DoS Cyber Attack on a Financial Institution in the U.S.A - April 2012
Pulling Large Resources

Table of Content

Preamble

This case summary describes one of the real life attacks experienced by Radware's customer and successfully mitigated thanks to Radware's DefensePro product and Radware's Emergency Response Team (ERT) expertise. The customer's name is undisclosed for privacy purposes and is referred to by "customer" in this report.

About Radware's DefensePro

Radware's award-winning DefensePro is a real-time network attack prevention device that protects the application infrastructure against network & application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft and other emerging network attacks. It combines a set of security modules which altogether provide a complete attack mitigation solution: Intrusion Prevention System (IPS), Network Behavioral Analysis (NBA), Denial-of-Service (DoS) Protection and Reputation Engine. The vast majority of the attacks are successfully mitigated and stopped by DefensePro alone.

About Radware's Emergency Response Team

Radware's Emergency Response Team (ERT) is a service, complementary to Radware's DefensePro, designed to provide 24x7 security services for customers facing a denial-of-service (DoS) attack or a malware outbreak. Often, these attacks require immediate assistance. The ERT provides instantaneous, expert security assistance in order to restore network and service operational status. IT is staffed by experts that have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience of the DefensePro family of products. In addition, the ERT takes information from each customer engagement and simulates the same scenario internally for further analysis and proactive implementation of defense techniques for other customers that may be facing a similar security threat.

Summary

Executive Summary

The customer, a major financial institution in the United States, was targeted with a multi-vulnerability DDoS attack by the Anonymous collective as part of a large attack campaign. This attack lasted for about nine hours.

On the same day, the customer notified ERT with the following information *"We have received credible information that an Anonymous kind of attack is being targeted on (our site) tomorrow";* the attack started three hours later than planned.

Attack Vectors

There were four confirmed attack vectors in this attack campaign:

Attack Vector Details

Attack Vector I: TCP SYN-FIN-RST Flood on TCP/80

Summary

A flood of non TCP-RFC compliant SYN-FIN-RST packets was targeting the environment.

Attack Measurements

73.3 Mbps

6.2 KPPS

Attack Description

This attack comprised of multiple SYN-FIN-RST packets targeting a specific IP address. All attack packets included similar characteristics:

- TTL 243
- TCP Source Port 3465 or 44444
- TCP Destination Port 80
- Packet payload length of 1400 bytes, constant 0xFF data

Some 52K Source IP addresses were identified, these are most certainly spoofed.

Time	Length	Source	SRC port	Destination	DST port	Protocol	Time to live	Info
8.239911	1458	[redacted]	3465	[redacted]	80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.240205	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.240623	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.240768	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.240950	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241012	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241124	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241136	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241408	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241632	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241722	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.241933	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242109	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242348	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242362	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242697	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242747	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400
8.242847	1458		3465		80	TCP	243	edm-mgr-cntrl > http [FIN, SYN, RST] Seq=0 Win=4000 Len=1400

Attack Impact

- Bandwidth consumption
- Resource consumption on RFC compliant elements

Attack Detection and Mitigation

This attack was initially detected and blocked by DefensePro Packet Anomaly 'Invalid TCP Flags' protection. Later, due to a human error, this protection was disabled and the attack impacted service. When enabled back, the attack was blocked.

Attack Vector II: Garbage Flood on UDP/53

Summary

Two high-rate UDP floods, targeting UDP/53 were detected and blocked by DefensePro.

Attack Measurements

First Attack

361 Mbps

32K PPS

Second Attack

417 Mbps

37K PPS

Attack Description

In this attack vector, attackers sent multiple garbage packets to UDP/53 targeting the customer's IP. Attack packets included similar characteristics:

- High UDP Source Port (30K-60K)
- UDP Destination Port 53
- Packet payload length of 1400 bytes, constant 0xAA data

Four attacking sources were identified which were probably spoofed.

Attack Impact

- Bandwidth saturation

Attack Mitigation

This attack vector was detected and blocked by DefensePro security protection BDoS (behavioral dos) using two different real time signatures.

