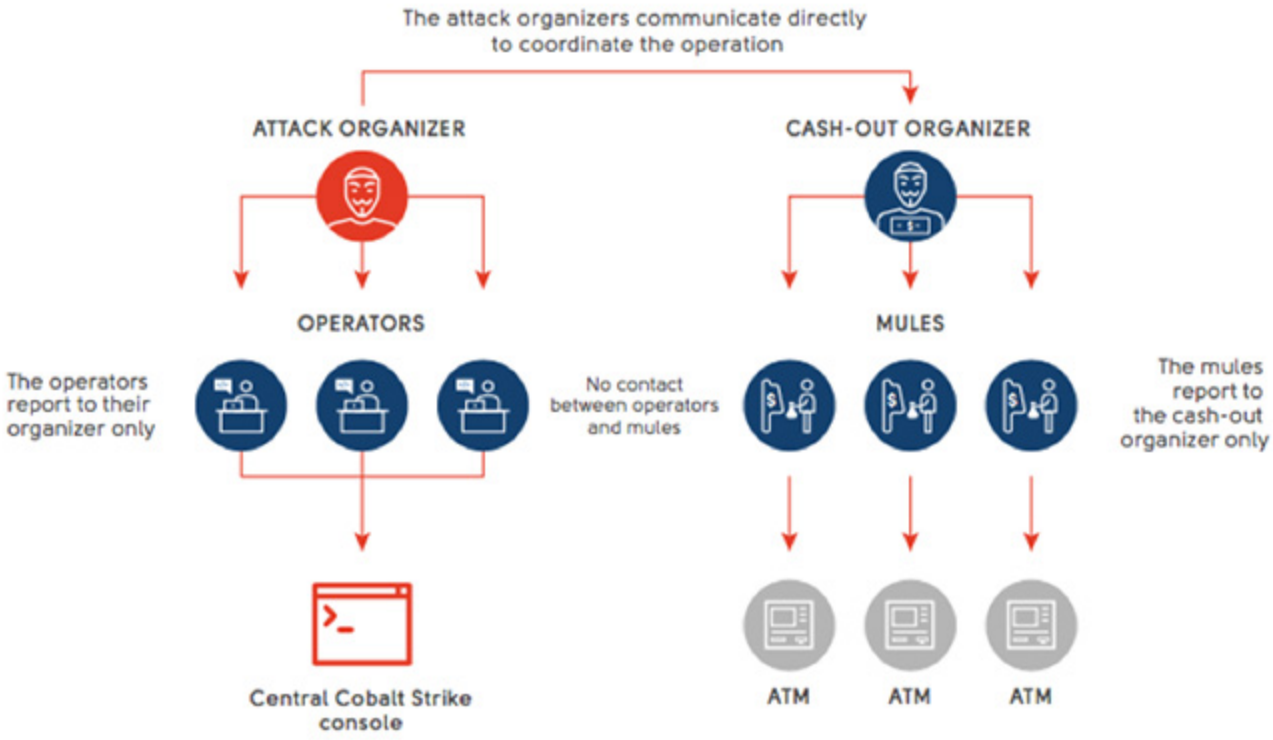
Cobalt hackers executed massive, synchronized ATM heists across Europe, Russia

helpnetsecurity.com/2016/11/22/cobalt-hackers-synchronized-atm-heists/

November 22, 2016

A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Malaysia being raided simultaneously, in the span of a few hours. The group has been active since June 2016, and their latest attacks happened in July and August.



Setup and execution of the attacks

The group sent out spear-phishing emails – purportedly sent by the European Central Bank, the ATM maker Wincor Nixdorf, or other banks – to the target banks' employees. The emails delivered attachments containing an exploit for an MS Office vulnerability.

"If the vulnerability is successfully exploited, the malicious module will inject a payload named Beacon into memory. Beacon is a part of Cobalt Strike, which is a multifunctional framework designed to perform penetration testing. The tool enables perpetrators to deliver the payload to the attacked machine and control it," the researchers explained in a recently released paper.

Additional methods and exploits were used to assure persistence in the targeted machines, to gain domain administrator privileges, and ultimately to obtain access to the domain controller. From that vantage point, they were able to obtain Windows credentials for all client sessions by using the open source Mimikatz tool.

The attackers would ultimately gain control over a number of computers inside the bank's local network. Some of them are connected to the Internet, and others not, but the latter would receive instructions from the central Cobalt Strike console through the former.

"After the local network and domain are successfully compromised, the attackers can use legitimate channels to remotely access the bank, for example, by connecting to terminal servers or via VPN acting as an administrator or a standard user," the researchers noted.

The attacker have also installed a modified version of the TeamViewer remote access tool on the compromised devices, just in case.

Once constant access was assured, the criminals searched for workstations from which they could control ATMs. They would load the ATMs with software that allows them to control cash dispensers.

The final strikes happened in a few hours on the same day, when money mules would go to the targeted ATMs, send an SMS with the code identifying the ATM to a specific phone number, the criminals would make it spit out all the cash, and the mules would leave with it.

Some interesting things about the gang's capabilities

The Cobalt gang uses a number of legitimate, open and closed source tools – Cobalt Strike (a tool for penetration testing), Mimikatz, SDelete (a free tool available on the Microsoft website that deletes files beyond recovery), and TeamViewer.

"Once an ATM is emptied, the operator launches the SDelete program, which removes les used with a special algorithm, which prevents information from being recovered. Thereafter, the ATM restarts," the researchers explained. "In addition, operators disable the bank's internal servers involved in the attack using the MBRkiller malware that removes MBR (master boot record). Such a careful approach significantly complicates further investigation."

The ATM manipulation software also contains code that allows it to record a log containing information about the banknotes dispensed – the gang obviously does not trust the money mules to correctly report the amount that was stolen from each ATM.

Which banks were hit?

IB Group did not name them, but only noted that they are based in Armenia, Belarus, Bulgaria, Estonia, Georgia, Kyrgyzstan, Moldova, the Netherlands, Poland, Romania, Russia, Spain, the UK and Malaysia.

According to Reuters, Diebold Nixdorf and NCR, the world's two largest ATM makers, have provided banks with information on how to prevent or at least minimize the impact of these attacks.

It is unknown how much money the group was able to steal.