

As Seen On



Monday, April 7, 2008

Move over Storm – there’s a bigger, stealthier botnet in town 400,000 machines get Kraken

By Dan Goodin (San Francisco), *The Register*

Researchers have unearthed what they say is the biggest botnet ever. It comprises over 400,000 infected machines, more than twice the size of Storm, which was previously believed to be the largest zombie network.

Machines from at least 50 Fortune 500 companies have been observed to be running the malicious software that’s at the heart of “Kraken,” the botnet that security firm Damballa has been tracking for the last few weeks. So far, only about 20 percent of PCs running anti-virus products are detecting the malware. Just as a con artist might throw off detectives by changing his hair color or other physical characteristics, Kraken’s ability to morph its code base has allowed it to evade the majority of malware detectors.

“Kraken, despite being on all these people’s computers, has such low anti-virus coverage,” said Paul Royal, principal researcher at Atlanta-based Damballa. “Anti-virus companies can’t keep up with the arms race because of the number of variants and the frequency of the updates.”

In addition, the code inside the executable file that infects a PC has been arranged in a way that makes it hard for malware analysis tools to accurately disassemble the malicious program.

“It raises the question of whether this basically has been authored specifically with anti-virus evasion in mind,” Royal added.

Kraken most likely spreads by tricking end users into clicking on a malicious file that’s disguised as an image. When it’s executed, the program automatically copies itself to the hard drive in a slightly altered format. In the event AV programs are eventually able to recognize the original file, Kraken can use the altered file to reinfect the machine. Moreover, zombie machines regularly update themselves as an additional measure to prevent detection.

Kraken’s primary activity is sending spam that advertises high-interest loans, male-enhancement techniques, fake designer watches and gambling opportunities. Damballa has observed as many as 500,000 pieces of junk mail being sent from a single zombie.

Estimates have varied wildly for the number of bots belonging to the Storm network. While some researchers have said millions of machines have been compromised, MessageLabs in February put the number of nodes at just 85,000. Whatever the number – Damballa estimates Storm has 200,000 victim - it was believed to be the biggest.

Until now, that is. It has clearly been eclipsed by Kraken, which on March 25 was observed to have compromised 409,912 unique IP addresses during a 24-hour period. Royal predicted the number will grow to more than 600,000 in the next two weeks.

Royal says he’s still trying to figure out how the bot is managing to horn its way on to so many machines, many of which are behind well-fortified networks of some of the world’s biggest companies.

“Somehow, this thing is evading the canonical defense techniques that the enterprises use,” such as intrusion detection systems and intrusion prevention systems, he said. “It should be caught by IDSes, IPSes and firewalls and it’s not.”