

Common Malware Enumeration — CME™

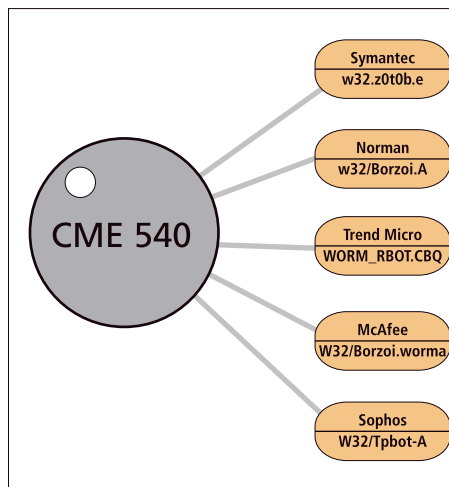
Reducing Public Confusion During Malware Outbreaks

CME PROVIDES SINGLE, common identifiers to new virus threats and to the most prevalent virus threats in the wild to reduce public confusion during malware incidents. CME is not an attempt to replace the vendor names currently used for viruses and other forms of malware, but instead aims to facilitate the adoption of a shared, neutral indexing capability for malware.

Why CME

From widespread outbreaks of computer viruses to more local and targeted threats, anti-virus companies have had an increasingly difficult time staying coordinated with names for all of the new viruses. Because of this their products use a variety of names and variant designations for the same threat. This results in widespread confusion, with members of the public having to determine whether they face a single threat, multiple threats, or a new threat altogether.

CME assigns a single, common identifier to the union of the components that make up a single threat. For example, all components of Nimda—the IIS buffer overflow byte stream, the file that is passed through TFTP, the mass-mailed email it creates that attacks via the audio/x-wav vulnerability, the appended html pages or any of its other forms—are referenced by a single CME identifier.



While the various anti-virus entities may still assign their own names, CME's common identifier enables network administrators to quickly identify the specific virus outbreaks and most prevalent virus threats in the wild to which their organizations might be susceptible and to ensure that they are properly protected.

CME Editorial Board Sample Redistribution Group & Technical Feedback Group

The CME Editorial Board includes members from the international anti-virus community, including product vendors, testing organizations, and government. The Board works collectively to define the goals and processes of the initiative. Many Board members also act as members of the CME Sample Redistribution Group (SRG), discovering and submitting possible threats for inclusion on the CME List. Other anti-virus and information security experts will be invited to participate on the Board on an as-needed basis based upon recommendations from Board members. Operational information security experts from large corporations, academia, government, and non-profit organizations serve on the CME Technical Feedback Group (TFG), providing an end-user perspective on CME activities. Refer to the CME Web site at <http://cme.mitre.org> for the most recent lists of members.



The MITRE Corporation—a Federally Funded Research and Development Center—maintains CME and its public Web site and provides impartial technical guidance to the CME Editorial Board, Sample Redistribution Group, and Threat Assessment Focus Group throughout the process to ensure CME serves the public interest.

202 Burlington Road, Bedford, MA 01730-1420
www.mitre.org

MITRE

The CME Identifier

CME identifiers are assigned in the format “CME-N” where N is an integer between 1 and 999, for example, “CME123”. Identifier numbers are assigned randomly, not sequentially. To accommodate space-deprived anti-virus products, CME identifiers can be abbreviated (e.g., M123 or M-123), but the official format (i.e., CME-123) should be used in places such as Web pages, alerts, encyclopedias, etc.

Visit the CME List on the CME Web site to review all identifiers assigned to date.

Each CME “profile” includes the following:

- CME Identifier
- Description of the malware and/or comments
- Vendor aliases with links to their malware encyclopedias or alerts
- Date assigned

How CME Works

CME identifiers are assigned to both high-profile threats and the most prevalent virus threats in the wild. As defined by the CME Threat Assessment Focus Group (composed of members of the Editorial Board, the SRG and the TFG), high-profile malware threats include “considerable or notable malware threat(s) potentially confusing users, malware threats posing a considerable risk to a user, and/or malware that draw media attention.” Specific threats are identified by the CME Sample Redistribution Group members who have access to malware samples. CME relies on the historical experience of these members, as well as the perspectives of the user representatives on the Technical Feedback Group, to know when an incident is noteworthy enough for inclusion on the CME List.

CME Identifier Assignment

When a qualifying threat occurs, organizations participating in the CME SRG will request a CME identifier from MITRE’S CME Submission Server. The participant will provide a sample and as much supporting information as possible. CME’s automated system redistributes the submitted information

to the members of the SRG and TFG. If the submission is endorsed by another member of the SRG or the TFG, CME’s automated system generates a CME identifier and notifies the CME participants. The CME identifier and supporting information is subsequently posted on the CME List on the CME Web site.

Dissemination

Once the CME identifier has been attached to the sample and its corresponding threat, each CME participant will then disseminate the CME identifier as quickly as possible to those entities with which they regularly communicate in the industry and will reference the CME identifier in their products, on their Web sites, in communications with their customers, and when providing information to the press.

Adoption

Widespread use of CME’s common identifiers will help the information security community—and the public—communicate more effectively during computer virus outbreaks, thereby reducing the extensive confusion that occurred in the past. For example, before CME one anti-virus product might name a computer virus ‘NewOutbreak.A’ and a second

product might name the same virus ‘OldFamily.CC’. By using a CME identifier, the names will be ‘NewOutbreak.A!M555’ and ‘OldFamily.CC!M555, indicating that the threat is the same.

We strongly encourage users of anti-virus products to ask

Benefiting the community

Adopting the use of CME identifiers is a significant first step in establishing a consistent approach by anti-virus entities that will benefit users and the entire information security community.

their preferred vendors to adopt CME identifiers. For anti-virus product vendors, supporting and participating in the CME Initiative announces to your users that you want to help alleviate their confusion and further protect their systems and networks.

See the CME Web site for a complete list of the numerous organizations already including CME identifiers in their information security and anti-virus products and services.