Commonly used strategy for website protection is not waterproof

April 12 2016

Credit: KU Leuven

Cloud-based security providers commonly use DNS redirection to protect customers' websites. The success of this strategy depends on shielding the website's original IP address. Computer scientists from KU

Leuven, Belgium, and digital research centre iMinds have now revealed that the IP address can be retrieved in more than 70% of the cases. This means that the DNS redirection security mechanism can easily be bypassed.

Websites and online services increasingly have to deal with acts of cybercrime such as 'distributed denial-of-service' (DDoS) attacks: the site or service is deliberately bombarded with huge numbers of malicious communication requests from different computers so that it collapses.

"Website owners can protect themselves against cyberattacks by installing dedicated hardware," says Thomas Vissers from the KU Leuven Department of Computer Science and iMinds. "Yet, this is typically too expensive and too complex for most of them. That's why website owners often rely on the services offered by cloud-based security providers. One strategy these providers commonly use to protect websites includes diverting incoming web traffic via their own infrastructure, which is sufficiently robust to detect and absorb cyberattacks. However, the success of this strategy heavily depends on how well the website's original IP address can be shielded. If that IP address can be retrieved, protection mechanisms can easily be bypassed."

According to the researchers, this is the Achilles heel of cloud-based security. Therefore, they set up the first large-scale research effort in this domain and actively explored vulnerabilities in the DNS redirection strategy that is used by many cloud-based security providers to intercept web traffic.

Nearly 18,000 websites, protected by five different providers, were subjected to the team's DNS redirection vulnerability tests. To this end, the researchers built a tool called CLOUDPIERCER, which automatically tries to retrieve websites' original IP address based on eight different methods, including the use of unprotected subdomains.

"Previous studies had already described a number of strategies that can be used to retrieve a website's original IP address. We came up with a number of additional methods. We were also the first to measure and verify the exact impact of these strategies on a larger scale," says Thomas Vissers.

"The results were pretty confronting: in more than 70% of the cases, CLOUDPIERCER was able to effectively retrieve the website's original IP address, thereby providing the exact info that is needed to launch a successful cyberattack. This clearly shows that the DNS redirection strategy still has some serious shortcomings."

The researchers have already shared their results with the cloud-based security providers under consideration, allowing them to respond properly to the risk that their customers are still running.

However, the researchers also want to inform the general public - and, more specifically, website owners - about the shortcomings of the popular DNS redirection strategy. That is why they've made CLOUDPIERCER available for free.

"With CLOUDPIERCER, people can test their own website against the eight methods that we have used in our research. CLOUDPIERCER scans the website, and indicates to which IP detection method it is most vulnerable," concludes Thomas Vissers.

When websites use DNS redirection as a defence mechanism against cyberattacks, two simple measures can be taken to prevent the original IP address from being retrieved. One option is adjusting the website's firewall settings to only allow web traffic from the cloud-based security provider. Alternatively, the IP address of the website can be changed once the contract with the cloud-based security provider is initiated.

CLOUDPIERCER will be presented at iMinds - The Conference. The research paper is available here.

Provided by KU Leuven

Citation: Commonly used strategy for website protection is not waterproof (2016, April 12) retrieved 25 April 2024 from https://phys.org/news/2016-04-commonly-strategy-website-waterproof.html