# Ransomware Decryptors

## System Specific Encryption

### System Specific Encryption

Ransomware variants like Phobos, Dharma or CryLock are file level encryption. The TA gains access to the system, copies specific encryption executables onto the systems then runs the executables to encrypt the files. The results are files with a new extension appended to the old file name. Sometimes it's a random sequence of numbers and letters (e.g. *.nocv) or a specific tag (e.g. *[CryLockDecrypt@****.com][1].[ID-*****-COM]). System specific encryption generates a unique key per encrypted system. The ransom note or the file extension may indicate an "ID" that would be different on each system.

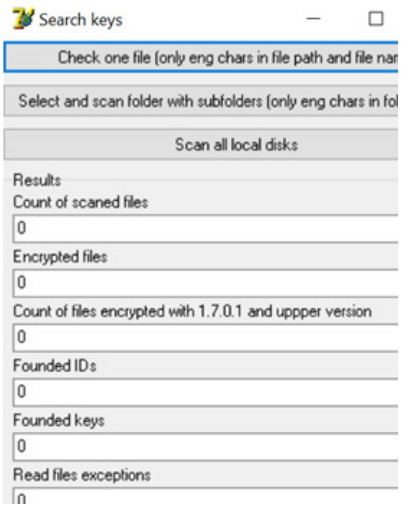


Figure 1 - CryLock Scanner and Decryptor

**Communication preference:** Email usually aol.com, protonmail.com, or cock.li domains

**Average ransom payment:** $27,000 - $500,000

**Preferred currency:** Bitcoin (BTC)

**Decryptor Received:** 95% of the time. Certain variants of Phobos and Dharma will attempt to re-extort a second payment if a large discount is negotiated.

**Watch out:** Phobos, Dharma, and CryLock are a two-step process. The TA will first send a "scanner" tool that needs to be run on every infected system. The scanner will look for the public keys used to encrypt the files, then write that information to a corresponding .txt or .ini file. Those corresponding files need to be sent to the TA in order to generate a decryptor. The TA in return will send the decryptors. The two-step process adds significant overhead due to the running of multiple tools on the infected system as well as the delay with communicating via email. On average after making a payment for the decryptor, clients are who are infected with Phobos are down for approximately 11 days whereas clients who are infected with Dharma experience downtime of about 7.75 days. The high number of days can be attributed to the two-step process and multiple

email communications.

**Notes:** Negotiating with the Phobos and Dharma group can be tricky. These variants are Ransom-as-a-Service (RaaS) model so you're not dealing with the same core group of people as you would with variants like Ryuk (or now Conti). Negotiating with RaaS groups can also create confusion and complexities with a different operator responding to each email. The groups who deploy these variants also look for exploiting publicly accessible Remote Desktop Protocol (RDP). Disable external access to RDP to lessen the chance of being infected by this variant.

## System Specific Encryption with a Universal Option

Ransomware variants like Sodinokibi are file level encryption with a unique ID per system. Once the TA gains access to the network, they release their Sodinokibi ransomware throughout the environment. The systems are infected with a unique randomly generated file extension per system. Their ransom notes are usually within a text file and explain what happened, including if any data was exfiltrated. The group is very organized and can often share information about their victim's networks including domain information, infected systems, and any stolen data.

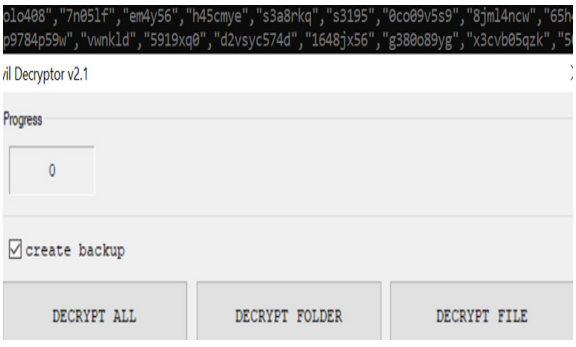


Figure 2 - Sodinokibi Decryptor

**Communication preference:** TOR Website via chat room. The ransom note contains a link to the TOR site as well as a unique key to gain access to a private chat room where the negotiations occur.

**Average ransom payment:** $170,000

**Preferred currency:** Monero (XMR)

**Decryptor received:** 100% of the time. Sodin offers a general decryptor which requires the victim to collect the file extensions from all of their infected systems. This can be very tedious once the payment is made, the victim can input any number of file extensions into the input box on the TOR site to generate a decryptor. Sodin will keep that private room open for 30 days after payment allowing victims to return if they find any extensions not previously found. A lesser known secret with Sodin, if you ask nicely for a universal decryptor, the operator may create the decryptor for you; providing a single decryptor that can be used across your network. The universal decryptor certainly saves a lot of time with decrypting files and minimizing the number of times having to launch the TOR browser.

**Watch out:** Earlier this year, Sodin changed their code base for their encryption payloads causing instability on certain Windows Operating Systems within the master boot files. Using certain security tools after a Sodin outbreak can cause systems to hang during reboot. Sodin encryption is one of the more aggressive encryptions.

Be sure to create a snapshot or backup the files prior to installing any new software or performing live forensics on critical systems.

**Notes:** Sodin has made headlines throughout 2020 for following Maze with exfiltrating data as well as being the first ransomware group to only accept Monero for payments.