# Distributed Denial of Service Active Termination Protocol

The UOS provides the functionality to actively react when a local system is infected and participates in a DDOS attack. This process requires a victim side to support this mechanism.

Figure 3. DDOS Active Termination Protocol

UOS

Warning!

Application #1 is suspected of malicious activity.

If you are not working with [site] using this app, consider blocking it.

Network Layer

DDOS ATP

Service

Outgoing Registration

App ID < - > Socket

Virtualization

and Isolation

Execution Supervisor

Attack

(Mass Requests Sending)

Block

Application #1 is suspected of malicious activity

If you are not working with [site] using this app consider to block it

Attacked Server

Set Isolation=Blocked

for App #1

The source is App #1

Who does send these requests?

Send App #1 executables to the Antimalware vendor for urgent analysis.

App #0

Virtualization

and Isolation

App #1

Virtualization

and Isolation

App #N

Suspicion (URL + Port)

In the case of a DDOS, the attacked server analyzes incoming traffic and sends a special signal (SUSPICION) back to each node that is sending too many requests. On the local side, the UOS stores application-to-destination mapping information and can use it to identify the suspicious application, warn the user about its malicious activity, and then block it if needed.

Once the UOS identifies an infected application, it then sends it to the MAs for urgent analysis. Anti-malware companies then identify malicious code signatures and add rejection records to the RDN database, or revoke approvals if they were issued previously.

With this technology, an attacked server has a weapon to not only to stop a DDOS attack but to shut down a whole botnet permanently.