U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

# ***Mining More than Gold***

**October 2016**

**Did you know that your file transfer protocols may be particularly vulnerable to cyber-attacks?** FTP (file transfer protocol) is a standard network protocol used to transfer computer files on a computer network. A type of data storage device, called a network-attached storage (NAS) device, started becoming victim to a serious type of malware which exploited the FTP service available on FTP servers, including FTP services available on NAS devices, beginning this year. NAS devices connect to a computer network and provide a way to access data for a group of persons or entities.

According to a recent report by Softpedia, Sophos, a computer security firm, gathered telemetry data that indicated 70 percent of a certain vendor's NAS devices connected to the internet were infected with a malware variant called Mal/Miner-C (also known as PhotMiner). Sophos researchers claim that out of 7,000 of these NAS devices connected to the internet, 5,000 were infected with this malware by cybercriminals who also collected $86,000, in cryptocurrency like bitcoin and monero, from cryptocurrency mining related to this attack.

Allegedly, the malware variant appeared in the beginning of June 2016. A report revealed that the malware was targeting FTP services, such as those available on NAS devices, and spreading to new machines by attempting to conduct brute-force attacks using a list of default credentials. Also, the researchers claim that a design flaw regarding the use of public folders on certain NAS devices permitted the Miner-C malware to more easily copy itself to the public folders.

The Mine-C or PhotoMiner (the malware) tricks users by copying files to the public folders that resemble a standard Microsoft folder icon. Once the user clicks on the folder, s/he activates the malware variant, and it installs the malware on the victim's laptop, desktop, or other computing device. The malware allows cybercriminals to generate cryptocurrency (*i.e.*, bitcoins, monero) by "mining". Cryptocurrency mining exploits computer processing power to solve difficult math problems. Essentially, attackers are rewarded with cryptocurrency for the amount of math problems they solve.

This type of malware can affect an information system's performance by eating up a system's computing power, and slowing down other system processes.

### ***Covered Entities and Business Associates should consider following the measures the SANS Institute provided for preventing and detecting cryptocurrency mining malware:***

- Limit the abilities of unauthorized users to access: PC basic input output systems (BIOS) that control the basic functions of the computer (*i.e.,* time and date, media boot order, and speeds at which the processor and memory run); data centers and server rooms; and corporate premises;
- Perform regular physical audits and checks for unauthorized equipment;
- Setup delivery and deployment processes to ensure only authorized access to equipment and facilities is permitted;
- Perform detailed network-traffic analysis;
- Block all untrusted websites and only allow communication that is approved;
- Keep anti-virus and anti-malware software up to date;
- Make use of whitelists for applications;
- Make use of approved software-asset-management applications;
- Perform active, real-time performance and system monitoring;
- Limit administrative privileges;
- Change generic/shared user passwords and reviewing access rights; and
- Implement segregation or separation of duties.

***Resources:*** SANS Institute https://www.sans.org/reading-room/whitepapers/threats/detecting-crypto-currency-mining-corporate-environments-35722. (Preventing and Detecting Cryptocurrency Mining Malware)

**Did you also know that October National Cybersecurity Awareness Month?!** This annual campaign raises awareness of cybersecurity. According to the Department of Homeland Security (DHS), National Cyber Security Awareness Month (NCSAM) is designed to involve and inform public and private sector associates through events and initiatives to heighten awareness about cybersecurity, supplement them with tools and resources needed to stay safe online, and upsurge the resiliency of the Nation in the event of a cyber-incident.

For more information about National Cyber Security Awareness Month (NCSAM) access the Department of Homeland Security (DHS) website: https://www.dhs.gov/national-cyber-security-awareness-month.