Shadow Brokers resurface again with alleged NSA hacking tools for SWIFT and Microsoft

Details on the individual or group's latest document leak

Background

- **After several quiet months, the Shadow Brokers have reappeared for the second time in the past week, posting more files it claims belong to the elite, NSA-affiliated hacking unit called the Equation Group**
- Though previous releases and unsuccessful bitcoin auctions have contained underwhelming and often outdated information, the most recent documents could be "the most damaging dump against the NSA to date, and … without question the most damaging post-Snowden release," according to Nicholas Weaver of the International Computer Science Institute

SWIFT

- **Included in the Shadow Brokers' latest release are tools allegedly used by the NSA to gain access to SWIFT, the international payment transfer system with more than 11,000 member banks**
- **The cyber technique targets SWIFT's service bureaus,** which manage SWIFT operations for their clients. Relying on these third-parties rather than hacking SWIFT's own infrastructure offers a convenient and efficient workaround: instead of hacking individual banks, the administrative privileges of a service bureau can provide an entry point into all of that firm's client banks
- **It appears from the documents that the SWIFT tools were used to monitor financial data and transfers at banks across the Middle East, including Abu Dhabi, Dubai, Kuwait, Qatar, Syria, Yemen, and the Palestinian territories**
- The absence of any apparent theft or manipulation would suggest that the NSA was potentially using these methods to track terrorist financing

Microsoft

- **Another portion of the Shadow Brokers' files details zero-day flaws for Microsoft Windows operating systems**
- An initial panic over what was termed the "Microsoft apocalypse" was soon tempered by a Microsoft blog post explaining that most of the flaws had already been patched in an update last month. The few remaining vulnerabilities do not apply to current software versions still supported by Microsoft

Sources: Nicole Perlroth, "Hacking group claims NSA infiltrated Mideast banking system," NYT, April 15, 2017; Joe Uchill, "Microsoft: all security issues from NSA leaks patched in current software," The Hill, April 15, 2017; Sean Carberry, "Shadow Brokers leak trove of NSA hacking tools," FCW, April 14, 2017; Images by iconsphere, Alexander Skowalsky and Till Teenck, The Noun Project, April 2017.