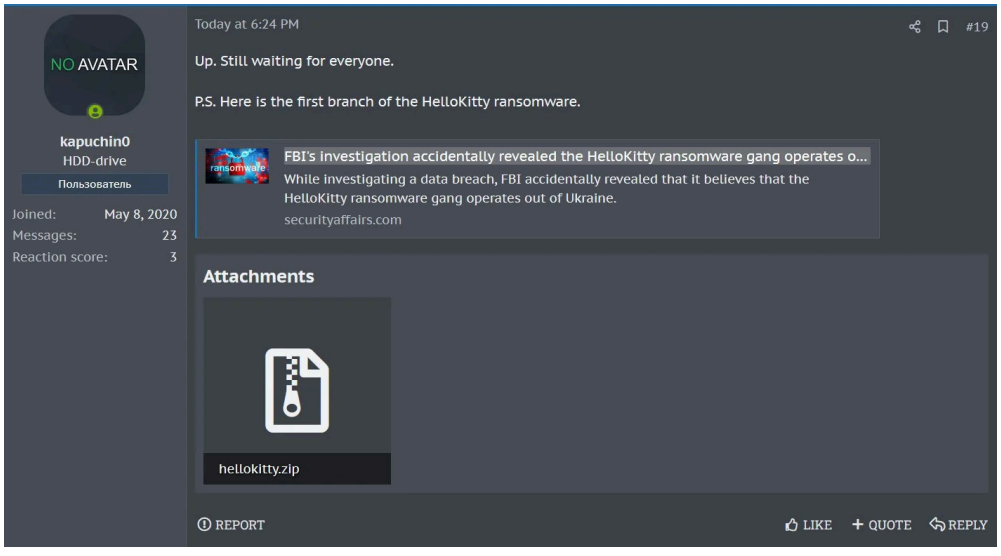
HelloKitty ransomware source code leaked on hacking forum

By Lawrence Abrams

Published: 2023-10-09 · Archived: 2026-04-05 19:03:15 UTC

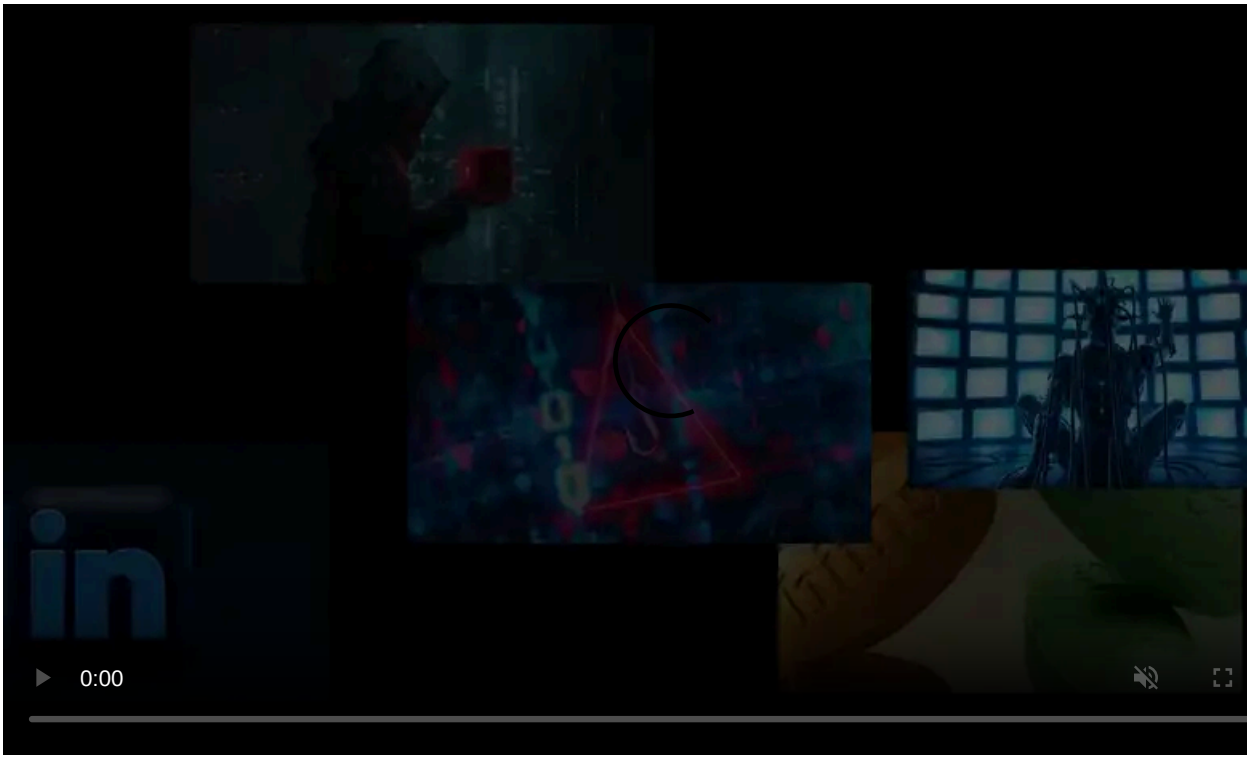
A threat actor has leaked the complete source code for the first version of the HelloKitty ransomware on a Russian-speaking hacking forum, claiming to be developing a new, more powerful encryptor.

