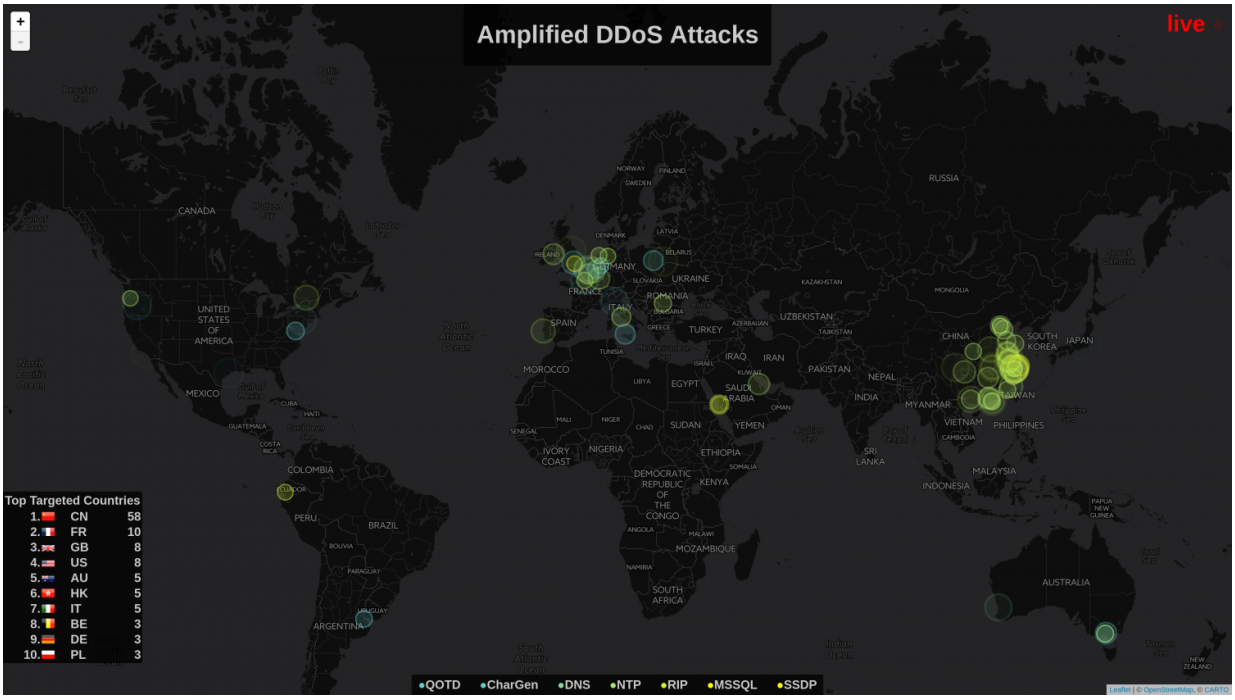
Researchers present early warning system for mass cyber attacks

March 15 2017



At CISPA researchers are mapping mass cyber attacks in real-time. Credit: Saarland University/CISPA

Mass attacks from the Internet are a common fear: Millions of requests in a short time span overload online services, grinding them to a standstill for hours and bringing Internet companies to their knees. The operators of the site under attack can often only react by redirecting the wave of requests, or by countering it with an exceptionally powerful

server. This has to happen very quickly, however.

Researchers from the Competence Center for IT Security, CISPA, at the Saarland University have developed a kind of early warning system for this purpose. Details and first results will be presented by the scientists at the computer fair Cebit in Hannover.

These mass cyber attacks, known as "Distributed Denial of Service" (DDoS) attacks, are considered to be one of the scourges of the Internet. Because they are relatively easy to conduct, they are used by teenagers for digital power games, by criminals as a service for the cyber mafia, or by governments as a digital weapon. According to the software enterprise Kaspersky, some 80 countries were affected in the last quarter of 2016 alone, and counting. Last October, for example, several major online platforms such as Twitter, Netflix, Reddit and Spotify were unavailable to Internet users in North America, Germany, and Japan for several hours. A new type of DDoS attack, a so-called amplification attack, was found to be the source of these outages.

"What makes this so insidious is that the attackers achieve maximum damage with very little effort," says Christian Rossow, professor for IT security at the Saarland University, and head of the System Security Group at the local IT Security Competence Center, CISPA. Remote-controlled computers are used to direct requests at vulnerable systems in such a way that the system's responses far exceed the number of requests. The request addresses are then replaced by the Internet address of the victim. Rossow has identified 14 different Internet protocols that can be exploited for this kind of attack.

To investigate these malicious attacks, and the people and motives behind them more closely, Rossow has developed a special kind of digital bait for distributed attacks (also known as honeypots), in collaboration with the CISPA researchers Lukas Kraemer and Johannes

Krupp and with colleagues from Japan. 21 of these honeypot traps were laid out in the more obscure corners of the Internet, enabling the researchers to document more than 1.5 million attacks. In this manner, he could identify the different phases of attacks which helped develop an early warning system from the data. He additionally attached secret digital markers to the attack codes he discovered in the digital wilderness, and was thus able to trace the source of the attacks. "This is quite impressive, because these address counterfeiters usually remain hidden by default," says Rossow.

This is not the first time that Rossow has systematically infiltrated cyber-criminals' networks. He also managed to take down the infamous botnet "Gameover Zeus" in a similar manner, on behalf of the US domestic intelligence service FBI. In the meantime, he has redesigned his bait to match the latest varieties of DDoS attacks. Cyber-criminals today no longer rely on vulnerable servers, but also attack networked televisions, webcams, or even refrigerators. The "Internet of Things" makes it possible.

More information: christian-rossow.de/publicatio … /iotpot-woot2015.pdf

Provided by Saarland University