radware

Smart Network. Smart Business.


## Threat Alert

# Ukraine-Russia Global Conflict

Emergency Response Team

May 5, 2014

## EXECUTIVE SUMMARY

The current conflict between Ukraine and Russia following the Ukrainian revolution, the Crimean peninsula crisis, and the recent fighting in Slovyansk and Odessa, has the potential of military and political escalation. This conflict takes a global form following the involvement of the USA, Europe, NATO and other actors.

This Threat Alert calls for multiple countries and organizations to be prepared for cyber-attacks and possibly even cyber-war as a direct result of this global conflict. The reason is simple: cyber-attacks nowadays accompany physical and political conflicts. This is especially true for conflicts in this geographical arena.

The countries and organizations in the ring-of-fire are Ukraine, Russia, USA, European countries (especially England, Germany, and France), and NATO organizations. The verticals in the ring-of-fire are all government agencies, the financial sector, utilities and infrastructure, news sites, and e-commerce sites.

Based on past experience, these attacks may include DDoS attacks, site defacements, intrusion and data theft attempts, and possibly even attacks on critical infrastructure. It is most likely that the attack campaigns will include multiple attack vectors. The attack may be carried by hacktivists or by more professional organizations with government or political associations.

Radware ERT has handled DDoS attacks in Ukraine in the last few days, and although there is no evidence whatsoever to tie them to the conflict, we nevertheless are informing you that the attack vectors seen were volumetric UDP floods: both DNS and NTP reflected floods causing pipe saturation.

This Threat Alert will be updated pending further developments.

## COUNTRIES AND ENTITIES UNDER THREAT

The countries and organization involved directly or indirectly in this conflict are the most likely to experience cyber-attacks, including:

- Ukraine
- Russia
- USA
- European countries (mostly England, Germany, and France)
- NATO

The verticals that are more likely to be targeted are:

- All types of government agencies
- Financial organizations
- Utilities and national infrastructures
- News sites
- E-commerce sites, especially leading ones

## ATTACK VECTORS

The list of possible attack vectors is rather large, and includes the following:

- DDoS attacks. including volumetric, application, and low-and-slow. May be used to directly cause outages or to smoke-stream other attack vectors.
- Web site defacement
- Intrusion and data-thefts attempts
- Attempts to impact critical infrastructure
- Revelation of private data stolen during the attack or prior the attack
- Brute force attacks
- All types of network and application scans

Nevertheless, the most trustworthy prediction is that the attack campaigns will include multiple attack vectors.

## GENERAL RECOMMENDATION

1. Organizations in the scope of the threat should increase their readiness level.
2. They should further follow Radware and other media channels to learn if such attacks have started, and if so, continue to increase the threat level and possibly harden security systems.
3. Under-attack organizations must focus not only on the obvious attack vectors, but also seek hidden ones.

## EXPERIENCED ATTACKS

Radware ERT has not handled any attack that can be associated to the conflict, however the following attack vectors have been identified in Ukraine in the last few days:

- Volumetric DNS Reflected Flood causing pipe saturation
- Volumetric NTP Reflected Flood causing pipe saturation

## INSTRUCTION FOR RADWARE CUSTOMERS

1. Radware customer are encouraged to review their security configuration and software version and if needed conduct modification to proof their systems. For any support in this process contact Radware Support.
2. Radware customers who are under attack should immediately contact the ERT (Emergency Response Team).