

Punk Kitty Ransom - Analysing HelloKitty Ransomware Attacks

cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks

February 10, 2021

enforce server for Cyberpunk 2077, Witcher 3, Gwent and the u
unting, administration, legal, HR, investor relations and mor
tand that you can most likely recover from backups.

s will be sold or leaked online and your documents will be se
ee how you shitty your company functions. Investors will lose



Blog

February 10, 2021

Yesterday, the company behind the gaming blockbuster Cyberpunk 2077 announced that it had been hit by a ransomware attack and the hackers claimed to have stolen source code for upcoming games. The most likely culprit at this time of the known ransomware groups is a group known as HelloKitty.

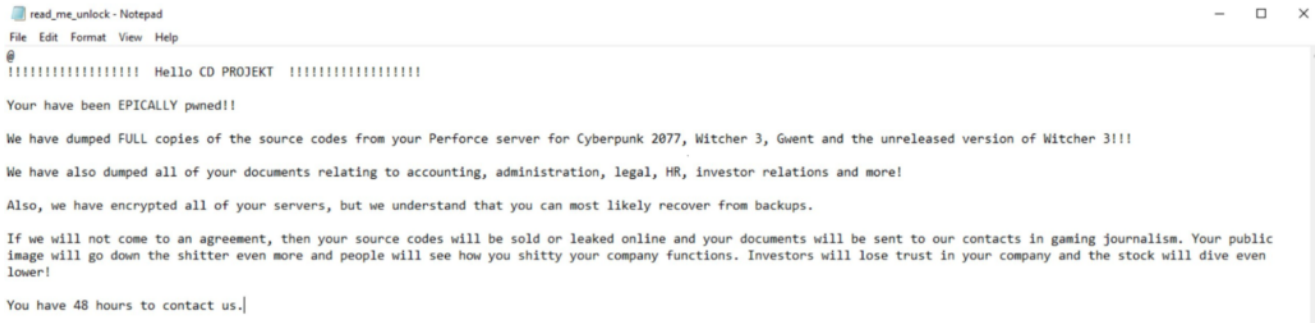
Below we have taken a look at previous HelloKitty attacks, and found a trail of victims. Previous attacks include potentially dangerous code to kill applications, including Industrial Control Systems. We also found links to earlier notable ransomware attacks.

Background

Yesterday CD Projekt Red revealed they had fallen victim to a ransomware attack:

“An unidentified actor gained unauthorized access to our internal network, collected certain data belonging to CD PROJEKT capital group, and left a ransom note the content of which we release to the public.”

They join a number of other gaming companies to have recently suffered the same fate.



```
read_me_unlock - Notepad
File Edit Format View Help
@!!!!!!!!!!!!!!!!!!!! Hello CD PROJEKT !!!!!!!!!!!!!!!!!!!!!
Your have been EPICALLY pwned!!
We have dumped FULL copies of the source codes from your Perforce server for Cyberpunk 2077, Witcher 3, Gwent and the unreleased version of Witcher 3!!!
We have also dumped all of your documents relating to accounting, administration, legal, HR, investor relations and more!
Also, we have encrypted all of your servers, but we understand that you can most likely recover from backups.
If we will not come to an agreement, then your source codes will be sold or leaked online and your documents will be sent to our contacts in gaming journalism. Your public image will go down the shitter even more and people will see how you shitty your company functions. Investors will lose trust in your company and the stock will dive even lower!
You have 48 hours to contact us.]
```

