WHITE PAPER

The Tale of Ultrasurf

ComSifter®
protect web users now!

Article Update: October 2011

IN THIS DOCUMENT

ISSUE

Local network administrator calls Comsift Technical Support stating that students are running a program called *Ultrasurf* from flash drives that were preloaded at home (or elsewhere, off the school's network).

When executed, the program was able to bypass ComSifter by opening up a proxy—allowing the student unfiltered access.

- Support asked the local administrator to turn on full logging in Advanced Firewall.
- Support observed the program making requests through open DNS ports, port 33190, and secure port 443.

Support setup a test environment at Comsift HQ. It was discovered that *Ultrasurf* was using open port 53 and port 443 to communicate with it pre-defined proxy sites.

RESOLUTION

- Support verified that customer was running the local network in proxy mode (required).
- A backup of the firewall was performed.
- Template 1 from Basic Firewall was performed.
- Two rules, allowing TCP and UDP port 53, were created. The rule only allowed DNS queries from the Domain Controller (Windows server).
- The Port 443 rule was deleted (443 is accessed through the proxy, port 8080).

When tested, *Ultrasurf* tried using port 80 to contact hard IP addresses in its database. *Ultrasurf* then tried to use port 443 and was blocked. It tried to adapt over a period of two to three minutes and was unsuccessful.

SUMMARY

Ultrasurf should be treated as a virus, as it modifies system files and erases its tracks. To stop this program you must lock down your firewall/portblocker, only allow proxied connections to port 8080, and limit port 53 to only your defined DNS servers. If open ports are required, access should be limited to only the IP addresses you are trying to reach.

Comsift, Inc. | **1646 Elderberry Way, San Jose, CA 95125-4507** | **866-875-1254** | **info@comsift.com** | **www.comsift.com**