Denial of Service Attack (Sept 15/09 - Present)

Sat, Oct 3, 2009 at 5:05 AM

To: abuse@knology.net

ABUSE DEPARTMENT (AUP) / NETWORK OPERATIONS
KNOLOGY-NET (KNOLOGY HOLDINGS)
ASN 12083

To whom it may concern,

A user on your network has been executing a denial of service attack against various game servers including mine. The users current IP is 24.214.153.9

The attack started on the 15th of September 2009 and are still ongoing.

For the past three weeks he has been attacking ALL public servers in the game "Red Faction" (THQ/Volition).

I do not know how familiar with the game you are, or if you have even heard of it, so please bear with me while I explain a bit about how the online functionality in this game works so you can have a better understand of what has been happening here.

There are three entities that make online play possible for this game:

1) Master Tracker (The server all Game Servers[2] announce themselves too and make a list of these game servers available to the Clients[3])
2) Game Server (The servers that Clients[3] connect to when joining a match, The server coordinates the transactions between Clients[3], facilitating game play)
3) Clients (Pretty self explanatory, The players of the game.)

When a user goes to play online the client[3] queries the Master Tracker[1] to obtain the IP's and ports of all the Game Servers{2] and then queries all the Game Servers[2] to obtain the following information:

Server Name, Number of Players in Server, Maximum Number of Player Slots, Current Map / Level , The Mod running, The Game Type, Passworded?, and Version.

Once the client [3] has queried all the game servers [2] the client sends a join packet containing Player Name and Password. The server[2] then acknowledges the client[3] with Level and Map confirmation information. The client[3] then returns that information to the server[2] and the handshake is complete.

(I hope I have made this information as clear as possible. If you need any additional information do not hesitate to contact me.)

The flaw the attacker is exploiting is in the fundamental design of the game protocol.

The server[2] allocates a player slot and broadcasts to all other clients that the Player[3] has joined immediately after the first packet is received from the client.

The attacker has been querying the Master Tracker [1] for the list of Gamer Server[2] IP's and has been rapidly sending Forged Join packets (with a forged source port) to all the Servers[2], filling up the servers with Bogus clients and consuming the player slots which prevent legitimate Clients [3] from connecting to the server [2]. The bogus client eventually time-out which frees up a slot (which immediately gets filled again by the attacker). For players[3] already in the Server [2] it causes a large disturbance in game play because of the "Player has Joined" broadcasts. It also causes game play to be filled with high latency because of the processing demand on the server[2] because of the Bogus clients.

For an example of the above see: http://www.rolphklos.com/KnologyAbuse/ServerFlood1.png

The attacker started by flooding all servers with fake clients. Server operators responded by passwording their servers and putting the password in the server name, which prevented the forged packet from affecting their server (although

the forged packets still consumed bandwidth) while allowing legit players access to the server. This worked for about a week until the attacker started requesting the server names from all the servers and started adding the password that is present in the server name to the forged Join packets.

This has deeply hurt the community of players, and because the source IP's have been forged, tracking and blocking this attack has been difficult. At first I used a Layer 7 Filter on my firewall to drop the attackers packets, but he has recently randomized the pattern of his packets making filtering the attacker and not real clients impossible. I have noticed that all the packets are coming from a fairly small port range (UDP Source port 2000-4000) and thus has allowed me to block his attack temporarily using a firewall rule. But this comes with a consequence. Any user who plays with a source port set between 2000 and 4000 cannot see or connect to my server, potentially blocking 3.05% of legitimate clients.

Because of the way the Red Faction protocol is designed. The attacker would have to expose himself everytime he queries the servers for the server passwords. (If he forged the IP on the query packet, the response would never reach him. thus making his attack pointless)

To determine the source of the attacks I setup a modified server that changed its server password (both the Join password and the password displayed in the server name (both to the same value each time) in realtime to a random value every 300 seconds. I then used my protocol analyzer and started dumping traffic. I created a marker every time the password changed, giving me a 300 second window to narrow down the real attackers IP address. During the first test, 5 clients had queried the server for information after the password was changed, before the attacks started . On the second test only 2 people had queried the server before the attacks started. Only 1 IP address remained the same both times when the server was queried. (I will supply the packet dump files upon request)

To make sure I had somehow not made a mistake, I setup a trap to determine if the IP I had deduced was the real attacker.

