

Emerging Threats FAQ

[What is Emerging Threats?](#)

[Are the Emerging Threats Rules REALLY free?](#)

[How do I send in an Idea or contact the Admins of the project?](#)

[Why is emerging-all.rules not in the tarball \(emerging.rules.tar.gz\) or the zip \(emerging.rules.zip\)?](#)

[What's the emerging-botcc.excluded and why aren't there rules in it?](#)

[What is the general intent of each ruleset category?](#)

[Attack-Response Rules](#)

[BotCC Rules](#)

[Compromised Rules](#)

[Current Events Rules](#)

[DOS Rules](#)

[DROP Rules](#)

[DShield Rules](#)

[Exploit Rules](#)

[Game Rules](#)

[Inappropriate Rules](#)

[Malware Rules](#)

[P2P Rules](#)

[Policy Rules](#)

[RBN Rules](#)

[Scan Rules](#)

[Virus Rules](#)

[VOIP Rules](#)

[Web Rules](#)

[Web-SQL-Injection Rules](#)

What is Emerging Threats?

Emerging Threats is a collection point for a number of security projects, mostly related to Intrusion Detection and network Traffic Analysis. Our primary project is the Emerging Threats Snort Ruleset contributed and maintained by the security community. This is just one of many projects. You can get information about many others on our [AllProjects](#) Page. We will make a home for any project that needs one and is related to security and network traffic. We are all open source and try to build our rulesets and projects with all users in mind. We have many satisfied users and contributors from the Corporate, Government, MSSP, and Home Users Worlds. There's something here for everyone.

Are the Emerging Threats Rules REALLY free?

Yup. Free, as in BSD licensed, which allows you to do what you like with them. All we ask is that when you have an idea, a new signature, or even just a theory, that you send it in to benefit everyone.

How do I send in an Idea or contact the Admins of the project?

You can post something to the [emerging-sigs mailing list](#), catch someone in IRC at freenode.net #emerging-threats, or email to emerging@emergingthreats.net.

Why is emerging-all.rules not in the tarball (emerging.rules.tar.gz) or the zip (emerging.rules.zip)?

Simple reason. The tarball/zip is intended to be ingested by everything from GUI rule managers to Oinkmaster. The emerging-all.rules has a copy of every rule, all those that are included in each file for each category of rules. If we included -all.rules the rule managers would ingest a duplicate of every sig.

The intent of having emerging-all.rules in the first place is to make a single file download for simplicity. We recommend using the tarball or zip as there are some supporting files in there, but emerging-all.rules will do fine if you just need the rules themselves and don't need to have them broken into categories by file.

What's the emerging-botcc.excluded and why aren't there rules in it?

This is a file of some public IRC servers that often get listed in the Shadowserver Bot C&C lists. We don't want to push out rules that will block IRC servers that are commonly used for legitimate purposes, and that are responsive to abuse complaints. Generally if a C&C channel is detected and reported to these IRC admins (as Shadowserver regularly does) the channels are shutdown within minutes/hours. So we do not feel it productive to push these IPs in the block signatures.

If you run an IRC net that gets listed and you feel you've been responsive to abuse complaints, please contact threats@emergingthreats.net to get added to the exclude list.

What is the general intent of each ruleset category?

Each major category of rules is there for general organization. We don't recommend that you turn on and off sets of rules purely by the category name. You MUST take a look at the entire rulesets. But you should only have to do this once, or on regular reviews.

To assist though here's a basic explanation of each category and the intent to help you find a rule you're looking for:

Attack-Response Rules

These are designed to catch the results of a successful attack. Things like "id=root", or error messages that indicate a compromise may have happened. Note: Trojan and virus post-infection activity is included generally in the VIRUS ruleset, not here.

BotCC? Rules

These are autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. Updated daily, primary data source is Shadowserver.org.

Compromised Rules

This is a list of known compromised hosts, confirmed and updated daily as well. This set varied from a hundred to several hundred rules depending on the data sources. This is a compilation of several private but highly reliable data sources. Warning: Snort does not handle IP matches well load-wise. If your sensor is already pushed to the limits this set will add significant load. We recommend staying with just the [BotCC?](#) rules in a high load case.

Current_Events Rules

These are rules that we don't intend to keep in the ruleset for long, or that need to be tested before they are considered for inclusion. Most often these will be simple sigs for the Storm binary URL of the day, sigs to catch CLSID's of newly found vulnerable apps where we don't have any detail on the exploit, etc. Useful sigs, but not for the long term.

DOS Rules

Intended to catch inbound DOS activity, and outbound indications. Relatively self-explanatory.

DROP Rules

This is a daily updated list of the Spamhaus DROP (Don't Route or Peer) list. Primarily known professional spammers. More info at <http://www.spamhaus.org>

DShield Rules

Daily updated list of the DShield top attackers list. Also very reliable. More info at <http://www.dshield.org>

Exploit Rules

Rules to detect direct exploits. Generally if you're looking for a windows exploit, Veritas, etc, they'll be here. Things like SQL injection and the like, while they are exploits, have their own category.

Game Rules

World of Warcraft, Starcraft, and other popular online games have sigs here. We don't intend to label these things evil, just that they're not appropriate for all environments.

Inappropriate Rules

Porn, Kiddy porn, sites you shouldn't visit at work, etc. Warning: These are generally quite Regex heavy and thus high load and frequent false positives. Only run these if you're really interested.

Malware Rules

My personal favorite. This set was originally intended to be just spyware. That's enough to several rule categories really. The line between spyware and outright malicious bad stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemes, User-Agent strings of known malware, and a load of other goodies. If you can only run one ruleset to justify your IDS infrastructure, this is it!

P2P? Rules

Peer to Peer stuff. Bittorrent, Gnutella, Limewire, you name it. We're not labeling these things Bad(tm), just not appropriate for all networks and environments.

Policy Rules

Rules for things that are often disallowed by company or organizational policy. Myspace, Ebay, that kind of thing.

RBN Rules

The Russian Business Network. These rules track the networks they're known to own and regularly used. Updated whenever information changes.

Scan Rules

Things to detect reconnaissance and probing. Nessus, Nikto, portscanning, etc. Early warning stuff.

Virus Rules

This is another large category. Includes Trojans, Worms and Viruses. Sigs to detect them in transit, active, infecting, attacking, updating, and whatever else we can see them doing. This is also a highly important ruleset to run if you have to choose.

VOIP Rules

A new and emerging ruleset. Small at the moment, but we expect it to grow soon.

Web Rules

Some SQL Injection, web server overflows, vulnerable web apps, that kind of thing. Very important if you're running web servers, and pretty reasonable load.

Web-SQL-Injection Rules

This is a large ruleset that intends to catch specific attacks on specific applications. There are some general SQL injection rules that work pretty well to catch most of what's covered here. But these rules are much more specific to apps and web servers. Run this if you run a highly critical web farm, or are interested in having exact information about incoming web attacks.

-- [MattJonkman](#) - 08 Jan 2008

Copyright © by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? [Send feedback](#)

