Oemichen, one day after the SoBig virus tore through computer systems around the world.

His GroupWise network was protected by Secure Gateway. While his colleagues throughout Wisconsin were scrambling to disinfect their systems from the the SoBig virus, the head of information services for the state-run Wisconsin Historical Society was able to rest easily. “GWAVA (now Secure Gateway) didn’t even slow down,” he reports.

SoBig-F arrives in emails with innocuous subject lines like ‘Your Details,’ ‘Your Application,’ ‘Thank You!’ and ‘Wicked Screensaver.’ If the recipient opens the .PIF or .SCR attachment, SoBig-F strikes, infecting the computer, then emails itself to other computers using the infected computer’s address book. The attack made many networks grind to a halt until IT staff could cleanse the computers. Mr. Oemichen, his staff, and their users were spared the trouble and frustration of having to do so because Secure Gateway kept their network inoculated.

Secure Gateway’s four strengths: post office protection, virus blocking, ease of administration, and flexible rules meant that GroupWise administrators could say “So what,” when asked about “SoBig.”

Results

LETTER OF THANKS
“My hats off to GWAVA (now Secure Gateway)! We were bombarded by the SoBig over the last couple of days, yesterday in particular—literally thousands of them. It was so bad we had to stop archiving blocked attachments to save space on the email volume. Can’t thank you enough,” he wrote to the Secure Gateway developers the attack was deflected. The state agency’s GroupWise network boasts more than 250 users and shares resources with other networks, like the University of Wisconsin. Academic users send many kinds of attachments to each other, and then leave the documents on the mail system for further study. “We have a lot of librarians and archeologists and museum curators who retain their data for a long time,” Mr. Omeichen explains. “We have 125,000 attachments in our message system.” Despite the colossal load of attachments, more than eight gigabytes in fact, Secure Gateway was able to weed through them and analyze and block SoBig, all the while allowing legitimate email and attachments through. “We never missed a beat,” Mr. Oemichen marvels. Secure Gateway’s Post-Office level scanning means

At a Glance

- Industry
  Government

- Location
  United States

- Challenge
  Emails containing the SoBig virus flooded the agency.

- Solution
  Use Secure Gateway to filter and block emails containing the virus.

- Results
  + Blocks specific attachments based on administrator-set policies
  + Offers flexibility with rule customization
  + Scans and blocks email at the perimeter
that even infected GroupWise networks can be disinfected. Even infected systems benefited from Secure Gateway on GroupWise. Adding the .SCR and .PIF attachment blocks and performing a post office sweep eliminated SoBig-F from their post offices.

EASY ADMINISTRATION
Staff providing information technology services have a different role every day. "I wear the email administrator hat and the network administrator hat." With many responsibilities, tools that make life easier are a must. Once Secure Gateway is installed on the MTA, the license key entered and the rules are set, Mr. Omeichen says, "you let it run." The heuristic analysis, real-time black lists, attachment blocking, and easy rule creation operate without supervision. Blocked messages are set aside automatically. Secure Gateway's archive viewer makes examining messages that were flagged as spam or suspicious attachments a simple task to complete upon request. "The other thing I like is the flexibility." Because so many users on his system send attachments, Mr. Oemichen says he had to cap the size of appended messages. Fortunately, rules are easy to generate and customize. "If I want to block at four megabytes, but I trust you enough to not to leave that on the server for a long while," he cites the example of a public relations employee who must transfer massive files to the media, "I can create an exception to that rule."

ALL THE INGREDIENTS FOR SUCCESS
Today's GroupWise administrators can count on the technologies Secure Gateway provides: post office protection, virus blocking, ease of administration, and flexible rules. These strengths make Secure Gateway the outstanding choice for maintaining a functioning network, even when faced with the most serious threat. Secure Gateway protects GroupWise inside and out.

“My hats off to GWAVA (now Secure Gateway)! We were bombarded by the SoBig over the last couple of days, yesterday in particular—literally thousands of them. It was so bad we had to stop archiving blocked attachments to save space on the email volume.”

PETER OEMICHEN
Email and Network Administrator
Wisconsin Historical Society

“My hats off to GWAVA (now Secure Gateway)! We were bombarded by the SoBig over the last couple of days, yesterday in particular—literally thousands of them. It was so bad we had to stop archiving blocked attachments to save space on the email volume.”

PETER OEMICHEN
Email and Network Administrator
Wisconsin Historical Society