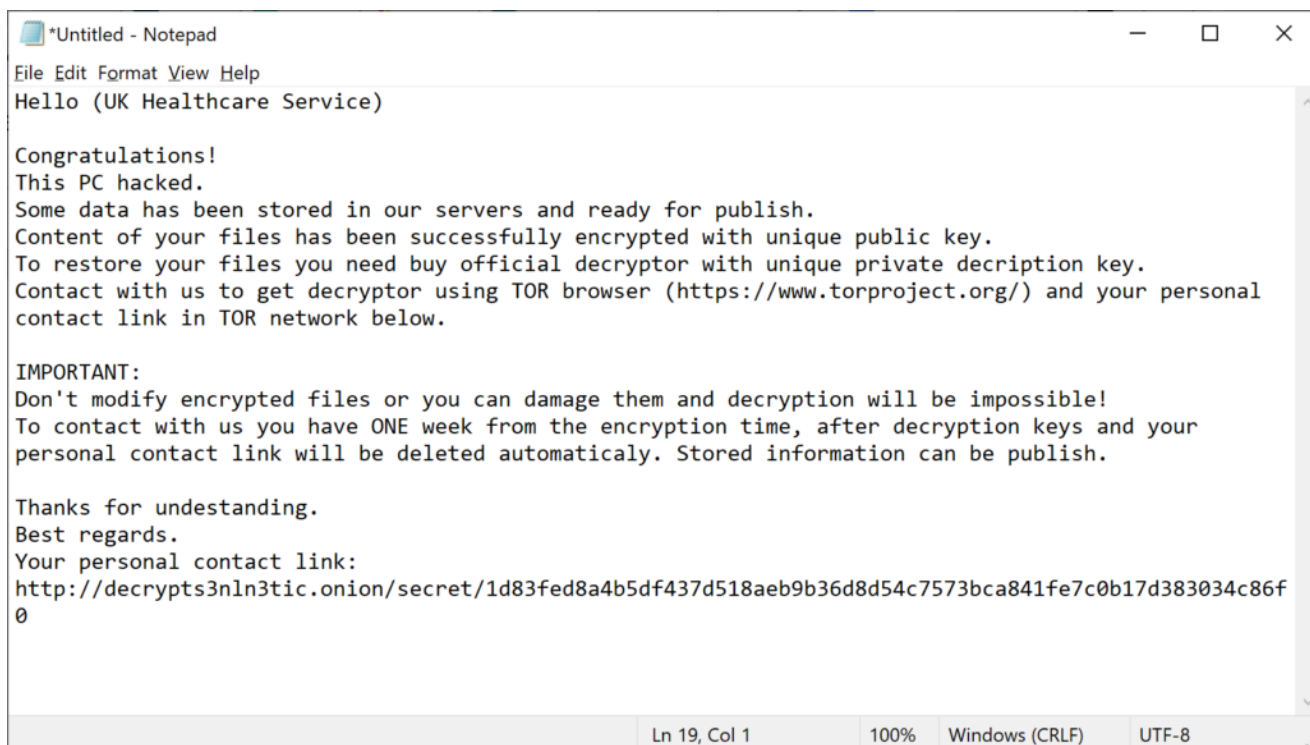
The ransomware note shared by CD Projekt Red

The Emsisoft CTO has suggested this may be the work of HelloKitty ransomware. That is based on the ransomware note and rare filename, and they caveat that it’s not possible to be sure without seeing the ransomware itself. We’d concur with that caution. Whilst the notes are certainly familiar (as shown below) – they are custom for most victims and not an exact match. As an anti-virus with a track record of ransomware analysis, it’s likely Emsisoft has seen samples of HelloKitty that we have not and have included that in their assessment.

With those caveats in hand – we took a look at previous HelloKitty attacks below.

