

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED: October 9, 2014

SUBJECT: Recent Sweet Orange Exploit Kit campaign

CIS recently identified a campaign where the Sweet Orange Exploit Kit is being used for distributing various malware, including Qakbot, onto unpatched end-user systems. This exploit kit is hosted on compromised websites and contains various exploits for vulnerabilities in IE, Adobe and Java vulnerabilities.

To lure unsuspecting users to websites hosting the exploit kit, threat actor(s) are primarily relying on malicious advertisements as well as compromising websites running outdated content management systems. Casual analysis of the websites listed below indicates that majority of them are running vulnerable versions of Wordpress and Joomla CMS. The most recent campaign also appears to be leveraging the slider revolution plugin vulnerability for Wordpress (<http://msisac.cisecurity.org/advisories/2014/2014-070.cfm>).

As of October 9, 2014, the following websites have been identified as redirecting users to the Sweet Orange Exploit kit:

- 110nationsports[.]com
- aspecialthing[.]com
- dresseslux[.]com
- electricbikereport[.]com
- englishrussia[.]com
- eofdreams[.]com
- franklinbarbecue[.]com
- gardein[.]com
- interiordesignable[.]com
- kdrama[.]ws
- lisc[.]org
- paleopot[.]com
- scam-detector[.]com
- siteimprove[.]com
- suicideproject[.]org
- thingkid[.]com
- tlcafrica[.]com
- whatsyourdeal[.]com
- www[.]accessdata[.]com

- www.allprodad.com
- www.aquariumdrunkard.com
- www.beckershospitalreview.com
- www.conestogalogcabins.com
- www.dadamo.com
- www.designlovest.com
- www.dissentmagazine.org
- www.dougandpolly.com
- www.dukeupdate.com
- www.edelbrock.com
- www.fitness19.com
- www.handicappedpets.com
- www.howitshouldhaveended.com
- www.howtodecorate.com
- www.independentsentinel.com
- www.kathysmith.com
- www.lisc.org
- www.mansionmiami.com
- www.mybrainfitlife.com
- www.naics.com
- www.pavtube.com
- www.rantchic.com
- www.ronedmondson.com
- www.sageenvironmental.com
- www.solarpowerinternational.com
- www.stats.org
- www.techo-bloc.com
- www.thebeardediris.com
- www.theus50.com
- www.thinkfun.com
- www.tlcafrica.com
- www.vastkid.com
- www.woodworking.com
- www.yoand.biz
- xnepalif.net

After visiting the above sites, users are then redirected to the following websites hosting the exploit kit:

- 8.28.16.201
- 8.28.16.203
- cdn.calhounacademyofdance.com
- cdn.jameswoodwardmusic.com
- cdn2.movetoclarksville.com
- img.broadviewhome.info
- img.ct-trainer.com
- img.greenwoodhouse.info
- img.paws4thesoul.com

- src[.]sandcastlesmagazine[.]com
- src[.]sheffieldwoods[.]org
- yimg[.]1208nw199thpl[.]info
- yimg[.]1stdayofwinter[.]com

Recommendations:

- Block all communications to the above indicators at your network perimeter.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Keep all operating system, applications and essential software up to date to mitigate potential exploitation by attackers.
- Update Content Management Systems such as Wordpress, Joomla and Drupal running on web servers.
- Update all plugins used by the webserver and disable/remove all unused plugins.
- Consider implementing a web application firewall and/or File Integrity Monitoring solution for greater risk management for web-based applications.
- Perform regular web application and vulnerability scans of all public facing equipment. These scans should be performed, at a minimum, quarterly, but ideally on a monthly basis.

Ensure that systems are hardened with industry-accepted guidelines.