'Cyberblackmail' on the rise

May 9 2006

As illegal moneymaking schemes go, it's certainly not a new one: Crooks steal something of value from their victims and then demand ransom for its safe return. The 21st-century twist in the tale is that now it's not just loved ones and pets being kidnapped, it's also the contents of your hard drive. According to a new report, a new generation of online criminals is now blackmailing victims for the safe "return" of data that has been stolen and encrypted from their computers.

"Cyberblackmail" is becoming an increasingly common activity, say experts from the software-security industry who have been monitoring virus activity for the first quarter of 2006. In a report released by the Kaspersky Lab, "Malware Evolution: January to March 2006," they stated that this type of cyberblackmail is on the rise as criminals continue to take more aggressive tactics in the quest to turn a profit on illegal software and hacking activities.

In the scenarios described, victims' computers are infected and hacked -- computer viruses are installed on them allowing the criminals to hack into them, and stored personal information is stolen. The virus writers then encrypt this data or corrupt the system information before demanding a ransom for its safe return. The ransoms seen by the Moscow-based Kaspersky research team varied from an almost-reasonable $50 to a much more costly $2,500 demand.

This direct blackmailing of victims marks a shift beyond the silent stealth virus attacks that have become commonplace online. Coordinated attacks for black-market profit using malware -- malicious software such

as viruses, spyware and adware -- have become increasingly common over the past five years, infiltrating and damaging users' computers without their consent. The SoBig attacks on Microsoft computers in August 2003 and the MyDoom attacks in January 2004 are two examples of recent wide-scale devastating hits. Networked computers, especially those using common operating systems, are particularly vulnerable and if attacked can become "zombie networks," interacting with other attacked computers in the network using Internet Relay Chat.

Networks of bots have been offered for hire by hacking groups and can be used for wide-scale spamming, phishing for passwords and bank-account details, or purely to bring down a rival's Web site. While devastating, these previous attacks have until now also been comparatively surreptitious -- personal data has simply been quietly stolen for use on the black market with the only obvious signs of theft occurring when the unexpectedly large credit-card bill turns up.

The move to directly contact victims to demand money seems to be part of a larger trend in aggressiveness within the illegal malware communities that are no longer satisfied with the profits to be gained from passive infection of customers. Greed is driving the hard-line tactics that are being adopted to increase the effectiveness of other malware attacks to gain greater illegal revenue. Groups of virus writers are now increasingly banding together to form new groups and creating malware packages consisting of multiple programs. Although industry reports from 2005 showed an increase in the focused attacks on governments and financial institutions, gangs are also turning on each other and writing malicious programs to destroy software developed by rivals.

The current spate of cyberblackmail may be less of a problem than the blackmailers would have their victims believe. The Kaspersky researchers found that they and other software-security firms were able

to restore most victims' encrypted data to its original, usable format. But they warned that this is part of the ongoing race in software development between legal and illegal firms and that hackers are using progressively more sophisticated encryption systems that are more difficult to break. Criminals are also now focusing their sights on mobile tools such as PDAs with the use of crossover viruses such as Cxivr, which scans the operating systems of PCs and uses Microsoft ActiveSync to search for mobile devices. Targets of attacks are also shifting to government-owned banks, e-trading portals and the military.

Despite the advances in software and the widening target base, the advice for avoiding such attacks remains the same as it ever has: Avoid downloading files from untrusted sources such as unwarranted e-mails, run up-to-date anti-virus protection and make regular backups.