SEPTEMBER 2005

virus BULLETIN

The International Publication on Computer Virus Prevention, Recognition and Removal

CONTENTS

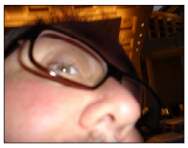
ISSN 0956-9979

IN THIS ISSUE

A NEW BREED

In the last year or two, an increasing number of *Symbian* threats have been reported. While there are not yet many malware writers who are interested in the *Symbian* OS, this may soon change. Robert Wang asks: is the *Symbian* OS in danger of further attacks?
page 6

A RIGHT PAIR



Although one always hears about 'Black Hat *and* DEFCON', they are in fact two very different events. *VB*'s intrepid reporter (aka AV industry miscreant) has a report on each.
page 11

A NEW NAMING INITIATIVE

The Common Malware Enumeration (CME) initiative is a new effort headed by the US-CERT, which aims to match a unique identifier to each threat. Jimmy Kuo and Desiree Beck explain how it is hoped this initiative will help alleviate the 'virus-naming mess'.
page 14

vbSpam supplement

This month: anti-spam news and events, and Sorin Mustaca provides *VB*'s first phishing analysis.

SPOTLIGHT

THE COMMON MALWARE ENUMERATION (CME) INITIATIVE

Jimmy Kuo
McAfee AVERT, USA

Desiree Beck
MITRE, USA

The Common Malware Enumeration (CME) initiative is an effort headed by the United States Computer Emergency Readiness Team (US-CERT, www.uscert.gov). Established in 2003 to protect the USA's Internet infrastructure, US-CERT coordinates defence against and responses to cyber attacks across the nation. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

Through the adoption of a neutral, shared identification method, the CME initiative seeks to:

- Reduce the public's confusion in referencing threats during malware incidents.
- Enhance communication between anti-virus vendors.
- Improve communication and information sharing between anti-virus vendors and the rest of the information security community.

CME is fashioned similarly to the Common Vulnerabilities and Exposures (CVE) initiative (http://cve.mitre.org/), which is also operated by *MITRE* in support of US-CERT. As experience with CVE shows, once all parties have adopted a neutral, shared identification method, effective information sharing can happen faster and with more accuracy.

A CME Preliminary Editorial Board (CME-PEB) has been brought together to work with US-CERT to help bring the CME concept to maturity and expand CME's reach to other members of the anti-malware community. At the time of writing, the members of the CME-PEB represent:

- *McAfee*
- *Symantec*
- *Trend Micro*
- *Microsoft*
- *Sophos*
- *Computer Associates*
- *Norman*
- *Kaspersky Lab*
- *MessageLabs*
- *F-Secure*
- *ICSA Labs*

Oversight of the board is provided by US-CERT and *MITRE*.

The CME Initial Operating Capability (CME-IOC) was stood up at the end of the first quarter of 2005 to provide a limited operational capability for CME identifier acquisition. A CME website will be available in the fourth quarter to introduce the initiative to the public (http://cme.mitre.org/).

REDUCING PUBLIC CONFUSION DURING MALWARE OUTBREAKS

It is apparent that anti-virus companies are having an increasingly difficult time staying coordinated with virus names during computer virus outbreaks. As a result, products report a variety of names and variant designations for the same outbreak. This results in widespread confusion, with members of the public having to determine whether there is a single outbreak underway, whether there are multiple outbreaks underway, or whether they are seeing a new and different outbreak altogether.

Having to determine whether the protection they have in place is effective against the current outbreak increases the public's burden further. For example, the spring of 2004 was an extremely difficult period. Three or more Netsky variants appeared along with new variants of Mydoom, Bagle and Beagle, all within a couple of days. Network administrators were pulling their hair out as they tried to determine whether or not they had the protection they needed.

The CME initiative does not offer to coordinate all the anti-virus companies so that they use one and the same name (although we hope that name coordination will improve eventually, as a side-effect). Rather, the CME initiative will match a CME identifier to a particular threat, with the hope that most anti-virus entities, as well as other security-related entities, will adopt its use. This will allow the public to cross-reference the disparate names through a common identifier.

Note the word 'threat'. This is different from the normal course of anti-virus procedure in detecting and naming singular virus-related files. A 'threat' is a single entity encompassing any number of files that may be involved in a single outbreak. For example, all the 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 – will be referenced by one CME identifier.

