Case Study:
Testing a DDoS Cloud Base Mitigation Service

THE THREAT

Organizations are making large investment in cyber defense, but are still in the dark in terms of how they would fare up against one of the simplest attacks that Cyber-criminals use to take down infrastructure and websites – the Distributed Denial of Service attack a.k.a. DDoS.

As botnets are a commodity, and can be rented for DDoS purposes by the hour (and inflict damage that even Fortune 100 companies are unable to deal with), such form of attacks has become a real threat.

"A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11…"

U.S. Defense Secretary Leon Panetta
Bloomberg News, October 12, 2012

For more information on any of our services please visit us at www.security-art.com or email info@security-art.com

Overview

Security Art is an internationally recognized cyber security company, specializing in providing advanced cyber security services to customers worldwide. Security Art was engaged to simulate a Distributed Denial of Service (DDoS) attack for a US-based financial institute, which provides full-service commercial, small business, and consumer banking services. This attack simulation was used to test the notification and customizable mitigation system provided on behalf of a third party. The test included numerous forms of DDoS attacks in increasing magnitude, offering the institute a glimpse at a real-world attack scenario, and enabling the institute to approximate the way with which a DDoS attack is identified and mitigated by the third party provider. In this case, the third party provider is one of the biggest players among providers of security services such as DDoS

The Challenge

The availability and reliability of a large financial institute is absolutely vital to ongoing operations, brand quality and consumer trust. Be it due to hacktivism or a politically motivated organization, DDoS is often a weapon of choice where brand damage is concerned, mostly because traffic-focused attacks only require a scalable set of traffic-generating resources, as opposed to leveraging security vulnerabilities.

Ensuring that the institute is resilient to such attacks is mission-critical. Part of ensuring such resilience is making sure that DDoS incidents are quickly identified and mitigated. It is, therefore, imperative to ensure that any solution implemented to alleviate the threat is viable, fully functioning and capable of both responding and reporting the incident in real time.

Security Art's DDoS mitigation testing involves triggering an event identical to a DDoS attack in a controlled manner. The purpose is to enable the target to test the quality of the mitigation service deployed and paid for, and to verify that the configurations and filters applied during mitigation reflect the client's needs. In this case, the client's need was accessibility to legitimate users at all costs.

When performing Security Art's DDoS mitigation testing, our team of security experts aims to:

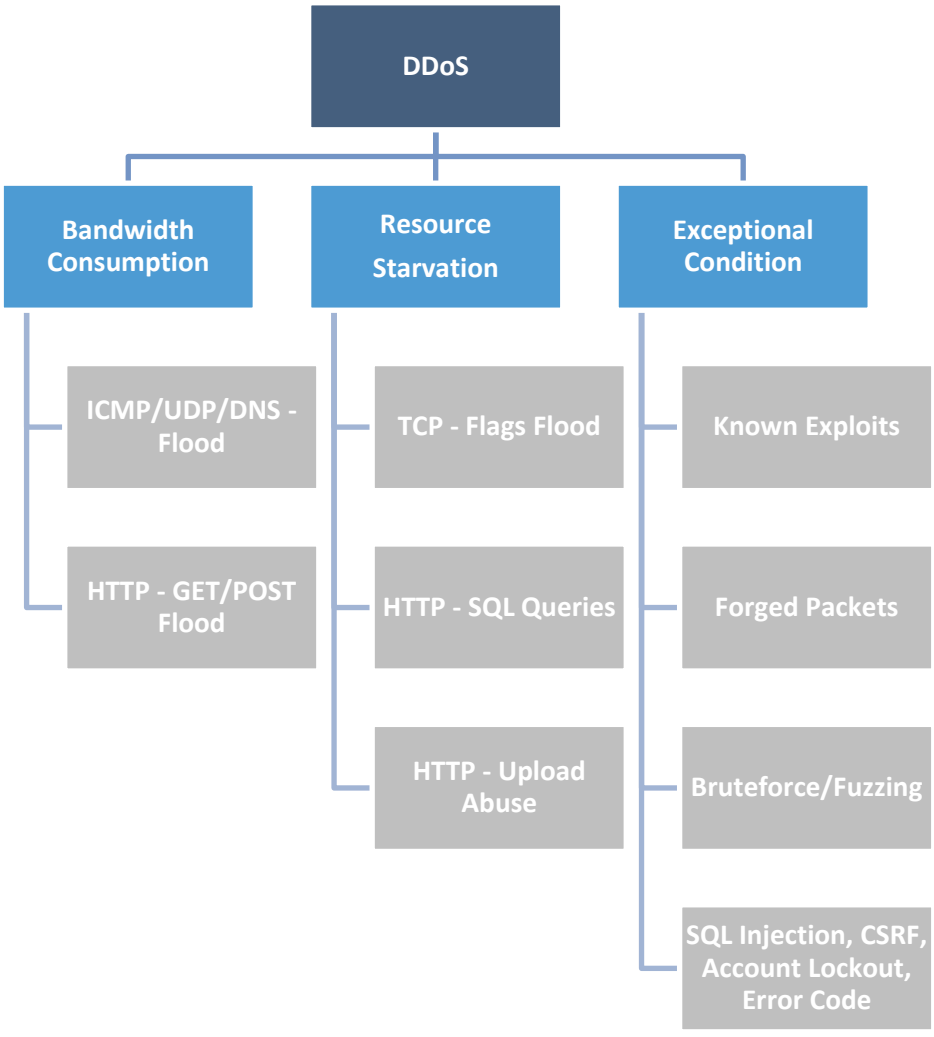
- Use various techniques of performing Distributed Denial of Service to engage the DDoS mitigation service provider, including:
  - ✓ Bandwidth consumption - With this technique, the attacker aims to deprive legitimate users of bandwidth, one of the most critical resources. Even if the attacker has no access to a large bandwidth, he can amplify his attack by a distributed approach in order to overwhelm the victim network.
  - ✓ Resource starvation – This technique focuses on consuming system resources such as CPU time, memory and space. By consuming these resources in an excessive manner, the attacker deprives legitimate system and user needs of those resources.
  - ✓ Exceptional condition – This advanced technique exploits design and programming flaws, resulting in failure of an application, operating system, or hardware device to handle certain exceptional conditions. By inducing such conditions, the attack may slow down or disable the affected system. Some of the well-known attack techniques in this category involve sending malformed network packets to cause system crashes.
- Use scalable resources to perform testing to:
  - ✓ Find the minimal threshold for third-party reporting.
  - ✓ Find the minimal threshold for third-party mitigation.
  - ✓ Produce granular results.
- Perform the attack from as many different locations as possible to prevent fingerprinting and mass blocking. (For the case described, Security Art used eight separate geo-locations throughout four continents, mimicking the behavior of a widely spread bot-net.)

