DNS Servers in Turkey Under Attack

Attack Background

Since Monday December 14, Turkey's DNS servers, ns1.nic.tr –ns5.nic.tr, have been the targets of a persistent denial of service attack. It appears that this attack was a 40Gbps DNS amplification attack that saw peaks upwards of 200Gbps. As a result, all traffic to Turkey was cut off in an attempt to mitigate the attack, leaving more than 400,000 websites offline and DNS servers unable to respond to queries. As of December 20 the DNS servers were still being targeted. Anonymous claimed responsibility for the attack.

Motivation Behind the Attacks

Recently Anonymous took credit for this attack under the campaign OpISIS *(see figure 1).* They have stated that they are targeting Turkey due to Erdogan's (the current president of Turkey) support of ISIS (*see figure 2*).

Figure 1 – Anonymous claiming responsibility for the attack via its Twitter account

Dear government of Turkey,

If you don't stop supporting ISIS, we will continue attacking your internet, your ROOT DNS, your banks and take your government sites down.

After the root dns we will start to hit your airports, military assets and private state connections. We will destroy your critical banking infrastructure

Stop this insanity now Turkey. Your fate is in your own hands.

-Anonymous

Figure 2 – Quote from Anonymous, as transcribed on the **announcement video**

Attack Targets

Three weeks ago a paste was found on kl1p.com that outlined several Turkish targets under the operation, OpTurkiye. This operation had a target list of Turkish entities that include government, DNS servers, universities, banks, etc.

The following is a list of Turkish Government DNS servers that are targets for the attack:

ns1.nic.tr	144.122.95.51
ns2.nic.tr	144.122.95.52
ns3.nic.tr	213.248.162.131
ns4.nic.tr	193.140.100.200
ns5.nic.tr	178.251.42.18

The following is an additional list of Turkish entities that are targets for the attack:

www.basbakanlik.gov.tr
www.bimer.gov.tr
www.dernekler.gov.tr
www.ubak.gov.tr
www.tbmm.gov.tr
global.tbmm.gov.tr
www.tccb.gov.tr
www.meb.gov.tr
www.treasury.gov.tr
www.ankara.gov.tr
www.istanbul.gov.tr
www.egm.gov.tr
dns.egm.gov.tr
dns1.egm.gov.tr
dnsb.egm.gov.tr
dnsa.egm.gov.tr
www.pa.edu.tr
www.ankara.pol.tr
www.iem.gov.tr
www.ipa.org.tr
www.polsan.com.tr
www.etik.gov.tr
www.ibb.gov.tr
www.mfa.gov.tr
www.iem.gov.tr
www.tsk.tr
www.kkk.tsk.tr
www.dzkk.tsk.trwww.hvkk.tsk.tr
www.jandarma.tsk.tr
www.sgk.tsk.tr
www.harpak.edu.tr
www.akbank.com
www.hsbc.com.tr
www.ziraat.com.tr
www.garanti.com.tr
www.bankasya.com.tr

www.turkiyefinans.com.tr
www.citibank.com.tr
www.isbank.com.tr
www.yapikredi.com.tr
www.halkbank.com.tr
www.fonbank.com.tr
www.adabank.com.tr
www.anadolubank.com.tr
www.fibabanka.com.tr
www.sekerbank.com.tr
www.tekstilbank.com.tr
www.turkishbank.com
www.teb.com.tr
www.ykb.com.tr

How to Prepare

While it is impossible to predict the next target of an ideological group such as Anonymous, expect to see more activity and potential attack campaigns targeting DNS servers. In addition, organizations involved in supporting, hosting or delivering IT services should proactively prepare networks and have an emergency plan in place for such an incident.

Organizations under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe.
- A hybrid solution that includes on premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitoring security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.