THE LIFE OF PETYA

hacker targets initially hr departments in germany

hacker launches **spam campaign**

user **clicks email** link to dropbox

fake chkdsk screen appears

system **reboots**

overwrites boot drive MBR with malicious loader

loads dropper that installs petya

master file table is **encrypted**

animation leads to **ransomware instructions**

user pays $400 and is given **decrypt code**

system apparently restored

To learn more, check out this blog by SentinelOne Labs:

Reversing Petya - Latest Ransomware Variant

SentinelOne