

Virtual Machine Based Rootkits

News Summary

Die Virtual Based Rootkits (VMBRs) entstehen aus einer Kombination von herkömmlichen Rootkit-Techniken mit einer virtualisierten Rechnerumgebung, wie sie sich vor allem in den Produkten VMWare und VirtualPC wiederfindet. Die im Rahmen des Projektes [SubVirt](http://www.eecs.umich.edu/virtual/software.html "SubVirt") entwickelte VMBR-Suite übernimmt den angegriffenen Host vollständig und emuliert sodann das hierauf befindliche Betriebssystem (Linux-Derivate bzw. Windows BS) innerhalb einer durch die Suite bereitgestellten virtuellen Maschine. Sodann kann das System auf dem "Wirtshost" weitere virtuelle Systeme starten, die der eigentlichen Schadfunktionen dienen.

Zwar sind derart technisch anspruchsvollen Angriffe auf Rechnersysteme bisher noch nicht "in the wild" gesichtet worden, jedoch steht zu erwarten, dass deren Realisierung angesichts der Lukrativität bestimmter rechnergestützter Delikte nicht mehr in weiter Ferne liegt. Die Problematik der Erkennbarkeit eines derartigen Rootkits äußert sich vor allem darin, dass jenes vollständig die Systemumgebung kontrolliert und insoweit bisherige Rootkit-Erkennungstechniken weitgehend wirkungslos sind. Auch ein Neustart des Systems beeinträchtigt die Funktionalität des Rootkits (wie auch schon bei den bisher angewandten Rootkit-Techniken) nicht: Die VMBRs emulieren ohne weiteres einen Shutdown bzw. einen Standby des Systems.

Die Forschungsergebnisse zum Thema sind im Paper [SubVirt: Implementing malware with virtual machines](http://www.eecs.umich.edu/virtual/papers/king06.pdf "SubVirt: Implementing malware with virtual machines") zusammengefasst, welches für das diesjährige IEEE Symposium on Security and Privacy eingereicht wurde.

News Text

weiterführende Links

[Leitseite smartnuts.com](#)

[Urteilsdatenbank smartnuts.com](#)