Ransomware Hit ATM Giant Diebold Nixdorf

krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/

Diebold Nixdorf, a major provider of automatic teller machines (ATMs) and payment technology to banks and retailers, recently suffered a ransomware attack that disrupted some operations. The company says the hackers never touched its ATMs or customer networks, and that the intrusion only affected its corporate network.

Canton, Ohio-based Diebold [NYSE: DBD] is currently the largest ATM provider in the United States, with an estimated 35 percent of the cash machine market worldwide. The 35,000-employee company also produces point-of-sale systems and software used by many retailers.

According to Diebold, on the evening of Saturday, April 25, the company's security team discovered anomalous behavior on its corporate network. Suspecting a ransomware attack, Diebold said it immediately began disconnecting systems on that network to contain the spread of the malware.

Sources told KrebsOnSecurity that Diebold's response affected services for over 100 of the company's customers. Diebold said the company's response to the attack did disrupt a system that automates field service technician requests, but that the incident did not affect customer networks or the general public.

"Diebold has determined that the spread of the malware has been contained," Diebold said in a written statement provided to KrebsOnSecurity. "The incident did not affect ATMs, customer networks, or the general public, and its impact was not material to our business. Unfortunately, cybercrime is an ongoing challenge for all companies. Diebold Nixdorf takes the security of our systems and customer service very seriously. Our leadership has connected personally with customers to make them aware of the situation and how we addressed it."

NOT SO PRO LOCK

An investigation determined that the intruders installed the **ProLock** ransomware, which experts say is a relatively uncommon ransomware strain that has gone through multiple names and iterations over the past few months.

For example, until recently ProLock was better known as "PwndLocker," which is the name of the ransomware that infected servers at Lasalle County, Ill. in March. But the miscreants behind PwndLocker rebranded their malware after security experts at Emsisoft released a

tool that let PwndLocker victims decrypt their files without paying the ransom.

Diebold claims it did not pay the ransom demanded by the attackers, although the company wouldn't discuss the amount requested. But **Lawrence Abrams** of *BleepingComputer* said the ransom demanded for ProLock victims typically ranges in the six figures, from $175,000 to more than $660,000 depending on the size of the victim network.

Fabian Wosar, Emsisoft's chief technology officer, said if Diebold's claims about not paying their assailants are true, it's probably for the best: That's because current versions of ProLock's decryptor tool will corrupt larger files such as database files.

As luck would have it, Emsisoft does offer a tool that fixes the decryptor so that it properly recovers files held hostage by ProLock, but it only works for victims who have already paid a ransom to the crooks behind ProLock.

"We do have a tool that fixes a bug in the decryptor, but it doesn't work unless you have the decryption keys from the ransomware authors," Wosar said.

WEEKEND WARRIORS

BleepingComputer's Abrams said the timing of the attack on Diebold — Saturday evening — is quite common, and that ransomware purveyors tend to wait until the weekends to launch their attacks because that is typically when most organizations have the fewest number of technical staff on hand. Incidentally, weekends also are the time when the vast majority of ATM skimming attacks take place — for the same reason.

"After hours on Friday and Saturday nights are big, because they want to pull the trigger [on the ransomware] when no one is around," Abrams said.

Many ransomware gangs have taken to stealing sensitive data from victims before launching the ransomware, as a sort of virtual cudgel to use against victims who don't immediately acquiesce to a ransom demand.

Armed with the victim's data — or data about the victim company's partners or customers — the attackers can then threaten to publish or sell the information if victims refuse to pay up. Indeed, some of the larger ransomware groups are doing just that, constantly updating blogs on the Internet and the dark Web that publish the names and data stolen from victims who decline to pay.

So far, the crooks behind ProLock haven't launched their own blog. But Abrams said the crime group behind it has indicated it is at least heading in that direction, noting that in his communications with the group in the wake of the Lasalle County attack they sent him an image and a list of folders suggesting they'd accessed sensitive data for that victim.

“I’ve been saying this ever since last year when the Maze ransomware group started publishing the names and data from their victims: Every ransomware attack has to be treated as a data breach now,” Abrams said.