Extortion (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Computer data can be held for ransom or used in attempted blackmail. Consider the following examples of various pressures on data and system owners:

* In 1971, two reels of magnetic tape belonging to a branch of the Bank of America were stolen at Los Angeles International Airport. The thieves demanded money for their return. The owners ignored the threat of destruction because they had adequate backup copies.

* In 1973, a West German computer operator stole 22 tapes and received $200,000 for their return. The victim did not have adequate backups.

* In 1977, a programmer in the Rotterdam offices of Imperial Chemical Industries, Ltd. (ICI) stole all his employer's tapes, including backups. Luckily, ICI informed Interpol of the extortion attempt. As a result of the company's forthrightness, the thief and an accomplice were arrested in London by officers from Scotland Yard.

* In September 1999, the Sunday Times reported in an article by Jon Ungoed-Thomas and Maeve Sheehan that British banks were being attacked by criminal hackers attempting to extort money from them. The extortion demands were said to start in the millions and then run down into the hundreds of thousands of pounds. Mark Rasch is a former attorney for computer crime at the United States Department of Justice and later legal counsel for Global Integrity, the computer security company that recently spun off from SAIC. He said, "There have been a number of cases in the UK where hackers have threatened to shut down the trading floors in financial institutions. . . . The three I know of (in London) happened in the space of three months last year one after the other. . . . In one case, the trading floor was shut down and a ransom paid." The International Chamber of Commerce (ICC) confirmed it had received several reports of attempted extortion. Ungoed-Thomas and Sheehan quoted Pottengal Mukundan, ICC Director of Commercial Crime Services, as saying, "We have had cases of extortion and the matter has been investigated internally and the threat removed. . . . I don't think you will find there are many companies which admit to having a problem." Finally, the authors spoke with Edward Wilding, Director of Computer Forensics at Maxima Group; he said, "Computer extortion is not rife, but we do get called to assist in incidents where extortionists have attempted to extract money by the use of encryption and where databases of sensitive information have been stolen."

* Also in 1999, a 19-year-old Russian criminal hacker calling himself Maxus broke into the Web site of CD Universe and stole the credit-card information of 300,000 of the firm's customers. According to New York Times reporter John Markoff, the criminal threatened CD Universe: "Pay me $100,000 and I'll fix your bugs and forget about your shop forever....or I'll sell your cards [customer credit data] and tell about this incident in news." When the company refused, he posted 25,000 of the accounts on a Web site (Maxus Credit Card Pipeline) starting
1999-12-25 and hosted by the Lightrealm hosting service. That company took the site down on 2000-01-09 after being informed of the criminal activity. The criminal claimed that the site was so popular with credit-card thieves that he had to set up automatic limits of one stolen number per visitor per request. Investigation shows that the stolen card numbers were in fact being used fraudulently, and so 300,000 people had to be warned to change their card numbers.

* In a similar case in August 2000, the Creditcards.com Web site was penetrated and the attacker copied 55,000 credit card numbers. When the criminal's demands for $100,000 in extortion money were refused, he published the card numbers on a Web site.

* In March 2001, the FBI reported that they were targeting criminal hackers in Russia and the Ukraine who copied more than a million credit card numbers from 40 sites in 20 states. The hackers tried to blackmail the victims by threatening to embarrass them publicly.

***

I'll continue with some more tales of extortion techniques in the next article in this series and will also look at defenses.

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.