Blaster

**A second look at the cost of Blaster
sheds new light on today's blended threats.**

JIM MORRISON, SYMANTEC SECURITY SERVICES

The following tale is based upon actual circumstances from corporate enterprises that were faced with confronting and eradicating the Blaster worm, which hit in August 2003. The story provides views from many perspectives, illustrating the complexity and sophistication needed to combat new blended threats.

THE STORY LINE

Mona is a single mother with two small children. She frequently falls short of money before the end of each month, and this month was no different. She was struggling to prevent the electricity from being disconnected at 5 p.m. She had to skip lunch again to pay the utility bill at the corner convenience store near where she works. The store had a payment station provided by the local electrical utility as a convenience to its customers and for people like Mona who had to juggle the struggles of barely surviving. She waited in line and presented her bill and cash to the store clerk. The clerk began to key in the account number and the payment. "That's strange," she remarked. "This has never happened to me before!" Mona asked what the problem seemed to be. She was running short of time and had to have the payment recorded to

Revisited

Blaster Revisited

beat the disconnect deadline. "This system just froze up then restarted on its own," related the clerk. She asked her coworker about what had just happened.

The other clerk was also processing payments. "Just reboot, that usually fixes the problem. Wait, did you say your system restarted on its own? The same thing just happened here. What's going on now?"

Mona left the store with her cash, her unpaid bill, and a very worried look. She had to get back to work to call the utility company before her short lunch break was over. Maybe she could buy just one more day before disconnection.

FIRST OBSERVATIONS

The utility company support line for the payment kiosks began to light up like a Christmas tree; every call that came in was a complaint that the XP systems kept restarting, hanging, or freezing in the payment application. The techs were baffled by the sudden instability of the program. An update had just been sent out last month; was there a bug in the code? The developers were quickly assembled in a conference room to decipher the strange behavior of the application. The test lab was reconfigured to test the latest update. The calls kept coming to the tech support line. By now, more than 100 of the payment systems were nonfunctional.

Four hours had passed since the first calls; most of the stores would be closed within the next two hours, giving the techs and developers a chance to work into the night to find the source of the problem. The network administrators were contacted to assist in troubleshooting the problems within the payment systems. Joining the group assembled in the development lab was a member of the security team. He had just been informed of a new worm that was spreading rapidly and reported by the security vendor. Early information indicated that the Microsoft DCOM (distributed component object module) vulnerability had been exploited. The vulnerability was described in Microsoft Security Bulletin MS03-026. The bulletin revealed a buffer overrun using RPC (remote procedure call), remotely using TCP/UDP port 135.

Now things started to make sense. The payment systems were connected to the accounting system via an ISP

dial-up connection and a VPN (virtual private network) link allowing a secure connection into the DMZ (demilitarized zone) established for the payment application. If these systems were hit by being on the Internet, the internal network should be safe. The majority of systems on the inside were unpatched, however. This made the security team very uneasy at the potential for the situation unfolding on company assets outside the production environment to somehow finding its way inside. Monitoring the network for unusual activity became an apparent necessity to try to stem any infection from spreading internally.

Information on what this new worm did and how it propagated began to flow from the security vendors. There was no doubt that this was the DCOM exploit everyone was expecting. Only 26 days had passed since Microsoft published the -026 bulletin. The name of this worm was Blaster. The first details revealed how Blaster affected the pay systems connected to the Internet and the propagation mechanism that made them fail.

The worm would target an IP segment and deliver packets designed to overrun the buffer on port 135. The volume of packets generated had the capacity to saturate and crash the RPC service. This no doubt was the reason the pay systems kept rebooting during the initial targeting by the worm. The early write-ups indicated that once the buffer was compromised, a command shell would trigger `tftp.exe` to pull `msblast.exe` across the network from the infected host. Once the command shell executed, the process would be repeated over and over again, with the newly infected host using the IP targeting routine to find another vulnerable computer.

