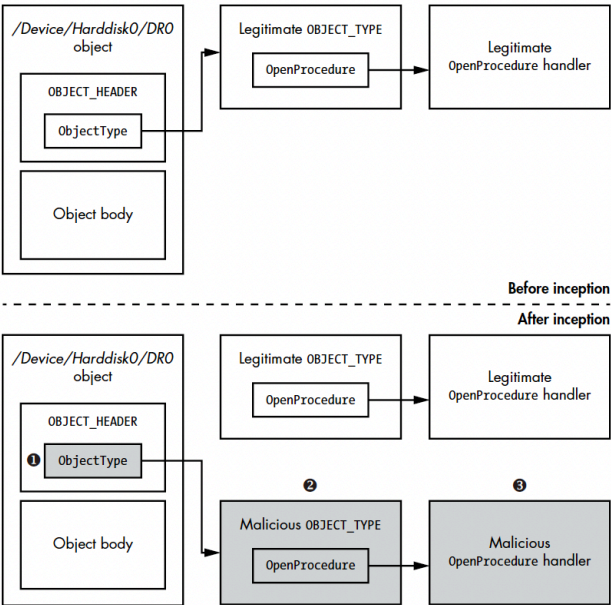
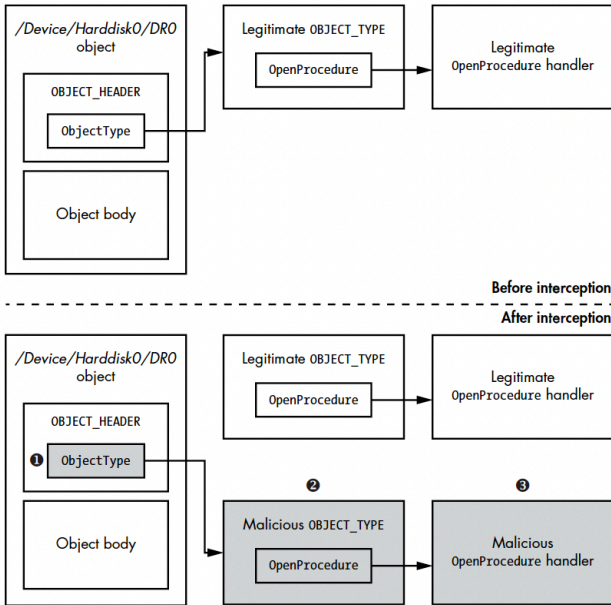


# Rootkits and Bootkits

## 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 <b>read</b> 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 <b>write</b> operation in the event of a write data request.	Pending
42	 <p>Figure 3-2: Hooking the <code>OpenProcedure</code> handler via <code>ObjectType</code> manipulation</p>	 <p>Figure 3-2: Hooking the <code>OpenProcedure</code> handler via <code>ObjectType</code> manipulation</p>	Pending
141	The bootkit's job is done once it has loaded the malicious kernel-mode driver (❸ 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 (❸ in Figure 10-3), which implements Olmasco's rootkit functionality.	Pending

Page	Error	Correction	Print corrected
210	<p>Figure 13-1: Modus operandi of modern ransomware</p>	<p>Figure 13-1: Modus operandi of modern ransomware</p>	Pending