# TTP Detail – T1198

## TTP Information

Name: SIP and Trust Provider Hijacking

Description: In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to [Code Signing](https://attack.mitre.org/techniques/T1116), adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and whitelisting tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017)

\* Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{SIP\_GUID}</code> that point to the dynamic link library (DLL) providing a SIP’s CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file’s real signature, an adversary can apply an acceptable signature value to all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function will not match the value computed from the file).
\* Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{SIP\_GUID}</code> that point to the DLL providing a SIP’s CryptSIPDllVerifyIndirectData function, which validates a file’s computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk.
\* Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy\{trust provider GUID}</code> that point to the DLL providing a trust provider’s FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP’s CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex).
\* \*\*Note:\*\* The above hijacks are also possible without modifying the Registry via [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence