

The Perfect Storm: applying a layered defence to fight today's cybercriminals



Exceed Together

Security attackers have evolved from malicious hackers looking to make a reputation to sophisticated cybercriminals looking to make money from extortion. As cybercriminals become more sophisticated and targeted in their attacks, Terry Quigley, Head of

Financial Services at COLT argues that financial institutions should put in place a layered defence both within their own enterprise network and beyond the firewall in the wider telecommunications infrastructure on which they depend.

While network security attacks have rarely been out of the news in the past few years, the threat is evolving - and not for the better

In the past, these attacks have been restricted to commercial organisations - online gambling sites being the most reported category - but their range is spreading. An IBM report commented, "High-profile arrests of cybercriminals in the US and around the world pointed to individuals linked to organised crime and motivated to make money. We are seeing organised, committed, and tenacious profiteers enter this space." One very large financial institution has calculated that network downtimes costs \$30m an hour: even if that number seems hard to believe, lowering it by an order of magnitude provides a figure of \$3m an hour - still enough to give any Chief Executive a disturbed night.

Understanding the threat

So, what kind of threats do financial organisations face? In its Service Provider Infrastructure Security Survey Arbor Networks found that DDoS (Distributed Denial of Service) attacks and the DoS implications of worm attacks were considered by almost 80% of respondents to be the primary network threats. Under a DoS attack, hackers use a botnet (robot network) of compromised computers to overwhelm a company's Web site with traffic, making it inaccessible. Depending on the motive, this may result in customers not being able to access online banking or disruptions to inter-bank communications. The proliferation of PCs connected via 'always-on' broadband connections is enhancing the ability of compromised devices to function as part of a botnet.

If DDoS packets do reach critical systems, the access network or customer premises, it's too late to prevent harm. In this event, the only option is to "blackhole" the destination IP address of an attack until it can be brought under control. This means making the organisation's server unreachable by dropping

all traffic - malicious or mission-critical - sent to it. Either way, an attacker has effectively achieved its intended goal.

Cybercriminals are using this threat as part of an 'extortion racket' with money being demanded to prevent the launch of such an attack. Today, the combination of sophisticated cybercriminals and increased broadband penetration - creating a high bandwidth and always connected environment - is creating a 'perfect storm' of security threats for which organisations must prepare. We believe that any household brand with a reputation to protect, particularly those in the financial services sector, is now at risk.

A layered approach to security

Layered security is promoted by network security vendors as the best way of dealing with evolving security threats. The difference between this and traditional perimeter security may be compared to that between a mediaeval fortress and a modern airport. In the former, if formidable exterior walls designed to keep everyone out are penetrated, no additional defences in place. In the latter, certain areas permit free access, some permit limited access and a few permit only a small number of trusted individuals to enter. We, at COLT, would argue that financial organisations need to protect themselves against DDoS attacks with defences built in at various points within an organisation's overall network infrastructure - including that of its Network Service Provider.

The need to move defences up the network chain increases as the scale of a potential DDoS attack increases. Small attacks can easily be defended by DDoS mitigation appliances close to mission-critical systems. However, these can easily be overwhelmed and are not sufficiently robust to handle the kind of attacks we are seeing today. A further layer of security can be achieved by scaling network infrastructure to absorb a potential DDoS attack: to logically segment the network (i.e. by application) and provide a mitigation appliance



The Perfect Storm: applying a layered defence to fight today's cybercriminals



Exceed Together

on each segment. However, given the scale of the latest attacks (and the Arbor research found that there were few differences between the largest attacks ever addressed and the largest addressed in the past few months, indicating a worsening of the problem), even this is likely to provide insufficient protection.

As a result, organisations need to take a close look at the DDoS protection provided by their Network Service Provider (NSP). A DDoS protection solution located at the edge of the NSP's network means they are as close as possible to the source of an attack. This enables the NSP to filter traffic at the network edge, where attacks are most easily detected and stopped. Using this solution, network events are displayed to the NSP's operations and engineering staff. When incoming traffic exceeds the parameters that define "normal" traffic, an event is displayed in the NSP's regional network operations centre. Personnel then make the decision to activate protection for that customer and traffic triggering the event is diverted to the nearest security unit for cleaning.

Conclusion

The reality of network security today is that a determined individual, armed with the resources and skills of a large criminal organisation, can muster the capabilities to overwhelm even the most sophisticated defences. The best we can do is to make their lives harder - and the fact that thousands of DDoS attacks happen around the world on a weekly basis with the majority doing no serious damage indicates that we are making progress. However, as the potential scale of the attacks increases, the various parties involved in network defence, including the bank's security professionals and their network service provider, will have to work more closely together to provide a truly layered approach. Governments have found that co-operation is the only way to fight the war on crime in the physical world: financial sector organisations will find that fighting cybercrime in the digital world is no different.

