# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:51:55 UTC

Description(Kaspersky) When we first encountered Lurk, in 2011, it was a nameless Trojan. It all started when we became aware of a number of incidents at several Russian banks that had resulted in the theft of large sums of money from customers. To steal the money, the unknown criminals used a hidden malicious program that was able to interact automatically with the financial institution’s remote banking service (RBS) software; replacing bank details in payment orders generated by an accountant at the attacked organization, or even generating such orders by itself.

In 2016, it is hard to imagine banking software that does not demand some form of additional authentication, but things were different back in 2011. In most cases, the attackers only had to infect the computer on which the RBS software was installed in order to start stealing the cash. Russia’s banking system, like those of many other countries, was unprepared for such attacks, and cybercriminals were quick to exploit the security gap.

So we decided to take a closer look at the malware. The first attempts to understand how the program worked gave our analysts nothing. Regardless of whether it was launched on a virtual or a real machine, it behaved in the same way: it didn’t do anything. This is how the program, and later the group behind it, got its name. To “lurk” means to hide, generally with the intention of ambush.

We were soon able to help investigate another incident involving Lurk. This time we got a chance to explore the image of the attacked computer. There, in addition to the familiar malicious program, we found a .dll file with which the main executable file could interact. This was our first piece of evidence that Lurk had a modular structure.

Later discoveries suggest that, in 2011, Lurk was still at an early stage of development. It was formed of just two components, a number that would grow considerably over the coming years.

---