

## COT Security Alert – Conficker/Downadup Threat

---

The COT Security Administration Branch has become aware of significant and widespread infection and propagation of the Conficker/Downadup worm among the general population. Conficker/Downadup has two variants, **Conficker/Downadup.A** and **Conficker/Downadup.B**. The MS08-067 patch will protect systems against the “.A” variant, but the “.B” variant can infect via removable media (USB drives) and brute-force password attacks even on patched systems.

Recommendations for prevention and mitigation include:

- Ensure the MS08-067 patch is installed on all Windows machines.
- Ensure the antivirus is up to date on all machines and review information your antivirus provides on this threat. (McAfee information can be found at [http://vil.nai.com/vil/content/v\\_153711.htm](http://vil.nai.com/vil/content/v_153711.htm) and [http://vil.nai.com/vil/content/v\\_153464.htm](http://vil.nai.com/vil/content/v_153464.htm) ).
- Enforce the use of strong passwords.

Some of the dangers of using USB drives are described in US-CERT Security Tip ST08-001 – Using Caution with USB Drives – which may be reviewed at <http://www.us-cert.gov/cas/tips/ST08-001.html> .

More information on mitigation of Conficker.B may be found at <http://support.microsoft.com/kb/962007>.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

**Security Administration Branch**  
**Commonwealth Office of Technology**  
**120 Glenn's Creek Road, Jones Building**  
**Frankfort, KY 40601**  
[COTSecurityServicesISS@ky.gov](mailto:COTSecurityServicesISS@ky.gov)  
<http://technology.ky.gov/security/>