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 crisis in the Crimean peninsula, and 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 United States, Europe, as well as other NATO countries.

This Threat Alert calls for multiple countries and organizations to be prepared for possible cyber-attacks or a potential cyber-war as a direct result of this global conflict. The reason is simple: cyber-attacks in this day and age, usually trail physical and political conflicts. This is especially true for 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. Those frequently targeted are all government agencies, the financial sector, utilities and infrastructure, news sites, and e-commerce sites.

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

The past several days, Radware's ERT has been mitigating DDoS attacks in Ukraine. ERT cannot confirm that the attacks handled were a direct result of 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 cyber attacks in this region.

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 that include volumetric, application, and low-and-slow. May be used to directly cause outages or to smokescreen 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 to the attack
- Brute force attacks
- All types of network and application scans

The most trustworthy prediction is that attack campaigns will include more than one attack vector.

GENERAL RECOMMENDATION

1. Organizations who fall within the scope of the threat should increase their readiness level.
2. They should follow Radware as well as media channels to learn if any attacks have started, and if so, continue to increase the threat level and possibly harden security systems.
3. Organizations that are under attack must focus not only on obvious attack vectors, but also seek out those that are less known.

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 customers are encouraged to review their security configuration, software version, and if any system modifications are needed. For further support, contact Radware Support (contact methods).
2. Radware customers who are under attack should immediately contact the ERT (Emergency Response Team). To invoke the ERT contact Radware support (contact methods, please call by phone and not by email or form)