

By John McCormick and Bill Detwiler, MS, MCP

Before an individual executes a serious attack against your network, he or she will likely spend time preparing for the event--just as traditional thieves often "case" their intended targets. Cybercriminals conduct pre-attack activities designed to identify the attack's goal, determine the attack's target, and detect the target's exploitable weakness. Being able to detect and appropriately react to attack precursors will increase your ability to recognize, defend against, and potentially prevent actual attacks. But even if you aren't the explicit target of an attack, there can be signs that a general probe for systems open to newly discovered vulnerabilities is in progress. This list gives valuable information to help you recognize, detect and react to the following attack precursors: increase in port scan activity; unauthorized access attempts; application scanning; discovery of malicious software or hardware; social engineering attacks.

<u>Attack precursor</u>	<u>Detection</u>	<u>Reaction</u>
<p>1 Increase in port scan activity: This is the primary indicator of an automated or targeted attack on any system connected to the Internet.</p>	<p>If your logs show an increase in scan activity, find out if the scans are linked to a general attack or point to a targeted attack at http://isc.sans.org and http://isc.sans.org/top10.php.</p> <p>Knowing the threat will help you determine how extreme your defensive measures should be.</p>	<p>If your services don't use the scanned ports, immediately block the ports at your firewall. If the ports are essential, increase your monitoring and move the services to alternative ports where feasible.</p> <p>If the port scan activity is targeted at a specific IP address and not a general sweep, changing your IP address may mitigate a future DoS attack. This technique has been used by many government agencies (even The White House) when there were Internet rumors of a pending attack or a virus carrying a DoS.</p> <p>You can find a downloadable plain text list of ports at http://www.iana.org/assignments/port-numbers and a searchable port database at http://www.cirt.net/cgi-bin/ports.pl.</p>
<p>2 Unauthorized access attempts: Obviously having an unusual number of failed password-based logon attempts may be a major clue that someone is probing your system.</p>	<p>Check your logs and try to determine the origin. The attempts may be an error from a telecommuter's automatic logon program or a user who has forgotten his or her password and is making a legitimate attempt to access the system.</p> <p>Once you determine that the unauthorized access attempts are malicious, you should take appropriate action.</p>	<p>Require that all users of the targeted system change their password and help users create strong passwords, which are not easy to guess or subject to simple dictionary attacks. If you haven't done so already, change all default administrative and guest passwords. Hackers often use lists of vendor default passwords. To quickly determine if your software or hardware is using a default password, try the user name and passwords on the following lists:</p> <ul style="list-style-type: none"> ➤ http://www.cirt.net/cgi-bin/passwd.pl (network-related systems) ➤ http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php (network-related systems) ➤ http://defaultpassword.com/?char=&action=dpl (cell phones)

<u>Attack precursor</u>	<u>Detection</u>	<u>Reaction</u>
<p>3 Application scanning: This attack precursor normally impacts Web-based applications.</p> <p>Typical application attacks begin with port scanning, but serious attacks attempt to make the application do something unusual in response to a “strange” message.</p> <p>Hackers may send the application a request using a malformed URL. Such a request will often generate error messages that a hacker can use to design a DoS attack.</p> <p>Hackers may also send malformed search or other requests that include meta characters not normally in such a request.</p>	<p>If an application slows unexpectedly or experiences other unanticipated problems (more restarts than usual), review the logs for malformed requests. The request will often contain single quotes, semicolons, greater-than and less-than signs, or other illegal characters (based on the particular application).</p>	<p>Protecting against application attacks is difficult because application security depends very heavily on how the application was designed and developed.</p> <p>You can, however, try to block access and traffic from the source(s) generating the malformed messages. You can also deploy a commercial intrusion detection/prevention system.</p>
<p>4 Discovery of malicious software or hardware: Malicious software includes viruses, Trojans, worms, root kits, adware, spyware, key loggers, and the like. Malicious hardware includes key loggers, rogue servers or clients, unauthorized wireless devices, and similar devices.</p> <p>You should protect every system with software that detects and removes viruses, spyware, and adware. Use real-time malware scanners when possible and back them up with scheduled, full-system scans.</p> <p>You should also regularly review your network logs for any unusual or unauthorized devices.</p>	<p>The following occurrences may indicate the existence of malicious software or hardware:</p> <ul style="list-style-type: none">➤ Unusual error messages➤ Increased outgoing traffic unrelated to normal activity--particularly during normally quiet times➤ System slowdowns➤ Increased use of system resources. <p>You may also see messages that an unidentified program is attempting to access some unknown or unusual URL, such as one associated with an instant messaging service.</p>	<p>The procedures used to disable and remove malicious software and hardware are determined by the specific threat.</p> <p>Malicious hardware should be physically removed from the network or denied access. You should maintain adequate physical security at all office locations and employ strong network security practices, particularly on wireless networks.</p> <p>If possible, remove malicious software using your organization's malware scanning and removal solution (antivirus software, spyware application, or adware detection tool). Depending on the malware, multiple tools/approaches may be needed to detect and completely remove the infection.</p>