Attack Vector III: Network Scans

Summary

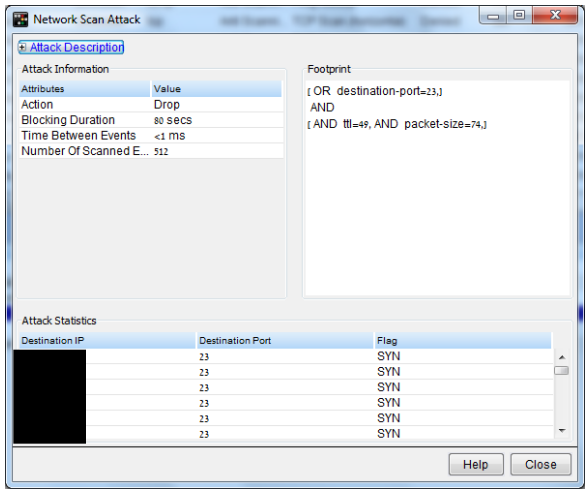
Dozens of network scans (including ICMP, TCP and UDP) were identified and blocked using Anti-Scanning protection.

Attack Description

The protected network was targeted with various reconnaissance scans, intended to identify target hosts and services. It should be noted that some of this activity might have been generated by legitimate sources.

Attack Mitigation

This attack vector was identified and blocked using DefensePro Anti-Scan protection Real time signature, for example- Footprint for one of the sources:



Attack Vector IV: HTTP Floods

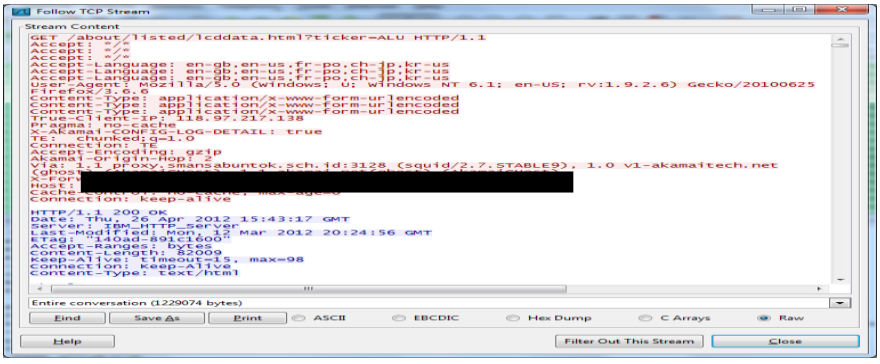
Summary

The customer environment was targeted with an HTTP Request flood which had several different variants. This attack vector was particularly significant as some of the pages on the customer's website were particularly "heavy" as they contained very large files – graphs, images – that were being loaded at each page request. The HTTP request flood was therefore highly effective with the attacker trying to pull those large files from the victim's website which caused high CPU use on the customer's servers. The attack traffic targeting the customer's server was directly s mitigated using DefensePro protection 302 Redirect Web Cookies. The one targeting the customer's server through Akamai was mitigated using ACL signatures.

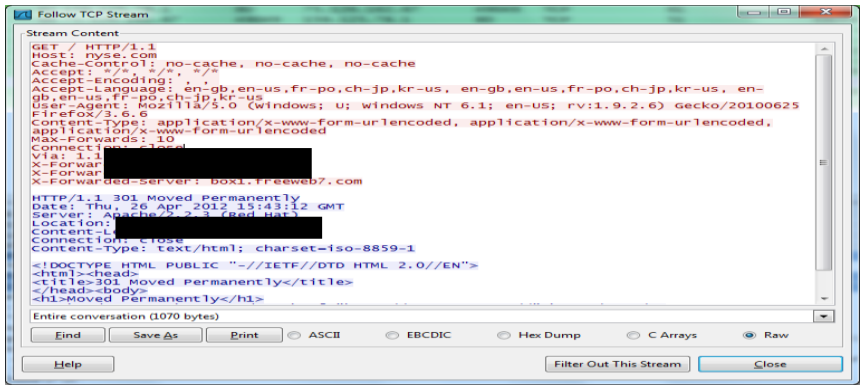
Attack Description

Though this is a single attack vector, multiple variants of HTTP packets were used. The packets contained multiple HTTP header values; one interesting attribute to note was akamai has been used by the attackers too.

You can see this in the following packet (Via Akamai):



Another HTTP packet (Not via Akamai):



Attack Mitigation

During the attack we used "Blacklists" and also "Web cookie challenges" (Javascript+302 redirect) in order to mitigate these vectors.