Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital.

About Boston Children's Hospital

- Ranked nationally in 10 pediatric specialties, with about 25,000 inpatient admissions each year and 557,000 visits scheduled annually through 200+ specialized clinical programs
- Experienced massive rate of several DDoS attacks from Anonymous—marking the first time a hacktivist group targeted a health care organization
- Seven other health care organizations that share the same ISP were affected, as well

Anyone is a Target: DoS Attack Case Analysis on Boston Children's Hospital

Have we entered an era in which cyber-attacks can be not just disruptive and expensive but also potentially deadly? In 2014, Boston Children's Hospital (BCH) became the first health care organization to be targeted by a hacktivist group. Because BCH uses the same Internet Service Provider (ISP) as seven other area health care institutions, the organized attacks had the potential to bring down multiple pieces of Boston's critical infrastructure for health care.

While BCH and the other institutions survived the attack, their experiences should serve as a proverbial "shot in the arm" for any health care entity that isn't already serious about security. To its credit, the medical community seems to have recognized the gravity of the situation. In fact, The New England Journal of Medicine—a publication normally focused on clinical studies—featured an article about the attacks authored by BCH's CIO, Dr. Daniel Nigrin.[1]

The attacks on BCH have illustrated that information security is no longer simply the purview of the IT department. With health care now highly dependent on digital records and network connectivity, inability to access systems has potentially far-reaching clinical and business impacts. Dollars could be lost. Patient and staff safety could be compromised. Lives could be lost.

What follows is a review by Radware's Emergency Response Team (ERT) as experienced from the front lines of the incident - and why it matters.

The Attacks on BCH: A Timeline

Purportedly the work of hacktivist group "Anonymous," the cyber-attacks launched against BCH—occurred in three major strikes launched:

Doxing[2]

On March 20, 2014, BCH leaders received word of a threatening Twitter message that was attributed to Anonymous. The message relayed information related to a high-profile child-custody case, in which a 15-yearold girl with a complex diagnosis was taken into custody by Massachusetts protective services. The message threatened retaliation if the hospital did not take disciplinary action against certain clinicians and return the child to her parents. Attackers posted personal information—including home and work addresses, email addresses and phone numbers—of some of the individuals involved in the case. This activity is known as 'doxing.' By posting technical information about Boston Children's website, the attackers also seemed to imply that the hospital's external site might become a target.

DDoS Strike #1— Attacks at Relatively Low Rates

Starting in early April, the attackers made good on their threats, targeting the hospital's external website with a DDoS attack. At this point, the attack was relatively slow, yet visible to BCH IT personnel.

DDoS Strike #2— Attacks Ramp Up, Mitigation Deployed

Over the course of a week, the attacks increased to the point that they slowed legitimate inbound and outbound traffic. This second string of attacks—comprised of DDoS attacks, scans and intrusion attempts—included TCP fragmented floods, out-of-state floods and DNS reflection floods (including UDP fragment floods). This also included the following non-DDoS attacks: UDP Scans, XSS, SQL-Injection and Directory traversal. At this point, mitigation was set in place and stopped the attacks from reaching the targeted servers.

DDoS Strike #3 — Attacks Peak with Round of Higher-Rate DDoS Attacks

The third strike of the attack peaked at nearly 4x that of the second strike, reaching 28 Gbps. This time, the attackers also made multiple attempts to penetrate the hospital's network through direct attacks on exposed ports and services. Additionally, the attackers used "spear phishing" emails. These emails tried to lure recipients into clicking embedded links or opening attachments, thereby granting access to a portion of the network behind the hospital's firewall.

---

1 When 'Hacktivists' Target Your Hospital", Daniel J. Nigrin, M.D., The New England Journal of Medicine 2014; 371:393-395
2 Document tracing, or "doxing," is the practice of using the Internet to research and then share personally identifiable information about a subject.

Have you experienced severe slowness to your application with an inexplicable steep increase in traffic volume?

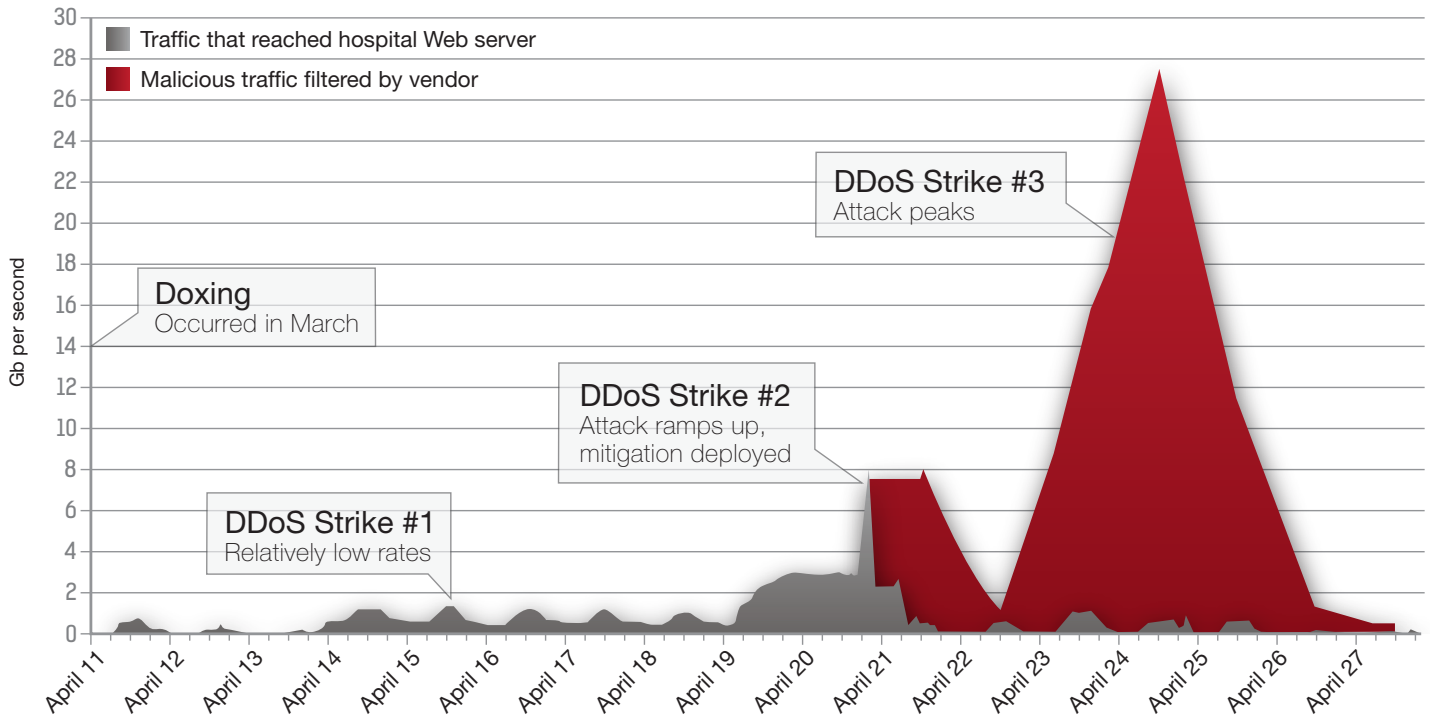

Figure 39: Internet traffic during DDoS Attack - The New England Journal of Medicine

The Response

As soon as it became aware of the initial threat, Boston Children's Hospital activated its multi-disciplinary incident response team. The team faced critical questions and decisions from a business, clinical and technical perspective.

From a business and clinical perspective, the team had to quickly assess what services would be compromised or lost if the hospital were to lose Internet connectivity. Significantly, the hospital had not conducted such an assessment prior to the attacks. In short order, the team identified three critical potential impacts:

- Inability to route prescriptions electronically to pharmacies
- Email downtime for departments where email supports critical processes
- Inability to access remotely hosted electronic health records (EHRs)

From a technical perspective, the BCH team invoked Radware's ERT and the Radware scrubbing center due to the massive rate of several of the DDoS attacks. Because BCH shares an ISP with other hospitals, seven other health care institutions—Massachusetts General Hospital, Beth Israel Deaconess Medical Center, Dana-Farber Cancer Institute, Joslin Diabetes, Harvard Medical School and Harvard School of Public Health—also faced potential impact to their network and operations.

"In clinical settings, {cyber} attacks can clearly have adverse effects on patient care. Healthcare organizations should strongly consider investing the time and resources in IT security systems and operational best practices to ensure that they are prepared to ensure and defend against these new threats, if and when they occur."

Daniel J. Nigrin, MD
"When 'Hacktivists' Target Your Hospital", Daniel J. Nigrin, M.D., The New England Journal of Medicine 2014; 371:393-395
The New England Journal of Medicine

Lessons Learned

The DDoS attacks against Boston Children's Hospital are not significant because of their technical sophistication. Rather, they are significant because they demonstrate that anyone—including health care entities—can be a target for cyber-attacks.

As Dr. Nigrin subsequently wrote in The New England Journal of Medicine, "In clinical settings, such attacks can clearly have adverse effects on patient care. Healthcare organizations should strongly consider investing the time and resources in IT security systems and operational best practices to ensure that they are prepared to ensure and defend against these new threats, if and when they occur."

The attacks on BCH also serve as a reminder that even an organization that has taken all the "right" technical steps can still become a victim. Further, just as health care entities must constantly stay ahead of tenacious infections, all organizations must ensure continual vigilance about information security. It's not enough to have a plan; it must be communicated well and updated constantly as threats and risks evolve.

That kind of vigilance becomes all the more important because of the potential for a massive "domino effect" across Boston's critical infrastructure. Had the DDoS attacks been successful, they could have affected not only BCH but also seven other hospitals. That could have put care delivery—and patients' lives—in peril.