Most Recent Attacks

The most recent attack we’ve seen from HelloKitty targeted a UK Healthcare organisation at the end of January 2021. Below is the ransomware note, with the name of the targeted organisation redacted:

A screenshot of a Notepad window titled '*Untitled - Notepad'. The window contains a ransomware message in a monospaced font. The message reads: 'Hello (UK Healthcare Service)'. 'Congratulations! This PC hacked. Some data has been stored in our servers and ready for publish. Content of your files has been successfully encrypted with unique public key. To restore your files you need buy official decryptor with unique private decryption key. Contact with us to get decryptor using TOR browser (https://www.torproject.org/) and your personal contact link in TOR network below.' 'IMPORTANT: Don't modify encrypted files or you can damage them and decryption will be impossible! To contact with us you have ONE week from the encryption time, after decryption keys and your personal contact link will be deleted automatically. Stored information can be publish.' 'Thanks for understanding. Best regards. Your personal contact link: http://decrypts3nln3tic.onion/secret/1d83fed8a4b5df437d518aeb9b36d8d54c7573bca841fe7c0b17d383034c86f0'. The status bar at the bottom shows 'Ln 19, Col 1', '100%', 'Windows (CRLF)', and 'UTF-8'.

It goes without saying that it is particularly irresponsible to be deploying targeted ransomware to organisations that provide key medical services during a global pandemic.

Christmas 2020 Attacks

Attackers are well aware of the importance timing can make to the impact of their attacks. Notably, Russian attackers successfully disabled Ukrainian power networks for two consecutive Christmas Eve's. The timing both left thousands of families without power on Christmas day, and only a skeleton crew at the power company to respond.

We're aware of at least two, and likely more, attacks that HelloKitty delivered on Christmas Day 2020. They likely had access for some time before, but chose to deploy their ransomware on Christmas day for maximum impact.

The first has previously been reported on. At Christmas 2020 the Brazilian powerplant operator CEMIG disclosed on Facebook that they had fallen victim to a ransomware attack:

“CEMIG informs that on December 25, 2020, the SOC (security operation nucleus) detected anomalous behavior on the internal network, with characteristics of a malicious ransomware attack. The teams responsible for the correct detection of the attack and subsequent adoption of the containment measures were immediately activated.

Less than 10% of servers on the Windows / Microsoft Hyper-V platform had their content encrypted. Workstations have also been partially compromised and are in the process of being verified. It is important to highlight that, thanks to the fast and effective containment action carried out by Cemig, the operation of the electrical system and the main databases (customers, billing, customer service and business management) were not compromised, thus guaranteeing the provision of services to our clients.”

The statement about the Hyper-V platform matches the ransomware note we've seen linked to the attack:

A screenshot of a Notepad window titled "read_me_lkdtt - Notepad". The window contains a ransomware note in plain text. The text reads: "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. -- Contact with us by method below 1) Open this website in TOR browser: http://x6gjpqs4jjvgpfvghdz2dk7be34emyzluimticj5s5fexf4wa65ngad.onion/0c04b15081595448821e25e8dd07423d9927fa54cd56d8797ea4d1315a682692 2) Follow instructions in chat. " The status bar at the bottom shows "Ln 15, Col 1", "100%", "Windows (CRLF)", and "UTF-8".

```
read_me_lkdtt - Notepad
File Edit Format View Help
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.

-- Contact with us by method below
1) Open this website in TOR browser:
http://x6gjpqs4jjvgpfvghdz2dk7be34emyzluimticj5s5fexf4wa65ngad.onion/0c04b15081595448821e25e8dd07423d9927fa
54cd56d8797ea4d1315a682692
2) Follow instructions in chat. "
```

The CEMIG Ransomware note

Reportedly, CEMIG had restored their system within four days.

As normal with targeted ransomware, the attackers provided a chat link for CEMIG. The conversation was captured by the site ID Ransomware (RU). Based on the conversation, we think it is unlikely that CEMIG* decided to pay the ransom:

You was attacked by Kitty ransomware

All your documents, photos, databases and other important files have been encrypted.

The only way to decrypt your files is to receive the decryption program.
For details talk with support in chat.

Hello CEMIG, i'll help you to recover your files, type first message here to start.

no thanks motherfucker

first

support

hello

Hello

Type message and press Enter

Send message

* Other analysts have pointed out that given the payment link was made public, this may not be CEMIG communicating with Hello Kitty.

