DDoS Case Study

International Bank strengthens its approach to cyber security following an extensive DDoS simulation conducted by Comsec's Cyber Defence Team.

The Challenge

"With massive botnets, willing accomplices and state players emerging on the scene, DDoS attacks now pose a greater risk and challenge than ever".

With DDoS attacks focusing on the financial sector reaching unprecedented levels over the past 12 months, this international bank recognised the need to act pre-emptively to uncover potential system flaws and design weaknesses that could be exploited to cause a DDoS attack.

Having persistently experienced attempted DDoS attacks the bank had already invested in ISP services and DDoS protection technologies to mitigate the impact of an attack.

However, against a backdrop of increasingly sophisticated and persistent attacks of over 100Gbit/s targeting both the infrastructure and application layer, the bank understood the need to be fully prepared to respond to a DDoS attack.

The Threat Vectors

Next Generation
New sophisticated botnets are capable of executing complex multi tired attacks against their targets.

Hacktivism
Hactivist groups, such as Anonymous exploit the combination of social media and the proliferation of ultra-fast broadband.

State Players
Some of the largest DDoS attacks against western targets have been initiated or sponsored by nation states.

Application Layer
Application layer attacks have sharply increased in popularity and now make up 25% of the total attack volume.

The Process

Extensive Research - The Comsec Cyber Defence team conducted extensive research over a two week period to gather intelligence on the banks perimeter, processes and network protocols. This process simulated the approach that would be adopted by a sophisticated attacker to gain behavioural insight into the bank's network and map transmission responses for each infrastructure component.

Formulation of custom attack scenarios - Utilising the information gathered during the initial phase, Comsec built a series of bespoke attack scenarios. The custom scripts developed to simulate the attack were unique to the bank and developed in-house by Comsec's Cyber Defence Team. The scenarios focused on exploiting four key attack vectors – CPU overload, flooding network traffic, overloading server system memory (RAM) and occupying system storage space.

The Team - Throughout the duration of the simulation, two distinct Comsec teams were in place. The Red (attack) team focused on executing the pre-defined attack scenarios, whilst the Blue team together with the bank's staff assessed the impact by closely monitoring traffic flows and server metrics (including memory, CPU and storage). The experience of an internal user, bank customer and the IT team were also tracked throughout the simulation which took place during an off-peak period to minimise the business impact.

The Simulation

Each of the scenarios were simulated utilising a network of over 10,000 botnets created by the Comsec's Cyber Defence Team from diverse geographical locations across several continents.

Storage - The information gathering phase identified a number of functions on the bank's website that make use of local or external storage. These functions, including the file upload mechanism, web server logs and Cache were targeted multiple times simultaneously resulting in a shutdown of the server and denial of service to customer wishing to access the bank's website.

CPU Overload - Application vulnerabilities were identified on the bank's website that cause heavy computation. In this scenario a custom script was developed to continually query the website database. This resulted in 100% utilisation of the CPU triggering the temperature of the targeted component to rise and the systems to re-boot or switch off.

Network Flooding - During the exercise the Comsec team simulated the impact on the bank of overloading the network bandwidth. This traditional attack was achieved using two methods. An ICMP attack was used to overload the network with multiple ping requests and a TCP Syn attack to exhaust all open connections. This was achieved by sending multiple Syn requests but delaying the Ack/Syc response to hog the server and cause a denial of service by preventing legitimate connections.

Memory (RAM) attack - This involved sending multiple data packets at a very slow rate. This caused the bank's servers to open a connection and allocate space for the data input. The slow delivery speed causes the server to hold memory for the multiple data causing the server to run out of memory. This caused the bank's servers to choke to a static state and shut down or re-boot.

The Impact

The DDoS simulation caused wide scale disruption to the bank's ability to operate and respond to the attack. Multiple servers were forced to re-boot or shutdown as a consequence of the simulation.

All customers logged on to the bank's website experienced session closure and were prevented from accessing their bank accounts. The simulation also caused network and infrastructure monitoring chaos, preventing the internal IT team from efficiently responding to the attack scenarios.

The Discovery

The DDoS simulation allowed the bank to replicate in a controlled environment the impact of a sophisticated persistent DDoS attack. In addition, the banks personnel learnt key lessons in crisis management enabling an improved response process to be established. Following the exercise the Comsec Cyber Defence Team built a detailed report to present the key findings and recommendations having analysed the impact of the successful attack scenarios.

The analysis concluded that alterations in the design and implementation of the bank's network and architecture can be made to successful defend against each of the attack scenarios .

Comsec's prioritised action plan enabled the bank to swiftly establish the high priority and quick win changes that would elevate the robustness of the bank's operations and prevent a future attack.

Why Are We Different

Proven Industry Knowledge - Our unique access to industry leaders and technologies enables us to provide services tailored to the sector's challenges.

Innovation Led Excellence - Capitalising on our leadership in one of the most IT and IS innovation led markets, our unique exposure to emerging technologies allows us to provide innovative solutions for tomorrow's challenges.

Product Independent - We are not tied into any technology or software vendor. All of our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

Centre of Excellence - We operate globally through offices across Europe with our main hub providing the technical expertise, allowing us to provide flexible service and unrivalled technical capabilities.

Our Commitment

Security as a Business Enabler

We believe that the role of information security is to enable business growth. At Comsec we are constantly looking for the synthesis of security into the business requirements. Our deep industry and business understanding enables us to tailor our services to facilitate specific business requirements.

Contact Us

Uri Bar-El
Director, Head of Professional Services
E: Uri@comsecglobal.com
T: 020 3846 8727
W: www.comsecconsulting.co.uk