Iran blamed for cyber onslaught on US banks

January 9 2013, by Glenn Chapman

US financial institutions are being pounded with high-powered cyber attacks that some suspect are being orchestrated by Iran as payback for political sanctions.

"There is no doubt within the US government that Iran is behind these attacks," James Lewis, a former official in the state and commerce departments and now a computer security expert at the Center for Strategic and International Studies, told the New York Times.

While the identities of those behind the online onslaught officially remain a mystery, it was clear they were using a potent new weapon for slamming bank websites with overwhelming numbers or requests for information.

The attackers infected datacenters used to host services in the Internet "cloud" and commandeered massive computing power to back distributed denial of service (DDoS) attacks, according to security experts.

DDoS attacks have been a basic hacker weapon for quite some time, but they have typically involved using armies of personal computers tainted with viruses and coordinated to make simultaneous requests at targeted websites.

"They are essentially going from a pistol to a cannon," Radware vice president of security solutions Carl Herberger said of cyber attackers using datacenters. "That was one major achievement."

The top 20 US banks on Wednesday were being hit with a third wave of attacks, each of which has been preceded by a claim of responsibility by a group calling itself Izz ad-Din al-Qassam Cyber Fighters.

The attacks began in September of last year, according to Radware, which specializes in commercial computer security and has been investigating the cyber assaults.

"The landscape we are seeing is essentially a persistent industry sector attack that is unprecedented," Herberger said.

"There have been a number of lulls in cyber fighting, with waves concluded and re-launched."

Attackers have shrewdly tailored requests to target encrypted pages or data, which are more complicated to process and therefore tax websites more, according to Radware.

"The world of DDoS is about consuming resources fast; however you can get inside an encrypted algorithm you can multiply your effect," Herberger said. "It is a wonderful tool from a perpetrator's perspective."

Such requests are particularly nefarious because encrypted exchanges are often shielded from security software intended to guard against attacks.

It appeared that no money was taken in the attacks, but Herberger warned that the full extent of the damage had yet to be assessed.

He described how hackers sometimes use DDoS attacks to trigger fail systems that can sometimes allow invaders to get to data.

"I call it the battering ram effect," Herberger said. "They literally batter in the front door; that is a really dark side of this world."

Attacks on banks could also be test runs for assaults on other business sectors or even smart systems controlling vital infrastructure.

"Let's suppose this is state sponsored," Herberger proposed. "Could these not be dry runs? If the banks are permeable what is the likelihood that other systems are?

John Bumgarner of the US Cyber Consequences Unit, a non-profit group that studies the impact of cyber threats, cautioned against rushing to assign blame for the attacks.

"These attackers are using the anonymity of the cyber space to mask who they are," Bumgarner said. "There is not irrefutable evidence that the Iranian government was responsible."

Citation: Iran blamed for cyber onslaught on US banks (2013, January 9) retrieved 23 April 2024 from https://phys.org/news/2013-01-iran-blamed-cyber-onslaught-banks.html