Business technology giant Konica Minolta hit by new ransomware

By Lawrence Abrams

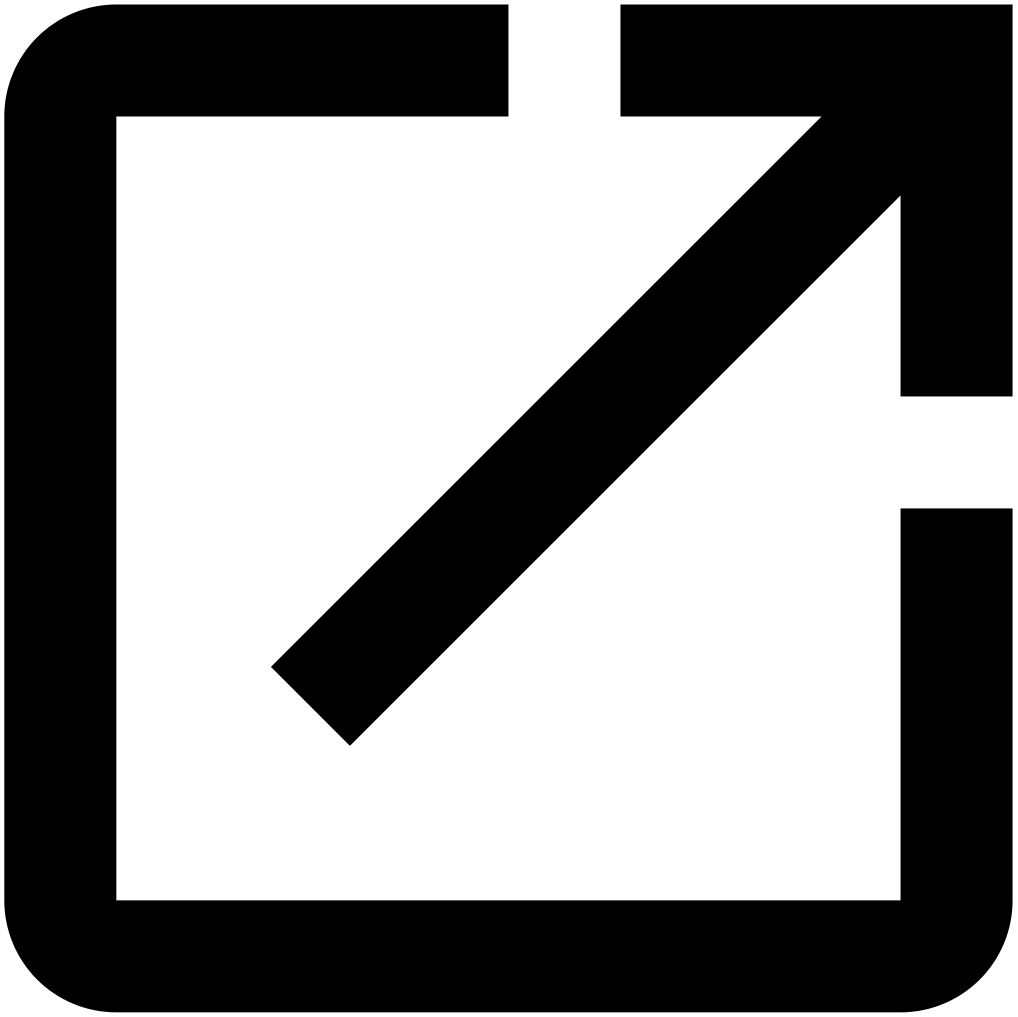
Published: 2020-08-16 · Archived: 2026-04-05 14:01:38 UTC

Business technology giant Konica Minolta was hit with a ransomware attack at the end of July that impacted services for almost a week, BleepingComputer has learned.

Konica Minolta is a Japanese multinational business technology giant with almost 44,000 employees and over $9 billion in revenue for 2019.