The director of security called a hasty meeting in one of the vacant conference rooms to ascertain the facts and determine what action should be taken. The entire team was now disrupted from the list of ongoing projects that also had priorities and deadlines. "OK, what have we got?" asked the director, very concerned about the early reports of a key revenue system now completely inoperative.

"It looks like a worm circulating outside, hitting our pay systems," volunteered the lead tech for the pay-system application.

Meanwhile, Mona was growing impatient with customer service. She had been put on hold after demanding to talk to a supervisor when the first customer service representative did not agree to extend the time she had to pay the electricity bill. Mona was told to pay her bill in person at the branch office before 5 p.m. or face disconnection. That was not an option—she could not leave work early to make it across town to the closest branch office in time, especially since she had had to take extra time off recently to care for her sick child. The supervisor took the hard-line approach. “But the systems in the stores went down, it’s not MY FAULT!” exclaimed Mona. “I’m sorry,” replied the supervisor, “that is our policy. We have to have payment from you by 5 p.m.” Mona hung up. Without an extra day to pay her bill she was facing certain disconnection, meaning extra reconnection fees and no lights or stove to fix hot meals for her kids.

Back in the conference room at the electric company, the security director asked the pay-system tech, “Weren’t these systems patched?”

“No, not all of them,” explained the tech. “We tried, but our patch agent was hanging when we tried to deploy through the slow link. Since most of the pay systems are unpatched, they went down first.”

The director asked how long these systems would be down.

“We hope to send out some people with the patch and latest virus definitions on CD to all of the stores,” the tech said, avoiding eye contact with the director, knowing that he could go ballistic.

SPREAD AND CONTAINMENT

The swing shift for the help desk was just coming on. The day shift was asked to stay on to field the increase in calls from users complaining of slow systems and unexpected reboots. They knew that

a worm was circulating from the security alerts arriving from subscription e-mail lists and from the report on CNN. The conclusion that the worm had found its way inside was a no-brainer. They had just finished cleaning up from Fizzer two months ago. That wreaked havoc with the corporate mail system. The task at hand was to identify the systems that were infected and pull them off the network. The admins of the firewalls had begun to sniff the network and monitor the logs to look for port-135 scans.

The latest write-up revealed the opening of a port as a backdoor for a potential hacker to gain access on an exploited system. Port 4444 needed to be blocked at the perimeter to prevent unauthorized access. One of the firewall admins compared the clues in the write-up with the data from the sniffer. Since the firewall was a Linux platform, the native TCPDUMP utility was able to capture the information, filtered for the suspected internal IP segment (see figure 1).

There was the port-135 hit from the 192.168.0.1

Filtered TCPDump logging

```
17:15:36.395032 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:15:36.395323 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:15:36.395436 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.508095 192.168.0.1.1294 > 192.168.0.3.135: tcp 72 (DF)
17:16:19.508310 192.168.0.1.1294 > 192.168.0.3.135: tcp 1460 (DF)
17:16:19.508346 192.168.0.1.1294 > 192.168.0.3.135: tcp 244 (DF)
17:16:19.508362 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.508541 192.168.0.3.135 > 192.168.0.1.1294: tcp 60 (DF)
17:16:19.508681 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.508720 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.512201 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.512346 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.904949 192.168.0.1.1314 > 192.168.0.3.4444: tcp 0 (DF)
17:16:19.905031 192.168.0.3.4444 > 192.168.0.1.1314: tcp 0 (DF)
17:16:19.905160 192.168.0.1.1314 > 192.168.0.3.4444: tcp 0 (DF)
17:16:19.952874 192.168.0.3.4444 > 192.168.0.1.1314: tcp 42 (DF)
17:16:19.984939 192.168.0.1.1314 > 192.168.0.3.4444: tcp 36 (DF)
17:16:19.985029 192.168.0.3.4444 > 192.168.0.1.1314: tcp 63 (DF)
17:16:20.083469 192.168.0.3.1049 > 192.168.0.1.69: udp 20
17:16:20.118800 192.168.0.1.69 > 192.168.0.3.1049: udp 516
```

