Cryptocurrency Mining Malware Discovered Targeting Seagate NAS Hard Drives

By Catalin Cimpanu

Published: 2016-09-09 · Archived: 2026-04-05 23:48:41 UTC

A malware variant named Mal/Miner-C (also known as PhotoMiner) is infecting Internet-exposed Seagate Central Network Attached Storage (NAS) devices and using them to infect connected computers to mine for the Monero cryptocurrency.

Miner-C, or **PhotoMiner**, appeared at the start of June 2016, when a report revealed how this malware was targeting FTP servers and spreading on its own to new machines thanks to worm-like features that attempted to brute-force other FTP servers using a list of default credentials.

Miner-C now specifically targets Seagate Central NAS hard drives

This same functionality is still present in the latest Miner-C version, but security researchers from Sophos say that recent Miner-C iterations are using a design flaw in the Seagate Central NAS devices to place a copy of itself on their public data folders.

NAS devices, which are network-connected hard drives, allow users to access files from the local network, but also via the Internet if the administrator chooses to open the NAS drive for remote access.

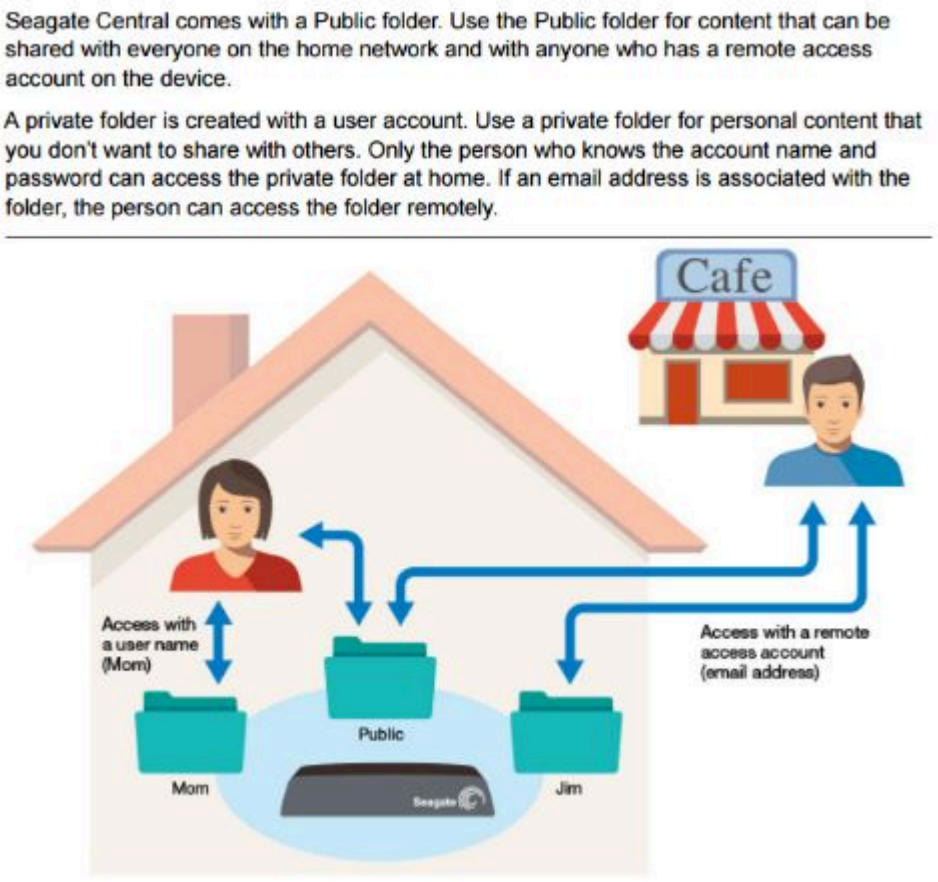
According to Sophos, Seagate Central devices contain a public folder accessible to all users, even anonymous non-logged-in users, which can't be deactivated or deleted.

Miner-C tricks users into installing the cryptocurrency miner

Miner-C is copying files to this public folder on all Seagate Central NAS devices it can find. One of the files it copies is called Photo.scr, a script file that malware coders have modified to use a standard Windows folder icon.

Because Windows has a bad habit of hiding file extensions, whenever the device owner accesses their NAS, they see this file as a folder, fooled by the fake icon.

When they try to access the folder, they're actually executing the Photo.scr file, which installs a cryptocurrency mining application on their PC.



Public and private folders on Seagate Central NAS drives

Miner-C also features a modular structure made of different parts that do different things, and it uses a unique method of loading its config file.

"Since it generates a new initialization file when it is launched, it helps the malware avoid security solutions. It also gives the botnet operators a chance to change the payload of the threat in the future, for example, dropping ransomware to the victim's machine after the mining business is no longer profitable," the Sophos team explains in a technical report.

Miner-C mines for Monero only

Right now, Monero is one of the most profitable cryptocurrencies from when it comes to mining operations. While Bitcoin mining difficulty has increased many times over the years, PC-based Bitcoin mining has ceased to be profitable in 2012 and is currently only an option if you're using special hardware and dedicated data centers.

Monero is one of the few cryptocurrencies that can still be mined using regular PCs, hence the reason the crooks chose it.

There are around 5,000 Seagate Central NAS devices infected

According to telemetry data Sophos researchers gathered, Miner-C has infected around 70 percent of all Seagate Central NAS devices available on the Internet.

Researchers discovered around 7,000 Seagate Central NAS devices connected to the Internet, which means crooks managed to infect around 5,000 such devices.

Since all the accounts to which crooks collect Monero are stored in the malware's config file, Sophos was able to estimate that they have made around €76,600 ($86,400) from their operations until now and are currently responsible for 2.5 percent of the entire Monero mining activity.

The quandary is that Seagate Central owners have no way to protect their device. Turning off the remote access NAS feature can prevent the infection, but also means they lose the ability to access the device from a remote location, one of the reasons they purchased the hard drive in the first place.

Map of infected Seagate Central NAS devices

Source: https://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml