proofpoint

ETPro Category Descriptions

ETPro features over 50 categories which may be assigned to individual signatures. These categories are assigned as signatures are created and updated. To help understand how these category names are selected and attributed to each signature, below is a list of definitions for each category.

1. **Activex** – Attacks and vulnerabilities(CVE, etc.) regarding ActiveX.

2. **Attack Response** – Responses indicative of intrusion—LMHost file download, certain banners, Metasploit Meterpreter kill command detected, etc. 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.

3. **Botcc** (Bot Command and Control) – 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. Bot command and control block rules generated from shadowserver.org, as well as spyeyetracker, palevotracker, and zeustracker. Port grouped rules offer higher fidelity with destination port modified in rule.

4. **Botcc Portgrouped –** Same as above, but grouped by destination port.

5. **Chat** – identification of traffic related to numerous chat clients, irc, and possible check-in activity.

6. **CIArmy** – Collective Intelligence generated IP rules for blocking based upon www.cinsscore.com.

7. **Compromised** – This is a list of known compromised hosts, confirmed and updated daily as well. This set varied from a hundred to several hunderd rules depending on the data sources. This is a compilation of several private but highly reliable data sources. Warming: 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.

8. **Current Events** – Category for active and short lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short lived nature of the threat. High profile items that we don't expect to be there long—fraud campaigns related to disasters for instance. 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.

9. **Decoder-events –** Suricata specific. These rules log normalization events related to decoding.

10. **Deleted –** Rules removed from the rule set.

11. **DNS** - Rules for attacks and vulnerabilities regarding DNS. Also category for abuse of the service for things such as tunneling.

12. **DOS** – Denial of Service attempt detection. Intended to catch inbound DOS activity, and outbound indications.

13. **Drop** – Rules to block spamhaus "drop" listed networks. IP based. 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.

14. **Dshield** – IP based rules for Dshield Identified attackers. Daily updated list of the DShield top attackers list. Also very reliable. More information can be found at http://www.dshield.org.

15. **Exploit** – Exploits that are not covered in specific service category. 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, whie they are exploits, have their own category.

16. **Files** - Example rules for using the file handling and extraction functionality in Suricata.

17. **FTP** - Rules for attacks, exploits, and vulnerabilities regarding FTP. Also includes basic none malicious FTP activity for logging purposes, such as login, etc.

18. **Games** – Rules for the Identification of gaming traffic and attacks against those games. 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.

19. **HTTP-Events -** Rules to log HTTP protocol specific events, typically normal operation.

20. **ICMP** - Rules for attacks and vulnerabilities regarding ICMP. Also included are rules detecting basic activity of the protocol for logging purposes.

21. **ICMP_info -** Rules to log ICMP protocol specific events, typically normal operation.

22. **IMAP** - Rules for the identification, as well as attacks and vulnerabilities regarding the IMAP protocol. Also included are rules detecting basic activity of the protocol for logging purposes.

23. **Inappropriate** – Rules for the identification of pornography related activity. Includes 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.

24. **Malware** – Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. 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 schemed, User-Agent strings of known malware, and a load of others.

25. **Misc**. - Miscellaneous rules for those rules not covered in other categories.

26. **Mobile Malware** – Specific to mobile platforms: Malware and Spyware related, no clear criminal intent.

27. **Netbios** - Rules for the identification, as well as attacks, exploits and vulnerabilities regarding Netbios. Also included are rules detecting basic activity of the protocol for logging purposes.

28. **P2P** – Rules for the identification of Peer-to-Peer traffic and attacks against. Including torrents, edonkey, Bittorrent, Gnutella, Limewire, etc. We're not labeling these things malicious, just not appropriate for all networks and environments.

29. **Policy** – Application Identification category. Includes signatures for applications like DropBox and Google Apps, etc. Also covers off port protocols, basic DLP such as credit card numbers and social security numbers. Included in this set are rules for things that are often disallowed by company or organizational policy. Myspace, Ebay, etc.

30. **POP3** - Rules for the identification, as well as attacks and vulnerabilities regarding the POP3 protocol. Also included are rules detecting basic activity of the protocol for logging purposes.

31. **RBN & RBN-malvertisers** – (Russian Business Network) – IP based rules for the identification of the Russian Business Network. [THIS RULESET HAS BEEN OBSELETED AND REMOVED. IT IS NO LONGER USED. IT IS INCLUDED AS A RULE FILE TO INFORM USERS OF ITS REMOVAL]

32. **RPC** – RPC related attacks, vulnerabilities, and protocol detection. Also included are rules detecting basic activity of the protocol for logging purposes.

33. **SCADA** – Signatures for SCADA attacks, exploits and vulnerabilities, as well as protocol detection.

34. **SCADA_special** – Rules written for Snort Digital Bond based SCADA preprocessor.

35. **SCAN** - Things to detect reconnaissance and probing. Nessus, Nikto, portscanning, etc. Early warning stuff.

36. **Shellcode** – Remote Shellcode detection. *Remote* shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections

to allow the attacker access to the shell on the target machine. Such shellcode can be categorised based on how this connection is set up: if the shellcode can establish this connection, it is called a "reverse shell" or a *connect-back* shellcode because the shellcode *connects back* to the attacker's machine.

37. **SMTP** - Rules for attacks, exploits, and vulnerabilities regarding SMTP. Also included are rules detecting basic activity of the protocol for logging purposes.

38. **SMTP-events** – Rules that will log SMTP operations.

39. **SNMP** - Rules for attacks, exploits, and vulnerabilities regarding SNMP. Also included are rules detecting basic activity of the protocol for logging purposes.

40. **SQL** - Rules for attacks, exploits, and vulnerabilities regarding SQL. Also included are rules detecting basic activity of the protocol for logging purposes.

41. **Stream-events –** Rules for matching TCP stream engine events.

42. **TELNET** - Rules for attacks and vulnerabilities regarding the TELNET service. Also included are rules detecting basic activity of the protocol for logging purposes.

43. **TFTP** - Rules for attacks and vulnerabilities regarding the TFTP service. Also included are rules detecting basic activity of the protocol for logging purposes.

44. **TLS-Events –** Rules for matching on TLS events and anomalies.

45. **TOR** – IP Based rules for the identification of traffic to and from TOR exit nodes.

46. **Trojan** – Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and whatever else we can detect on the wire. This is also a highly important ruleset to run if you have to choose.

47. **User Agents** – User agent identification and detection.

48. **VOIP** - Rules for attacks and vulnerabilities regarding the VOIP environment. SIP, h.323, RTP, etc.

49. **Web Client** – Web client side attacks and vulnerabilities.

50. **Web Server** – Rules for attacks and vulnerabilities against web servers.

51. **Web Specific Apps** – Rules for very specific web applications.

52. **WORM** – Traffic indicative of network based worm activity.