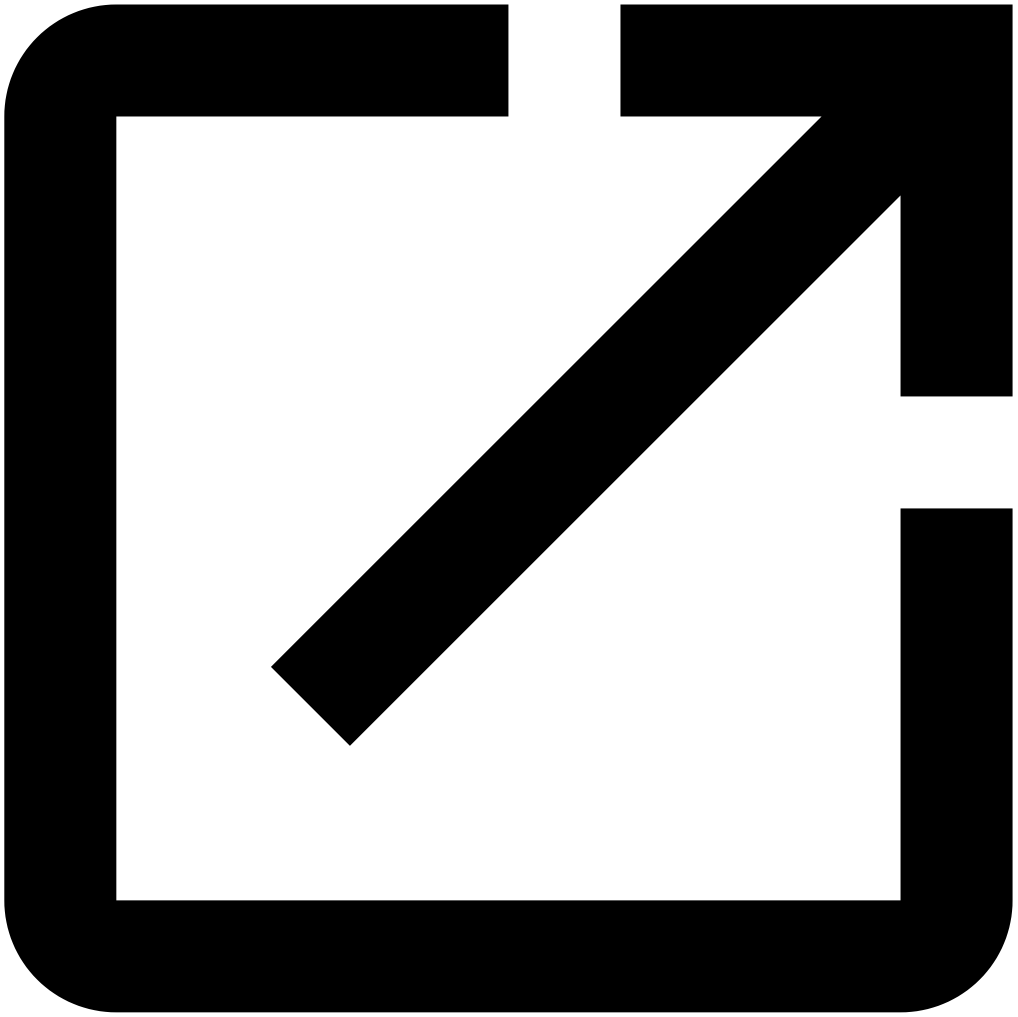
The leak was first discovered by cybersecurity researcher 3xp0rt, who spotted a threat actor named 'kapuchin0' releasing the "first branch" of the HelloKitty ransomware encryptor.



