Abstract

The online editions of Sweden's media elite were knocked offline for several hours on March 19th. Hackers were able to cripple the media organizations with volumetric DDoS attacks, resulting in 3 hours of downtime for several media outlets, including Dagens Nyheter, Svenska Dagbladet, Expressen, Aftonbladet, and others.

The attack traffic originated from a computer network in Russia, though these machines could have possibly been hijacked. Since the beginning of 2016, improvements to DDoS attack tools have made them more powerful and allowed perpetrators to generate high volumes of traffic, challenging the most sophisticated network protection solutions (see Figure 1).

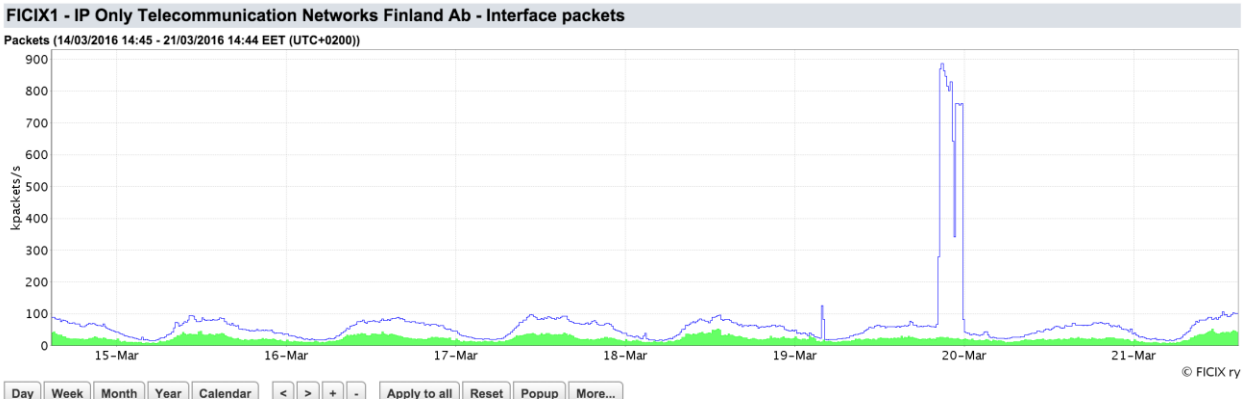

Figure 1: Traffic map from attack[i]

Background

On Saturday March 19th, an unknown source launched a series of coordinated denial of service attacks against a number of Swedish newspapers. Early reports suggested that Russia was behind the attack following a Swedish announcement on having to adopt a military strategy considering Russia's alleged "aggression."[1]

An attacker on twitter going by the name J, @_notJ, claimed responsibility for the attacks, citing that Swedish newspapers are spreading false propaganda (see Figure 2).

Figure 2: @_notJ claims to be behind the attacks in Sweden

[1] http://www.defensenews.com/story/defense/international/europe/2016/03/17/sweden-defense-military-strategy-doctrine/81908664/

Sweden's Minister of Interior stated that the police have launched an investigation[ii] and that the government is following the situation closely (see Figure 3). This evidence is based off of public network statistics found on Netnod[iii]. Forty-eight hours later, the account of J @_notJ was suspended, most likely by authorities.

Figure 3: Anders Ygeman, Interior Minister, addresses the attacks

Reasons for Concern

Numerous, high-profile media outlets around the world (including CBS.com) have faced denial of service attacks that caused network outages and website downtime, resulting in reputational and financial losses due to consumers turning to other outlets to receive their news.

Attacks that target news and media sites can range from nation state attackers attempting to silence media outlets to hackers testing and demonstrating the power of their stresser services. On March 18th the New World Hackers conducted a test of their stresser service that resulted in an hour long outage for CBS.com (see Figure 4). This group has also targeted the BBC with an alleged 602Gbps attack that crippled their network and affected many of BBC's services.

Figure 4: New World Hackers take CBS offline on March 18th and 20th

Targeted Sites (Confirmed)

- SvD.se
- Aftonbladet.se
- Expressen.se
- DN.se
- GP.se
- DI.se
- HD.se
- Sydsvenska.se

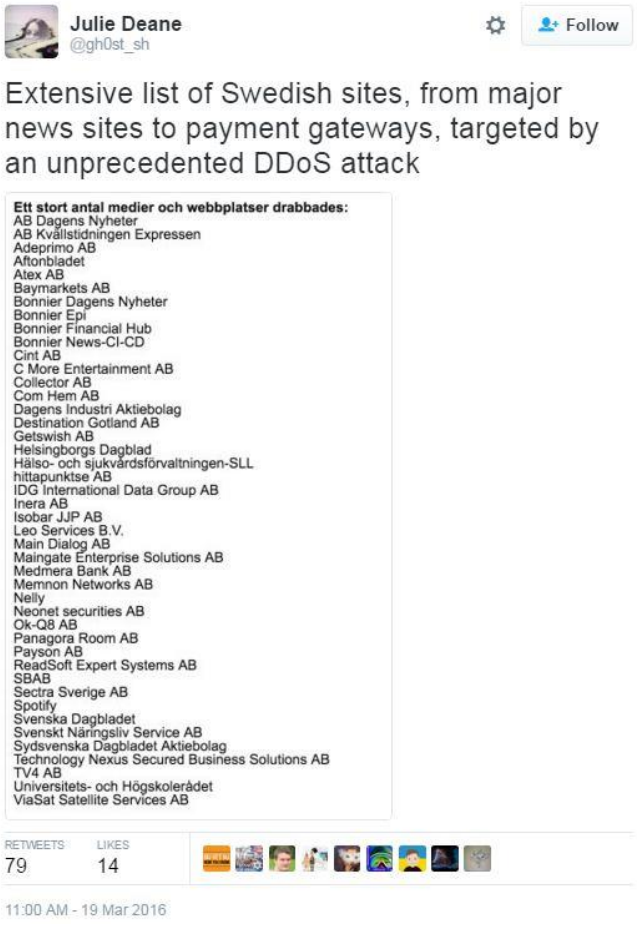

Figure 5: @gh0st_sh presents a list of targeted sites

Suspected Attack Vectors

- **DNS:** Attackers send frequent spoofed DNS request packets. The victim's DNS servers proceeds to respond to all requests until becoming overwhelmed.
- **Reflective NTP**: Very hard to detect since attackers spoof a victim's NTP infrastructure. Requests look 100% normal, amplifying the target's responses by both size and frequency, thus taking them offline.
- **SNMP Reflection:** Generating large responses to small queries. Attackers send requests with IPs belonging to the victim and tricks servers until it is flooded with data.

Scope and Volume

Figure 6: Traffic maps from DDoS attack

What's Expected Next?

Currently, denial of service attacks against Swedish media outlets appear to be over and affected websites are back online. Before the suspension of its Twitter account, the alleged attacker, J @_notJ, threatened additional attacks until Sweden changed its official news stance (see Figure 7).

Figure 7: Alleged attacker claims further attacks against Sweden (account suspended)

Organizations Under Threat Should Consider

Effective **DDoS protection** elements:

- 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.
- Solution must distinguish between legitimate and malicious packets, protecting the SLA while rejecting attack traffic
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- 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.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Need an 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.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT) it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://www.sunet.se/blogg/showerthoughts-ddosing-an-important-social-institution-and-fixing-it-part1/
[ii] https://polisen.se/Aktuellt/Nyheter/2016/Jan-Mars/Mars/Inledd-forundersokning-med-anledning-av-it-attacker/
[iii] http://www.netnod.se/ix-stats/14all_ix-packets-public.pl?dir=Stockholm/GEB/