ERT Threat Alert
Web Hosting Companies Under Attack
February 12, 2016

Abstract
Over the past few days a number of web and cloud hosting companies based in the United Kingdom have experienced long term outages. Two of these outages were caused by a power failure in a shared data center. The other three outages were caused by a denial of service attack.

Background
Over the last few days Radware has observed a number of web and cloud hosting companies based in the United Kingdom experiencing long term outages due to either a denial of service attack or power failure. The series of events started on Monday February 8 and continued through Thursday February 11.

- On Monday February 8, TSO Host began experiencing a DDoS attack on its load balancer[i]. As of this report TSO is still migrating affected customers to new IP addresses.

- On Wednesday February 10, 123-reg experienced a power interruption in one of its data center halls.[ii] The outage appeared to be cause by a safety warning that was triggered and resulted in a power shut down. As of Thursday February 11, everything but a few VPS hosts is back online.

- On Wednesday February 10, Heart Internet experienced the same power interruption as 123-reg due to a shared datacenter hall[iii]. Heart Internet originally stated that they went offline due to a DDoS attack but then later removed the status and stated they were experiencing a power interruption. Later Heart Internet clarified that they had experienced a denial of service attack moments before they went offline due to a power interruption[iv]. As of Thursday February 11, a majority of services have been restored but support continued working through the night to resolve the remaining issues.

- On Wednesday February 10, Hartserver experienced a DDoS attack against its shared web hosting network[v]. As of Thursday February 11, Hartserver has restored a majority of its services though some customers are still experiencing issues.

- On Thursday February 11, HostPresto! experienced a DDoS attack on its server, homer.enixns.com[vi]. The attack was quickly mitigated and the server is back online.

These are all UK based companies that manage a variety of services for thousands of business. These services include web hosting, website builder, domain names, email, SSL and Virtual Private Servers. During the outage the clients of these companies experienced a loss of availability to webmail, virtual private servers and hosting services.

Reasons for Concern
When a single industry is targeted in a specific region it's important to take notice. For small and medium sized hosting companies, the consequences of service outages can have a significant impact on its business. Restoring network services can be very costly and could take an extended amount of time to bring your services back online. Even worse, the reputation damage for a small or medium sized company could be devastating. Hosting services are usually targeted due to their large user base and also makes them a prime target for ransom attacks.

Targeted Hosting Companies

- TSO Host
- Heart Internet
- HartServer
- HostPresto!

Power Outage

- Heart Internet
- 123-reg

What's Expected Next

The denial of service attacks against the hosting companies seems to be over. Those that were affected by either the power interruption or denial of service attacks are currently recovering. It's expected that other web hosting services will be targets by DDoS and ransom attacks in the future due to their large user base and that user bases dependence on service availability.

How to Prepare

While it is impossible to predict who will be the next target of a DDoS campaign, 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 Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe.
- 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.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- 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. Monitoring security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition to Radware products, we recommend that you review your network patch your system according. Maintaining and inspecting your network often is necessary in order to defend against these types of risks and threats.

Under Attack and in Need of 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] http://status.tsohost.com/
[ii] https://www.123-reg.co.uk/support/system-status/
[iii] http://www.webhostingstatus.com/
[iv] https://www.heartinternet.uk/blog/service-outage-faq/
[v] https://twitter.com/hartserver/status/697474607692050432
[vi] https://twitter.com/hostpresto/status/697794726766997504