

Netwalker ransomware hits Pakistan's largest private power utility

By Lawrence Abrams

Published: 2020-09-08 · Archived: 2026-04-05 14:43:27 UTC



K-Electric, the sole electricity provider for Karachi, Pakistan, has suffered a Netwalker ransomware attack that led to the disruption of billing and online services.

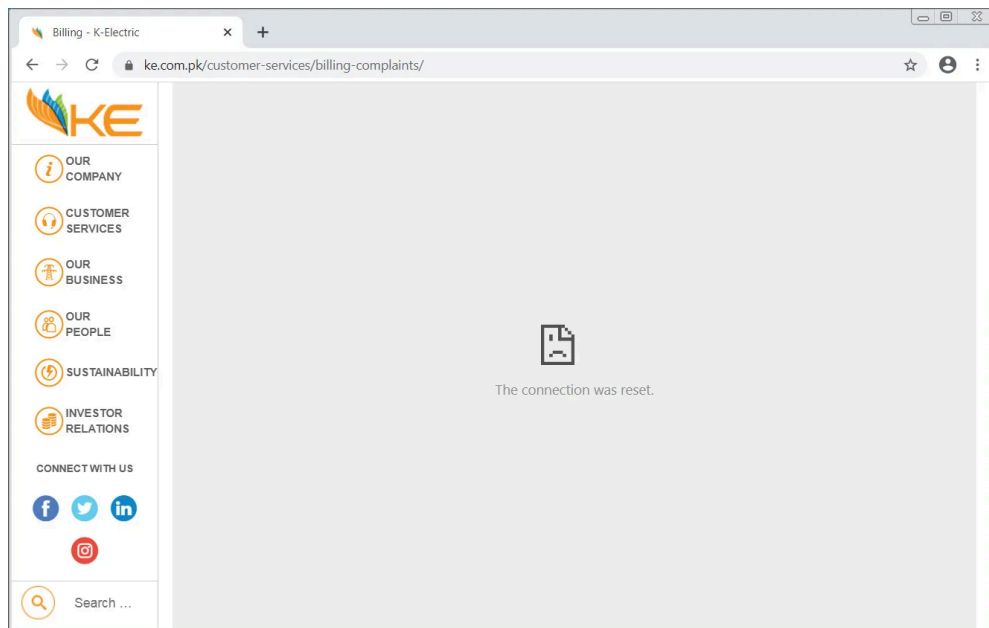
K-Electric is Pakistan's largest power supplier, serving 2.5 million customers and employing over 10 thousand people.

Starting yesterday, K-Electric customers have been unable to access the online services for their account.



Visit Advertiser website [GO TO PAGE](#)

To resolve this issue, K-Electric appears to be trying to reroute users through a staging site, but are currently having difficulties.



Errors accessing account

Ransomware researcher [Ransom Leaks](#), who told BleepingComputer about this attack, was tipped off by a local Pakistani security company that this attack is impacting K-Electric internal services.

According [Rewterz](#), the cyberattack occurred on the morning of September 7th and is disrupting K-Electric's online billing services and not the supply of power.

BleepingComputer has emailed K-Electric about this attack but has not heard back.

In a statement to BleepingComputer, K-Electric states that their initial investigations shows that no data was stolen, but that they continue to work with local law enforcement and IT security experts.

