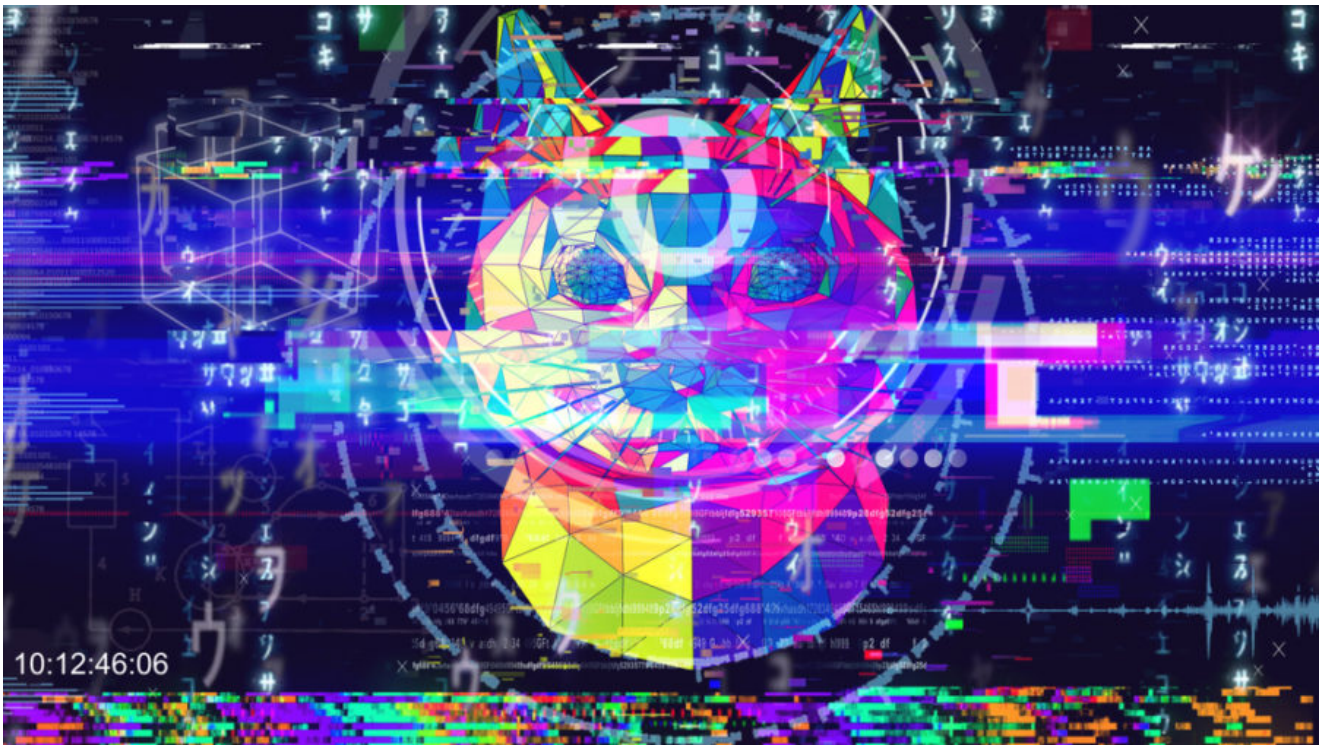
HelloKitty: When Cyberpunk met cy-purr-crime

blog.malwarebytes.com/threat-spotlight/2021/03/hellokitty-when-cyberpunk-met-cy-purr-crime/

Jovi Umawing March 18, 2021



On February 9, after discovering a compromise, CD Projekt Red (CDPR) announced to its 1+ million followers on Twitter that it was the victim of a ransomware attack against its systems (and made it clear they would not yield to the demands of the threat actors, nor negotiate).

Cyberpunk 2077, the latest game released by CD Projekt Red and once hailed as the “most anticipated game of the decade”, was released in December 2020 with many calling it an “unplayable mess”.

No surprise then that some people suspected that enraged gamers were hitting back at the company for releasing the game in that state. But infamous ransomware hunter Fabian Wosar (@fwosar), of Emsisoft begged to differ.

