HelloKitty ransomware behind CD Projekt Red cyberattack, data theft

By Lawrence Abrams

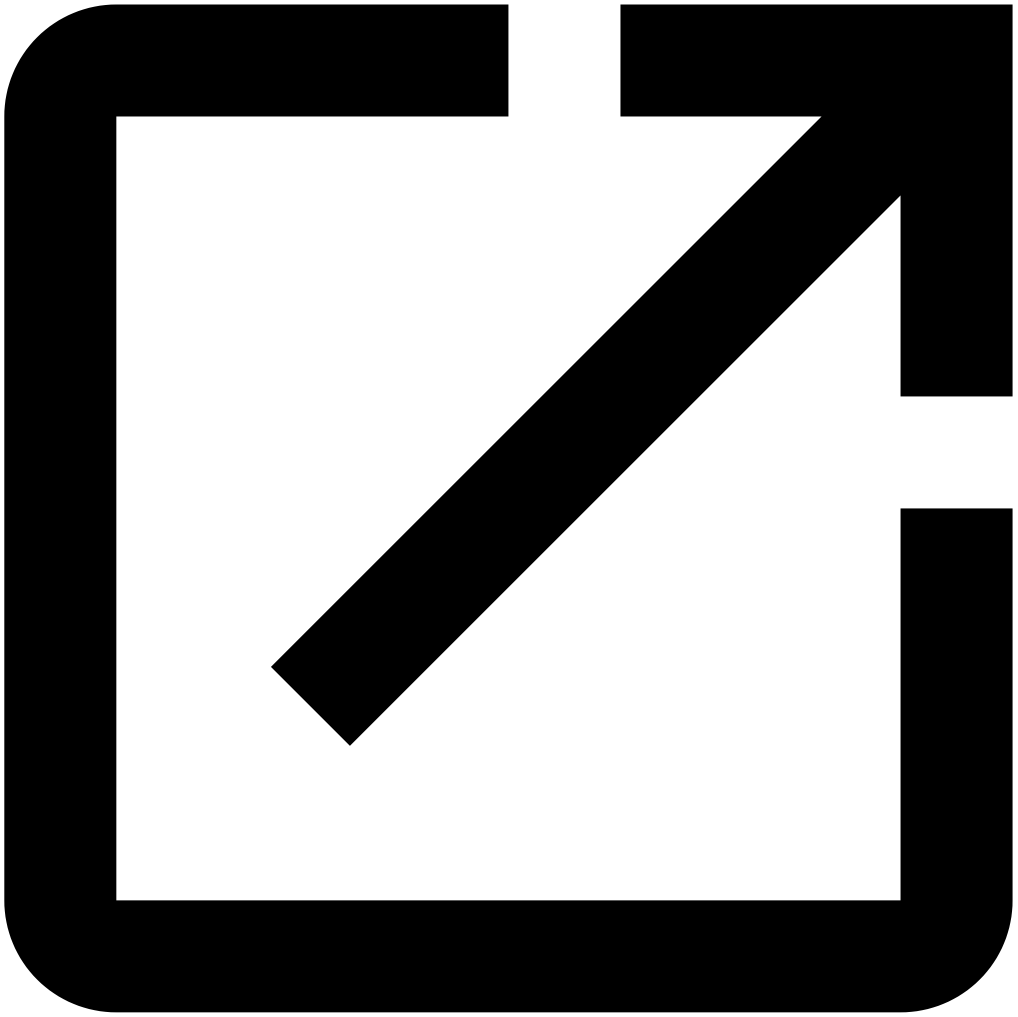
Published: 2021-02-09 · Archived: 2026-04-05 13:04:39 UTC

The ransomware attack against CD Projekt Red was conducted by a ransomware group that goes by the name 'HelloKitty,' and yes, that's the name the threat actors utilize.

Today, CD Project disclosed that they were the target of a ransomware attack that encrypted devices on their network and led to the theft of unencrypted files.