"Izz ad-Din al-Qassam"

Since mid-September, the hacktivist group Izz ad-Din al-Qassam has taken credit for DDoS attacks launched against leading U.S. banks. So far, the group, in protest of a YouTube video deemed offensive to Muslims, has claimed attacks against PNC Financial Services Group, BB&T Corp., Fifth Third Bank, Bank of America, JPMorgan Chase, Citigroup, Wells Fargo, U.S. Bancorp, CapitalOne, HSBC, Ally Bank, SunTrust Banks, Regions Financial Corp. Zions Bancorp and, most recently, Amex.

or more information on any of our services please visit us at www.security-art.com or email info@security-art.com

- Test incident response over an attack timeline:
  - ✓ Relative to the commencement of a DDoS attack.
  - ✓ Relative to surpassing the minimal threshold to qualify as such an attack as deemed by the client or the service provider.
- Entrust the client with full command of the engagement, to ensure that no actual damage is done to live production environments. Testing is only performed live with the client and their response team. No action is taken without the client's approval.
- Reliably terminate the testing at any given time. Security Art places at top priority the ability to terminate any and all testing instantaneously, assuring availability throughout the testing process.



STATISTICS & INFO

Infrastructure attacks against Layers 3 and 4 of the OSI model -- the network and transport layers -- accounted for nearly 77 percent of the attacks during Q1. Layer 7 application attacks accounted for the remaining 23 percent.

High packet rates are more damaging than high bandwidth rates, as well as the number of gigabits per second being transmitted during attacks. That's because a large number of small packets per second that consume 100 Gbps of bandwidth, for example, are harder to deal with than a smaller number of large packets consuming 100 Gbps.

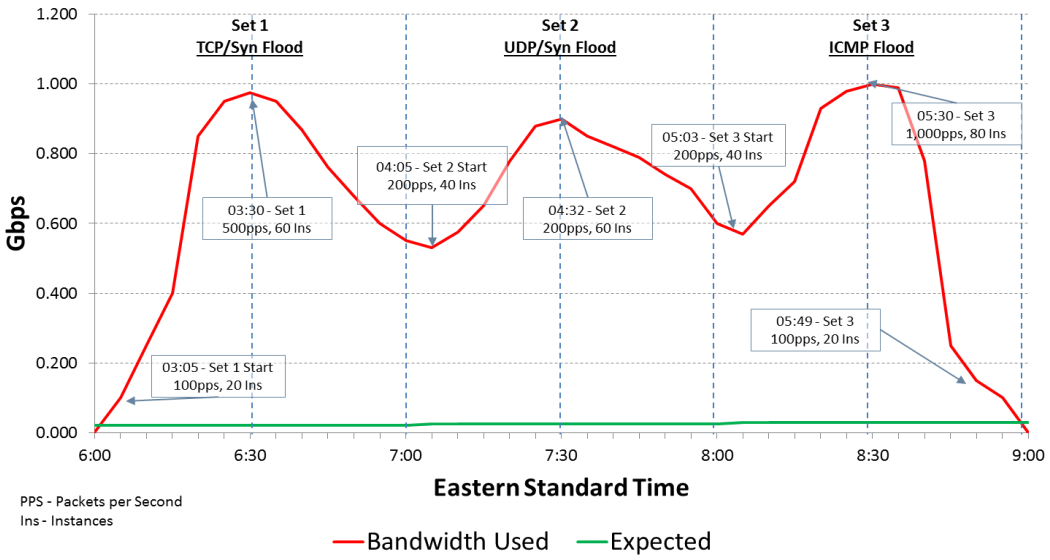
The most DDoS attacks came from China, but the U.S., Germany and Iran were also sources.