But CEMIG was not the only target at Christmas. We've seen another HelloKitty ransomware note from a different target that was uploaded to the site VirusTotal.com on Christmas day 2020:



The screenshot shows a Notepad window titled "*Untitled - Notepad". The text inside the window is a ransom note. The note starts with "Hello (French IT Service)" and "Congratulations!". It states that the PC has been hacked and that data has been stored on servers. It demands the purchase of an official decryptor with a unique private key to restore files. It provides a contact link in the TOR network: <https://www.torproject.org/>. It includes an "IMPORTANT" warning not to modify encrypted files and a one-week deadline for contact. The note ends with "Thanks for understanding.", "Best regards.", and "Your personal contact link: <http://decrypts3nln3tic.onion>". The status bar at the bottom indicates "Ln 15, Col 30", "100%", "Windows (CRLF)", and "UTF-8".

```
*Untitled - Notepad
File Edit Format View Help
Hello (French IT Service)

Congratulations!
This PC hacked.
Some data has been stored in our servers and ready for publish.
Content of your files has been successfully encrypted with unique public key.
To restore your files you need buy official decryptor with unique private decription key.
Contact with us to get decryptor using TOR browser (https://www.torproject.org/) and your personal
contact link in TOR network below.
IMPORTANT:
Don't modify encrypted files or you can damage them and decryption will be impossible!
To contact with us you have ONE week from the encryption time, after decryption keys and your
personal contact link will be deleted automaticaly. Stored information can be publish.
Thanks for undestanding.
Best regards.
Your personal contact link:
http://decrypts3nln3tic.onion

Ln 15, Col 30    100%    Windows (CRLF)    UTF-8
```

The ransom note to a French IT service (we have redacted the name)

Application Termination

One sample of HelloKitty, compiled on 26th December 2020, contains a large list of applications to terminate:

```
prdatasemgr.exe
sschk.exe
preventmgr.exe
trjscan.exe
prreader.exe
trupd.exe
prwriter.exe
ssecuritymanager.exe
prsummarymgr.exe|
dltray.exe
prstubber.exe
dlservice.exe
prschedulemgr.exe
almon.exe
musnotificationux.exe
savadminservice.exe
npmdagent.exe
savservice.exe
client64.exe
sweepsrv.sys
```

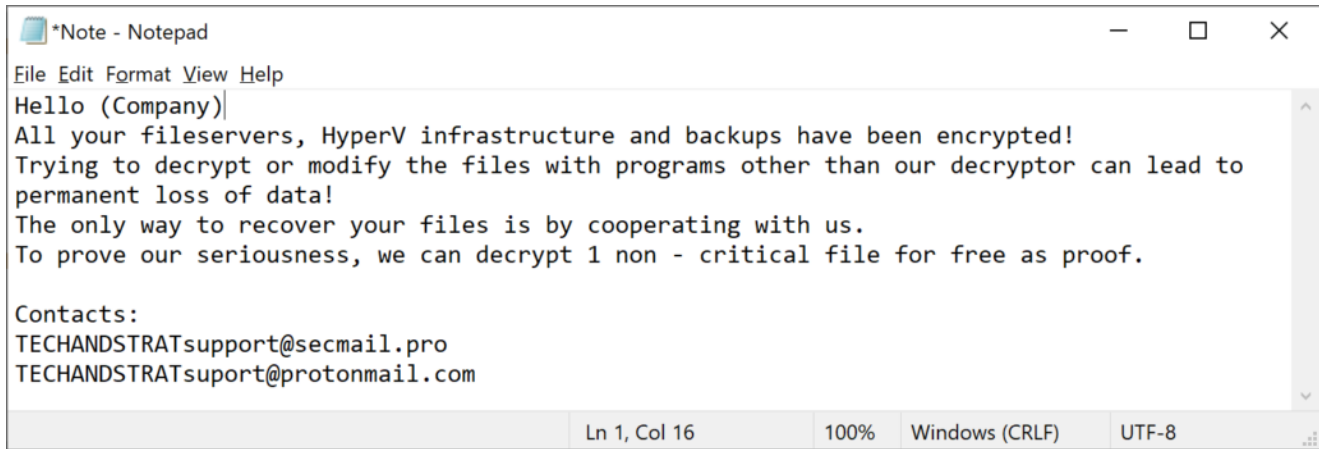
We were disturbed to see terminated applications included Industrial Control System software such as GE Proficy and Honeywell HMIWeb. Investigating this list, it appears it is copied from the MegaCortex/Ekans/Snake ransomware.