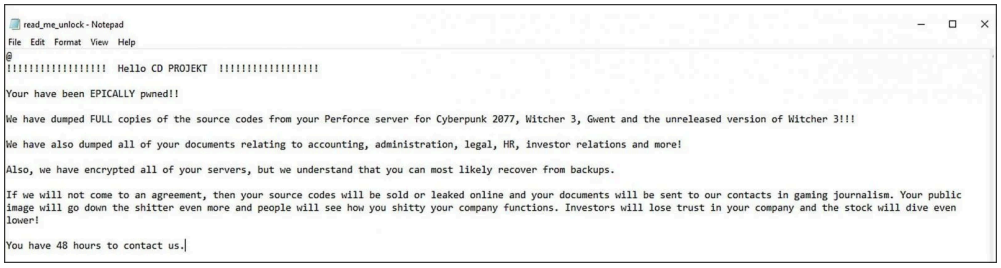
"Yesterday we discovered that we have become a victim of a targeted cyber attack, due to which some of our internal systems have been compromised.


DIE LINKE.
0:00



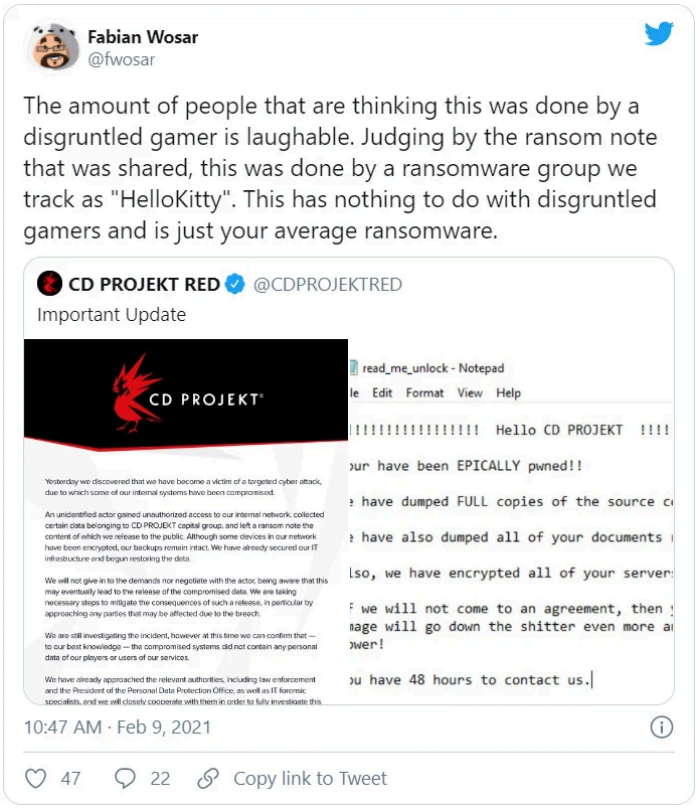
"An unidentified actor gained unauthorized access to our internal network, collected certain data belong to CD PROJEKT capital group, and left a ransom note the content of which we release to the public. Although some devices in our network have been encrypted, our backups remain intact. We have already secured our IT infrastructure and begun restoring the data," CD Projekt disclosed today.

As part of the announcement, CD Projekt also released a screenshot of the ransom note that was left behind by the attackers.



Ransom note from CD Projekt Red ransomware attack

According to Emisoft's Fabian Wosar, the ransomware responsible for this cyberattack is called 'HelloKitty.'



