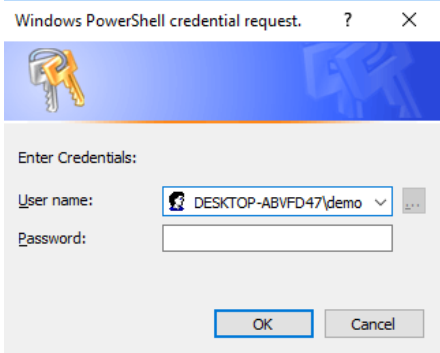


## PowerShell-Skript zum Diebstahl von Zugangsdaten

	Risiko ■□□□□
<b>Sachstand:</b>	<p>Aktuell wird von einem PowerShell-Skript gewarnt, welches das Ausspionieren von Zugangsdaten im Fokus hat. Das Skript basiert auf dem Commandlet (Cmdlet) „<i>Get-credential</i>“, welches das Standard-Eingabefenster von Windows öffnet und den Benutzer nach der Eingabe seines Benutzernamens und Passworts auffordert.</p>  <p><b>Abbildung 1: Interface des Get-Credential Cmdlet</b></p> <p>Daraufhin prüft das Skript die Zugangsdaten gegen einen Domain-Controller. Waren die Daten korrekt, werden diese an einen Server unter der Kontrolle des Angreifers übertragen, andernfalls erscheint das Fenster kurze Zeit später erneut. Mit diesem aufdringlichen Verhalten soll der Benutzer praktisch zu einer Eingabe seiner Daten gezwungen werden. Zudem lassen sich Titel und Nachricht in dem Cmdlet anpassen, sodass eine Nachricht wie „<i>Virus gefunden! Bitte geben Sie zur Bereinigung des Systems ihre Zugangsdaten ein!</i>“ in einer höheren Wahrscheinlichkeit für einen erfolgreichen Angriff resultieren können.</p> <p>Das permanente Auftreten der Eingabemaske lässt sich nur durch das Beenden des entsprechenden PowerShell-Prozesses im Task-Manager erreichen.</p>
<b>Bewertung:</b>	<p>Dieser Angriffstyp ist nicht neu, sondern ein klassischer Bestandteil der Post-Exploitation Phase (Phase, die nach erfolgreicher Ausnutzung einer Schwachstelle eintritt). Gängige Exploitation-Frameworks haben vorgefertigte Module zum Ausspionieren von Zugangsdaten integriert. Ein erfolgreiches Abgreifen der Zugangsdaten dürfte kein unrealistisches Szenario sein, die Herausforderung auf Seiten eines Angreifers besteht darin, das Skript auf einem Ziel-System zur Ausführung zu bringen.</p>
<b>Empfehlung:</b>	<p>Sowohl durch technische als auch organisatorische Methoden kann einem Angriff vorgebeugt werden. Technisch kann die Ausführung von PowerShell-Skripten (beispielsweise per Gruppenrichtlinien-Objekt) unterbunden werden. Organisatorisch können die Mitarbeiter eines Unternehmens sensibilisiert werden, zum Beispiel im Rahmen einer Warnung im Intranet. Auch wenn der Angriff nicht vollständig neu ist, verstärkt eine aktuelle Warnung das Bewusstsein eines</p>
<b>Quellen:</b>	<p>[1] <a href="#">PSA: Beware of Windows PowerShell Credential Request Prompts</a></p>