Department of Defense Ensures Success of Its First Bug Bounty Program by Calling Upon Akamai for Site Uptime and Protection

The Situation

When you are the U.S. Federal Government, how do you uncover security weaknesses and vulnerabilities without jeopardizing the country's most critical systems and data? The answer is to follow in the footsteps of leading technology brands that crowdsource vulnerability discovery and disclosure while ensuring uptime and security by using Akamai's services. That was the idea proposed by the Defense Digital Service (DDS), the Department of Defense's arm of the White House's U.S. Digital Service.

Created by Secretary of Defense Ash Carter to transform the way the Department of Defense (DoD) builds and applies technology the DDS is charged with leveraging private sector talent and best practices to improve the federal government's most critical services. Recognizing that security through obscurity is not realistic or viable, in early 2016 the DDS convinced the DoD to launch its first ever bug bounty, called Hack the Pentagon. By taking advantage of the innovations and new thinking that characterize the private sector, the DoD found a cost-effective way to support its internal cybersecurity experts and better protect its systems and networks.

> *"As I delivered regular program updates to the Secretary of Defense and other senior government leaders, the infographs and reports automatically generated through the Akamai customer portal were incredibly valuable. They showed potential attacks unfolding along while also helping illustrate the success of the program and the value of using a solution like Akamai's on our sites to defend against a broad array of attacks."*
>
> *– Lisa Wiswell, Digital Security Lead, Defense Digital Service*

Defense Digital Service

COMPANY

Defense Digital Services
Department of Defense
The Pentagon, Washington, DC

INDUSTRY

Public Sector

SOLUTIONS

- Web Application Firewall
- Client Reputation
- SiteShield
- Ion
- Professional Services

KEY IMPACTS

- Protected against DDoS attack originating from 250 IP addresses in 83 countries
- Denied more than 19 million malicious requests
- Defended against 55 sophisticated attacks
- Absorbed DNS domain floods
- Maintained 100% availability of high-visibility sites
- Ensured no DMA sites protected by Akamai were compromised

Defense Digital Services & Defense Media Activity

The Challenge

While bug bounties are common in the private sector, the federal government had never before implemented this approach. That said, the concept is relatively simple: An organization incentivizes outside researchers – or white-hat hackers – to test the security of its networks and applications and report what they find so the organization can address the vulnerabilities. In this case, the U.S. Federal Government hired a third party, HackerOne, to organize and manage the "hackers" who would try to identify vulnerabilities.

To ensure the success of this program, the DDS worked closely with Defense Media Activity (DMA), which provides DoD enterprise-wide cloud services consisting of a web-based content management system for more than 700 public-facing military and DoD websites. Both the DDS and DMA understood the risks involved and realized that the more hackers it invited to participate, the more bugs the DoD would find. They also knew that to provide both experienced researchers and novice hackers with a meaningful challenge, the program needed to include sites that were significant targets, along with some sites that were outside the DoD perimeter. Finally, in addition to launching and managing the overall program effectively, the DDS and DMA also needed to manage all external communications with the press regarding every aspect of the program.

The Goals

The DDS needed to meet two key requirements to support its objectives:

- *Thwart Internet-based attacks. DoD-related sites are high-visibility targets and the program would shine even more media attention on them, increasing the likelihood of attacks*
- *Ensure availability. To get the most value possible from the hackathon, the DoD needed to ensure the sites it offered up for vulnerability testing stayed online*

Why Akamai?

Taking Advantage of Proven Protection

From the start, DMA recommended that defense.gov be included in the Hackathon since it was already protected by Akamai. The DDS also put other security measures in place to discourage nefarious activity during the event.

At the same time, DMA engaged Akamai's Professional Services to prepare for the program. Because Akamai already has a bug bounty program in place, Akamai's experts provided invaluable insights and suggestions for consideration throughout the program. In addition, DMA implemented Akamai's Client Reputation service as an additional security layer. Client Reputation leverages advanced algorithms to compute a risk score based on prior behavior observed across the entire Akamai network, and profile the behavior of attacks, clients, and applications. Based on this information, Akamai assigns risk scores to each client's IP address and allows DMA to choose which actions it wishes Akamai's security services to perform. By using Client Reputation, DMA had actionable intelligence on approximately 54,000 unique client IP addresses trying to target defense.gov from day one of the program.

