FBI Warns of Continuing Threat from "ATM Cashout" Scheme

Insights
8.22.18

The FBI is warning banks to be on guard against possible attacks on ATMs.

In an alert sent to banks on August 10th, the FBI warned banks that it had "obtained unspecified reporting indicating cyber criminals are planning to conduct a global Automated Teller Machine (ATM) cash-out scheme in the coming days, likely associated with an unknown card issuer breach and commonly referred to as an 'unlimited operation'."

The FBI alert states that "unlimited operations" compromise financial institutions with malware, allowing cybercriminals access to bank customer card information, enabling large-scale theft on a global scale. The malware used to effect these "unlimited operations" is typically installed using phishing or hacking schemes. Once inside, intruders can steal card numbers, and create "clones" of those cards. Crooks can then remove fraud controls such as maximum withdrawal amounts or daily transaction limits. The alert warns that, historically, small-to-medium size banks, which typically lack robust cybersecurity controls, budgets, and/or have vulnerability through third-party vendors.

Since the FBI alert, the potential threat has become clear following a 13.5 Million theft from Cosmos bank based in Pune, India on August 11. Using malware, hackers were able to break into the bank's servers and steal $2 million through fraudulent bank transfers and $11.5 million through unauthorized ATM withdrawals in at least twenty-eight countries.

Similar attacks have also occurred in the United States. Security publication, Krebs, published reports of breaches, totaling $2.4 million, at two Virginia banks in 2016 and 2017. In the Virginia breaches, hackers used the bank's computers to inflate account balances before making ATM withdrawals.

The FBI provided recommendations all businesses can take to protect themselves

The FBI is urging banks to review security measures, which are also more broadly applicable to employers aiming to protect confidential business and employee information.

FBI recommendations include:

- Implement "whitelisting" applications (a list of programs allowed on your system) to block the execution of malware.
- Monitor, audit and limit administrator and business critical accounts.

- Monitor for encrypted traffic (SSL or TLS) traveling over non-standard ports.
- Monitor for network traffic to regions wherein you would not expect to see outbound connections from your institution.

Related People

Robert Fallah
Attorney
610.230.2150
Email