I S LITERACY, LEARNING AND LESSON

LLL: 12/19	**Sophos Ransomware**
16.12.2019 **IS LITERACY, LEARNING**	A new variant of ransomware called Snatch ransomware is capable of encrypting critical system files. Snatch ransomware affects Windows 7 through Windows 10 in 32- and 64-bit versions.
Source	**Sophos.com**
How it works	Snatch runs itself in an elevated permissions mode, sets registry keys that instructs Windows to run it following a Safe Mode reboot, then reboots the computer and starts encrypting the disk while it's running in Safe Mode. It takes advantage of the fact that anti-malware solutions are not loaded in Safe Mode, the Snatch ransomware component installs itself as a Windows service called 'SuperBackupMan' that has the ability to run in Safe Mode and also can't be stopped or paused. To install the malware, attackers penetrate enterprise networks via automated brute-force attacks against vulnerable, exposed services, and then leverage that foothold to spread internally within the targeted organization's network.
Recommended action	• Don't expose your Remote Desktop interface to unprotected internet access. If Remote Desktop Access is required, secure it through VPN. • Use multi-factor authenticator for administrators. • Inventory your devices and monitor your network for any malicious activity. • Use Strong Password and Identity Management tool.