Abstract

Web and cloud service providers, which have faced an increased likelihood of being attacked since 2015, are now the target of a global cyber campaign that has stricken several Web and cloud hosting companies for nearly a month. Since the beginning of February, Radware identified an ongoing cyber-assault that has targeted hosting providers in the UK. Since then, activity has grown and several other companies from various locations around the globe have experienced long-term outages as a result of denial of service attacks.

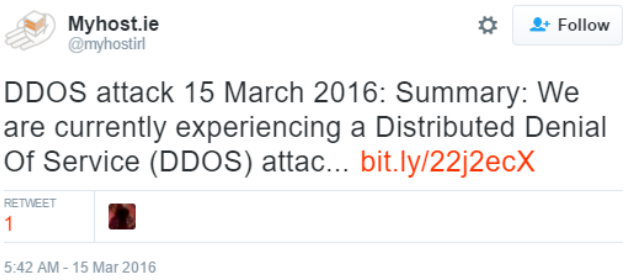

Figure 1: Myhost.ie

Background

Since the beginning of 2016, there has been an increase in attacks against hosting companies and website owners. Reasons vary and include ransomware, protests and other motivations. Assaults have included a wide range of attack vectors, including volumetric L3/L4 network floods (such as ICMP or fragmented UDP floods, which consume the bandwidth and keep the victim's servers unable to respond) and TCP & HTTP application floods, resulting in denial of service, network downtime and SLA disruption (see Figure 2).

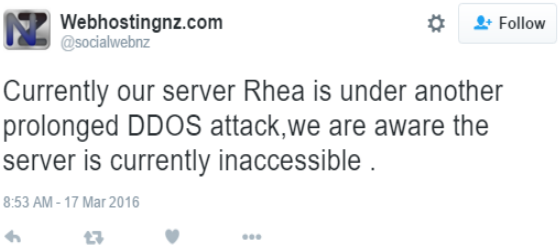

Figure 2: Webhostingnz.com

Reasons for Concern

For small and medium-sized hosting companies, the consequences of service outages can have a significant impact on business. Restoring network services is costly and takes time. Moreover, the reputation damage for a hosting company can have a long term impact. For this reason, hosting services are a prime target for ransom attacks. In addition, the "collateral damage" to a hosting company's large customer base can yield high visibility and have a far ranging impact.

Targeted Hosting Companies

New

- Yoctobox.com[i]
- A2hosting.com[ii]
- Codeenigma.com[iii]
- Webhostingnz.com[iv]
- Webdrive.co.nz[v]
- Ips.nl[vi]
- Myhost.ie[vii]

Previously Reported

- 123-reg
- Heart Internet
- TSO Host
- HostPresto!
- Hart Server

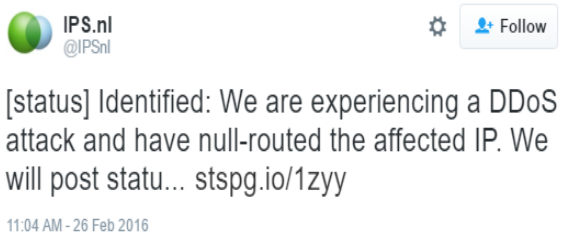

Figure 3: ISPl.nl

How to Prepare

Organizations should proactively prepare their networks and have an emergency plan in place for an incident such as a power failure or a denial of service attack. It's important for web hosting companies to routinely check and audit their systems for possible hardware failure and their resiliency from a denial of service attack.

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://twitter.com/yoctobox/status/707767361567195136
[ii] https://twitter.com/a2hosting/status/708814687073386497
[iii] https://twitter.com/codeenigmahosts/status/707876546242076673
[iv] https://twitter.com/socialwebnz/status/710554717693333504
[v] https://twitter.com/webdrivenz/status/705503443100823552
[vi] https://twitter.com/IPSnl/status/703339824615260160
[vii] https://twitter.com/myhostirl/status/709781903692279808