UltraSurfを使用できないようにする

内容

はじめに

このドキュメントでは、ユーザがUltraSurfを使用できないようにする方法について説明します。

問題

UltraSurfプロキシを使用してコンテンツフィルタリングとセキュリティ設定をバイパスするユーザ。

原因

UltraSurfは、一般的なコンテンツフィルタリングソリューションを回避するために、多くの対策を組み合わせています。SSLを使用してリモートホストへの接続を作成し、データを暗号化して、ほとんどのソリューションで「ピーク」を防止します。

現在、UltraSurfは、無効なSSL証明書を使用してこれらの接続を確立するため、ブラウザのセキュリティ設定を下げるように変更を加えています。以前のバージョンでは、UltraSurfはコンテンツフィルタリングソリューションをバイパスするメカニズムとしてDNSを使用していましたが、UmbrellaはDNSサーバを特定してアクセスを防止することで、この問題を緩和することができました。しかし、UltraSurfの背後にあるグループは常に新しいバージョンのソフトウェアをリリースしているので、彼らが再びアプローチを変更するのは時間の問題です。

解決方法

UltraSurfで使用されることが判明しているサブネットをブロックするなど、追加の対策を講じることができます。これらは通常、ISPによって割り当てられるダイナミックIP範囲であり、ビジネスユーザによる正当な使用はほとんどありません。また、Active Directory環境では、ソフトウェア制限ポリシーを使用してアプリケーションを制限できます。このオプションを使用すると、現在および以前のバージョンのUltraSurfソフトウェアをネットワーク上で実行することを制限できます。

新しいバージョンがリリースされたら、追加のソフトウェア制限ポリシーを追加する必要があります。また、Internet Explorerのセキュリティオプションに対してユーザーが実行できる変更を制限して、無効なセキュリティ証明書の使用を防止することもできます。Ultrasurfが各リビジョン

で行ったバージョンと変更を引き続き監視し、UmbrellaがUltrasurfへのアクセスを防ぐのに役立つ方法を検討しています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。