I did this as follows.

I ran a public server with the name "pw=dogs AntiFlood DM" listening on UDP Port: 6655
I ran a second public server with the name "pw=cats AntiFlood CTF" listening on UDP Port: 6656

I then added a rule to my firewall to drop packets from Source IP: 24.214.153.0/24 destination UDP Port : 6655
I allowed 24.214.153.0/24 to connect to UDP Port : 6656

You can see the results of the experiment here: http://www.rolphklos.com/KnologyAbuse/RFHackerConfirmed.jpg
I also took a screenshot of the firewall rules and of the the Server Browser which showed which one of my servers were running on what port.

I had the server configured to reload the Map / Level every 20 minutes. (You can get an approximate time for how long the two servers were up from the "-Level Initializing-" markers on the server console.)

As you can see from the results of the test, the server which I had my firewall blocking traffic from 24.214.153.9 had no successful attack, because he was unable to query that one server to obtain the server password.

This user has assisted another hacker (originating netblock 121.72.0.0/14) in performing an attack against Red Faction during September 2008. The users IP address during that time was 24.236.95.239 (also within Knology's Netblock). I didn't bother sending Knology an abuse email back then because the attacks were small scale and I thought the user had turned over a new leaf and had learned from his mistakes, but he continues to abuse his Internet Connection causing major inconvenience and fiscal damages to server operators.

As per your Residential Terms of Service (http://www.knology.com/about/res.cfm) this user has violated:

1) *"Impersonation/Forgery: Adding, removing, or modifying identifying network header information (a.k.a. "spoofing") in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is especially frowned upon. Please note the use of anonymous re-mailers and nicknames does not constitute impersonation."*

The user has been forging his IP Headers with random source IP's for the malicious intent of hiding his identity and preventing interception of his attacks.

2) *"Network unfriendly activity: Any activities which adversely affect the ability of other people or systems to use Knology services or the Internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual user."*

The user has been maliciously filling servers with bogus clients for the soul intent of disrupting access to these servers by legitimate clients (aka DoS attack).

also mentioned under IRC but is still applicable in this case, the TOS states:

3) *"These Services may not be used to "flood" a chat room or to perform acts of "flooding" of chat services. Flooding is defined as the deliberate act of repeating text-generating actions in quick succession in order to prevent other service users from utilizing the chat service."*

The attacker flooded the server with forged chat packets during the first week of his attack. Please see:
http://www.rolphklos.com/KnologyAbuse/FloodChat.jpg

As per your Residential Terms of Service it also states:

"If a Knology account is used to violate the AUP, we reserve the right to terminate service without notice. Our preferred course of action would be to advise the account owner of the inappropriate behavior and corrective action necessary. However, flagrant violations of the AUP may result in immediate termination of service."

The user has Flagrantly violated your Terms of Service on multiple occasions, and I believe this user is 100% aware that his actions are illegal and therefore should be subject to the maximum punishment for his actions. I strongly urge Knology to permanently remove this user off the network in a timely fashion. I will be contacting the United States Federal Bureau of Investigation Cybercrime Division about this infraction on behalf of myself and 40 other Red Faction server operators.

In regards to your Investigation into this user I would like to note that the majority of Red Faction Game Servers [2] are still being attacked. The attacks sometimes stop for a couple hours at a time but always resume. As I stated above if you want my packet dump files please contact me, but if you were to monitor this user you would see large amounts of data with forged source IP's coming from this Host. The current pattern for this traffic is UDP Source Port 2000 to 4000.

I would also like to make a request to Knology's Network Operations. This user is able to perform this type of attack because your network allows any source IP to be routed by your routers. I would like to request that to prevent future attacks like this from occurring from your network, Knology should reconfigure their routers to drop packets that do not originate from Knology's Netblock before they reach the public Internet. 70% of the world's ISP's already have adopted this process and most modern ISP's in North America have done so already.

I hope I have provided all the required Information and would like to thank you for your patience and time dealing with this matter.

If you have any questions feel free to contact me anytime by email or phone.

Rolph Klos
IT Project Manager
W & K Computer Solutions
Winnipeg, Manitoba