Xortify 2.44 - Anti #Spam, #Anti #Hacking #Cloud #Protection - Modules

NEWS_PDF_AUTHOR: wishcraft

NEWS_PDF_DATE: 2011/3/30 8:10:00

Xortify - Fortify your XOOPS.

Xortify is a network security drone that uses Web 2.0 techniques to link between your XOOPS installs and other via a Server Cloud. This will prevent security intrusions to your xoops with accurate deceptive notation of the intruder and prevent any farmed attacks. It is an accessory and required Protector to be installed an running to be part of the hookup. Otherwise it will run without protector just make sure you deselect protector as a provider.

It will display a template if you are banned and is an accessory to protector or any other firewall technology. The site itself is driven from http://xortify.chronolabs.coop and mirrored at http://www.xortify.com .. Cloud computing is web 2.0/3.0 stuff it used a SOAP or JSON, XML or Serialisation to exchange on the API backend to work.

A cloud computing process is one which staggers multiple networks sometime and mainly unknown to the webmaster into a network or cloud of data. In this example it is IP and Netaddy names to control access lists.

This will prevent predators or even spammers now from exposing your network to lag and other attacks from link farming, often this means many xoops are attacked in occasions which is all the time caught by protector, this way if an attack is in process across a large spectrum of links, your site will down itself to your sourced attack even if it is discovered on a completely unaffiliated site that is link farmed to yours or on a XOOPS User list.

Xortify is a cloud solution to protectors Bad IPs, if someone attempts to hack your site and becomes a bad IP it will then send the IP to the Ban Cloud on Xortify.com and its paired cloud Xortify.chronolabs.coop. It will also poll the server to make sure it has the latest ban list so your website will be aware of malusers before they attack through farming IP from services like Google or bing.

Xortify is an *application or process* which first started as a *practial application to cloud computing* for the XOOPS Community which shares protectors bad IPs with a contingent of end users of the Xortify application and one you have signed up ensures that members share their bad ips in IPv4 or IPv6 for the host or proxy with each other so that we are protected from each others website forensically with protector. Here at http://xortify.chronolabs.coop (AUS) (Mirrored on http://www.xortify.com our backup cloud in Germany) we host the current Bad IP List for the community so your website with the Xortify client running is pre-aware of a bad user and announces to them on all pages that they are banned unless the ban is cleared with one of our

forms.

To be a contributor to the Xortify cloud you will need a username and password which you can sign up for in the software, you only need really one username and password per website or even per webmaster, it it really upto you. We also contribute to **Stop Forum Spam** as well as using **Project Honeypot** as a resource and are receiving their ban list as well. <u>A ban is kept for 3 months then automatically removed</u> from the system to ensure truency is in check we also only list a ban really only once not multiple times, sometimes a ban is listed twice when it is causing multiple intrusions on the network but this is a rarity.

Anyone can join Xortify and you don't need to use xortify's software to maintain, or put additional bans on the framework. If you happen to be a webmaster then you are welcome to view our API Documentation to see how we can intergrate with your environment. We offer wGET, CURL and SOAP api for you use. *All you need is a username which you can sign up openly for in the software.*

Whats New in this feature

- [Project Honeypot](#) Preference Thresholds
- [Stop Forum Spam](#) Preference Thresholds
- Log Delete Time Threshold
- Ban summary provided comment on sending a ban
- Ban Language Constants & Log Constants
- Provider Post/Pre Logging Plugins
- Admin Accessible Usage Log
- [Project Honeypot](#) Provider
- [Stop Forum Spam](#) Provider
- Spider Module Provide
- XML Polling Protocol
- Serialisation API Protocol

Bugs Fixed

- WSOD on Upgrade
- Anonymous/Guest Being Permanentness of a Ban Notice
- Slow Page Loading Due to Constant Polling
- CRON Job - Fixed
- cURL Polling
- Protector provider
- Xortify Provider
- cvalue not a global
- Header being sent by providers
- Warnings & Notices Fixed

Download: xoops2.5_xortify_2.44.zip - 149Kb

Contributions:

Special thanks to **trabis** for his congruency testing and comments and his suggestion of having a usage log so you can see what it is doing! also he help with the hooks and encoragement to get this application to a finalised state like it is in 2.44

Xortify - Fortify your XOOPS.

