KillDisk Disk-Wiping Malware Adds Ransomware Component

By Catalin Cimpanu

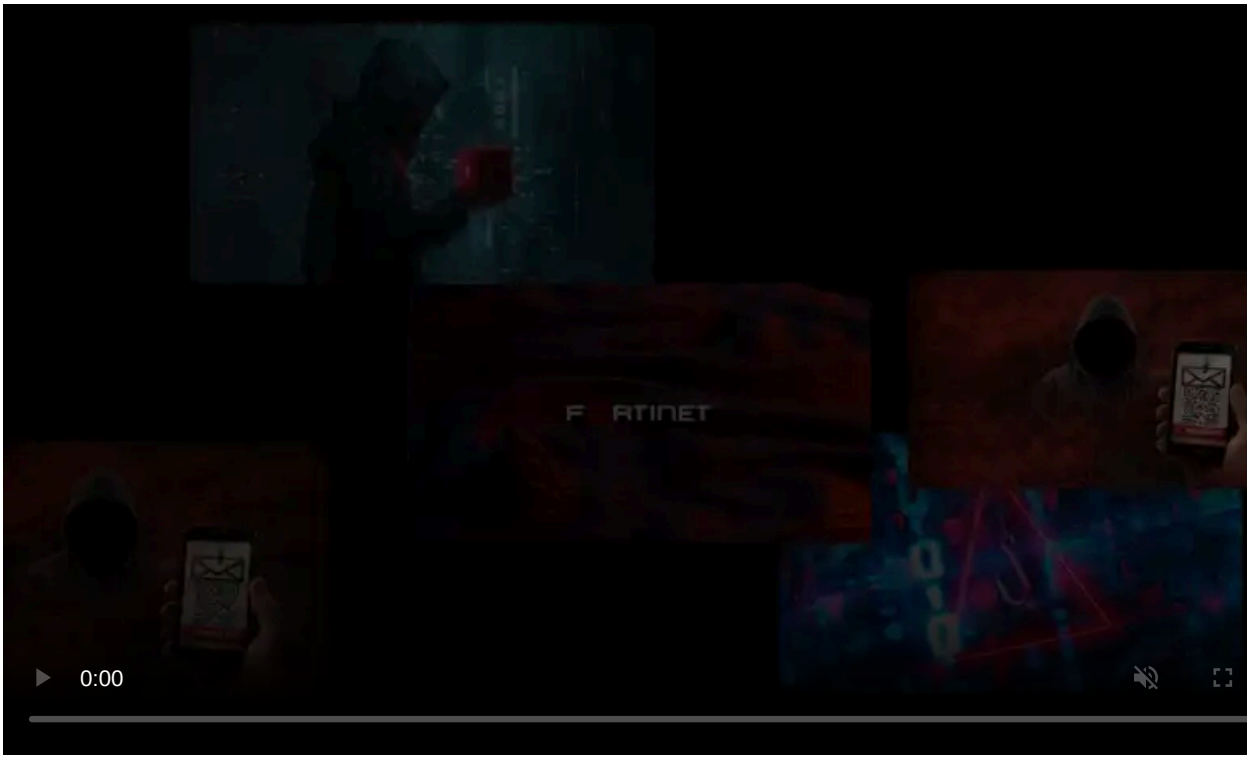
Published: 2016-12-29 · Archived: 2026-04-06 02:04:28 UTC