FIG 1

Blaster Revisited

system targeting the 192.168.0.3 machine. The shell opened the backdoor element within the worm on TCP port 4444. Port 69 identified the propagation of the worm targeting another system, listening for tftp.exe on the next vulnerable system to pull across the executable. An infected system was found, except that segment was in the range for the guest offices located throughout the campus. This system could be anywhere. Obviously, this was not a company system, but where was it located?

ON THE TRAIL

Day had turned into night and the application team was now testing in the lab the scripts that would automate the patch for the XP systems at the various remote locations throughout the region. The internally developed payment application provided a level of security when in use. The kiosk user at local log-in triggered the ISP dial-up and the starting of the payment-entry application. To patch the system, an administrator account on the XP system had to be used to run the security patches. Trying to script the process so that nontechnical people could accomplish the task had its challenges.

Windows XP System Shutdown Window

FIG 2

The monitoring of the network continued using TCPDUMP, recording different IP segments. The initial discovery of the port-135 scans somewhere in the guest offices was no longer active. The help-desk swing shift had been developing a list of users, machine names, and IP addresses that had called with sudden restarts, unresponsive systems, and anything that seemed suspicious.

The word had not gotten out to the majority of users in time for them to shut down their systems before leaving for the day. Hopefully, any systems that had become infected and were pinging the network could be located during the night. The system in the guest offices was gone, but the sniffer trace located another system on the same IP segment. The machine name indicated it was the system assigned to the front-desk security counter.

Further investigation revealed that the system was not used except for the occasional need to modify badge images for long-term contractors. This was done with a digital image-processing application. For convenience, the system was on the same IP segment as the guest offices, but it was given access to the main production network to place image files on an open share on the server used by human resources. The server was scheduled to be decommissioned and was hardly used, except for image storing. Had this system been overlooked during the blitz to patch the servers once Microsoft made the -026 patch available?

The next morning staffers in the human resources department began to power up their systems and start their day like any other. It didn't take long before the XP laptops they took home every night started to exhibit the same characteristics as the payment systems: sudden reboots, the loss of drag-and-drop functionality, and other strange behavior. The HR staff called the help desk. A technician was able to remote into one of the systems and saw a telltale sign that the Blaster worm was affecting the HR department (see figure 2).

This was a smoking gun! Now the task was to find the source of the infection.

The conference room used for the first discussions had been converted to a war room. The whiteboards were filled with IP addresses gathered by the help desk of systems suspected of being infected and trying to propagate the worm. Another list for all of the nonfunctional pay

systems covered the entire portable whiteboard. These systems would have to be patched before they could be used to receive payments again.

The security director asked for the latest reports of systems pinging port 135 to be able to locate them and get them off the network. One suspected system was the HR server. The IP address seen yesterday in the guest offices was also on the list. The director assigned one of the firewall techs to sniff the HR segment. "Why is the HR server infected?" he asked. One of the network admins in the room suggested that it was not on the active server list and was passed over to touch all of the critical servers first. This one had fallen through the cracks. "What are the latest technical details from our vendors on how this thing works?" the security director asked. Several techs were monitoring the vendor's security Web sites for the latest details and began to offer the latest postings of details. They were able to supply the propagation routines used by Blaster.

The tech sent to sniff the HR segment came back with a handful of printouts, and we were able to isolate the infector. The HR server was trying to spread the worm on the same network segment. It looks like the routine also seeks out nearby segment octets (see figure 3).