Attack precursor

5

Social engineering attacks:

Social engineers are essentially "con artists" who call someone (usually outside the security structure) and pretend to be from the help desk, telephone company, network vendor, a new employee, a salesman on the road, or anyone else who might conceivably be authorized to access a network, and simply ask for a username and password.

They may first call the switchboard and ask for someone in the MIS department or simply do an online search for the names of staff or management, then call a remote office and impersonate them.

But often these scammers need only to sound confused, drop a few company-specific buzzwords, and ask for help.

Detection

These attacks can be extremely difficult to detect because people who are ready to give out such information to a strange voice on the telephone, or a stranger wearing a uniform and carrying a clipboard, won't realize this is an attack and therefore won't report the incident, especially if they actually give out the information and later realize their mistake.

Regularly warning and educating your end users and IT staff to recognize social engineering attacks is the only way to prevent and detect them. End users should also be told how to report such incidents.

Reaction

If an employee reports a social engineering attack there's little you can do to trace or catch the offender. Unless the social engineer returns and you have evidence of a serious crime or there's a national security interest, the telephone company and law enforcement won't get involved.

Your best course of action is to determine what, if any, information the offender received and then take steps to mitigate the potential damage the social engineer could cause with that information.

It's also possible that only one employee reported an incident, but several occurred. You should contact managers throughout your organization and inform them of the incident. Ask them to report any suspicious activity recently witnessed by their employees and then follow up a few days later.



John McCormick is a freelance technology writer and reporter for multiple online and print publications. He is a member of The National Press Club of Washington and has been a contributing editor/writer to *PC Companion*, *CD-ROM Review*, *ComputerCraft*, *Shareware Magazine*, *ID Systems*, *Capital Computer Digest*, *Computer Press (Moscow, U.S.S.R)*, was the *Macintosh Editor* for *Vulcan's Computer Monthly*, and *Senior Editor* for both *Computer Monthly* and *Reseller World* magazines. John was a major contributor to *Computer Shopper*. He served as the *Washington Bureau Chief* for *NewsBytes News Network* and has also written reviews for *PC Magazine*.



Bill Detwiler is a Section Editor for CNET Networks where he works on the *TechRepublic.com* team. Previously he worked as a *Technical Support Associate* and *Information Technology Manager* in the social research and energy industries. Bill is a *Microsoft Certified Professional* with experience in *Windows administration*, *data management*, and *desktop support*. He has bachelor's and master's degrees in the *Administration of Justice* from the *University of Louisville*, where he guest lectures on *high-tech and computer crime*.

Additional resources

- **Subscribe to TechRepublic's [Downloads RSS Feed](#) [XML](#)**
- Sign up for TechRepublic's [Downloads Weekly Update newsletter](#)
- Sign up for TechRepublic's [Windows XP newsletter](#)
- Check out all of TechRepublic's [free newsletters](#)
- [Virus prevention checklist](#)
- [Computer crime evidence-preservation checklist](#)
- [Computer crime reporting checklist](#)
- [Windows XP services that can be disabled](#)
- [Windows Server 2003 services that can be disabled](#)

Version history

Version: 1.0

Published: August 10, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team