

Forum:[Hack Forums](#)

Thread: [IronLantern recovery tool for a specific "Yogi" virus](#)

bitGnome_7 - August 22, 2026, 2:35 pm

I RE'd a shitty ransomware that was lately uploaded to Malware Bazaar and thought I would do my own recovery tool.

Ransomware sha256:ecc42df31157857f6bb17e6fd458b8bf10047a80edff10f76a3ad7126fdc6926
Attributed to the "Adware Yogi" family on Malware Bazaar but don't get fooled, it is a Windows targeting ransomware with C2 capabilities written in python and compiled via pyinstaller.

The ransomware uses two persistence methods:

- 1- HKCU registry key creation pointing to a randomly named copy of Yogi in a randomly named folder under %APPDATA%/Windows/Crypto
- 2- Creation of a randomly named copy of Yogi under Windows Startup folder

It communicates with a C2 server :

- 1-Primary endpoint: go-ns[dot]org[dot]ua
- 2- Using HTTP POST and GET, the POSTS are setup via .json files that are dumped into a POST request
- 3- A fallback method with go-ns[dot]org[dot]ua/wp-content/themes/go-ns/send-message-to-telegram.php which signals the C2 admin on telegram in case the connection with C2 failed

It encrypts files using a basic XOR key retrieved from several possible hardcoded URLs' sha256 hash

From the malware's architecture I'd say it targets non tech savvy people, like my grandma... or yours!

My reversal tool is a bit of an overkill for this shitty bug :

- 1- Two modes : Quarantine with encryption of samples or samples deletion
- 2- Process crawling in case watchdog process exist (not the case on that sample)
- 3- Persistence removal
- 4- Quarantine samples decryption
- 5- File decryption with file signature header detection in order to use the right encryption key on the right file

IronLantern is available on github : [github\[dot\]com/bitGnome7/IronLantern](#)

All of this has been achieved through static analysis and OFFLINE dynamic analysis

In case anyone wants to take this further, by taking down their servers or help me blackhat the shit out of them do not hesitate to contact me (they should pay for bad OPSEC at least...)

I was hesitating to put this on greyhat channels...

But the primary goal is actually to help people recover from Yogi with IronLantern

#NoRansom

For the links, I replaced . with [dot] because apparently I'm too much of a p*\$\$y down here to post

links in my threads

See ya ????