When comparing the printout to the information provided by the vendors, the routine began to make sense. Reviewing one of the write-ups, the sniffer printouts confirmed the documented behavior. Blaster generates an IP address and attempts to infect the computer that has

that address. The IP address is generated according to the following algorithms:

- For 40 percent of the time, the generated IP address is of the form A.B.C.0, where A and B are equal to the first two parts of the infected computer's IP address.
- C is also calculated by the third part of the infected system's IP address; however, for 40 percent of the time the worm checks whether C is greater than 20. If so, a random value less than 20 is subtracted from C. Once the IP address is calculated, the worm will attempt to find and exploit a computer with the IP address A.B.C.0.
- The worm will then increment the 0 part of the IP address by 1, attempting to find and exploit other computers based on the new IP address, until it reaches 254.

Mona's alarm woke her up—a good sign that she still had electricity. Maybe, because of the problems with the pay systems, the power company was giving her extra time. She set out to fix a hot breakfast for her children, get them dressed, and walk them to school before facing another day of dealing with customer service to buy more time before disconnection.

In the war room they were able to identify several XP laptops assigned to HR that had not been updated by the patch. "Why did these systems not update?" asked the security director. He had brought in the team for patch deployment. Not being standardized on a patch technology, the team had to use different methods to try to stay ahead of the vulnerabilities.

"From what we can determine there is something a little different with these XP laptops," remarked one of the deployment techs. "The logs show the patch ran, but in checking the files, we see that some of the DLLs did not update."

Table 1 is the list of files that should have been updated, pulled from the Microsoft Web site:

Spot checks revealed that the file versions were the same as before and thus were never updated. For some reason, the update failed without reason on these systems. "Are we doing anything special with group policy on these systems?" asked the

Network Packet Sniff Report

```
17:07:54.032412 15.54.153.107.1038 > 15.54.152.106.135: tcp 0 (DF)
17:07:54.032657 15.54.153.107.1039 > 15.54.152.107.135: tcp 0 (DF)
17:07:54.032901 15.54.153.107.1040 > 15.54.152.108.135: tcp 0 (DF)
17:07:57.032668 15.54.153.107.1039 > 15.54.152.107.135: tcp 0 (DF)
17:08:14.060589 15.54.153.107.1074 > 15.54.152.125.135: tcp 0 (DF)
17:08:14.062041 15.54.153.107.1078 > 15.54.152.129.135: tcp 0 (DF)
17:08:14.064937 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:17.061195 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:23.069724 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:35.489747 15.54.153.107.1104 > 15.54.152.141.135: tcp 0 (DF)
17:08:44.307318 15.54.153.107.1145 > 15.54.152.177.135: tcp 0 (DF)
17:08:44.308202 15.54.153.107.1148 > 15.54.152.180.135: tcp 0 (DF)
```

FIG 3

Blaster Revisited

Heads Up

The mass media, cable channels, and the news services report on the latest computer worms that are able to sweep the globe and cause attention with their effects. By the time the mass media reports on the worm, it is already too late. First-response reporting services can be of great benefit during the initial stages of a global outbreak.

EARLY INFORMATION WARNING

These security vendors offer subscription services that provide early information warning systems on the latest threat.

Symantec

<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=158&EID=0>

Trend Micro

<http://www.trendmicro.com/en/home/us/enterprise.htm>

iDefense

<http://www.iddefense.com/main.jsp?flashstatus=true>

ALERT AND INFORMATION SERVICES

These industry organizations also provide alert and information services to subscribers.

CERT (The U.S. Computer Emergency Readiness Team)

<http://www.us-cert.gov/>

CSRC (Computer Security Resource Center)

<http://www.csrc.nist.gov/pcig/ppsp.html>

The SANS (SysAdmin, Audit, Network, Security) Institute

<http://www.sans.org/index.php>

director. He was shooting in the dark to get some answers to this latest twist and hurdle to bring all of the corporate systems up to date and help curtail the spread of the worm, now infecting about 500 internal systems.

"The only thing we did differently on these XP systems is to restrict user policies," the lead tech admitted.

