



Blackmail by internet as gangs target sites

Criminals in online protection racket exploit hacking techniques to overwhelm and shut down businesses

By Chris Nuttall in London

Gangs based in eastern Europe are exploiting computer hacking techniques to launch waves of attacks on company networks, costing the victims millions in lost business and exposing them to blackmail.

They commandeer as many as hundreds of computers through hacking to use without their owners' knowledge. A command is then issued to each one simultaneously to make a series of bogus requests to the servers of the victim. The weight of traffic brings the servers to a halt and legitimate requests to carry out transactions cannot be completed.

The most recent cases of affected companies have surfaced in Britain where the National Hi-Tech Crime Unit (NHTCU) is investigating how one betting site was brought down and then received a threat that it would be attacked again unless tens of thousands of pounds were paid.

It is co-operating with international police forces, with the perpetrators thought to be based in eastern Europe.

Police and security companies say many victims are reluctant to report attacks for fear of any resulting negative publicity, but there is increasing evidence that the problem is growing.

Ian Morris, founder of Equip Technology, a systems security integrator, said: "We've dealt with six cases now and it's got to be multiples of that, and not just in the UK. It's obviously a world-wide problem.

"They seem to be targeting

high-volume low-value transactional sites."

As well as online gambling sites, web retailers and payment providers have also been hit.

One UK company was reported to be losing £1m (€1.45m) a day in lost business as its service remained down.

More than a dozen offshore gambling sites serving the US market were hit by the so-called distributed denial of service attacks and extortion demands in September and the tactic is now spreading.

Sites have been asked to pay up to \$50,000 (€43,500) to ensure they are free from attacks for a year. Police are urging any victims not to give in to blackmail and to report the crime.

Detective Superintendent Mick Deats, head of operations at the NHTCU said: "This is a protection racket. The message to these companies is 'You pay and we leave you alone'.

"If the demand comes in for \$40,000-50,000, compared to the losses they're suffering, there's an attraction for the companies to pay and hope it goes away. But there's nothing to say it will go away."

WorldPay, the online payments service owned by the Royal Bank of Scotland that serves 27,000 online retailers globally, admitted to suffering a DDoS attack last week. It said no customer data were compromised in the attack and people close to the company said there was no evidence of any blackmail threat.