The company offers a wide variety of services and products ranging from printing solutions, healthcare technology, to providing managed IT services to businesses.


DIE LINKE.
0:00



It started with an outage

On July 30th, 2020, customers began reporting that Konica Minolta's product supply and support site was not accessible and was displaying the outage message shown below.

The Konica Minolta MyKMBS customer portal is temporarily unavailable. We are working hard to resolve the issue and apologize for any inconvenience this may have caused you. If you need immediate assistance for service, please call our Global Customer Services at 1-800-456-5664 (US) or 1-800-263-4410 (Canada).

The site remained down for almost a week, and customers stated that they could not get a straight answer as to what was causing the outage.

Some Konica Minolta printers were also displaying a 'Service Notification Failed' error, which led Konica Minolta to update their outage message to contain a link to this support document.

After some customers stated that their Konica contacts indicated a breach caused the outage, BleepingComputer attempted to contact the company numerous times via email and phone calls.

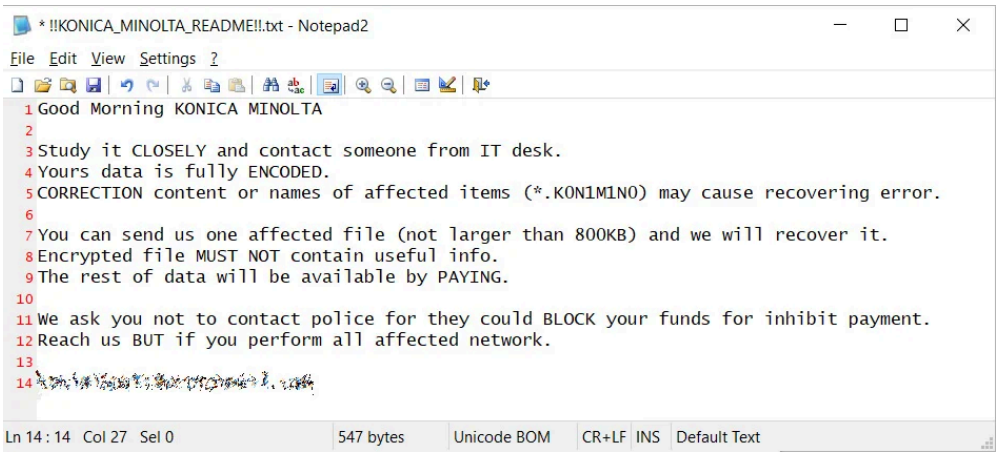
BleepingComputer never received a response to our inquiries.

Do you have information about this attack or another ransomware attack? If you have information to share, contact us securely on Signal at +1 (646) 961-3731, via email at lawrence.abrams@bleepingcomputer.com, or using our tips form.

Konica Minolta hit by the RansomEXX ransomware

Soon after, a source shared a copy of the ransom note used in the attack on Konica Minolta with BleepingComputer.

This ransom note is named '!!KONICA_MINOLTA_README!!.txt,' and as you can see below, clearly targets the Konica Minolta company.



Konica Minolta ransom note

BleepingComputer also learned that devices in the company were encrypted, and files had the '.K0N1M1N0' extension appended to them.

This ransom note belongs to a relatively new ransomware called RansomEXX, which we reported on at the end of June 2020 when it was used in an attack on the Texas Department of Transportation.

Like other enterprise-targeting ransomware operations, RansomEXX is human-operated, which entails threat actors compromising a network, and over time, spreading to other devices until they gain administrator credentials.

Once they gain admin rights and access to the Windows domain controller, they deploy the ransomware on the network and encrypt all of its devices.

Based on the RansomEXX ransom notes seen by BleepingComputer, it does not appear that the ransomware operation steals data before encrypting devices.

This tactic may be adopted, though, as the ransomware operation grows.

Source: https://www.bleepingcomputer.com/news/security/business-technology-giant-konica-minolta-hit-by-new-ransomware/