"Can you research if policies somehow are getting in the way?" asked the director. His patience was starting to wear thin, and everyone knew it.

Everyone on the help desk, every local network and firewall administrator, the mail administrators, and the network operations center were focused on finding systems broadcasting on the network, pulling them off the wire, and getting them patched manually. Everyone was tired; the food brought in for the troops helped, but everyone silently wished they were somewhere else.

Mona skipped her lunch to try to make her payment at the same store where she was turned away yesterday. "Are you taking payments yet?" The clerk said no and didn't know when someone would be out to get the systems back online. Mona was dreading the call to customer service to plead for an extension.

PREPARING FOR THE SECOND ATTACK

The end of the week had arrived and the war room was still in operation. The lists of systems on the whiteboard were getting smaller, and the majority of pay systems were patched and processing payments. Some were down for three days, like the one near Mona's workplace.

The network operations folks were called together to discuss the next issue to deal with regarding Blaster. They knew that they had not found all of the unpatched systems. The laptops, usually out in the field, were always a hit-and-miss proposition to find on the network and deliver a patch or to have the user take the machine to a field office. That meant that on the 16th they could see a flood of traffic launched against Microsoft. The second phase of Blaster, launching a DoS (denial of service) attack against windowsupdate.com, was imminent.

The network operations team was briefed on the SYN flood attack that Blaster was triggered to launch over the weekend. The specifics were reviewed. The DoS traffic has the following characteristics:

- Is a SYN flood on port 80 of windowsupdate.com.
- Tries to send 50 HTTP packets every second.
- Each packet is 40 bytes in length.
- If the worm cannot find a DNS (Domain Name System) entry for windowsupdate.com, it uses a destination address of 255.255.255.255.

Some fixed characteristics of the TCP and IP headers are:

- IP identification = 256
- Time to Live = 128
- Source IP address = a.b.x.y, where a.b are from the host IP and x.y are random. In some cases, a.b are random.
- Destination IP address = DNS resolution of "windowsupdate.com"
- TCP source port is between 1000 and 1999
- TCP destination port = 80
- TCP sequence number always has the two low bytes set to 0; the two high bytes are random.
- TCP window size = 16384

The new task was to devise a plan to monitor outbound traffic over port 80 destined for windowsupdate.com to try to trace back systems still infected but previously unknown. One by one, the systems were removed from the network, patched, scanned, repaired, and sometimes reimaged altogether. Systems launching the DoS could be traced through the firewall or proxy logs. The crew would have to put in extra hours over the weekend.

POSTMORTEM RESULTS

The entire team that participated in the Blaster mitigation was now assembled for a postmortem meeting to review what happened and to develop something of substance to prepare for the next time. A month had slipped away since the first gathering in the vacant conference room to analyze the problem. From the first pay system that rebooted suddenly to this meeting, everyone involved

had contributed a huge amount of human effort chasing infections, patching systems, repatching systems that had failed originally, and working in the field touching, manually, more than 100 pay-system locations. This meeting was to review how this could have been different.

The security director presented his agenda of items. Technical leads from the various teams had been asked to summarize their groups' tasks and responsibilities and to honestly detail the failures and find plausible explanations. The patch deployment team was called on first.

"To summarize," said the lead tech, "we should look into standardizing on a single patch technology. From our previous growth by acquisition and the legacy patch system that came with these acquired business units, we should have one standard software solution for the entire enterprise." This was a logical conclusion, but the budget for this year did not include a line item to purchase new licenses for the 20 percent of the enterprise using the nonstandard solution, not to mention the resource issue to implement such an upgrade.

"Did we find out why the XP systems in HR did not get patched on the first go-round?" asked the director.

"We had to do some research, but we found out that the way we locked down the users prevented the patch from running properly," lamented one of the policy admins. "What we discovered was that the software restriction policy for the local computer allowed only local computer administrators to select trusted publishers. Because our patch agent ran as a pseudo user, the agent did not have the necessary rights. This was causing the failure. We changed the group policy for the HR systems so that we can patch remotely from now on."

