

MARC BLANCHARD VIRUS DOCTEUR

[Définition&Explications] La technologie MUTEX

De nombreux codes malicieux, aujourd'hui, utilisent une technologie un peu particulière qui se nomme MUTEX.

Définition :

C'est une technique permettant d'allouer physiquement un emplacement mémoire particulier et de le réserver.

Toute application utilisant la technique Mutex ne peut PAS être déchargée, arrêtée ou détruite sans en avoir détruit son parent.

La notions de gestion des processus parents/enfants est alors utilisée.

On dira dans ce cas un « programme persistant ».

Pour exemple plus concret, il est quasiment impossible d'arreter un serveur de mail de type Exchange....

Il en est de même avec le process SVCHOST !

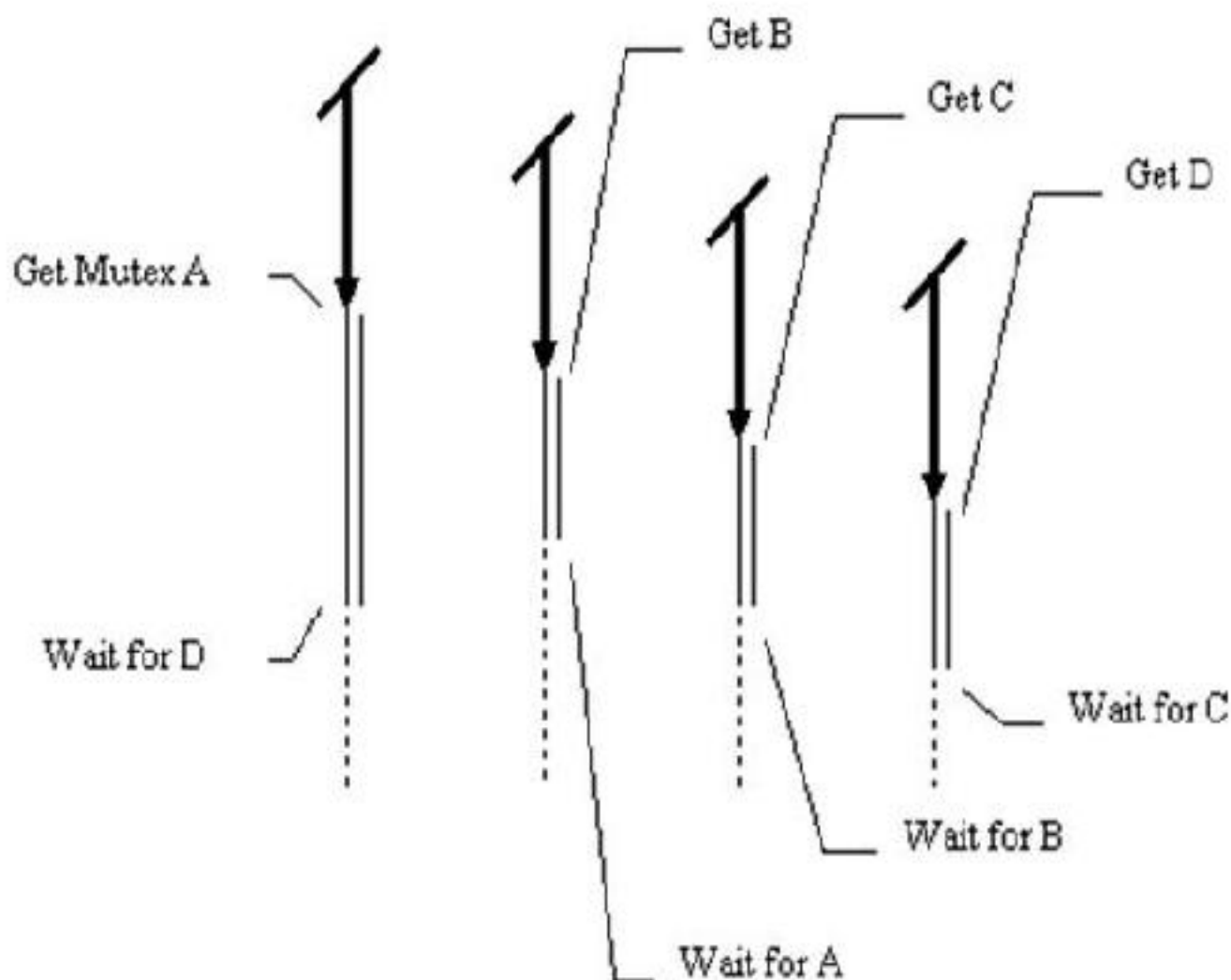
Pour stopper un programme persistant, il suffit de stopper tous les processus enfants pour finir par arrêter le programme parent.

