UA ccTLD Infrastructure: Resilient to the War, with help from CZ.NIC

Dmitry Kohmanyuk :: Hostmaster.UA
CSNOG Meeting :: Brno 2022:06:21

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 (like 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. Development infrastructure (Git)
10. DDOS Protection Services **
11. Cloud services ***
12. Business back office (accounting, ticketing system)
13. BACKUPS

Decisions

Outsource or not?

1. Hardware, datacenter: YES and YES
2. DNS secondary service: YES – we got several
3. Registry, EPP and WHOIS: NO
4. Our business and financial operations - NO
5. Virtual servers - prefer our own virtualization
6. DNS primary and DNSSEC signing - NO
7. Calendars, documents, email – YES (Google Workspace)

Lessons

Lessons

1. Must have: server hosting company, multiple locations
2. Reach out to lots of people, select few to work with
3. Even with free help, keep track of estimated costs
4. People are more valuable than computers
5. Time is more valuable than money
6. Smaller companies usually react faster
7. Those that knew us already, were more helpful

CZ.NIC

CZ.NIC

1. contacted CZNIC immediately
2. received assurance of help
3. first servers configured within 72 hours
4. Migration of infrastructure in stages
5. communication: signal chat/calls, Google docs, email
6. DNS cluster designed, and re-designed again
7. Partner project (Secondary.net.UA) included
8. Pure IPv6 uplink to DNS node; dual FRR, VRRP

Gratitude

Acknowledgements

1. 6connect, Anycast DNS: CloudNS, CDNS (*), Cloudflare, Gransy, Netnod, Packet Clearing House, RcodeZero
2. CZNIC for hosting our core infrastructure and DNS
3. Our colocation partners in Ukraine and abroad (**)
4. IANA staff, for updating .UA NS on Sunday
5. CENTR board, for suspending .RU membership (***)
6. Netnod, CENTR, CSNOG for inviting to their meetings

Gratitude

1. My fellow colleagues, all of you
2. Our hardware and services suppliers, acting quickly
3. Staff, management, and members of CZ.NIC z.s.p.o.
4. MFA of Sweden: ***Utrikesdepartementet***
5. Global NOG Alliance for helping ISPs in Ukraine
6. 6connect staff for deployment of custom anycast cloud
7. Many members of ccTLD and RIPE communities
8. Ukrainian armed forces (MIL.UA)

Questions?

Dmitry Kohmanyuk <dk@cctld.ua>

Hostmaster.UA

Running UA ccTLD since 1992

Under Russian state military attacks since 2014

2022-06-20