



# Early Warning and Indicator Notice (EWIN)-11-077-01A **UPDATE**

March 26, 2011

## US-CERT Early Warning and Indicator Notice

Information in this US-CERT Early Warning and Indicator Notice represents initial reporting of suspected malicious activity on critical infrastructure / key resources (CIKR) networks. This information should only be distributed to organization personnel who implement network security measures or make cybersecurity decisions.

### Technical Details

US-CERT is aware of malicious activity related to the following domains:

**---Begin Update A (1 of 1)---**

These indicators include information derived from analysis of activity at RSA.

**---End Update A (1 of 1)---**

good[dot]mincesur[dot]com  
football[dot]dynamiclink[dot]ddns[dot]us  
alvinton[dot]jetos[dot]com  
superaround[dot]ns02[dot]biz  
prc[dot]dynamiclink[dot]ddns[dot]us  
smtp[dot]dynamiclink[dot]ddns[dot]us  
www[dot]cz88[dot]net  
www[dot]alvinton[dot]jetos[dot]com  
obama[dot]servehttp[dot]com  
domikstart[dot]hopto[dot]org  
Buffet80[dot]itsaol[dot]com  
www[dot]cometoway[dot]org  
buffet[dot]bbsindex[dot]com  
safecheck[dot]organiccrap[dot]com  
free2[dot]77169[dot]net

Billgates[dot]itsAOL[dot]com  
/dom/getcmd[dot]php?id=  
agoogole[dot]in  
albertstein[dot]ddns[dot]us  
Blizzcon[dot]sexxy[dot]biz  
Blizzcon[dot]sexidude[dot]com  
ftp[dot]xmahome[dot]ocry[dot]com  
up82673[dot]hopto[dot]org  
www[dot]usgoodluck[dot]com

US-CERT will provide additional information related to these indicators as it becomes available.

#### Contact Information

(UNCLASS) Phone: 1-888-282-0870

(UNCLASS) E-mail: [soc@us-cert.gov](mailto:soc@us-cert.gov)

## Document FAQ

***What is an EWIN?*** An Early Warning and Indicator Notice is intended to provide indicators derived from new cyber incidents and/or malicious code that can pose a threat to federal and state government, critical infrastructure, private industry, or a country CERT that US-CERT collaborates with.

***I see that this document is labeled as UNCLASSIFIED. Can I distribute this to other people?*** Yes. This information should only be distributed to organization personnel who implement network security measures or make cybersecurity decisions.

***Can I edit this document to include additional information?*** This document is not to be edited, changed, or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or [soc@us-cert.gov](mailto:soc@us-cert.gov).