Corkow, Metel - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Corkow, Metel

Names	Corkow *(Group-IB)* Metel *(Kaspersky)*
Country	Russia
Motivation	Financial crime
First seen	2011
Description	(Group-IB) In February 2015 the first major successful attack on a Russian trading system took place, when hackers gained unsanctioned access to trading system terminals using a Trojan resulting in trades of more than $400million. The criminals made purchases and sales of US dollars in the Dollar/Ruble exchange program on behalf of a bank using malware. The attack itself lasted only 14 minutes, however, it managed to cause a high volatility in the exchange rate of between 55/62 (Buy/Sell) rubles per 1 dollar instead of the 60-62 stable range. To conduct the attack criminals used the Corkow malware, also known as Metel, containing specific modules designed to conduct thefts from trading systems, such as QUIK operated by ARQA Technologies and TRANSAQ from ZAO “Screen market systems”. Corkow provided remote access to the ITS-Broker system terminal by «Platforma soft» Ltd., which enabled the fraud to be committed. In August 2015 a new incident related to the Corkow (Metel) Trojan was detected. An attack on a bank card systems, which included about 250 banks which used the bank card system to service cash withdrawals from Visa and MasterCard cards under a special tariff. This attack resulted in the hundreds of millions of rubles being stolen via ATMs of the systems members.
Observed	Sectors: Financial. Countries: Argentina, Austria, Belarus, Brazil, Croatia, Cyprus, Denmark, Estonia, France, Germany, Italy, Kazakhstan, Latvia, Mexico, Peru, Poland, Singapore, Spain, Switzerland, Russia, Thailand, Turkey, UK, Ukraine, USA.

Tools used	Corkow, Metel.
Information	<https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf> <https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/> <https://www.kaspersky.com/resource-center/threats/metel>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