Withstanding Traffic Surges

The program launched with just three sites, with only www.defense.gov protected by Akamai at the start. However because of such tremendous interest from the hacker community – more than 1,400 hackers registered – the DDS needed to widen the scope. DMA suggested adding two more sites to show diversity while enabling even less-skilled hackers to find vulnerabilities on outdated and poorly configured web domains.

Defense Digital Services & Defense Media Activity

Two of the five total sites – defense.gov and dodlive.mil – were well-hardened because the DMA had previously engaged Akamai to shore up protection with Akamai's always-on Web Application Firewall (WAF), SiteShield, and Client Reputation services. When a third site buckled under the traffic surge in less than a day, DMA offered umbrella protection via Akamai's WAF. The WAF solution is designed to deny application-layer and volumetric attacks 24/7, including DDoS, SQL injections, and cross-site scripting. Once it was in place, the site withstood the onslaught of attack and testing traffic to become available again for its end users.

Putting the DoD's Cybersecurity to the Test

The Hack the Pentagon program ran from April 18 – May 12, 2016, during which time 252 vetted hackers submitted at least one vulnerability report, for a total of 1,189 reports. As the hacker reports were submitted, the DDS worked to remediate them in real time with support from HackerOne. A little more than a month after the pilot finished, the DDS had remediated each reported vulnerability.

One-hundred thirty-eight reports qualified for the bounty, and 58 of the 1,410 registered hackers received payouts ranging from $100 to $15,000. The total contract value, including the paid out bounties, was approximately $150,000. In the Secretary of Defense's estimation, the DoD would have spent more than $1 million uncovering the same vulnerabilities if it had undergone its typical process of hiring an outside firm to conduct a security audit and vulnerability assessment.

Thwarting All Potential Compromises

Akamai delivered and protected three of the five participating sites without interruption throughout the program while serving 213 million hits and 10 terabytes of data, and absorbing traffic spikes of approximately 2,000 hits per second. Not surprisingly, the bug bounty program attracted attention from nefarious actors.

For example, Akamai protected defense.gov against 55 sophisticated attacks with more than 19.2 million malicious requests denied, including two notable DNS domain flood attacks, and a DDoS attack originating from 250 IP addresses in 83 countries. Using Akamai Client Reputation, DMA also forecasted malicious intent associated with more than 1 million requests. As a result, DMA was able to automatically deny all known high threats at the edge of the Internet and far away from DMA's web server infrastructure.

By baselining website activity before, during, and after the challenge, DMA could see higher scanning and research activity on sites protected by Akamai.

Expanding the Program

To commemorate the event, HackerOne gave out a Hack the Pentagon challenge coin for successful hackers. Pleased with the success of the program, Secretary Carter has already released detailed plans to expand the bug bounty program to other parts of the DoD.

"We want to put lots of DoD assets through this type of security program to streamline and shorten the time to discover vulnerabilities while allowing our internal teams to focus on remediation. As we launch more bug bounties, we will need to make sure the participating sites are exercised enough from a vulnerability perspective to make the challenge worthwhile. Ideally, we will have a commercial solution, such as Akamai's, in place to help make this vision a reality," concludes Lisa Wiswell, the Digital Security Lead for the Defense Digital Service.

Defense Digital Services & Defense Media Activity

About Defense Digital Services

The Defense Digital Service (DDS) was created in November 2015 by Defense Secretary Ash Carter and is an agency team of the U.S. Digital Service at the White House. The mission of the DDS is to drive game-changing evolution in the way the DoD builds and deploys technology and digital services. The DDS exists to apply best-in-class private sector practices, talent, and technology to transform the way software products are built and delivered within the DoD.

About Defense Media Activity

Defense Media Activity (DMA) serves as a direct line of communication for news and information to U.S. forces worldwide. The agency presents news, information, and entertainment on a variety of media platforms, including radio, television, internet, print media, and emerging media technologies. DMA informs millions of active, Guard, and Reserve service members, civilian employees, contractors, military retirees and their families in the United States and abroad.