Forum post leaking HelloKitty encryptor
Source: 3xp0rt

While the source code was released by someone named 'kapuchin0,' 3xp0rt told BleepingComputer that the threat actor also utilizes the alias 'Gookee.'

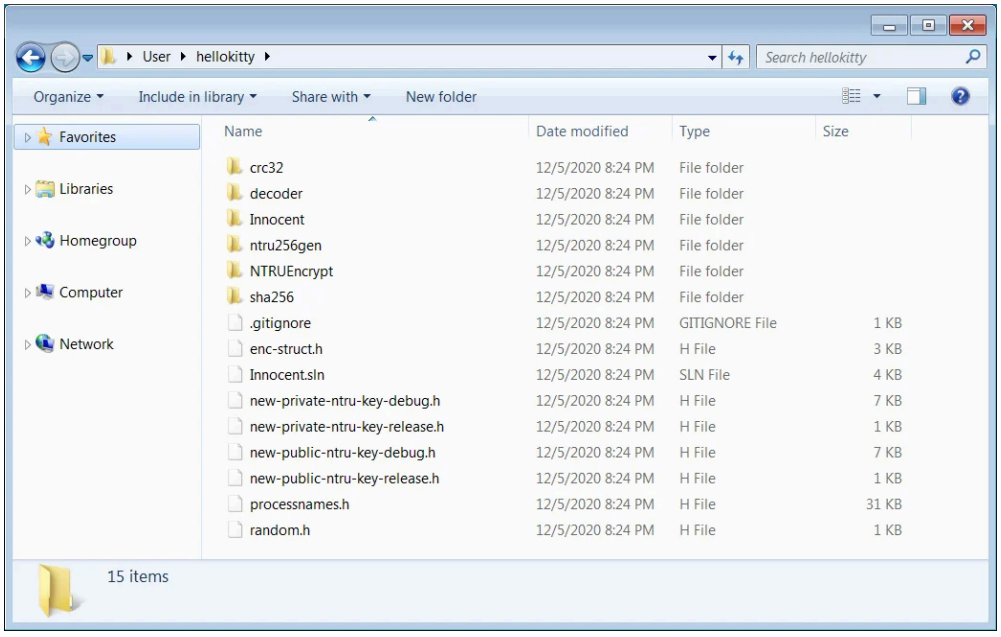

0:00



A threat actor named Gookee has been previously associated with malware and hacking activity, attempting to sell access to Sony Network Japan in 2020, linked to a Ransomware-as-a-Service operation called 'Gookee Ransomware,' and trying to sell malware source code on a hacker forum.

3xp0rt believes kapuchin0/Gookee is the developer of the HelloKitty ransomware, who now says, "We are preparing a new product and much more interesting than Lockbit."

