Prevent Users From Using UltraSurf

Contents

Introduction

This document describes how to prevent users from using UltraSurf.

Issue

Users bypassing content filtering and security configurations by using the UltraSurf proxy.

Cause

UltraSurf combines a number of measures in order to allow circumvention of common Content Filtering solutions. It creates a connection to a remote host using SSL to encrypt the data and prevent “peeking” by most solutions.

Currently, UltraSurf makes changes to lower the browser’s security settings as it uses an invalid SSL certificate to establish these connections. In previous versions, UltraSurf used DNS as a mechanism to bypass Content Filtering solutions and Umbrella was able to slow it down by identifying those DNS servers and prevent access to them. However, the group behind UltraSurf is constantly releasing new versions of their software so it’s only a matter of time before they change their approach again.

Solution

There are additional measures that can be taken including blocking subnets known to be used by UltraSurf. These are normally ISP assigned Dynamic IP ranges with little to no legitimate use for business users. Also, in Active Directory environments, it is possible to restrict applications using Software Restriction Policies. This can be used to restrict current and previous versions of the UltraSurf software from being run on your network.

As new versions are released, you would need to add additional Software Restriction Policies. It can also be possible to restrict the changes the user can make to Internet Explorer’s security options to prevent the use of invalid security certificates. We continue to monitor the versions and changes Ultrasurf makes in each revision and are looking at ways Umbrella can help with preventing Ultrasurf access.