Rootkits and Bootkits

Reversing Modern Malware and Next Generation Threats

by Alex Matrosov, Eugene Rodionov, and Sergey Bratus

Errata updated to print 3

Page	Error	Correction	Print corrected
10	When a read operation is encountered, TDL3 zeros out the return buffer on completion of the I/O operation, and it skips the whole read operation in the event of a write data request.	When a read operation is encountered, TDL3 zeros out the return buffer on completion of the I/O operation, and it skips the whole write operation in the event of a write data request.	Pending
42	/Device/HarddiskO/DRO object OBJECT_HEADER ObjectType Object body Legitimate OBJECT_TYPE UpenProcedure OpenProcedure OpenProcedure	/Device/Harddisk0/DR0 object OBJECT_HEADER ObjectType Object body	Pending
	Before inception After inception	Before interception After interception	
	/Device/HarddiskO/DRO object OBJECT_HEADER ObjectType ObjectType	/Device/HarddiskO/DRO object OBJECT_HEADER ObjectType Legitimate OBJECT_TYPE OpenProcedure OpenProcedure handler	
	Object body Malicious OBJECT_TYPE OpenProcedure OpenProcedure handler Figure 3-2: Hooking the OpenProcedure handler via ObjectType manipulation	Object body Malicious 0BJECT_TYPE Malicious OpenProcedure OpenProcedure handler Figure 3-2: Hooking the OpenProcedure handler via ObjectType manipulation	
141	The bootkit's job is done once it has loaded the malicious kernel-mode driver (6 in Figure 10- 4), which implements Olmasco's rootkit functionality.	The bootkit's job is done once it has loaded the malicious kernel-mode driver (6 in Figure 10- 3), which implements Olmasco's rootkit functionality.	Pending