The director then inquired about the HR server that was the source of the original infection in the HR department.

"That is another interesting story," answered the lead tech. "We bypassed patching the HR server because we

were going to take it offline and replace it at the end of the same week that Blaster hit. A contractor using the guest offices brought Blaster inside. His laptop infected the security-counter image-storage system, which then found its way to the HR server. That in turn spawned the infections to the HR XP laptops where the patch failed.

TABLE 1

For Windows XP Professional and Windows XP Home Edition

Date	Time	Version	Size	File name
05-Jul-2003	19:14	5.1.2600.115	1,092,096	Ole32.dll pre-SP1
05-Jul-2003	19:14	5.1.2600.109	439,296	Rpcrt4.dll pre-SP1
05-Jul-2003	19:14	5.1.2600.115	203,264	Rpcss.dll pre-SP1
05-Jul-2003	19:12	5.1.2600.1243	1,120,256	Ole32.dll with SP1
05-Jul-2003	19:12	5.1.2600.1230	504,320	Rpcrt4.dll with SP1
05-Jul-2003	19:12	5.1.2600.1243	202,752	Rpcss.dll with SP1

Blaster Revisited

"It looks like we need to revisit our network access policy again. We can't let people on our network without doing some types of checks for compliance or scanning their systems," remarked the security director. "I want to move onto the payment systems. They were hit first. Why didn't they get patched like our internal systems?"

It was now time for the payment-system application developers to answer some very tough questions. In the rush to develop the payment system application internally, the operating system was not scrutinized. The design of the application and the modifications to user authentication and rights upon log-in and connection to the local ISP made patching the systems extremely difficult. With the connection into the special DMZ, they were not seen on the production network. Using dial-up links made for issues as to when a patch could be triggered. Obviously, these payment systems had to be rethought and hardened.

LESSONS LEARNED

The utility company in this story struggled to beat Blaster and to clean up from its lasting effects. What "lessons learned" can be derived from the circumstances that allowed Blaster to disable systems that were used to generate revenue? Which policies did not work or were breached, allowing internal penetration by the worm? What operational shortcomings were revealed that made it more difficult to accomplish the tasks to secure the environment?

What did Blaster cost in lost revenue, delay of other projects, human resources, frustration, and lost time?

THE COSTS

1. Personal. To Mona, the cost was dealing with the utility company when she could not pay her bill on time. She was disconnected, but was finally able to make a payment, three days late when the pay system was back

Getting to the Bottom of Blaster

Blaster generated considerable traffic on corporate networks once it permeated perimeter security or was brought inside the firewall. With an infected system inside, infecting or attempting to infect unpatched systems, network administrators had the challenge of locating the infector.

The characteristics of Blaster and later Welchia heavily utilized port 135 to take advantage of the Microsoft DCOM (distributed component object module) vulnerability. Using this characteristic, network administrators can trace the IP address back to the system that attempts to find vulnerable systems. With tools such as TCPDUMP included in Unix/Linux firewalls, the source IP addresses can be discovered by keying on port-135 requests. Commercial or freeware packet-sniffing tools such as Network Instruments' Observer or Ethereal placed on the network segment can also capture and filter the port-135 pings and identify the source IP. The volume of pings identifies a potential infector from normal port-135 traffic. Whether you use a software sniffer package or an appliance that

performs the same way, it is important to isolate the source.

Antivirus vendors also provide tools and utilities that can assist in tracking the source of specific infections. Contact your antivirus vendor for available tools and utilities.

Personal firewall components now being bundled with antivirus technologies can also block or log connections from other systems. Review of these logs may also pinpoint the potential Blaster infector. The latest generation of antivirus technology is offering backtrace techniques that can use the network to discover the source of an infection. Symantec's Client Security version 2.0 provides a backtrace component within the corporate antivirus client.