Définition de cette technique par les codes malicieux :

Technologie MUTEX : « Le chat qui se mord la queue! »

On sait, de par cette technique, que les process enfants doivent être stoppés afin que le dernier enfant puisse faire un 'kill' du parent

Les développeurs de virus ont légèrement modifié le processus mutex.



Comme on peut le constater sur cette image, le parent GetMutex A pour être stoppé attend la fin du process D, qui lui-même attend la fin du process C, qui lui-même attend la fin du process B, qui lui-même attend la fin du process A...MAIS comme le process A attend la terminaison du process D, on dit que le chat se mord la queue !!!

CONCLUSION :

Des fonctionnements cycliques sont difficiles à décharger de la mémoire dues à leurs dépendances inter-liées

Une application telle qu'un Antivirus peut rencontrer des problèmes pour décharger un process utilisant Mutex (un cleaner spécifique, dans ce cas, est obligatoire).

Cela permet aux codes malicieux de devenir de VRAIs programmes résidant et persistant en mémoire.

Commentaires

2007-11-16 20:51:33 - Simon - <http://www.carantec-pc.com>

C'est intéressant mais trop court. J'ai eu affaire à quelques virus du type. La solution la plus simple est le LiveCD qui évite au processus parent de se lancer...

Dans l'exemple donné, s'agit-il du même fichier image chargé plusieurs fois ? Ou de plusieurs processus ayant des sources et des noms différents ?

2007-11-19 10:34:46 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Oui Simon, le fait de redemarrer avec un LiveCD est une bonne solution, un autre solution (dépendra de la technologie utilisée par le code malicieux) est de redémarrer en mode sans echec, Relancer un Scan Antivirus, et effectuer le nettoyage.... Il y a une autre solution, comme je l'ai indiqué, qui consiste à utiliser des Cleaners...ce sont des outils, spécifiquement développés pour ce type de code malicieux, notamment aujourd'hui avec les Storm Worms et Storm Botnet.

2007-11-19 15:59:33 - catz

Comment le cleanner peut-il se détourner des sauts cycliques dans ce type de cas, peux-tu donner un exemple de ces cleaners

2007-11-19 16:38:20 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Je ne peux pas vous donner des secrets de fabrications, sinon certaines personnes mal intentionnées pourraient exploiter la chose, mais les procédés utilisés en pour ces nettoyeurs fonctionnent relativement bien ;-). Cependant, si les codes malveillants utilisent une technologie rootkit en plus du mutex, qui est fortement utilisé actuellement, il devient difficile de les eradiquer en mode normal, d'où le mode sans echec! Cependant, chez KL, nous utilisons une console d'administration (AdminKit) qui, en conjointe utilisation avec nos cleaners, permettent d'avoir des droits plus intimes avec l'OS :-)

2007-12-17 11:50:19 - sopsoph - vallet_soph@yahoo.fr

Un virus de ce type n'est donc pas détectable par kaspersky, c'est ça? Quels sont les signes apparants de ce type d'infection?

Cordialement

2007-12-17 12:44:43 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Non, je n'ai pas dit cela. Juste que ces technologies sont difficiles à éradiquer. Par conséquent, lorsqu'il n'est pas possible d'éradiquer ce type de technologie, soit un redémarrage sans échec est indispensable, soit un nettoyeur indépendant est nécessaire.

Copyright : Blanchard [Virus Docteur] Marc - 2007-11-15 18:40:12
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>