Techniques	Defensive Recommendations
Spearphishing	Antivirus/Antimalware (M1049)
	NIPS (M1031)
	User Training (M1017)
	Software to detect spoofing Microsoft. (2020, October 13). Anti-spoofing protection in EOP. Retrieved October 19, 2020.
	Email detonation softwares
Exploitation for Client Execution	Monitoring for abnormal processes (DS0009)
	Security patches should be installed immediately to disable vulnerabilities
Windows Command Shell	Execution Prevention (M1038)
	Command Execution Detection (DS0017)
Scheduled Task	Scheduled tasks should not run with SYSTEM permission (M1028)
	Scheduling priority to be given only to Admin (M1026)
System Service	Prevent users from installing their own launch daemons (M1018)
	Disable higher permission service execution by users (M1026)
Malicious File Execution	User training (M1017)
	AV
	Monitor for File and Process Creation for eg. Using Sysmon (DS0022)
Abuse Elevation Control	Remove users from the local administrator group on systems (M1026)
	The sudoers file should be strictly edited such that passwords are always required. Setting the timestamp_timeout to 0 will require the user to input their password every time sudo is executed. (M1022)
	Detect every time a user's actual ID and effective ID are different. Read logs generated by sudo to check for privilege escalation (DS0022)
Masquerading	Require signed binaries (M1045)
	User Training - For any critical update, first verify whether Microsoft has actually released the update informtion on their official website
Forge Web Credentials	User training – Look for header information as well when viewing unexpected emails.
Process Discovery AND	Difficult to stop as a lot of genuine requests may stop
Query Registry	Create Logs to detect the API calls for process discovery/query registry, might give a pattern for adveresary behaviour
Software Discovery	Logs must be maintained for each such API call for retrospective analysis
C2- Application Layer Protocol AND	NIDS and NIPS can identify traffic associated with malware (M1031)
Encrypted Channel AND Web service: Bidirectional	Use a proxy server to analyse traffic flows and immediately block outgoing /incoming traffic
Ingress Tool Transfer	Monitor for file creation and file downloads
Exfiltration over C2 channel	Use automatic authentication for any file upload by a process.
	User Training – Avoid sending sensitive data over unencrypted channels