# New POS Malware PinkKite Takes Flight

threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/

Twitter

Microsoft Word also leveraged in the email campaign, which uses a 22-year-old Office RCE bug. https://t.co/pr5jq08fPx

## Suggested articles

### Dark Web Pricing Skyrockets for Microsoft RDP Servers, Payment-Card Data

Underground marketplace pricing on RDP server access, compromised payment card data and DDoS-For-Hire services are surging.

### Clop Gang Gallops Off with 2M Credit Cards from E-Land

The ransomware group pilfered payment-card data and credentials for over a year, before ending with an attack last month that shut down many of the South Korean retailer’s stores.

## Hacked Security Software Used in Novel South Korean Supply-Chain Attack

Lazarus Group is believed to be behind a spate of attacks that leverage stolen digital certificates tied to browser software that secures communication with government and financial websites in South Korea.

### Discussion

While this article has more detail than another I saw on this, more clarity and less jargon would be useful. Calling out windows as the POS is better than "device". But the researcher seems to be making up useless jargon, "double XOR" is meaningless without explanation. Binary operations 101 (pun intended) means XORing twice undoes the XOR (A = A xor B xor B). So is this BS or are there different keys that change in different instances?

### Subscribe to our newsletter, *Threatpost Today*!

Get the latest breaking news delivered daily to your inbox.

Subscribe now