When the MegaCortex list was first identified it generated significant concern about the impact it could have on SCADA systems. However, more day to day applications such as backup software and accounting software are also terminated. As researchers noted at the time – the attackers seem concerned with stopping any software that may limit its impact, rather than specifically targeting SCADA.

Nonetheless it is concerning to see such careless code in a sample of malware, which was compiled at the same time that a Powerplant operator was enduring their attack.

Links to Earlier Campaigns

We quickly found links to the “TechStrat” ransomware identified in October 2020. The ransomware note is named the same (“read_me_lkdtt.txt”) as many HelloKitty ransomware notes. And the note itself is very similar to the note that was deployed to CEMIG:



*Note - Notepad

File Edit Format View Help

Hello (Company)|

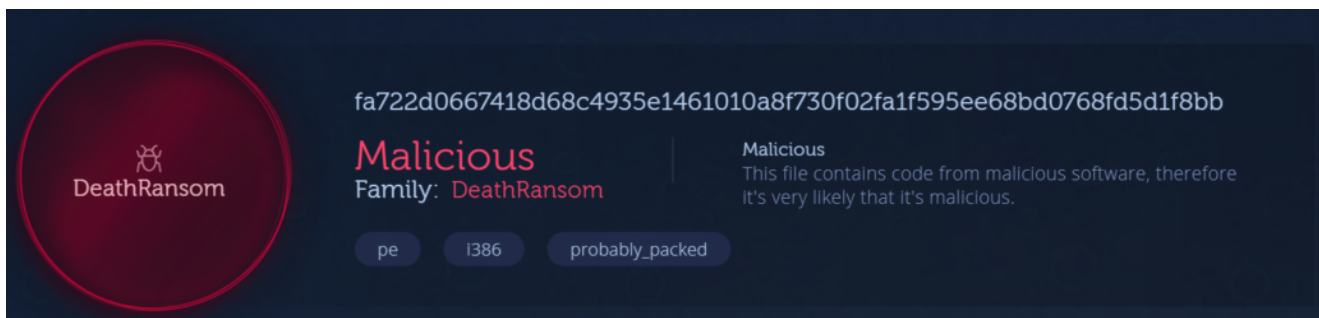
All your file servers, HyperV infrastructure and backups have been encrypted!
Trying to decrypt or modify the files with programs other than our decryptor can lead to permanent loss of data!
The only way to recover your files is by cooperating with us.
To prove our seriousness, we can decrypt 1 non - critical file for free as proof.

Contacts:
TECHANDSTRATsupport@secmail.pro
TECHANDSTRATsuport@protonmail.com

Ln 1, Col 16 100% Windows (CRLF) UTF-8

Decompiling the [code of a sample](#), shows it to also be extremely similar to other HelloKitty samples. It also contains the code to kill a range of applications that was borrowed from MegaCortex.

In addition, [we](#) (and others [1](#), [2](#)) spotted possible overlaps with an earlier family called “DeathRansom”. A quick review is shown from [Intezer’s analysis](#) and Antivirus vendors often detecting both HelloKitty ransomware binaries and notes as DeathRansom:



If so, that may be particularly interesting given that Fortinet tracked down the DeathRansom author in an involved blog post in [January 2020](#).

