Frankenstein Campaign

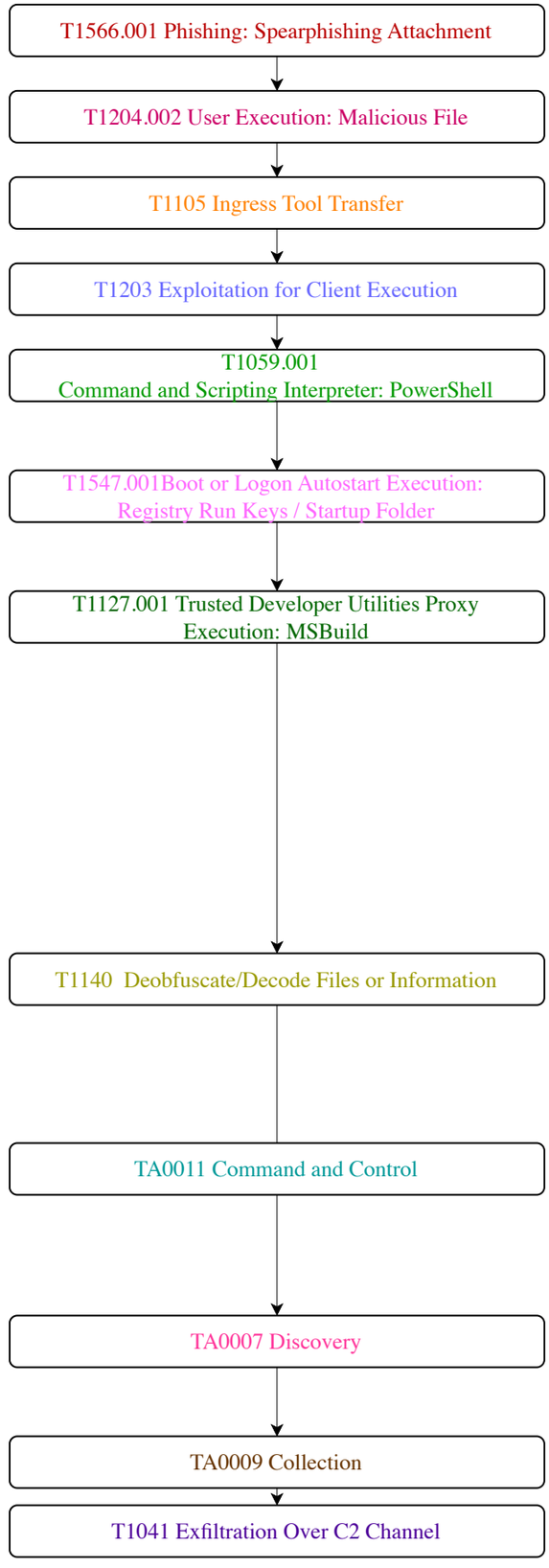
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named MinutesofMeeting-2May19.docx. Once the victim opens the document, it fetches a remove template from the actor-controlled website, hxxp://droobox[.]online:80/luncher.doc. Once the luncher.doc was downloaded, it used CVE-2017-11882, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run Registry key.

Once the evasion checks were complete, the threat actors used MSbuild to execute an actor-created file named "LOCALAPPDATA\Intel\instal.xml". Based on lexical analysis, we assess with high confidence that this component of the macro script was based on an open-source project called "MSBuild-inline-task." While this technique was previously documented last year, it has rarely been observed being used in operations. Talos suspects the adversary chose MSBuild because it is a signed Microsoft binary, meaning that it can bypass application whitelisting controls on the host when being used to execute arbitrary code.

Once the "instal.xml" file began execution, it would deobfuscate the base64-encoded commands. This revealed a stager, or a small script designed to obtain an additional payload. While analyzing this stager, we noticed some similarities to the "Get-Data" function of the FruityC2 PowerShell agent. One notable difference is that this particular stager included functionality that allowed the stager to communicate with the command and control (C2) via an encrypted RC4 byte stream. In this sample, the threat actors' C2 server was the domain msdn[.]cloud.

The C2 would return a string of characters. Once the string was RC4 decrypted, it launched a PowerShell Empire agent. The PowerShell script would attempt to enumerate the host to look for certain information. Once the aforementioned information was obtained, it was sent back to the threat actor's C2.

Ground Truth



RAF-AG's Attack Path