# IT ARMY OF UKRAINE

https://t.me/itarmyofukraine2022
itarmyua@gmail.com

We get a lot of questions from people asking us "Why would we only attack a site for a few hours and then when it's down, stop the attack and move on to the next targets. Surely this cannot be effective." Yes, it can be.

Let me explain to you briefly what the consequences are for a business and then a little bit about the mess you have to clean up as a network administrator and a business in general after you've been hit with a DDoS.

There are many consequences if a website is attacked, or only brought down for a few hours. For example : an unreachable online platform; loss of confidential data; loss of productivity; for example an online portal; turnover decline, if it concerns a web shop; reputation damage of a brand. Yesterday the Russian train ticket system was brought down. Russian citizens were not able to buy a train ticket online. That is a serious pain, only if it is for a few hours. The Russian Stock Exchange not working for a few hours will cause serious economic damage. A bank does a considerable amount of its business everyday online. Think about if they can't be accessed for a few hours. That will hurt. Period.

And then there is the additional headache for your IT department:

**Reestablish Your BGP Connections** — Odds are that if you're hit with a Layer 3 or 4 DDoS attack, connections with your transit providers and peering partners will be dropped. The BGP protocol uses what are called keepalive messages to let a peering partner know that a route is still up. Every provider will configure differently, but to illustrate, by default these are sent every 60 seconds. Failing to send three in a row means that a route will be dropped by your providers and partners in only a minute and a half. You will be considered down and routes from you will be flushed. Again, exactly how long depends on your providers and their configurations, but that only highlights the uncertainty of how long it will take to recover.

Once the attack is over, you will need to announce your network again. Transit providers will likely accept your connection request right away (typically in a few minutes). Peering partners may take longer. Meaning that the peering connection that cost you the least will not be available. This will increase the overall cost of the DDoS attack as you will be on more expensive routes for the first hour or so after you are back up.

**Check/Restart Firewalls and Other Appliances** — As you bring network devices back online, another risk you run is that the sudden surge in pent up traffic will cause a flood — like a secondary attack — as those connections attempt to reestablish themselves. Bring up equipment in the wrong order and you could potentially be setting yourself up to come down again as the load will appear all at once. The only way to do it is to know your application and have a plan for an orderly restoration.

**Get Unblocked by Your ISP** — Many, if not all, ISPs will cut off and not offer connectivity to customers who are hit by DDoS and consume bandwidth needed by other customers. We sometimes call this the "noisy neighbor problem." The DDoS attack on your site is costing them business and what you pay them may not be worth it.

So, you may need to convince your provider to let you back on its network, and they may ask you to prove to them that it won't happen again. If you suffered a volumetric attack, you'll need to demonstrate some kind of DDoS attack mitigation. Otherwise, you'll be shopping for a new ISP, and negotiating a contract and reconfiguring an entire network will take several days at least.

**Application Recovery** — When your network is back online, your customers may try to connect all at once. They may have been trying to connect for the time you were down, and that pent up demand coming all at once could be a problem, potentially creating an application layer DDoS effect with thousands of sessions reconnecting.

To prevent this, you are expected to devise a strategy for gradually reconnecting customer sessions. There are several ways to do this, and it may depend on your business. You could, for example, intelligently route to different data centers based on IP address range or geography. Or, you could also simply meter the number of connections that can be established. Many companies don't have the expertise in house to gradually reconnect customers to avoid damage and they'll usually just flick the switch.

There may be other things to clean up too. If you use a cloud service like AWS, you may find yourself with a large bill to pay. This is because application layer DDoS attacks that use lots of CPU can trigger additional instances to be spun up. You may need to work with Amazon on settling your bill. It's possible you may need to clean up or purge your logs.

The hardest conversations to have are the ones with your customers. They have an expectation that you have this covered in your operating plan. Many companies haven't. When they find out that you haven't and now have a new expense, that could trigger a need to discount or offer credits to your customers to keep them.

In short, the calm after the storm may not be as restful as you hope. The cost of a DDoS attack often extends beyond the incident.

Sources :

IT army of Ukraine
**https://www.imperva.com/blog/recover-aftermath-ddos-attack/**