Xortify is a network security drone that uses Web 2.0 techniques to link between your XOOPS installs and other via a Server Cloud. This will prevent security intrusions to your xoops with accurate deceptive notation of the intruder and prevent any farmed attacks. It is an accessory and required Protector to be installed an running to be part of the hookup. Otherwise it will run without protector just make sure you deselect protector as a provider.

It will display a template if you are banned and is an accessory to protector or any other firewall technology. The site itself is driven from http://xortify.chronolabs.coop and mirrored at http://www.xortify.com .. Cloud computing is web 2.0/3.0 stuff it used a SOAP or JSON, XML or Serialisation to exchange on the API backend to work.

A cloud computing process is one which staggers multiple networks sometime and mainly unknown to the webmaster into a network or cloud of data. In this example it is IP and Netaddy names to control access lists.

This will prevent predators or even spammers now from exposing your network to lag and other attacks from link farming, often this means many xoops are attacked in occasions which is all the time caught by protector, this way if an attack is in process across a large spectrum of links, your site will down itself to your sourced attack even if it is discovered on a completely unaffiliated site that is link farmed to yours or on a XOOPS User list.

Xortify is a cloud solution to protectors Bad IPs, if someone attempts to hack your site and becomes a bad IP it will then send the IP to the Ban Cloud on Xortify.com and its paired cloud Xortify.chronolabs.coop. It will also poll the server to make sure it has the latest ban list so your website will be aware of malusers before they attack through farming IP from services like Google or bing.

Xortify is an *application or process* which first started as a *practial application to cloud computing* for the XOOPS Community which shares protectors bad IPs with a contingent of end users of the Xortify application and one you have signed up ensures that members share their bad ips in IPv4 or IPv6 for the host or proxy with each other so that we are protected from each others website forensically with protector. Here at http://xortify.chronolabs.coop (AUS) (Mirrored on http://www.xortify.com our backup cloud in Germany) we host the current Bad IP List for the community so your website with the Xortify client running is pre-aware of a bad user and announces to them on all pages that they are banned unless the ban is cleared with one of our forms.

To be a contributor to the Xortify cloud you will need a username and password which you can sign up for in the software, you only need really one username and password per website or even per webmaster, it it really upto you. We also contribute to **Stop Forum Spam** as well as using **Project Honeypot** as a resource and are receiving their ban list as well. A ban is kept for 3 months then automatically removed from the system to ensure truency is in check we also only list a ban really only once not multiple times, sometimes a ban is listed twice when it is

causing multiple intrusions on the network but this is a rarity.

Anyone can join Xortify and you don't need to use xortify's software to maintain, or put additional bans on the framework. If you happen to be a webmaster then you are welcome to view our API Documentation to see how we can intergrate with your environment. We offer wGET, CURL and SOAP api for you use. *All you need is a username which you can sign up openly for in the software.*

Whats New in this feature

- [Project Honeypot](#) Preference Thresholds
- [Stop Forum Spam](#) Preference Thresholds
- Log Delete Time Threshold
- Ban summary provided comment on sending a ban
- Ban Language Constants & Log Constants
- Provider Post/Pre Logging Plugins
- Admin Accessible Usage Log
- [Project Honeypot](#) Provider
- [Stop Forum Spam](#) Provider
- Spider Module Provide
- XML Polling Protocol
- Serialisation API Protocol

Bugs Fixed

- WSOD on Upgrade
- Anonymous/Guest Being Permanentness of a Ban Notice
- Slow Page Loading Due to Constant Polling
- CRON Job - Fixed
- cURL Polling
- Protector provider
- Xortify Provider
- cvalue not a global
- Header being sent by providers
- Warnings & Notices Fixed

Download: [xoops2.5_xortify_2.44.zip](#) - 149Kb

Contributions:

Special thanks to **trabis** for his congruency testing and comments and his suggestion of having a usage log so you can see what it is doing! also he help with the hooks and encoragement to get this application to a finalised state like it is in 2.44