Issued 11/20/18

Hackers Cram Make-A-Wish Website with Coin-Mining Malware

One or more completely feckless scumbags have loaded the Make-A-Wish foundation's international website with crypto-mining malware scripts. Researchers with Trustwave say the (now clean) WorldWish.org site was compromised via a Drupal exploit and seeded with malicious JavaScript that enlisted the CPU cycles of visitor's machines to covertly generate cryptocurrency. It seems that the site was using an older version of the Drupal CMS that was vulnerable to CVE-2018-7600, the remote code execution bug known for marketing purposes as "Drupalgeddon 2." The successful exploit of the vulnerability gives an attacker the current user's access level and, in the case of web servers, this means the ability to access and modify pages. In the context of a crypto-jacking attack, the compromised page has a short script embedded into it that calls another server to get the actual cryptocoin mining script. That server can also be obfuscated by changing its address or bouncing the connection off other servers. When a user visits the infected page, the mining script is called and the user's machine is used to generate cryptocurrency for the attacker. The time of year might also have had something to do with the filth choosing Make-A-Wish as their target. Sigler said that during the holiday season attackers tend to look to infect sites and pages that get high amounts of traffic, and the sites of charity organizations are a particularly good target, (so long as one is unhindered by morals and a sense of basic human decency.) Protecting against the attack is easy enough: Make sure Drupal (and all other web server

apps) are updated and fully patched. Admins should also keep a close eye on any changes or unusual activity on their pages that could signal an attack.