Additionally, [Emsisoft](#) caveat here:

“Some analysts may refer to HelloKitty as DeathRansom, a strain of malware that was originally only capable of renaming files. Different versions of DeathRansom were later developed that could encrypt files in various ways. However, the relationship between DeathRansom and HelloKitty is still not fully clear.”

In Closing

It’s clear that HelloKitty is yet another set of targeted ransomware operators that have moved to threaten their victims with impact going beyond the immediate destruction of data. If they are indeed linked to the earlier DeathRansom attacks, they have improved significantly from their initial forays into ransomware. The first version didn’t even encrypt anything. We have provided some suggested mitigation strategies below.

Mitigation

We have included a number of mitigation strategies that Cado Security recommends both for HelloKitty and ransomware in general:

- Consider utilising separate IT systems (privileged access workstations) for used by network and system administrators. For these systems, utilise additional two-factor authentication and ensure there is no direct access to the Internet.
- Consider employing an “allowed list” to restrict server outbound communications to IP’s / Domains that they need access to.
- Consider storing backups of key business and critical IT infrastructure systems e.g. ActiveDirectory, off of your network.
- Avoid opening up RDP services to the internet, if it’s required consider using an ALLOW LIST approach only, and DENY all unknown IPs by default.
- Ensure you have the ability to restore to a segregated network environment.
- Ensure you have tested the restore capabilities of your backups.

Both the [UK NCSC](#) and [ICS-CERT](#) provide more extended mitigations for destructive attacks.

About Cado Security

Cado Security specialises in providing tooling and techniques that allow organisations to threat hunt and investigate cloud and container systems. If you are interested in knowing more, please don’t hesitate to reach out, [our pilot program is now open](#).

Updates to this Blog

12th February 2021:

- Updated to add link to Emsisoft’s new blog post on 12th February
- Added reference to MalwareHunterTeam saying it may not be CEMIG communicating with Hello Kitty

Indicators of Compromise

fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb
9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0
c7d6719bbfb5baaadda498bf5ef49a3ada1d795b9ae4709074b0e3976968741e
56978ab3cb8172239da8742ebe41ef099bb9e1b58e23956a82bf495d7cc94c00
a6067ecff5c441c2e9654abfe928ae5a81b57e19f3a80ac945a7780f92b39ff3
613f9fb99d927e02ba4d7b7122df577fe775e2e56d7ddce5636fd810fc1392ad
a63879a8f90286ca0ba54b446f94dd2e51da549dc4ebd91cb67018e910436280
78afe88dbfa9f7794037432db3975fa057eae3e4dc0f39bf19f2f04fa6e5c07c
02a08b994265901a649f1bcf6772bc06df2eb51eb09906af9fd0f4a8103e9851
38d9a71dc7b3c257e4bd0a536067ff91a500a49ece7036f9594b042dd0409339
9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0

MITRE Attack

T1059 Enterprise — Command and Scripting Interpreter
T1047 Execution — Windows Management Instrumentation
T1135 Discovery — Network Share Discovery
T1082 Discovery — System Information Discovery
T1124 Discovery — System Time Discovery
T1012 Discovery — Query Registry
T1045 Defense Evasion — Software Packing
T1486 Impact— Data Encrypted for Impact
T1490 Impact — Inhibit System Recovery

About The Author



Chris Doman

Chris is well known for building the popular threat intelligence portal [ThreatCrowd](#), which subsequently merged into the [AlienVault Open Threat Exchange](#), later acquired by AT&T. Chris is an industry leading threat researcher and has published a number of widely read articles and papers on targeted cyber attacks. His research on topics such as the North Korean government's [crypto-currency theft schemes](#), and China's attacks [against dissident websites](#), have been widely discussed in the media. He has also given interviews to print, radio and TV such as [CNN](#) and BBC News.

About Cado Security

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit <https://www.cadosecurity.com/> or follow us on Twitter [@cadosecurity](#).

[Prev Post](#) [Next Post](#)