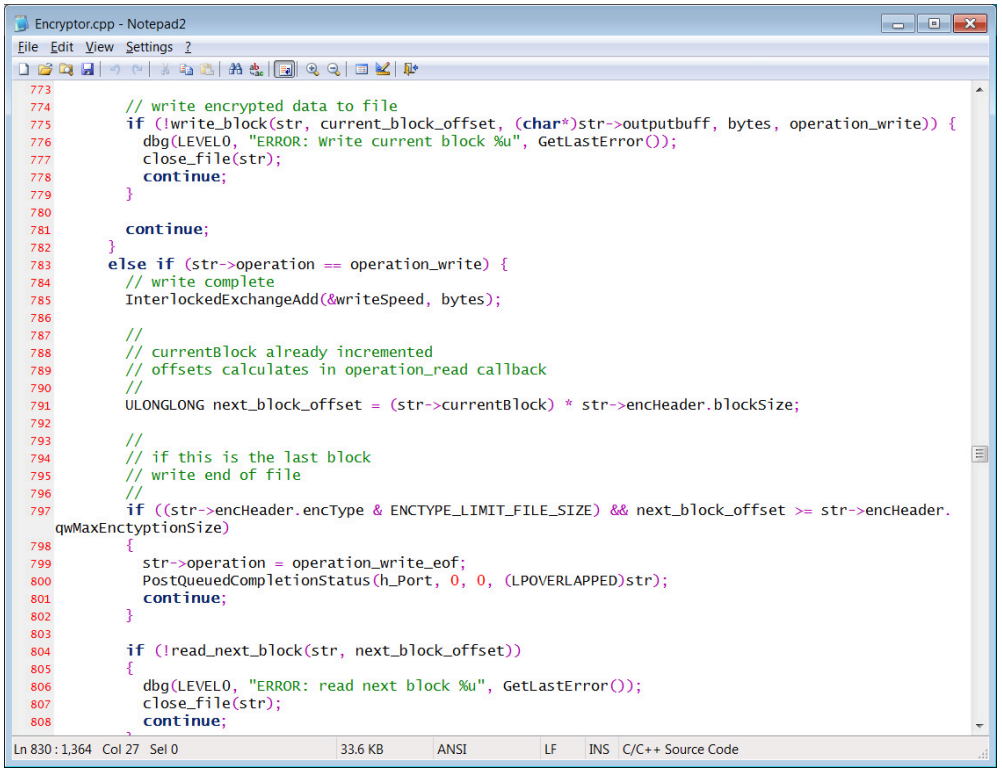
The released hellokitty.zip archive contains a Microsoft Visual Studio solution that builds the HelloKitty encryptor and decryptor and the NTRUEncrypt library that this version of the ransomware uses to encrypt files.



HelloKitty source code

Source: BleepingComputer

Ransomware expert Michael Gillespie confirmed to BleepingComputer that this is the legitimate source code for HelloKitty used when the ransomware operation first launched in 2020.



Part of the encryption code for HelloKitty

Source: BleepingComputer

While the release of ransomware source code can be helpful for security research, the public availability of this code does have its drawbacks.

As we saw when HiddenTear was released (*for "educational reasons"*) and Babuk ransomware source code was released, threat actors quickly used the code to launch their own extortion operations.

To this day, over nine ransomware operations continue using the Babuk source code as the basis for their own encryptors.

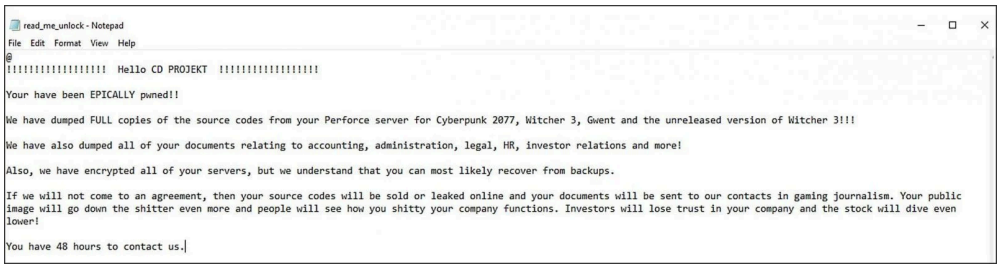
Who is HelloKitty?

HelloKity is a human-operated ransomware operation active since November 2020 when a victim posted to the BleepingComputer forums, with the FBI later releasing a PIN (private industry notification) on the group in January 2021.

The gang is known for hacking corporate networks, stealing data, and encrypting systems. The encrypted files and stolen data are then utilized as leverage in double-extortion machines, where the threat actors threaten to leak data if a ransom is not paid.

HelloKitty is known for numerous attacks and is used by other ransomware operations, but their most publicized attack was the one on CD Projekt Red in February 2021.

During this attack, the threat actors claimed to have stolen Cyberpunk 2077, Witcher 3, Gwent, and other games' source code, which they claimed was sold.



HelloKitty ransom note from CD Projekt Red attack

In the Summer of 2021, the ransomware group began utilizing a Linux variant that targets the VMware ESXi virtual machine platform.

The HelloKitty ransomware or its variants have also been used under other names, including DeathRansom, Fivehands, and possibly, Abyss Locker.

The FBI shared an extensive collection of indicators of compromise (IOCs) in their 2021 advisory to help cybersecurity professionals and system admins guard against attack attempts coordinated by the HelloKitty ransomware gang.

However, as the encryptor has changed over time, these IOCs have likely become outdated.

Source: https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/