For more information on any of our services please visit us at www.security-art.com or email info@security-art.com

Analysis and Conclusions

The DDoS testing engagement was executed during the client's weekend and consisted of three sets of attacks. These attacks utilized a scalable number of automated agents ("instances") which performed the attack, and whose individual capability was also scalable with modifiable amounts of packets per second fired at the test target, peaking at around 1 Gigabyte per second per attack set.

Following is a diagram derived from data received from the client after testing:



During this event, a Denial of Service state occurred, as the filters applied to the client were too strict – this caused the detection of the attack to be mitigated by cutting off all external access, failing the mission-critical objective of availability. Security Art's attack was instantaneously called off, and soon enough the application was available again. Had this been a real-world scenario where attacks cannot be called off, such an event could have caused prolonged unavailability. This could have resulted in serious damage to the brand and to any business conducted during such an attack. By being proactive and testing their mitigation system, such an eventuality has been prevented without any actual risk. On the client's end, numerous alerts and notifications were generated, and mitigation soon followed. This assured the client that the third party DDoS mitigation provider did indeed deliver with their product in terms of SLA and availability, allowing the client to rest assured that the mechanisms currently in place are working to their satisfaction.

SECURITY ART' SELECTED SERVICES

Red Team Exercise

Preparedness to Cyber Attacks

Ethical Phishing Campaign

APT and Malware Insertion

DDoS Testing

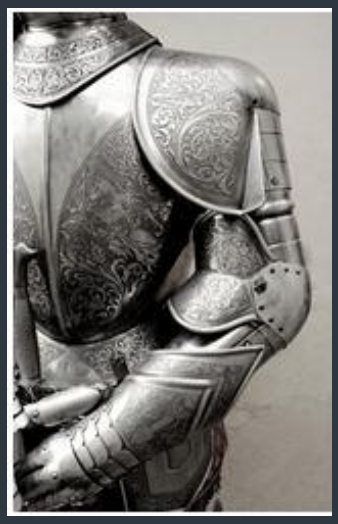
Penetration Testing

Cyber Risk Assessments

Digital Forensic Services

Secure Development Life Cycle

For more information on any of our services please visit us at www.security-art.com or email info@security-art.com



About Security Art

At Security Art we've demonstrated and concluded that an organization's security posture is derived from its stamina to withstand those threat actors that are relevant to its particular line of business. We focus on the attack vectors they typically employ in cyber-attacks and on security incidents pertaining to the organization's market vertical.

In order to assess a client's security posture, we employ "red team" type exercises, which are more comprehensive in nature and cover a variety of activities not typically included in standard security assessments.

Following is an example of the content of such a red team exercise:

- ✓ Collection of open source intelligence (OSINT) and digital footprint
- ✓ Social engineering
- ✓ Ethical spear phishing
- ✓ APT and malware insertion
- ✓ Testing of DDoS mitigation services
- ✓ Physical penetration testing for sensitive locations (HQ, DC, etc)
- ✓ Penetration testing for the infrastructure including VPN
- ✓ Penetration testing for Wi-FI networks, possibly including senior executives' residences
- ✓ Penetration testing and code review of applications, including mobile applications
- ✓ Penetration testing of mobile phones
- ✓ Quantification of the identified risk to monetary values and provision of meaningful deliverables to business executives

Each of the above listed services can be executed individually. In addition, we provide a variety of "blue team" type services, including, but not limited to:

- ✓ Forensic and incident response
- ✓ Threat modeling
- ✓ Quantitative risk analysis
- ✓ Applications and infrastructure design review
- ✓ Architecture and design of an application level DDoS mitigation mechanism
- ✓ Secure development life cycle
- ✓ Reverse engineering

For more information on any of our services please visit us at www.security-art.com or email info@security-art.com