Note: Before vendors deliver virus definitions, they must employ standard network forensic methods. Once vendors release detection capabilities, then the security products can not only protect against unknown infectors but also aid in the identification of the source.

online. Because of the circumstances, the reconnection fees were waived. Unfortunately, she had to serve cold cereal by candlelight to her kids for dinner; the food spoiled in the refrigerator; there was no TV to distract the kids—it was a rough few days.

2. The company. The utility company lost more than \$1 million in revenue that would normally have been generated from the pay systems during the time they were down. Current projects had to be tabled during the Blaster crisis because everyone was needed to mitigate the situation that Blaster caused. Overtime pay put the quarterly budget over the top, affecting bonus calculations. Those workers who were involved daily were challenged, overworked, and frustrated.

The weaknesses in the company's policies and technical solutions became evident. It came to realize that there was much more work to be done to prevent any future threat bouncing around the internal network. It failed because:

- The patch technology was incomplete and not standard.
- The processes to administer patches and audits had holes, allowing vulnerable machines on the production network.
- The internal development processes did not have a security-review component to ensure compliance with acceptable security standards.
- Network-access policy was not being enforced, allowing a noncompliant, noncorporate asset on the network.
- Convenience took precedence over security.

3. The world. The month of August 2003 cost millions in lost productivity, the time required to mitigate Blaster and later Welchia exploiting the DCOM vulnerability, not to mention the inconvenience to the public at large. The propagation was comparatively slow compared with other blended threats seen before. The time of exploit, the time from when the vulnerability was disclosed to the appearance of Blaster, had been reduced from what was seen in previous malicious events.

Estimates of losses vary, but economists and industry analysts believe that the losses in productivity, lost revenue from disabled systems, and the human cost to patch systems and restore those that became nonfunctional are substantial—somewhere between \$320 million and \$500 million or more. The most recent estimates provided by Microsoft estimate that 16 million or more systems fell victim to the Blaster worm. The Blaster epidemic was far larger than many believe.¹

Exploit of the DCOM vulnerability created the need for Internet service providers to employ higher security

standards. The resulting reactions changed the Internet landscape. Use of DCOM by legitimate programs had to be rewritten to circumvent port blocking instituted by ISPs around the world. The cost of redevelopment is almost immeasurable.

Blaster took a toll on those involved in this story. The IT workers saw little of their families during the course of the events of Blaster. The weaknesses of internal security, the non-enforcement of policies, the lack of patch deployment, and the rush to deploy applications became very apparent to the security director. This was a very tough lesson to learn. The setback of IT project schedules as a result of Blaster further upset the security director and his goal to protect the enterprise.

The utility company lost significant revenue from the payment systems when they were disabled. Those individuals, like Mona, who had to juggle money and stretch financial deadlines to the extreme and who relied on the payment systems were dealt financial and personal setbacks. The application development of the payment systems without the necessary security scrutiny became very apparent.

All who were affected by Blaster invading their lives in one way or another recovered from the disruptions. The memories of August 2003 are fading with time. Everyone, if given a choice, would probably have chosen to have never met Blaster in the first place. Q

REFERENCES

1. For the latest discussion regarding the breadth of the Blaster infection, see Remos, R. MSBlast Epidemic Far Larger than Believed. CNET News; http://news.com.com/2100-7349_3-5184439.html.

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

JIM MORRISON is a senior security consultant with Symantec Security Services, where he manages antivirus security audits and evaluations; leads antivirus planning, implementation, and administration; implements intrusion protection at the gateway and groupware levels; and provides overall project management. Morrison first worked in Symantec's support organization, providing subscriber-based support to Fortune 500 corporations. His past experience includes teaching biology and chemistry at secondary and college levels. Morrison earned a B.S. degree in biological sciences with a minor in chemistry from Northern Illinois University.

© 2004 ACM 1542-7730/04/0600 \$5.00