Cybersecurity

Case Study - Logic Bombs

1.2.7 Logic Bombs

Article:

Programmer Jailed Three Years Over Plot to Wipe Out All of Fannie Mae's Financial Data
DEC 31, 2010
Retrieved from: https://www.rawstory.com/2010/12/indian-programmer-jailed-years-plot-destroy-fannie-maes-financial-data/
Source: Raw Story
Author: Stephen C. Webster

A computer programmer who almost succeeded in wiping out all of the Federal National Mortgage Association's financial data at the height of the housing market crash was sentenced to three years in prison earlier this month.

Rajendrasinh Babubhai Makwana, 36, worked as a contractor with the home mortgage lender, better known as Fannie Mae, from 2006 through Oct. 2008. He was abruptly fired for writing an erroneous piece of software code that changed settings on the company's Unix servers without proper authorization. Ordered to turn in his equipment and security badge on Oct. 24, 2008, Makwana, a foreign national from India, complied and returned to his workstation to finish out the day. His administrative access to the company's 4,000 servers, however, was not terminated until that evening.

In the interim, sometime between 1:30 p.m. and 4:30 p.m., Makwana created a potentially devastating logic bomb script that authorities claimed would have wiped out all of the home lender's financial data, causing untold damage to the US financial system and erasing the mortgages of millions of homeowners.

The software was set to auto-execute on Jan. 31, 2009 — but that never happened.

Instead, on Oct. 29, a senior Unix engineer found the code embedded below a legitimate script. The two scripts were separated by about a page of blank lines, according to a criminal complaint (PDF) filed with a US district court in Maryland by FBI Special Agent Jessica Nye.

The script would have disabled all server login attempts and blocked the company's server monitoring systems. Any effort to access the network would have resulted in a message that read "Server Graveyard," the complaint said. It would have also erased log files, ensuring Makwana's trail would not be followed. When the script was discovered days later, Fannie Mae's IT department went into full emergency mode, locking down their servers to ensure no other malicious scripts had been inserted. A criminal complaint was soon to follow.

Makwana was convicted on October 4, 2010, and faced up to 10 years in jail. He was sentenced to 41 months in prison on December 17 by US District Judge J. Fredrick Motz.

His professional profile on business networking website LinkedIn was still available and featured a small image of Makwana apparently skydiving.

"Computer intrusion cases are a high priority for federal law enforcement because of the potential to cause serious damage," US Attorney Rod J. Rosenstein said, according to a US Department of Justice advisory. "Mr. Makwana was trusted with access to the computer system, and he violated that trust."

Summary

In October of 2008, Rajendrasinh Makwana was informed he was being fired from the Federal National Mortgage Association (known as Fannie Mae). Fannie Mae is a U.S. government-sponsored enterprise whose goal is to ensure "homeowners, homebuyers, and renters across the country have access to affordable financing opportunities," according to their website, www.fanniemae.com . Makwana was a contractor at a Maryland facility. Upon being told he was terminated in the afternoon, he returned to his desk and installed a logic bomb on Fannie Mae's servers. This logic bomb was set to go off on January 31, 2009, which was 100 days later. The payload of this logic bomb would clear all the files on the Fannie Mae servers, stop all access to the servers, and erase all log files (to help hide his tracks). This would have had a huge impact on the U.S. financial system since it would have erased the mortgages of millions of American homeowners.

Only five days after he planted the logic bomb, another Fannie Mae software engineer found the logic bomb and was able to get rid of it. They also made sure no other logic bomb was planted on the system and notified the FBI. Makwana was arrested and ended up receiving over 3 years of prison time for making and planting this logic bomb.

Questions

- What cyber laws are broken if a logic bomb is created or used?
- Should Makwana have served jail time for a logic bomb that never went off?
- How could Fannie Mae have stopped Makwana from planting this logic bomb?
- Should only one person be able to make changes to an important server like Fannie Mae's?
- Could new processes help protect servers? (e.g. having at least two people approve changes)
- Had the logic bomb went off, would Makwana be viewed as a "Robin Hood" hero since he would have erased the home mortgages of millions of people?
- Why is it important for companies to trust their contractors? Should companies limit what contractors can do on their servers?

Further Study

- FBI's press release on the conviction of Makwana: https://archives.fbi.gov/archives/baltimore/press-releases/2010/ba121710.htm
- More information on Fannie Mae: https://www.investopedia.com/articles/investing/091814/fannie-mae-what-it-does-and-how-it-operates.asp