

初期侵入	検出回避	事前調査	クレデンシャルアクセス	水平移動・内部活動	情報送付	被害規模
<p>ConnectWise</p> <p>- セキュリティ対策ソフトをアンインストールすることで防御力を低下させる</p> <p>- パスワードやその他のアカウント情報なしで認証情報を照会する</p>	<p>防御力を低下させる</p> <p>- ランサムウェア</p> <p>BlackCat は、被害者のネットワークにアクセスすると、セキュリティソフトをアンインストールすることが確認されています。</p>	<p>AdFind、ADRecon</p> <p>- 感染端末のドメインアカウントに関する情報を検索するために使用されます。</p>	<p>Process Hacker, Mimikatz</p> <p>- 被害者の認証情報をダンプしてアクセスするために使用されます。</p>	<p>PSEXec</p> <p>- コマンドを実行し、ランサムウェア BlackCat のバイナリを水平移動・内部させるために使用されます。PsExec は BlackCat のバイナリ自体に埋め込まれています。</p>	<p>ExMatter</p> <p>- 二重恐喝での情報窃取に使われるマルウェア</p>	<p>BlackCat</p> <p>- ランサムウェアによる暗号化</p>
<p>Microsoft Exchange Server の脆弱性</p> <p>CVE-2021-26855</p> <p>CVE-2021-26857</p> <p>CVE-2021-26858</p> <p>CVE-2021-27065</p>		<p>SoftPerfect</p> <p>- 感染端末のネットワークに関する情報を調べるために使用されます。</p>		<p>RDP, MobaXterm</p> <p>感染端末のネットワーク内の他のエンドポイントにアクセスし、水平移動・内部活動するために使用されます。</p>	<p>7zip, RClone, MegaSync, WinSCP</p> <p>窃取した情報をアーカイブして送付させるためのサードパーティツール</p>	

