Issued 12/11/17

Hackers Hit Key ATM Network In Crime Spree That Clears $10 Million

A previously undetected hacker group has netted around $10 million in heists on at least 20 companies, in some cases by targeting the transfer networks banks use to transfer money, a Moscow-based security firm said Monday. Members of the MoneyTaker group, named after a piece of custom malware it uses, started its heist spree no later than May 2016. That's when it penetrated an unnamed US bank, according to researchers with Group-IB in a report titled MoneyTaker: 1.5 Years of Silent Operations.

Over the past 18 months, Group-IB has uncovered evidence that MoneyTaker has successfully breached 18 banks or credit unions, two financial services businesses, and one law firm.
Two of the targets were located in Russia, one target was in the UK, and the rest were in the US. The average amount stolen in each hack was $500,000.

The hackers use malware that's stored almost entirely in computer memory, a feature that makes them extremely hard to detect by antivirus defenses. The in-memory malware also makes it hard for targets to know they were hacked since all traces are destroyed as soon as a computer is rebooted.