THE CME IDENTIFIER

Initially, CME identifiers will be in the format 'CME-N' where N is an integer between 1 and 999. Digits will be added when the remaining unused identifier space becomes too small.

To accommodate space-deprived anti-virus products, CME IDs can be abbreviated (e.g. M123 or M-123), but the

official format (e.g. CME-123) should be used in places such as web pages, encyclopedias, etc.

For the sake of successful text-based comparisons, leading zeros will always be omitted in an identifier. For example, CME-00123 will always be written as CME-123. Identifiers will be generated randomly within each size range (e.g. CME-439 might be issued before CME-28). This way, it will not be possible for someone to assign their own identifier by guessing the next in sequence.

By minimizing the number of characters used initially, it is hoped that many anti-virus products will be able to add the CME identifier directly to the names their products display for the user. For example, a virus named 'NewOutbreak.A' will be shown to the user as 'NewOutbreak.A!M-555', while at the same time, another anti-virus product might report the same outbreak as 'OldFamily.CC!M-555'. In this way, a user will be able to ascertain quickly whether or not two viruses are the same, and as a result user confusion will be reduced.

THE PROCEDURE

The public needs the most guidance during virus outbreaks. For that reason, the CME-IOC will begin by addressing only the situations that satisfy outbreak conditions. Since most of the initial member organizations on the CME-PEB have representatives who also participate on the Anti-Virus Emergency Discussion list (AVED, http://www.aved.net/), the CME-PEB will follow a similar approach during IOC to identify high visibility threats warranting CME identifiers.

When a qualifying threat occurs, a CME participant will request a CME identifier. The participant will provide a sample and as much supporting information as possible. In response, an automated system will generate a CME identifier and will redistribute the submitted information to the other participants.

A CME identifier will then have 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 it regularly communicates in the industry and will reference the CME identifier on their web pages, in their product, or when speaking to the press, as best as can be achieved.

Use of the CME identifier is completely voluntary. However, we hope that anti-virus product users will encourage their preferred vendors to adopt CME identifiers. Widespread use of the CME identifier will help us all communicate more effectively about threats. Using CME identifiers, we will know when two threats are equivalent and when they are not.

DECONFLICTION

Deconfliction is a term that originated in the military. Here, we use it to refer to the activity required to avoid issuing more than one CME identifier to equivalent threats.

The first step in deconfliction is when a CME identifier is issued automatically. At this point, automated issuance of CME identifiers is turned off for the next two hours. Two hours was chosen as a reasonable amount of time for the CME-IOC. It may be adjusted as needed. This two-hour moratorium prevents messages that may have passed in the ether to cause two CME identifiers to be issued for the same event.

During the two hours following the issuance of a CME identifier, additional CME identifier requests will be deferred until the participants can decide whether the submitted samples constitute a new threat or are equivalent to the previous threat. If the participants agree that a submitted sample is a new threat, then an additional CME identifier can be 'forced'.

ADOPTION

Samples distributed. Matching CME identifier produced. The next step is the most critical. We must garner adoption of the CME initiative among anti-virus product producers.

Long ago, one of the authors argued that the 'virus-naming mess' is not a technical problem. The problem and solution lie in the willingness of the product producers to *want* to help resolve this mess. Supporting and, as applicable, participating in the CME initiative is a bold first step in announcing to your users that you want to help alleviate their confusion. There are certainly technical challenges to coming out of the gate with all products all using the same name. But these challenges cannot be said to hold true 48 hours, one week, or many weeks after an outbreak.

First, coordinated CME identifiers. Then, maybe we can solve this naming mess!

Editor's note:

The CME-PEB will be holding a Birds of a Feather session at the Virus Bulletin conference in Dublin, as an opportunity for VB2005 delegates to learn more about CME and its current status, as well as provide feedback and express interest in future involvement. The BoF session will take place after the close of the first day of the conference: 6pm–7pm Wednesday 5 October 2005 at the conference venue. Also at VB2005, Vesselin Bontchev will be presenting his take on the 'virus-naming mess' with a paper on the current status of the CARO malware-naming scheme. Register for the conference now at http://www.virusbtn.com/conference/vb2005/.