



*The art of securing your business*

## Tackling a new wave of DDoS attacks

*With the recent spate of sophisticated high profile DDoS attacks the message is clear – no organisation can afford to be complacent.*

Over the past few months DDoS (Distributed Denial-of-Service) attacks have continued to gain media attention with a number of high profile organisation coming under attack, including MasterCard, PayPal, Oxford & Cambridge University and Kent Police Force.

Recently a London jury found Christopher Weatherhead, guilty of carrying out a campaign of DDoS attacks against major credit card companies. According to the Crown Prosecution Service, the cost of these campaigns on businesses amounted to more than £3.5 million in additional staffing, software, and loss of sales.

In a separate incident, HSBC were forced to release a statement following an attack that impacted a number of its global website.

*“HSBC servers came under a denial of service attack which affected a number of HSBC websites around the world. This denial of service attack did not affect any customer data, but did prevent customers using HSBC online services, including internet banking” (HSBC Statement, October 19, 2012).*

However, it is perhaps the recent wave of attacks that disrupted the operations of a number of major US banks, including JP Morgan Chase, Citigroup and the Bank of America, that provide us with the greatest insight into the increasing sophistication of DDoS attacks.

*“What we are seeing this year is just a tip in the ocean of what is planned for 2013”.*

– John Walker, member of ENISA and chair of ISACA's Security Advisory Group, in relation to rising DDoS attacks on the banking sector.

Whilst traditional DDoS attacks have relied upon a single attack method, in the recent wave of attacks on US banks, advanced techniques were deployed by the attackers to maximise their impact. In this instance, using an array of changing attack methods, the attackers continually recalibrated their attacks dependent upon the results achieved.

Additionally, rather than utilising a network of compromised PC's to perform the attack, in these cases a number of powerful Web servers were used to flood the targets. This enabled the attackers to hit their targets with an unprecedented volume of Internet traffic.

This trend of smarter, more sophisticated, attacks rely upon gathering intelligence on the technology and business logic of the environment under attack, analysis of critical weaknesses (in relation to the Web, Operating System and Database platforms in use) and creating the right conditions to perform a more accurate and focused attack.

Whilst it tends to be incidents effecting high-profile corporations that take the headlines, DDoS attacks are prevalent amongst businesses operating on-line and smaller organisations, typically with weaker defence capabilities.

Comsec has invested in researching and developing a new service to assist organisations prepare for sophisticated DDoS attacks and similar exploits, by conducting real-time attack simulations. Replicating in a controlled manner, the impact of a DDoS attack, assists an organisation in evaluating their readiness to defend and respond to a number of sophisticated attack scenarios.

*Adam Finkelstein, Comsec Consulting UK*

---

## About Comsec

For more than two-decades we have been working with leading organisations across the private and public sectors. Comsec's professional excellence, deep technical capabilities and unique access to cutting edge technologies has enabled us to assist a range of industry leaders overcome their security challenges.

We continually strive to maintain our position as thought leaders in the information security arena and stay abreast of the latest security threats and trends in relation to risk management, compliance, mobile computing, cyber-security and the drive towards cloud computing.

Comsec's professional excellence and deep technical capabilities has enabled us to work with a range of market leading companies and Government organisations. With specialist in application, infrastructure and cyber security, we aim to maintain our outstanding reputation in the UK market for delivering value and excellence to all our clients.