Issued 8/10/18

The PGA Possibly Infected With the BitPaymer Ransomware

A threat actor that is relatively new to the scene relies on open-source tools for spear-phishing attacks designed to steal credentials from government and educational institutions in the Middle East. The group is being tracked as DarkHydrus by researchers at Palo Alto Networks Unit 42, who observed it using Phishery in a recent credential harvesting attack. Previous campaigns utilized Meterpreter, Cobalt Strike, Invoke-Obfuscation, Mimikatz, PowerShellEmpire, and Veil. The typical method employed is to weaponize Office documents that retrieves malicious code from a remote site when executed.