> The amount of people that are thinking this was done by a disgruntled gamer is laughable. Judging by the ransom note that was shared, this was done by a ransomware group we track as "HelloKitty". This has nothing to do with disgruntled gamers and is just your average ransomware. https://t.co/RYJOxWc5mZ
>
> — Fabian Wosar (@fwosar) February 9, 2021

Although what he said was an informed claim, we cannot say for sure what hit CDPR until a ransomware sample is retrieved and analyzed. Nevertheless, the name-check was enough to put the HelloKitty ransomware family in the headlines.

HelloKitty ransomware

The HelloKitty ransomware, also known as Kitty ransomware, was first seen in November 2020, a few months after the first variants of Egregor were spotted in the wild.

CEMIG (Companhia Energética de Minas Gerais), a Brazilian electric power company, revealed on Facebook in late December 2020 that it was a victim of a cyberattack. Succeeding reports revealed that HelloKitty was the ransomware behind it, and that this ransomware strain was used to steal a large amount of data about the company. The attack didn't cause any damage, however, but it caused the company to suspend its WhatsApp and SMS channels, and its online app service.

This ransomware family was named after a mutex it used called "HelloKittyMutex."

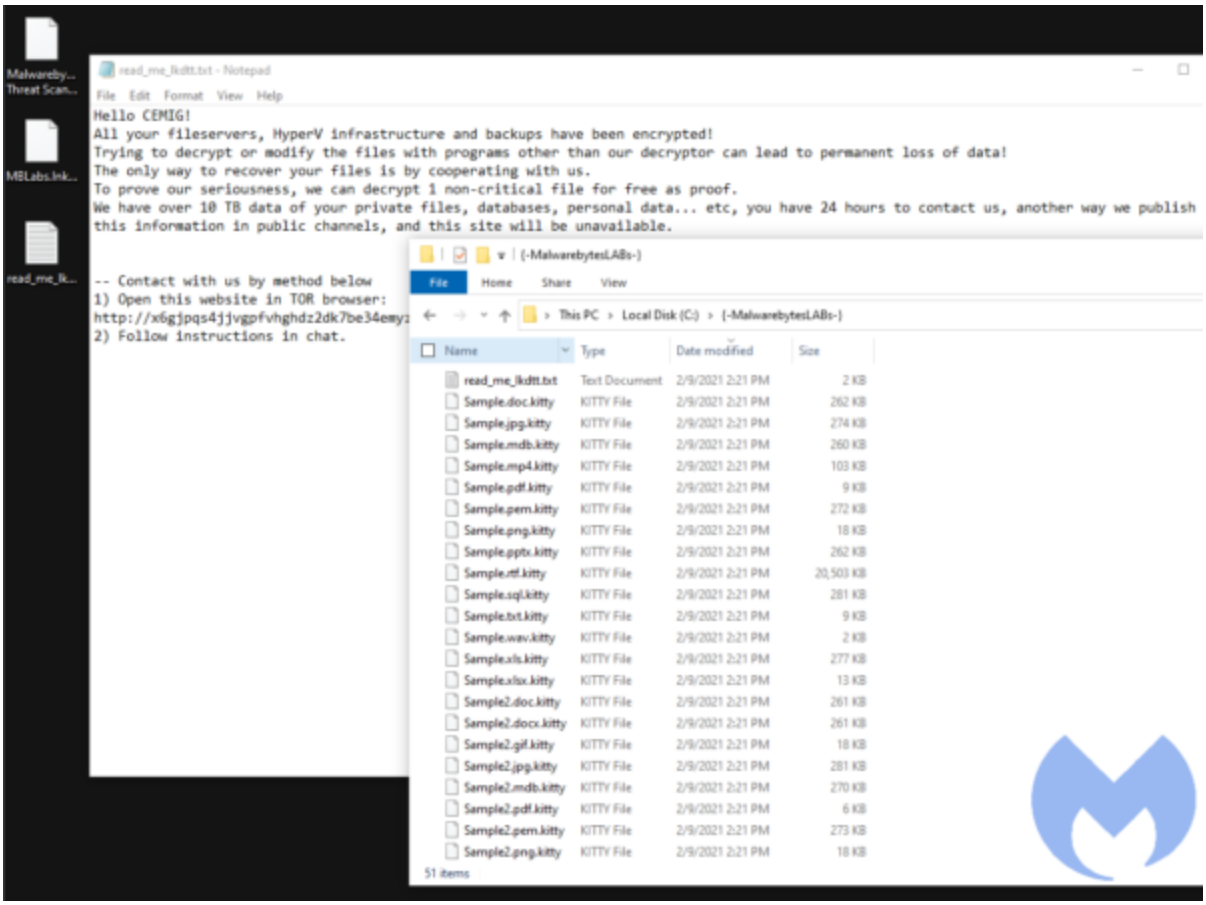
Some researchers refer to HelloKitty as DeathRansom—a ransomware family that, based on its earlier variants, merely renames target files and doesn't encrypt them. We speculate, however, that HelloKitty was built from DeathRansom. As such, Malwarebytes detects this ransomware as Ransom.DeathRansom.

