Initial Access: Spearphishing Link, T1192

Email to target with link to PDF download

Execution: User Execution, T1204

Malicious PDF file opened by User

PowerShell, T1086

PDF contains an exploit that is based on a buffer overflow that grants remote powershell access.

Persistence: Logon Scripts, T1037

Modify the registry and place script in startup directory

Privilege Escalation: Process Injection, T1055

In the reverse shell a payload is delivered that is based on Process Injection. It exploits a weakness that allows for Process Injection into applications that are signed with the Windows Publisher Certificate. It will spawn a second shell that has the UAC flag turned off.

Defense Evasion: Bypass User Access Control (UAC), T1088

This allows us to perform Administrator level tasks without the target being prompted for a password

Discovery: File and Directory Discovery, T1083

With the reverse shell we can navigate user’s file structure to locate directory of interest for exfil

Collection: Data from local resources, T1005

We will find a local directory that contains articles of interest and exfil the files from it

Command and Control: Remote File Copy, T1105

With our initial access we copy files onto the victim machine that will reconnect to our listener and periodically upload files

Exfil: Automated Exfiltration, T1020

Files are automatically encrypted and exfiltrated from the victim machine every time they log on

Impact: Resource Hijacking, T1496

We use the victim machines resources to mine crypto currency