HelloGookie. HelloKitty. Hello, LockBit

By Barracuda Networks

Published: 2024-04-24 · Archived: 2026-04-05 13:17:32 UTC

In yet another ransomware rebrand, the operator of the defunct HelloKitty operation has launched a new threat called ‘HelloGookie.’ The new name likely comes from one of the operator's nicknames, ‘Guki’ or ‘Gookee.’ He also uses the name ‘Kapuchin0,’ which he seems to prefer when posting to forums.

HelloGookie

HelloGookie has already published two attacks on a leak site, but the attacks aren’t current. These posts reference attacks from 2021 and 2022 in which HelloKitty was either attributed or named as a possible affiliated actor. Unlike the typical threat actor rebrand, HelloGookie hasn't tried to hide its past.

HelloKitty

Researchers first observed HelloKitty ransomware in late 2020. The first big target was Brazilian energy company CEMIG (Companhia Energética de Minas Gerais), which announced on Facebook that it had been the victim of a ransomware attack. Here’s a portion of the note left behind:

In February 2021, CD Projekt Red (CDPR) announced that it had been the victim of an unknown threat actor. CDPR develops popular role-playing games like The Witcher and Cyberpunk 2077. Many people thought a disgruntled gamer had launched the attack, or that CDPR was faking the threat to distract the public from flaws in its newly released game. Researchers quickly pushed back on this narrative, and it was later confirmed that HelloKitty was auctioning off the stolen CDPR data. Throughout 2021 the operator expanded attack capabilities by adding a Linux variant and a distributed denial-of-service (DDoS) threat. The additional threat of a DDoS attack elevated HelloKitty from a double-extortion to a triple-extortion threat actor. HelloKitty conducted aggressive campaigns against SonicWall CVEs in June 2021, and was named as part of a Cisco breach in May 2022.

On October 6, 2023, Kapuchin0/Gookie/Guki shut down the HelloKitty operation. He gave away his ransomware and took a passing shot at LockBit on his way out.

HelloKitty family tree

HelloKitty is reported to be a rebuild of DeathRansom, which was only bluff ransomware when it was first observed in 2019. Bluff ransomware is also called fake ransomware because it there’s no real file encryption, though there is usually a file locker that disrupts access to the files. File lockers are malware that targets the operating system functions and not the files. For example, there could be a lock screen on the workstation that prevents a user from interacting with the computer, or the files on a computer could be restricted with modified system permissions. DeathRansom didn’t even have a file locker when it first appeared. It simply renamed the

files and left a ransom note. However, it was only a few weeks after their first attacks that DeathRansom became a fully operational ransomware threat. DeathRansom activity died down after a period of aggressive research into the group, though that may have been coincidental and not due to the results of the investigation.

HelloKitty has also been closely linked with FiveHands ransomware, which is also a novel rewrite of DeathRansom. FiveHands was a ransomware-as-a-service (RaaS) operation that also developed Thieflock ransomware. The operators of Thieflock were later linked to a newer group, Yanluowang ransomware. We'll come back to Yanluowang in a minute.

Although HelloKitty was mentioned in the 2022 Cisco breach, that attack was formally attributed to an affiliate of UNC2447, Lapsus$, and Yanluowang. Cisco security teams detected the breach and purged the threat before ransomware could be deployed. Since there was no ransomware to analyze for this incident, Cisco teams reported on the known past behavior of threat actor UNC2447, saying it has consistently used "a variety of ransomware, including FIVEHANDS, HELLOKITTY, and more."

In separate research on the 2021 SonicWall attacks, Mandiant researchers noted,

Based on technical and temporal observations of HELLOKITTY and FIVEHANDS deployments, Mandiant suspects that HELLOKITTY may have been used by an overall affiliate program from May 2020 through December 2020, and FIVEHANDS since approximately January 2021.

Mandiant has also published detailed comparisons of HelloKitty, FiveHands, and DeathRansom.

