MWR INFOSECURITY

Supported by CPNI Centre for the Protection of National Infrastructure

CASE STUDY:

Attack Type – Distributed Denial of Service

Scenario:

A successful distributed denial of service (DDoS) attack on any company is often evident not only to the business itself but also the broader public. Org 8, a payments company headquartered in the UK, became the victim of a successful DDoS attack on 18th December, one week prior to Christmas, traditionally the busiest online shopping period for the company. Online sales during this period typically generates Org 8 over 25 percent of its annual revenue.

Alerts that the payment processing servers and associated services were not responding began appearing on the company's monitoring services, and a large number of employees contacted the IT Service Desk. It was immediately apparent to the technical teams the systems were offline. There was delay in correctly identifying the outage was the result of a DDoS attack directly targeting Org 8, and as such, Org 8 were slow to implement the appropriate incident handling procedures. Org 8 had to call on several third party companies to help fully restore the affected services. In this instance, Org 8 was fortunate that the response time and effectiveness of those companies was very good.

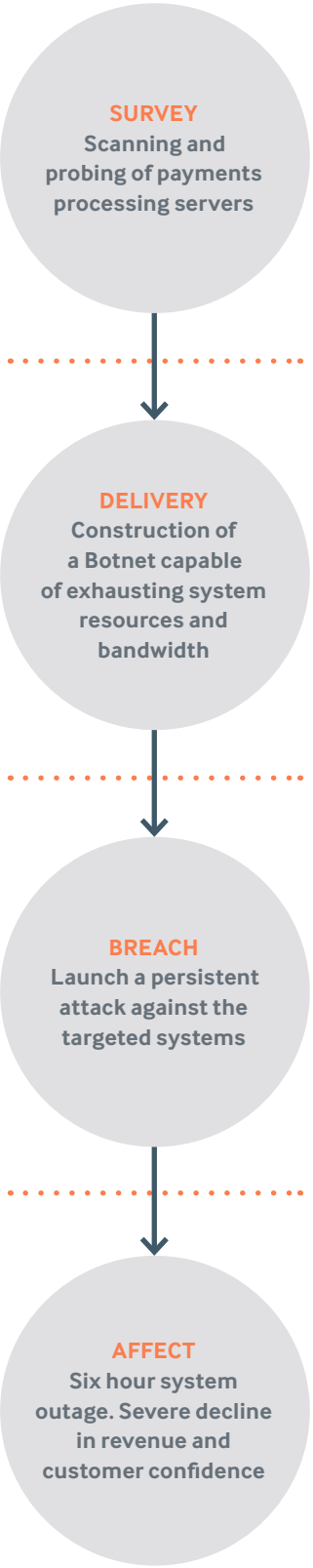
Both Org 8's primary and backup servers were overloaded with excessive malicious requests designed to exhaust all available resources to its essential business services. Org 8 engaged the assistance of their Internet Service Provider (ISP) to block the malicious traffic. Findings from the investigation into the attack, found that no specific DDoS filtering services were in place, and that the attackers had been probing the network for several weeks in a build up to the DDoS attack. The alerts generated by probing had not been raised internally by the Org 8 security operations team, who were busy responding to priority security incidents.

While some services were restored within six hours of the outage, users of Org 8's payment cards were frustrated by being unable to make purchases and in many instances turned to other payment methods to achieve their transactions. Org 8 found that it took many months for customers to return to regularly using their services and noted a minor drop in spending around the same time the following year. Org 8 was impacted by the loss of revenue from the initial DDoS attack and continued to suffer reputation and customer trust issues for some time following the incident.

Specific Failures Leading to Compromise

- Lack of DDoS protection for business critical systems

STAGES OF ATTACK



ATTACK TIMELINE

Targeting to Compromise:	2-3 weeks
Compromise to Exfiltration:	N/A
Compromise to Discovery:	Immediate
Compromise to Containment:	6 hours – 3 days
Method of Discovery:	Internal investigation following service outage
Threat Actor:	External – Believed to be targeted
Assets Compromised:	Payment processing services
Business Impact:	High – Direct loss of revenue and ongoing customer faith