The threat actors behind HelloKitty ransomware aren't as active as some other threat groups, so there is little information about it. Below is what we know so far.

Infection vector

According to SentinelLabs, current intelligence suggests that HelloKitty arrives via phishing emails or via secondary infection from an initial malware attack.

Symptoms



HelloKitty ransom note

Systems affected by HelloKitty ransomware display the following symptoms:

1. Terminated processes and Windows services. Once it reaches an affected system and executes, HelloKitty terminates processes and Windows services that may interfere with its operation. These processes are generally associated with security software, backup software, accounting software, email servers, and database servers (to name a few). Overall, it can target and terminate over 1,400 processes and services.

It performs the termination process using *taskkill.exe* and *net.exe*, two legitimate Microsoft Windows programs.

SentinelLabs also notes that if there are processes HelloKitty cannot terminate using these executables, it then taps into Windows's Restart Manager to perform the termination.

2. Encrypted files with .`KITTY` or .`CRYPTED` file extensions. On Windows systems, HelloKitty ransomware uses a combination of AES-128 + NTRU encryption. On Linux systems, it uses the combination AES-256 + ECDH. These encryption recipes are not known to have any weaknesses, making decryption impossible without a key.

Encrypted files will have the `.kitty` or `.crypted` file extension appended to the file names. For example, an encrypted `sample.mdb` file will either have the `sample.mdb.kitty` or `sample.mdb.crypted` file names.

3. Targeted ransom note. The HelloKitty ransom note is usually a plain text file bearing either the name `read_me_lkdtt.txt` or `read_me_unlock.txt` that references its target and/or its environment. For a sample content of the note, below is a portion of the CEMIG ransom note as follows:

> Hello CEMIG!
>
> All your fileservers, HyperV infrastructure and backups have been encrypted!
>
> Trying to decrypt or modify the files with programs other than our decryptor can lead to permanent loss of data!
>
> The only way to recover your files is by cooperating with us.
>
> To prove our seriousness, we can decrypt 1 non-critical file for free as proof. We have over 10 TB data of your private files, databases, personal data… etc, you have 24 hours to contact us, another way we publish this information in public channels, and this site will be unavailable.

The ransom note also includes a `.onion` URL that victims can open using the Tor browser. URLs are different for each victim.

4. Deleted shadow copies. Similar to other well-known ransomware families like Phobos and Sodinokibi, HelloKitty deletes shadow copies of encrypted files on affected systems to prevent victims from restoring them.

Indicators of Compromise (IOCs)

Tor Onion URLs:

- 6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion
- x6gjpqs4jjvgpfvhghdz2dk7be34emyzluimticj5s5fexf4wa65ngad.onion

SHA256 hashes:

- 78afe88dbfa9f7794037432db3975fa057eae3e4dc0f39bf19f2f04fa6e5c07c
- fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb
- c7d6719bbfb5baaadda498bf5ef49a3ada1d795b9ae4709074b0e3976968741e
- 9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0
- 38d9a71dc7b3c257e4bd0a536067ff91a500a49ece7036f9594b042dd0409339