ISIS Cyber Attacks

ERT Threat Alert

April 2015

Islamic State in Iraq and Syria (ISIS), an Al-Qaeda splinter group, is infamous for its malicious, physical attacks. Recently, however, ISIS has also been credited with cyber-attacks. As a result, organizations such as Anonymous have started to counter-attack ISIS sites.

The most widely known attack occurred on French TV5Monde, a global television network (similar to CNN or MTV) that broadcasts several channels in French. At 10:00pm CET on April 8th, the network station experienced an attack that caused a three hour downtime to eleven networks.. In addition the attackers gained control of the networks' social media sites and suspended its email system.

Although the attack on TV5Monde is considered the most notable, it is definitely not the only one. In January ISIS supporters seized control over several social media accounts of U.S. Central Command and numerous French sites were hit with DDoS attacks. In April the biography page of Huffington Post blogger was also defaced.

These assaults were followed by several attacks against ISIS, mostly by branches of the Anonymous group. This started an online debate as CloudFlare ─ a US-based company that provides a content delivery network and distributed domain name server systems ─ was evidently protecting ISIS sites and stated it had no plans to stop. As a result, many argued that CloudFlare should not be able to maintain freedom of speech for an organization like ISIS.

Although there is no explicit security threat alert, the ISIS activity and Anonymous responses makes it hard to predict what the next target will be. It is however evident that ISIS supporters are capable of launching different types of attack vectors: DDoS, intrusion and defacement activities, and therefore Radware's Emergency Response Team (ERT) recommends an integrated security solution to protect against a wide variety of attack vectors.

Attacks by ISIS and Against ISIS

The following is a list of attacks performed by or against ISIS. It is important to note that attacks attributed to ISIS are not necessarily done by its members, but rather assigned to them by different groups.

Activity	**French TV5Monde Channel**
Date	April 8th , 2015
Impact	• Eleven TV networks experienced downtime for 3 hours • Attackers gained control of networks' social media sites • Negative impact on email system • Network disruptions the following day

Activity	**Various French Websites**
Date	Between January 3rd and January 18th , 2015
Impact	• 19,000 sites were attacked in 16 days • Consisted of primarily DDoS attacks

Activity	**Anonymous Published Personal Details of ISIS Activists**
Date	February 21st , 2015
Impact	• Anonymous published a hacked ISIS database containing 2,000 personal records of alleged ISIS members.

Activity	**Anonymous Attacks ISIS Related Websites**

Date	January 2015
Impact	• Number of ISIS related sites were taken down

Activity	**Pro-Islamic State Hacking Groups Attacked Russian Websites**
Date	March 25th, 2014
Impact	• 600 Russian websites were attacked • Website of banks, construction companies, government organizations, schools and a local history museum were damaged

Activity	**Hacker Group Associated with ISIS Seized Control on Twitter and YouTube Accounts of U.S. Central Command**
Date	January 12th , 2015
Impact	• Hacked accounts were used for ISIS propaganda

Activity	**Hacker Group Associated with ISIS Attacked PlayStation and Xbox Websites**
Date	August 26th , 2014
Impact	• Sony PlayStation and Xbox Live networks hit by DDoS attacks

Activity	**Hacker Group Associated with ISIS Hacks Huffington Post Blogger**
Date	April 12th , 2015
Impact	• Defaced biography of a Huffington Post blogger

Recommendation

Radware's ERT is monitoring these events, and will update on this threat alert as needed. There is no specific recommendation at this point; however, we recommend organizations review the following checklist in preparation:

- ✓ Protect against application based attacks including intrusion attempts, brute force, and application level DDoS
- ✓ Protect against network based attacks including DDoS and scans
- ✓ Cloud/ISP based protection to ensure Internet pipe is not saturated by a volumetric DDoS attack
- ✓ Availability of a cyber-emergency response team available to instantly handle cyber attacks
- ✓ Monitor systems to quickly identity suspicious activity and provide a clear view of all on-going attack vectors

ERT also emphasizes that DDoS is often used to conceal intrusion attempts (both as a smoke stream and to impact security devices that fail-open under DDoS) and therefore it is important to confine DDoS to prevent intrusion background attempts.

Radware Customer

If your organization is under attack, contact Radware ERT immediately.