Hackers stole $800,000 from ATMs using Fileless Malware

	Hackers stole $800,000 from ATMs using Fileless Malware

Hackers targeted at least 8 ATMs in Russia and stole $800,000 in a single night, but the method used by the intruders remained a complete mystery with CCTV footage just showing a lone culprit walking up to the ATM and collecting cash without even touching the machine.

Even the affected banks could not find any trace of malware on its ATMs or backend network or any sign of an intrusion. The only clue the unnamed bank's specialists found from the ATM's hard drive was – two files containing malware logs.

The log files included the two process strings containing the phrases: « Take the Money Bitch! » and « Dispense Success. »

This small clue was enough for the researchers from the Russian security firm Kaspersky, who have been investigating the ATM heists, to find malware samples related to the ATM attack.

In February, Kaspersky Labs reported that attackers managed to hit over 140 enterprises, including banks, telecoms, and government organizations, in the US, Europe and elsewhere with the 'Fileless malware,' but provided few details about the attacks.

According to the researchers, the attacks against banks were carried out using a Fileless malware that resides solely in the memory (RAM) of the infected ATMs, rather than on the hard drive.

Now during the Kaspersky Security Analyst Summit in St. Maarten on Monday, security researchers Sergey Golovanov and Igor Soumenkov delved into the ATM hacks that targeted two Russian banks, describing how the attackers used the fileless malware to gain a strong foothold into bank's systems and cash out, ThreatPost reports.

Mysterious ATM Hack Uncovered by Researchers

Dubbed **ATMitch**, the malware – previously spotted in the wild in Kazakhstan and Russia – is remotely installed and executed on ATMs via its remote administration module, which gives hackers the ability to form an SSH tunnel, deploy the malware, and then sending the command to the ATM to dispense cash.

Since Fileless malware uses the existing legitimate tools on a machine so that no malware gets installed on the system, the ATM treats the malicious code as legitimate software, allowing remote operators to send the command at the time when their associates are present on the infected ATM to pick up the money.

This ATM theft takes just a few seconds to be completed without the operator physically going near the machine. Once the ATM has been emptied, the operator 'signs off,' leaving a very little trace, if any, of the malware.

However, this remote attack is possible only if an attacker tunnels in through the bank's back-end network, a process which required far more sophisticated network intrusion skills…[lire la suite]

Réagissez à cet article

Source : *Hackers stole $800,000 from ATMs using Fileless Malware*