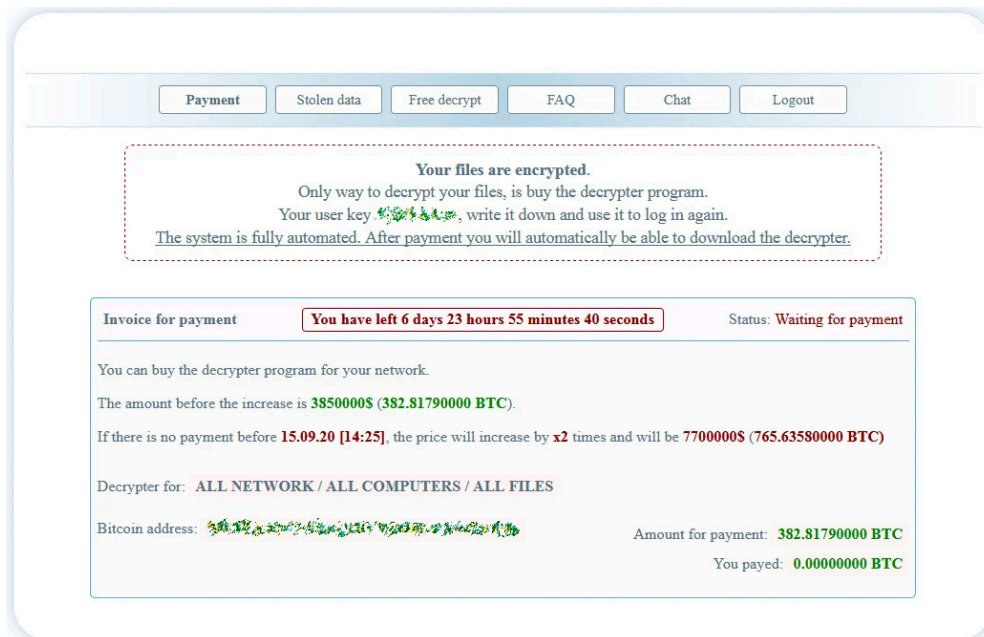
"Karachi, 11th September 2020: Following the attempted cyber incident earlier this week and its on-going forensic investigation, the power utility has confirmed that initial investigation shows all customer data has remained intact and secure, reiterating that critical customer services including bill payment solutions, customer care centres and 118 call-centre are operational and fully functional.

Further forensic analysis is on-going with international IT security experts along with coordination with local law-enforcement officials. In parallel, all efforts are also being made to enhance system robustness. With regard to on-going conjecture that a ransom of USD 3.8 million has been demanded, Mahreen Khan, K-Electric's Chief Marketing and Communication Officer (CMCO), refuted these claims saying, "KE has not been directly approached with any such request and we are categorically not engaged in any such communication."

Netwalker is demanding a \$3.8 million ransom

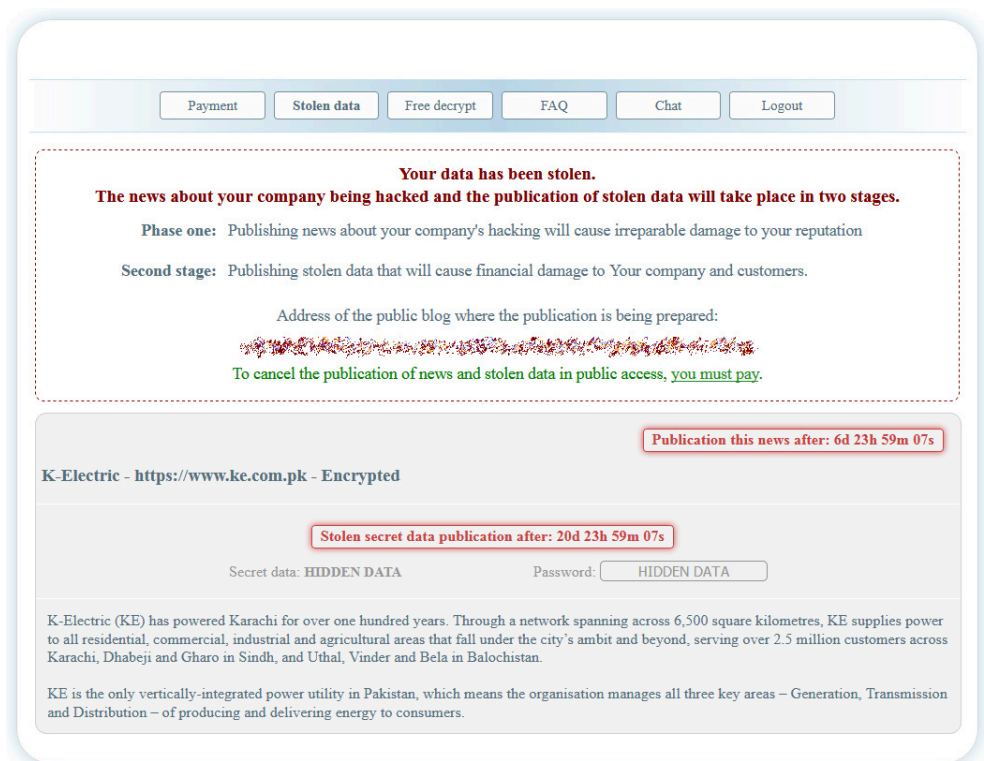
After being told about this attack, BleepingComputer has learned from cybersecurity sources who wish to remain anonymous that the Netwalker ransomware attacked K-Electric.

