‘Destructive’ cyberattack hits National Bank of Pakistan

therecord.media/destructive-cyberattack-hits-national-bank-of-pakistan/

November 2, 2021

Image via NBP's Facebook page

- A "destructive" cyberattack has crippled the operations of the National Bank of Pakistan on Friday night.
- The incident impacted the bank's ATMs, internal network, and mobile apps.
- The incident is currently being investigated as a data-wiping malware attack, rather than ransomware.

The National Bank of Pakistan (NBP) has suffered what two sources have described to *The Record* as a “destructive” cyberattack.

The incident, which took place on the night between Friday and Saturday, impacted the bank’s backend systems and affected servers used to interlink the bank’s branches, the backend infrastructure controlling the bank’s ATM network, and the bank’s mobile apps.

While the attack crippled some of these systems, no funds were reported missing, according to the bank and people familiar with the attack and the current investigation.

“Immediate steps were taken to isolate the affected systems,” the bank said in a statement on Saturday.

ATMs and some branches restored by Monday

Recovery efforts were in full swing over the weekend, and by Monday, NBP reported that more than 1,000 branches opened and catered to customers as normal and that all ATMs nationwide had been fully restored.

But despite the clear communication from NBP officials, news of the hack did not stop some scared customers from rushing ATMs to withdraw funds Monday morning.

> There's like a huge rush at the NBP atm at work since yesterday, looks like they haven't restored services and people need cash.
>
> — Essa Malik (@Yeezus_Chwist) November 2, 2021

Together with some inaccurate reporting in local news outlets that up to nine different banks were hacked, the Pakistani government had to step in and issue a statement in order to calm spirits and prevent a run on all Pakistani banks on Monday.

> Some fake news regarding cybersecurity attack on banks is in circulation including remarks attributed to Chief Spokesman, Mr. Abid Qamar. According to these fake news, 9 banks have been affected by the attack and that money has been withdrawn and data stolen. SBP rejects these news. No bank, other than NBP, has faced a cyberattack. Further, no financial loss or data breach has been observed so far. SBP is monitoring the situation closely and it will share any update or information about the incident through its official channels.
>
> *State Bank of Pakistan*

The incident is currently not being investigated as a ransomware attack but rather as a sabotage attempt, according to people familiar with the investigation.

Pakistani security researcher Rafay Baloch shared a screenshot on Twitter earlier today claiming to portray one of the affected NBP systems. The screenshot showed a Windows computer failing to start due to a missing boot configuration file error.

The Record was able to verify the validity of Baloch's claim that the screenshot came from NBP's network.

> The malware was pushed via privileged account in active directory which corrupted the boot sequence of the computers and hence prevented them from booting. (Screenshot Attached) 5/6 pic.twitter.com/qAJhnXTNvu
>
> — Rafay Baloch (@rafaybaloch) November 2, 2021

Tags

- bank
- cyberattack

- National Bank of Pakistan
- NBP
- Pakistan
- wiper

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.