Anonymous hacktivists prefer penetration, but choose targets of opportunity

By Stilgherrian | The Resource For Security Executives | 09 May 12

Hacktivism, as practiced under the name Anonymous, is about public relations opportunism and any organisation could become a target if a political rationale can be retro-fitted to the attack, according to a leading web security researcher.

Read more: http://www.pcadvisor.co.uk/news/security/3356768/anonymous-hacktivists-prefer-penetration-but-choose-targets-of-opportunity/#ixzz1wHBpd1R8

"In hacktivism it's all about the PR impact," Tal Be'ery, web security research team leader at Imperva's Application Defense Center (ADC), told CSO Online. "It doesn't matter to the press whether a really significant site was taken down, DDoSed or whatever. It's all about being successful, no matter what."

From a PR point of view, the specifics of how the hacktivist affects the target don't matter. Whatever happens, the hack will generate media coverage for the cause.

Nor does it matter specifically who the target is. Be'ery reckons the targets are chosen opportunistically, based on a wide search for vulnerable sites.

"Sometimes you find the target first, and then come up with the cause or a [justification for] the cause to be relevant," he said--although he was reluctant to generalise about motives.

"There are many groups out there doing hacktivism, and it's not like you have to get a license," he said.

However it does seem that the hacktivists prefer a real hack over a DDoS.

"We believe that DDoS is the last resort of the hacker, because if the hacker can do a real hack on the server... to steal the data or deface the site, then it's the preferable mode of operation because you need less resources in order to do it," Be'ery said.

"We can prove it over specific cases we've seen that only when the attackers were not successful in hacking the site using a web application vulnerability then they went to the DDoS option, because ultimately DDoS doesn't need any vulnerability really in order to be successful. You just have to create enough traffic in order to take the site down and jam the connection or other resources."

Be'ery was reluctant to identify those specific cases, saying only that Imperva's team has monitored Anonymous' attacks unfolding in real time within the last twelve months through their clients' networks as well as their own honeypot array.

A DDoS significantly increases the visibility and exposure of the attackers as they recruit hundreds or thousands of participants, using familiar Web 2.0 tools like Facebook pages, Twitter accounts, YouTube movies and blogs.

"Having some kind of Google Alert from the defending side point of view is a smart thing to do," Be'ery said.

Be'ery will be presenting further findings from his team's research at the AusCERT information security conference later this month.

Contact Stilgherrian at Stil@stilgherrian.com or follow him on Twitter at @stilgherrian

Read more: http://www.pcadvisor.co.uk/news/security/3356768/anonymous-hacktivists-prefer-penetration-but-choose-targets-of-opportunity/#ixzz1wHBfVqtq