SLEDGEHAMMER

FORCEPOINT™
SECURITY LABS™

AN ANALYSIS OF THE GAMIFICATION OF DDOS ATTACKS IN TURKEY

DDoS (Distributed Denial Of Service) package shared on Turkish hacking forum

Participants gain points which are exchanged for software

1 point awarded for every 10 minutes they attack a website

24 sites in the list of DDoS targets – including Kurdish, German, Israeli, Armenian websites

Hacking teams compete against each other for awards

Software tools that can be won: click-fraud bots, scareware programs, upgraded version of DDoS tool

The author of the DDoS tool can activate a backdoor to access the competitor's machines

Author disguises tool's behaviour with: backdoor, steganography, Tor

READ OUR REPORT
www.forcepoint.com/sledgehammer

FORCEPOINT
POWERED BY Raytheon

SLEDGEHAMMER

The Gamification of DDoS Attacks

FORCEPOINT™
SECURITY LABS™

Operation Sledgehammer

Operation Sledgehammer translated into Turkish is Balyoz Harekâtı, which was the name of a 2003 attempted military coup d'etat in Turkey. It's also the name of a recent Distributed Denial of Service (DDoS) attack that targeted organizations with political affiliations that the attacker deems out of line with Turkey's current government. These organizations include the German Christian Democratic Party (CDU), The People's Democratic Party of Turkey, the Armenian Genocide Archive and the Kurdistan Workers Party (PKK).

DDoS Attack Games for Hackers

Operation Sledgehammer's author runs a DDoS collaboration program named Sath-ı Müdafaa or "Surface Defense." Using a DDoS tool named Balyoz, hacking participants are asked to attack a limited set of political websites, but can also suggest new websites to add to the list of targets.

For every ten minutes spent attacking one of these websites, users receive points that can be traded in for rewards, such as a stand-alone version of the Sledgehammer DDoS tool and "click-fraud" bots used to generate revenue on pay-to-click (PTC) sites. There is even a live scoreboard so participants can see their point rank.

What is the motivation of the hackers?

Forcepoint Security Labs focus on enabling the awareness and understanding of intent. This is useful in order to identify likely future behaviour. The attacker initially attracts subscribers with the promise of participating in a collaborative DDoS system targeting websites of a political nature. "Click-fraud" bots add a monetization aspect to the system. A final twist in the tail was discovered when we uncovered a backdoor in the DDoS toolkit – the author is hacking the hackers.

Who led this research?

Forcepoint's Special Investigations team is an elite group of threat researchers and incident response experts specializing in threats exhibiting unique tools, tactics and processes (TTPs). In the past year, highlights of the Special Investigations team's work include discovering a new botnet campaign dubbed JAKU and cracking a persistent strain of ransomware known as Locky.

READ OUR REPORT
www.forcepoint.com/sledgehammer

FORCEPOINT
POWERED BY Raytheon