ARTICLE

Internet Corporate Blackmail: A Growing Problem

Professor MARK GRIFFITHS*

Over the last year, hackers (particularly from Eastern European crime syndicates) have been blackmailing online businesses in an attempt to extort money from them. Any company in e-commerce that allows acceptance of online payments via credit and debit cards are potential targets for hackers. The most common technique is the use of distributed denial of service (DDoS) attacks to force retailers and payment providers into protection rackets (Leyden, 2003a). Typical DDoS attacks deluge companies with requests for information that paralyse web sites for up to 24 hours or more. If they don't pay, they use DDoS to bring online sites to a standstill thus causing huge losses of revenue. The mechanism of the scam has been known for a number of years but the scale of its use has grown dramatically in the last 12 months or so. Unfortunately, law enforcement agencies do not have time to become involved in every DDoS service attack. They are also extremely difficult to anticipate. Most of them are nuisance attacks, and are not performed by organised criminals. However, if accompanied by blackmail threats, it is a clear indication that a criminal attack is in progress.

Nuisance attacks can be just as bad as extortion attempts for those in e-commerce. At the end of 2003, *WorldPay,*

• Psychology Division, Nottingham Trent University.

the Royal Bank of Scotland's online payments service, was subject to a three-day orchestrated and sustained DDoS attack by unidentified computer criminals (Leyden, 2003b). As a consequence, the online payment and administration systems were reduced to a trickle due to a flood of traffic directed at its Web-based systems. Although the systems worked safely and securely throughout the attack, the networks around them were systematically flooded with requests for the service on a massive computer-generated scale. The ability to process payments ended up being substantially slower and at lower volumes than normal as a result. What was worse for *WorldPay* was that during the attack, other businesses attempted to profit from *WorldPay's* misfortune. For instance, *Netbank* (among others) attempted to poach *WorldPay* customers by offering "emergency services" to allow "e-tailers" to continue to **trade** online (Ledyen, 2003b).

So how exactly do the criminals carry out DDoS attacks? IT experts say hackers most likely use a network of compromised hosts in educational institutions (Chaudhary and Wood, 2004). A network of infected PCs with Trojan horse infiltration tools can target spurious traffic to drown out legitimate business on any chosen site. (Tools like *Stacbeldraht* [German for "barbed wire"| and *TrinOO* have been commonly used). These methods have also been used in DDoS attacks against *Yahoo, Excite* and *eBay.* There appears to be little that companies can do up front to prevent DDoS attacks being launched against them. Avoiding attacks can be difficult because companies are bombarded from dozens (or even hundreds) of directions at once. Peering arrangements and clever network design can also minimize disruption but they are still notoriously difficult to defend against. However, the damage is dependent on how well prepared an organisation is to fend off assaults. When attacks occur, target organizations are advised by law enforcement agencies to contact their Internet Service Provider immediately to discuss potential configuration changes and mitigation techniques. The good news is that in many cases, a reasonable level of networking connectivity can be maintained.

More worrying than nuisance DDoS attacks are those criminals that use the threat of a DDoS attack to blackmail companies. In most instances, criminal hackers appear to be targeting high-volume, low-value transactional sites such as online bookmakers. The criminal hackers have been operating for almost two years from offshore locations such as Gibraltar and Antigua. Up until recently they were targeting sites mainly used by US gamblers betting on sporting events. However, more recently, they have turned their attention to British and Australian online based bookmakers. Typically, the hackers threaten to disrupt and paralyse bookmakers' web sites. Earlier this year, the police's National Hi-Tech Crime Unit (NHTCU) started to investigate six cases of British Internet bookmakers allegedly-being blackmailed by hackers threatening to disrupt online betting ahead of major sports events such as the Grand National, FA Cup final and the European Championship. Analysts estimate that the online betting market is worth over £3bn per year. For online bookmakers, several hours of downtime would be extremely expensive - especially if it coincided with an event such as the Grand National, which attracts more than £l00m in bets.

Sites are frequently blackmailed into paying between £20,000 and £30,000 a year in return for respite from further attacks. The police urge businesses to report such instances and not to give into the blackmail demands. However, £30,000 a year may be a relatively small amount compared to the potential losses so some organizations appear to be paying up. For instance, targeted bookmakers say the money the criminals ask for is about one hour's **worth** of business (Chaudhary and Wood, 2004).

The Irish bookmaker Paddy Power (one of the six Internet firms targeted) said "They're not really hackers, it's more like spammers - they keep logging on so that the site slows right down and no one else can get in. It's like putting 100 people in front of a betting shop to jam up the door" (Chaudhary and Wood, 2004). Typically, the online bookmakers were sent an e-mail saying that they had slowed the site down and that if the company paid them lots of money they would be left alone. Hackers know that DDoS attacks cost bookmakers hundreds of thousands of pounds in turnover because most gamblers are unable to place bets via the Internet because they cannot gain access to them. For instance, Paddy Power was targeted on the night of the US Super Bowl final and lost a lot of money as the system was paralysed for a few hours by a DDoS attack. Most bookmakers have now put measures in place with their Internet Service Providers to strengthen their defences.

Thankfully, in July 2004, the NHTCU, in a joint investigation with the Russian Federation, arrested three key members of the Russian gang involved in extortion. The success of the operation was built on the foundation of international partnerships between law enforcement and business. In Russia, the NHTCU worked closely over many months with the Investigation Department of the Investigative Committee attached to the Ministry of Internal Affairs (MVD) and the MVD's computer crimes specialist department (World Online Gambling Law Report, 2004). The cash was being transferred by a number of money transfer agencies who helped the NHTCU track the money and thereby identified members of the gang. However, the NHTCU have stressed that while bookmakers might be under the spotlight now, web-based extortion is a generic high-tech crime that has been a problem for some time. Therefore, it is clear that the problem of corporate blackmail is growing and that law enforcement agencies will have to work together on a global level if it is ever going to be beaten.

References

Chaudhary, V. and Wood, G. (2004) "Web bookies held to ransom." *The Guardian,* February 24, p.33.

I.eyden, J. (2003) East European gangs in online protection racket". *The Register.* Novemher 12, 2003. htrp://www.theregister.co.uk/2003/1 l/l 2/east_european_gangsJn_online/

I.eyden, J. (2003) "WorldPay recovers from massive attack." *The Register.* Novemher II, 2003. www.theregister.co.uk/2003/11/11 /worldpay_recovers_from_massive_a track/

World Online Gambling Law Report (2004) Global protection racket smashed in joint operation between UK's national hi-tech crime unit and Russian police. July 21, 2004. vvwvv.e-comlaw.com/vvoglr/index.asp.