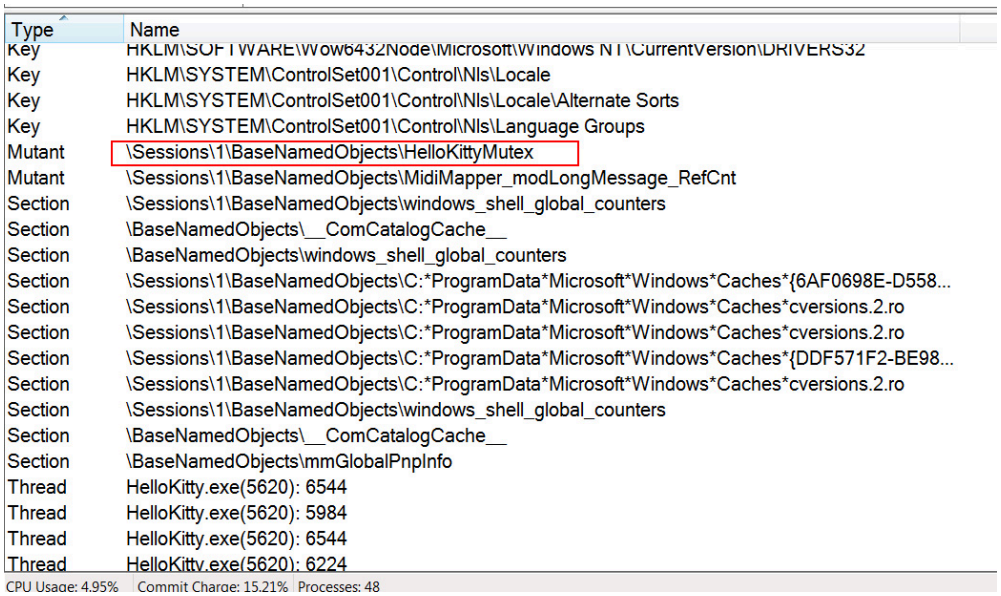
This ransomware operation has been active since November 2020 and has targeted other large companies, such as the Brazilian power company CEMIG last year.

```
If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Sig
```

What we know about the HelloKitty group

As the HelloKitty malware is not particularly active, there is not much information about the ransomware. However, BleepingComputer was able to gain access to a sample after a victim posted it in our forums in November 2020.

The HelloKitty ransomware is named after a mutex named 'HelloKittyMutex' used when the malware executable is launched.



HelloKittyMutex mutex shown in Process Explorer

Once launched, HelloKitty will repeatedly run taskkill.exe to terminate processes associated with security software, email servers, database servers, backup software, and accounting software, such as QuickBooks.

An example of the taskkill.exe command is below:

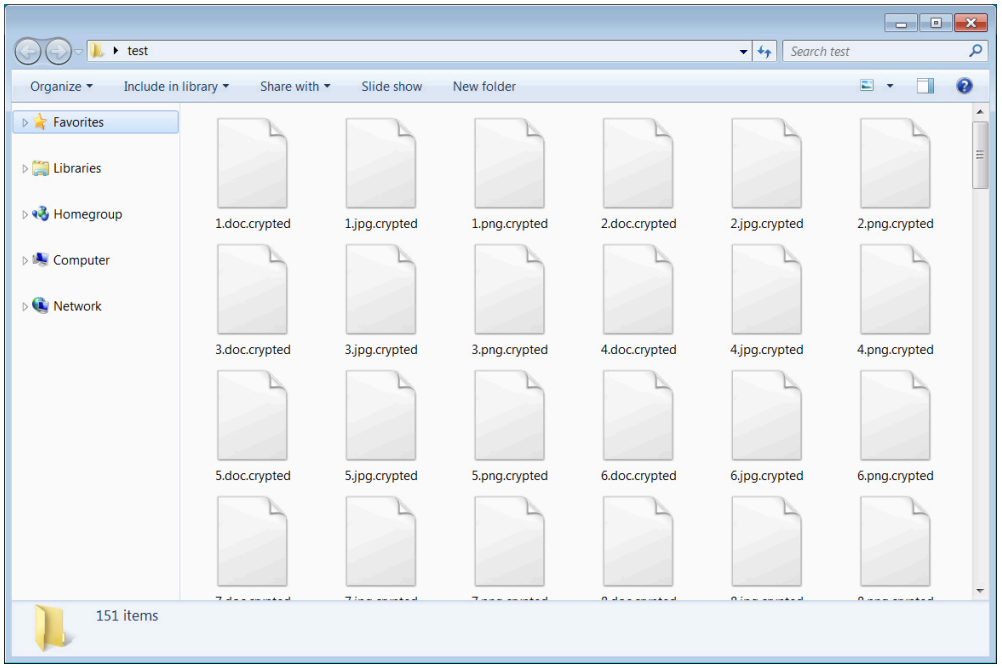
```
"C:\Windows\System32\taskkill.exe" /f /im postg*
```

The ransomware will also attempt to shut down related Windows services with the net stop command, like the following:

```
"C:\Windows\System32\net.exe" stop MSSQLServerADHelper100
```

In total, HelloKitty targets over 1,400 processes and Windows services.