Now back to Yanluowang. This was a ransomware-as-a-service (RaaS) group that targeted U.S. companies of all types but primarily focused on financial companies. Threat actor 'Saint' represented Yanluowang in the crime forums and private messaging. In October 2022 the private chatlogs of Yanluowang were leaked to the public, revealing many new insights into the group. The interesting part for us is that Guki of HelloKitty was one of the most active members in the Yanluowang logs. One of the conversations included Guki asking Saint for assistance with future attacks. HelloKitty was 'human-operated' ransomware, and Guki didn't have the manpower to leverage all the working credentials in his arsenal. Yanluowang was a RaaS group that could either buy his assets or give him a cut of any ransom collected through his data.

The Yanluowang group and Saint went quiet after the leak of the chatlogs in 2022.

Hello, LockBit

And now we are back to those HelloGookie forum posts.

Gookee/Guki/Kapuchin0 has been posting on the forums since at least early March 2024. A researcher (@3xp0rt) captured some of the posts:

I've redacted URLs and some language, but most of the content is intact here. The March 18 message is looking for 'large, interesting targets, for experience I have.' The March 25 message asks for a message from Yanluowang/Saint, possibly to discuss future collaboration. It also calls out LockBit again. Threat Intelligence Analyst Alexander Leslie explained the relationships between ransomware operators in a recent webinar:

"… all of these major ransomware groups, they make money off of each other. They all share affiliates, they all share infrastructure. They're all attacking some of the same victims at the same times. They're all using the same forums. They're all in private chats with each other. Yes, there is animosity at times, especially when an affiliate will double post victims on two different blogs, right, that actually does cause a bit of a rift between the affiliate and the group or between two groups. Yes, there is issues about market share about deals that they have with certain tool providers. But those disputes, again, are relatively surface level compared to traditional forms of crime, because it's in ransomware's best interest that nobody is taken down, that nobody has a significant disruption either internally or by law enforcement, because all of them staying in business means more and better business for every other ransomware group."

On April 22, 2024, Gookee/Guki/Kapuchin0 posted a 'help wanted' ad for someone to make phone calls to ransomware targets:

Recruiting a caller means HelloGookie is likely to employ voice phishing, or vishing. This is interesting because vishing was used in the 2022 Cisco attack:

The attacker conducted a series of sophisticated voice phishing attacks under the guise of various trusted organizations attempting to convince the victim to accept multi-factor authentication (MFA) push notifications initiated by the attacker. The attacker ultimately succeeded in achieving an MFA push acceptance, granting them access to VPN in the context of the targeted user.

Human-operated ransomware attacks like HelloKitty and presumably, HelloGookie, are very dangerous to the organization. This Microsoft document explains the higher risk associated with skilled criminals conducting reconnaissance and directing the attack.

When combined with tactics like vishing and MFA fatigue, these attacks can be very effective at gaining access and elevating privileges.

Assume the threat is real.

It's possible that Guki/Gookee/Kapuchin0 has no new attack and is just trying to get attention. You can't believe anything that any of these criminals say, and HelloGookie hasn't listed any new victims yet. When new victims are listed, they might not even be victims of HelloGookie attacks. Sometimes threat actors just repost someone else's victims. But if the HelloKitty operator is back with better software, and he's connecting with old friends like Saint, and he's getting a caller into his operation … that's a legitimate risk. And even though the HelloKitty family tree looks like Harry Lauder's walking stick, you can find a seven year path of potential cybercrime experience as these malware strains are reborn and threat actors move between groups.

We don't know with certainty that HelloGookie will be a real threat, but this is another example of why you should adopt a Zero Trust mindset. Verify everything, including phone calls and multi-factor authentication prompts. Defend all of your threat vectors with comprehensive, multi-layered security, and make sure your users have security awareness training.

Barracuda can help

Only Barracuda provides multi-faceted protection that covers all the major threat vectors, protects your data, and automates incident response. Over 200,000 customers worldwide count on Barracuda to protect their email, networks, applications, and data. Visit our website to explore our comprehensive cybersecurity platform.