In a Tor payment page seen by BleepingComputer, the ransomware operators demand a \$3,850,000 ransom payment. If a ransom is not paid within another seven days, the ransom will increase to \$7.7 million.



Tor payment page for K-Electric

The Tor payment site also includes a 'Stolen data' page that states the Netwalker operator stole unencrypted files from K-Electric before performing the attack. This page does not reveal how much or what data was stolen.



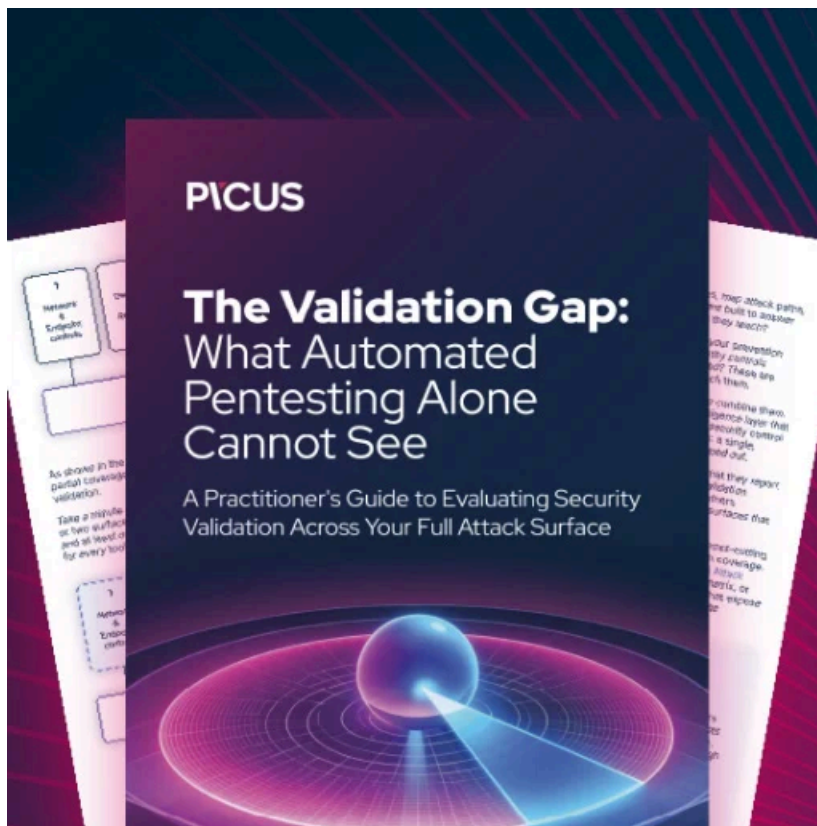
Tor stolen data page for K-Electric

Since the summer of 2019, Netwalker has been actively infecting victims. It wasn't until March 2020, when the threat actors [began recruiting skilled hackers](#) and [focusing entirely on enterprise networks](#), that we began to see widespread attacks.

According to a report by McAfee, this change in tactics has led to the ransomware gang earning \$25 million in just five months.

Recent Netwalker attacks include Argentina's [immigration offices](#), [US government agencies](#), and the [University of California San Francisco \(UCSF\)](#), who paid a \$1.14 million ransom.

Update 9/11/20: Added statement from K-Electric



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/>