After it has shut down the various targeted processes and services, it will begin to encrypt files on the computer. When encrypting files, it will append the **.crypted** extension to an encrypted file's name, as shown below.



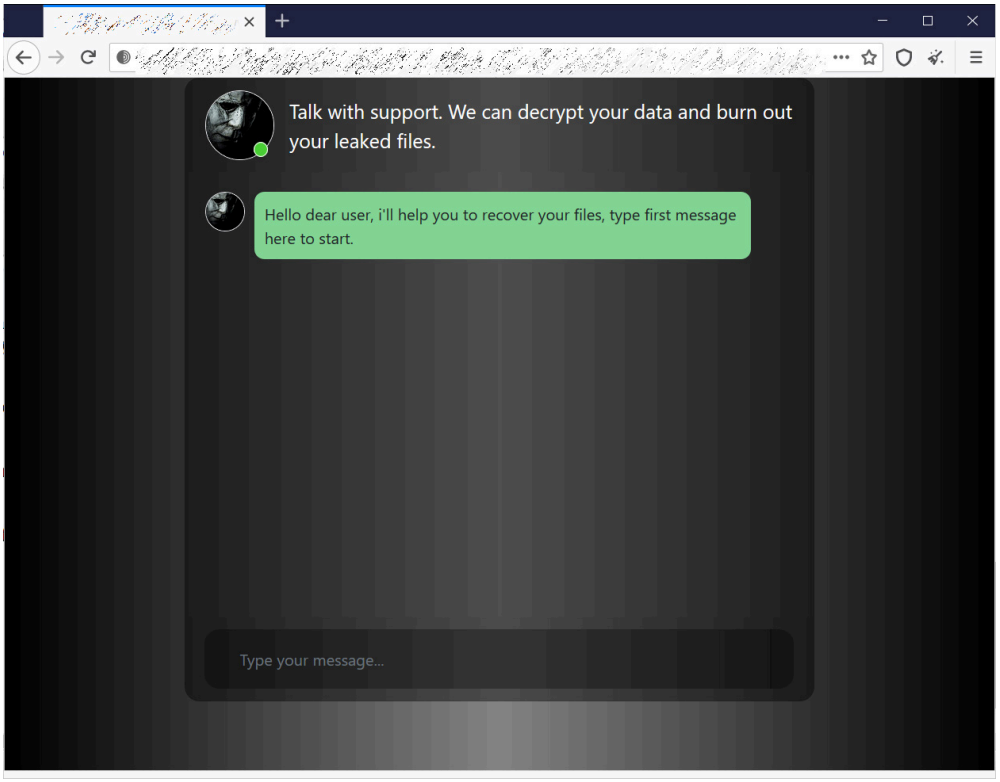
HelloKitty encrypted files

If the ransomware encounters a locked file when encrypting, it will use the Windows Restart Manager API to automatically terminate processes or Windows services that are keeping the file open.

As each HelloKitty executable is customized with a custom ransom note, the ransom note name may change depending on the victim. For the HelloKitty victims that BleepingComputer has seen, the ransom name is typically named 'read_me_unlock.txt,' which was also the same name used in the CD Projekt cyberattack.

These ransom notes are customized on a per-victim basis to include the amount of data that was stolen, what data was targeted, and in many cases, the name of the company. This custom text indicates that the attackers lurk in the compromised network for some time as they steal data, and when finished, deploy the ransomware.

Enclosed in the ransom note is a Tor dark web URL that victims can visit to negotiate with the ransomware actors. This Tor URL is different for each victim and contains a simple chat interface to talk to the threat actors.



Tor chat site

It is unknown how great the ransom demands are for this ransomware gang and whether victims have paid in the past.

At this time, no known weakness could allow a victim to decrypt their files for free.

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.
