Cyberattacks on South Korea-US a test run: McAfee (Update 2)

July 5 2011, by Glenn Chapman

The McAfee logo is displayed outside of the company's headquarters in 2010 in Santa Clara, California. Cyber attacks on US and South Korean military websites in March may have been a test by North Korea or sympathizers, according to a report released Tuesday by computer security firm McAfee.

Cyberattacks on US and South Korean military websites in March may have been a test by North Korea or sympathizers, according to a report released Tuesday by computer security firm McAfee.

"We believe this incident... has very clear anti-Korean and anti-US political motivations," McAfee said in a report titled "Ten Days of Rain."

"The combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome is analogous to bringing a Lamborghini to a go-cart race," McAfee said in its findings.

"As such, the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe response capabilities," it said.

McAfee security researchers said it was 95 percent likely that the culprits behind the online assault in March were also behind July 4, 2009 cyberattacks on US and South Korean websites.

Banking, military and government websites in South Korea and sites for US forces in that country were hit with distributed denial of service attacks on March 4.

DDoS attacks overwhelm websites with requests, causing them slow down or be inaccessible.

McAfee security researcher Georg Wicherski deemed the attacks "an armed cyber reconnaissance operation of sorts" aimed at assessing defenses and reaction times of South Korean government and civilian networks.

"Knowing that would be invaluable in a possible future armed confrontation on the peninsula, since cyberspace has already become the fifth battlespace dimension, in addition to land, air, sea, and space," Wicherski said.

The DDoS attacks were made by usurping control of virus-infected computers in South Korea to overwhelm targeted websites with simultaneous requests for pages or information.

Tactics used in the attacks were more destructive than typically seen when legions of infected computers are commanded in "botnets" by hackers, according to McAfee.

The botnet in South Korea was programmed to perform DDoS attacks for 10 days and then self-destruct, frustrating investigators by overwriting or deleting files and codes to the extent the computers could not be booted up.

While the Match attacks were underway, encryption algorithms were used to mask parts of malicious code and stymie analysis by defenders.

"This wasn't a surgical strike; it was more like a sledgehammer, as most DDoS attacks are," the McAfee report said.

"The attackers relied on the encryption to buy them more time against reverse engineering until the DDoS attack window expired."

Steps were taken to ensure that the mission was executed without interruption, within the predefined attack window, and then all vehicles of attack would be destroyed, the report concluded.

Updates were sent to the botnet by servers in various parts of the world including Taiwan, Russia, Saudi Arabia, India and the United States to make it resistant to takedown, according to McAfee.

The McAfee study revealed that pieces of the malicious code used in the attacks were built by a number of different people, each with limited knowledge of the overall program.

Last week, South Korea's defense ministry announced that it would expand its cyber warfare unit to help combat growing Internet attacks from North Korea.

The ministry said its cyber command, launched in January last year, would increase the number of personnel from 400 to 500, following an earlier announcement that it would open a cyber warfare school next

year.

North Korea reportedly maintains elite hacker units.

Seoul accused Pyongyang of staging the cyberattacks on websites of major South Korean government agencies and financial institutions in March this year and in July 2009.

Pyongyang rejected those allegations, accusing Seoul of inventing the charges to raise tensions.

In May, South Korea said a North Korean cyberattack paralyzed operations at one of its largest banks.

Citation: Cyberattacks on South Korea-US a test run: McAfee (Update 2) (2011, July 5) retrieved 10 May 2024 from https://phys.org/news/2011-07-cyber-south-korea-us-mcafee.html