Cybraics Identifies P2P Software Attempting to Download Ransomware

Challenges

- Third party vendors have access to the network
- Many devices are not maintained by the hospital, making it hard to enforce policies

Existing Security Tools

- SIEM, Advanced Threat Detection, MSSP

Results

- Multiple P2P clients from vendors and unmanaged networks attempting to download Ransomware.

Background

A healthcare provider's network consists of a core network that they manage and several joined networks that they only partially manage. They range in scope from other tenant networks to 3rd party vendor networks. The Provider has invested significantly in modernizing their operations and capabilities to provide leading edge care; however, they have limited capability to enforce policies on their endpoint devices across these multi-diverse networks. To compensate, the security team deployed an advanced threat detection service to identify threats across the entire IT network. The advanced threat detection services conduct log analysis on-site using a Security Incident and Event Management (SIEM) system and a Managed Security Service Provider (MSSP), based on traditional signature-based products and endpoint protection.

What We Found:

The healthcare provider has policies on their direct network that restrict the use of peer-to-peer (P2P) software as it can pose a significant security risk to the network. P2P software is typically used to download copyrighted material; however, it is not uncommon for them to also download malware and other hostile files that can be leveraged to exfiltrate sensitive data or impact daily operations. The nLighten platform detected several instances of P2P downloads and uploads from the 3rd party networks that have access to the healthcare provider's primary network. A few users had also changed the default settings attempting to mask their use of P2P services and bypass network security and. However, nLighten provided a clear view of which devices were using the P2P services, how much data they transferred, and the external host machines. In one case, the user was a doctor on a tenant network who had installed a torrent app on his phone. In another case the device was a laptop connected to the customer's VOIP network, owned and operated by the Provider's VOIP vendor. Also detected was a P2P client connecting to an IP address in China known to distribute Ransomware.

Result:

Despite having a suite of security tools, only the nLighten platform detected this P2P behavior. This allowed the healthcare's security team to take appropriate action to block the unwanted activities and eliminate the introduction of malicious software such as Ransomware into their environment.