Cyberextortion by Denial-of-Service Attack

by Ron Lepofsky

Extortion has found a new breeding ground in cyberspace. According to the FBI, blackmailers are increasingly attacking corporate websites and networks, crippling their ability to operate and then demanding protection payments to restore service.

The reason why executives rarely read about cyberextortion is because most cases go unreported in order to keep the victim's name out of the public domain.

Such high-tech extortion is one of the least reported, yet most lucrative, forms of cybercrime. The FBI and Secret Service receive at least 20 new cases per month, with demands for funds sometimes reaching $1 million or more. It is not unreasonable to believe that the value of the demands will only increase as these cybercrimes continue.

However, some companies refuse to pay extortion demands and do go public. For instance, the Cyber Crime Research Centre reports that Authorize.Net went public about its attack after the Bellevue, Washington-based company had its Internet-based service disrupted by extortionists demanding payment. Authorize.Net issued a statement apologizing for the intermittent disruption in its service, spoke out about the extortion demands and is reported to have refused to pay the extortion demands.

How do the extortionists do it? In a typical attack, the perpetrator enlists the unwitting cooperation of thousands of "zombie" computers, which he or she gains control of (often by using viruses) for the purpose of mounting an overwhelming attack in unison. This is called a distributed denial-of-service (DDoS) attack. The network traffic from thousands of hacked computer systems located all over the Internet overwhelms a targeted network or computer, thereby preventing it from doing its normal work.

Since many DDoS attacks and cyberextortion demands are initiated from locations other than North America, particularly in jurisdictions that are logistically difficult with regard to cooperation, it is a daunting task for law enforcement to find and prosecute the offenders. Many times, DDoS attacks are transnational, requiring law enforcement coordination with foreign counterparts and introducing investigative delays. The bottom line is that executives need to take primary responsibility for handling their own cyberextortion preparedness.

The first step is to create a cyberextortion response policy. The policy may be as simple as agreeing to pay extortion demands and keeping silent about the incident. This is not recommended by the FBI or by other law enforcement agencies, however. Executives would be better served by creating a policy that may contain some or all of the following steps:

1. Create a clear policy including procedures to deal with an extortion incident and distribute it to the appropriate employees.

2. Prepare a list of appropriate law enforcement contacts to alert in the case of an extortion attempt.

3. Ensure their corporate network is tuned to minimize susceptibility to a DDoS attack. This includes steps to ensure your company's servers are not manipulated to participate in an attack on another party.

4. Create a written working framework with their ISP(s) of steps they will take to deal with attacks and with extortion threats.

5. Consider purchasing anti-DDoS services from service providers.

6. Create an IT policy for monitoring firewalls, IDS/IPS, servers and network traffic with the specific goal to identify attacks as early as possible.

7. Consider acquiring anti-DDoS technology for direct deployment into their networks to assist with early detection and with mitigation of an attack.

8. Consider deploying "sinking routing" which is a technical process of preventing DDoS attacks. This technique should be considered for use by both the ISP and the corporate network.

The purpose of the DDoS attack has mutated from fun to extortion. But specific steps can be taken by executives to mitigate the damage, including creating a cyberextortion response policy, implementing technical mitigation steps and closely liaising with law enforcement. Of course, these mitigation steps can be costly. But so is paying extortion demands. ■

Ron Lepofsky *is the president and CEO of ERE Information Security Auditors, an information security and security standards compliance auditing firm. ERE provides services to large publicly traded corporations, the financial industry, electrical utilities and large law firms.*