Technical Note
2011-18003 Lionic App-Guard can block UltraSurf 10.08

1. Product

Lionic App-Guard Signature Database.

2. Description

UltraSurf is a very sophisticated P2P software. It uses a distributed network of proxy servers, installed and maintained by volunteers around the world. Completely transparent data transfer and high level encryption of the content allow you to surf the web with high security. It uses port and protocol tunneling in order to trick security devices into ignoring it or mishandling it.

3. Versions Supported

1. Lionic IDP signature database v2.346 can prevent this attack since 4/5/2011.
2. App-Guard will block the following versions of UltraSurf:
   - UltraSurf 9.5
   - UltraSurf 9.95
   - UltraSurf 9.96

- UltraSurf 9.97
- UltraSurf 9.98
- UltraSurf 9.99
- UltraSurf 10.01
- UltraSurf 10.02
- UltraSurf 10.03
- UltraSurf 10.04
- UltraSurf 10.05
- UltraSurf 10.06
- UltraSurf 10.07
- UltraSurf 10.08

4. How To

1. Enabled block UltraSurf in App-Guard.
2. Setting firewall rule to block TCP ports from 1024 to 65535. Since the version of 10.01, UltraSurf will cache super nodes data on the utmp folder. So you have to setup this firewall rule to block obfuscated behavior. Few false-positive events could be triggered.