Issued 2/22/17

Hackers Behind Bank Attack Campaign Use Russian Decoy

The hackers behind a sophisticated attack campaign that has recently targeted financial organizations around the world have intentionally inserted Russian words and commands into their malware in an attempt to throw investigators off.

Researchers from cybersecurity firm BAE Systems have recently obtained and analyzed additional malware samples related to an attack campaign that has targeted 104 organizations -- most of them banks -- from 31 different countries. "In some cases the inaccurate translations have transformed the meaning of the words entirely," the researchers said in a blog post. "This strongly implies that the authors of this attack are not native Russian speakers and, as such, the use of Russian words appears to be a 'false flag'."

This unusual behavior is most likely intended to make attribution harder and throw investigators on a false lead. In reality there is technical evidence to link these malware samples and the overall attack campaign to a group known in the security industry as Lazarus.