ccTLD Infrastructure: Surviving the attack

Dmitry Kohmanyuk :: Hostmaster.UA
ICANN 73 :: Virtual 2022-03-07

DDOS Attack

2022-02-15

Impact

1. DNS Service for UA TLD and GOV.UA domains server
2. Took out one of our anycast nodes…
3. …That was also zone transfer server
4. Impact: none of other UA zones did update
5. Lesson learned: separate public and private
6. Used Signal chat already established for ops team
7. Anycast fortunately remained available, mostly

Post-Impact

1. Deployed partner anycast service at night…
2. …which was configured incorrectly…
3. …which was fixed after I contacted CEO on messenger
4. Lesson learned: know your CEO’s direct contact
5. Press release about the attack
6. Created post-mortem write up, entire team participated
7. Created spare transfer server on unused host we had

Military Attack

2022-02-24

Events

1. 04:00 (just like Hitler in 1941) Kyiv bombings started
2. I was awake at 06:00, accidentally
3. First reaction was denial and panic
4. Next was to call everyone in my team
5. I assessed the situation and created “to save” list
6. For major services, I had allocated a backup location
7. Signal team chat was used to communicate

Priorities

Priorities

1. PEOPLE
2. DATA
3. SERVICES
4. MONEY

Components

Components

1. PEOPLE
2. EPP service, back end database
3. DNSSEC Signing and key management, zone generation
4. DNS Service for TLD and our own domains
5. WHOIS (and RDAP) services
6. Websites for public, registrars, government
7. Email, chat, phone*, for support

Components, continued

8. Datacenter space, internet, networking hardware

9. DDOS Protection Services **

10. Cloud computing ***

11. Business back office (accounting)

12. PEOPLE

Decisions

Outsource or not?

1. Hardware, datacenter: YES and YES
2. DNS secondary service: partially – we got several
3. EPP and WHOIS: NO
4. Our business and financial operations - NO
5. Virtual servers - SURE but it is tricky
6. Your registry database - NO
7. Your DNSSEC signing - NO
8. Your email – YES (Google Workspace)

Costs

Costs

1. We already had bare metal hosting company, abroad
2. I reached out to 42* people, known already or not
3. I got free help, but I kept track of estimated costs
4. People were more valuable than computers
5. Time was more valuable than money
6. Smaller companies generally react faster

Gratitude

Gratitude

1. My fellow colleagues
2. Our hardware and services suppliers, acting quickly
3. Supporting members of ccNSO and TLD community
4. IANA staff, for updating UA NS on Sunday
5. CENTR, for terminating .RU membership
6. RIPE community, except to those “let us be neutral”
7. DNS-OARC staff

Questions?

Dmitry Kohmanyuk

<dk@cctld.ua>

Running TLD since 1992

(Resisting Russian government military attacks since 2014)

2022-03-07