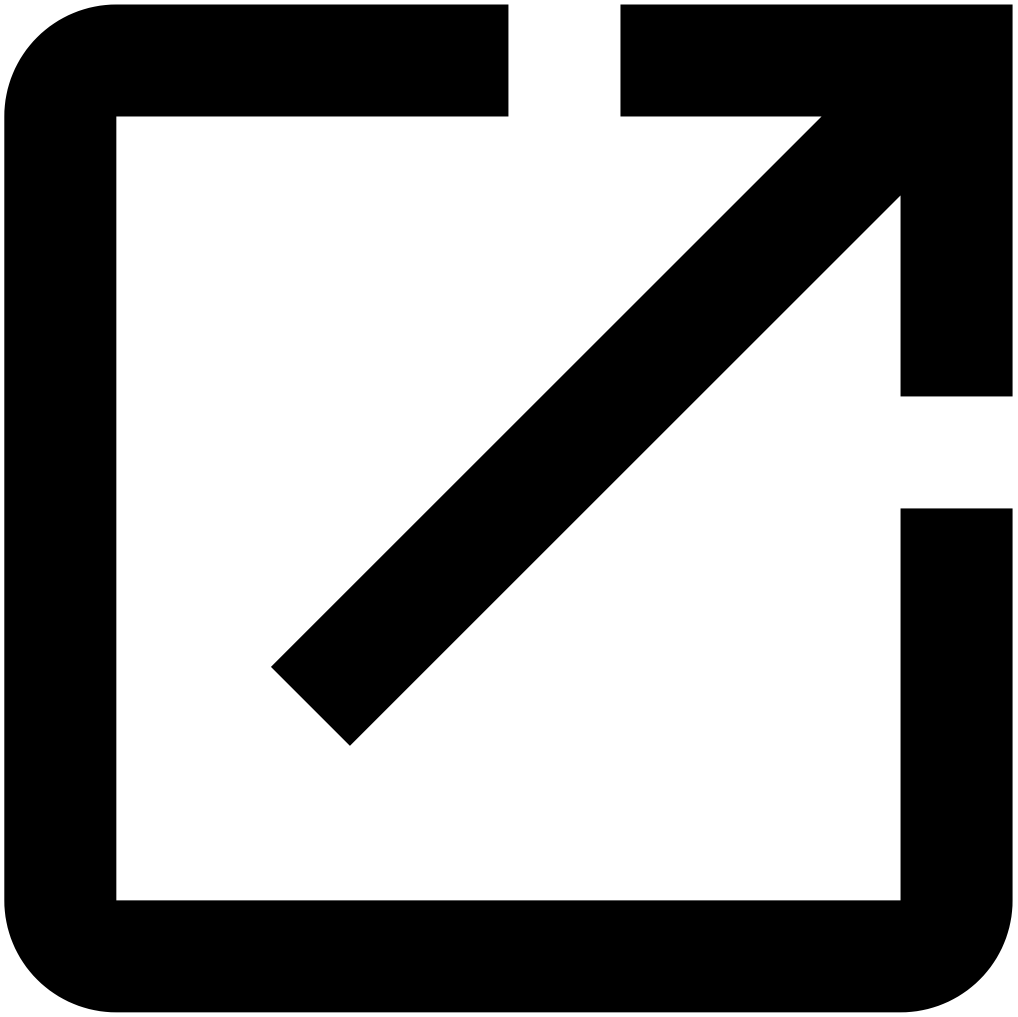
A malware family previously used to sabotage computers by deleting and rewriting files has added a ransomware component, now encrypting files and demanding a huge ransom.

Until now, the KillDisk malware family has been only associated with cyber-espionage and cyber-sabotage operations, most of which had been carried out in the industrial sector.

The group behind this malware is known under two names: Sandworm or TeleBots.

The Sandworm gang is known for its work on the Sandworm malware that targeted and sabotaged industrial control systems (ICS) and supervisory control and data acquisition (SCADA) industrial devices in the US in 2014.


F RTINET
0:00



KillDisk previously used in cyber-espionage and cyber-sabotage operations

It is believed that the Sandworm gang later evolved into the TeleBots gang, which developed the TeleBots backdoor trojan, and the KillDisk disk-wiping malware.

KillDisk gained some notoriety in the past two years because it was also used in 2015 and 2016 when another gang, the BlackEnergy cyber-espionage group used the malware to attack and sabotage Ukrainian companies activating in the energy, mining, and media sectors.

Currently, the connection between the BlackEnergy, a clearly state-sponsored cyber-espionage group, and the TeleBots/Sandworm gang is unknown.

KillDisk used recently against Ukrainian banks

What it is known is that the TeleBots gang has been involved in cyber-sabotage operations that have crippled the activities of several businesses around the world.

The most recent of these attacks were against Ukrainian banks. These attacks infected bank workers with the TeleBots backdoor trojan via malicious email attachments. TeleBots is a unique malware because it uses the Telegram protocol to communicate with its operators.

After collecting data from infected systems, such as passwords and important files, the TeleBots gang would deploy the KillDisk component, which deleted crucial system files, replaced files, and rewrote file extensions. The purpose was to make the computer unbootable and also hide the intruder's tracks.

In the recent attacks against Ukrainian banks, the KillDisk malware had also been altered to use the Windows GDI (Graphics Device Interface) and draw a picture inspired by the Mr. Robot TV series, showing the logo of the FSociety hacktivism group, portrayed in the show.

Picture displayed by KillDisk component [Source: ESET]

At one point in the TV show, the FSociety group also infected the eCorp bank network with ransomware. The same is now true for the TeleBots gang, who added a ransomware component to KillDisk, as an alternative to disk-wiping operations.

KillDisk ransomware demands over $215,000

The reasons for this change is that it's much easier to hide the gang's tracks if KillDisk would pose as ransomware.

Targets would think they suffered a mundane ransomware infection, and they wouldn't go looking for the TeleBots backdoor or other data exfiltration malware. Targets would restore from backup or pay the ransom and move on, trying to avoid the bad publicity.

According to the team at CyberX, the KillDisk ransomware component shows the following message on infected computers and asks for a huge ransom demand of 222 Bitcoin, which is about $215,000.

KillDisk ransom note [Source: CyberX]

The KillDisk encryption system is also very robust, encrypting each file with its own AES key, and then encrypting the AES key with a public RSA-1028 key.

To unlock the files, the victim must contact the TeleBots gang via an email address, pay the ransom, and receive the private RSA key that decrypts all the files.

The ransom demand is huge compared to other ransomware variants, but higher ransom demands are normal in targeted attacks such as these, where the crooks might attempt to extort the target in subsequent email conversations, threatening to dump sensitive files they stole via the TeleBots backdoor.
