УДК 004.056
ББК 32.973.202
М33

Алекс Матросов, Евгений Родионов, Сергей Братусь

М33 Руткиты и буткиты. Обратная разработка вредоносных программ и угрозы следующего поколения / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2022. – 442 с.: ил.

ISBN 978-5-97060-979-8

Эта книга посвящена обнаружению, анализу и обратной разработке вредоносного ПО. В первой части описываются примеры руткитов, показывающие, как атакующий видит операционную систему изнутри и находит способы надежно внедрить свои импланты, используя собственные структуры ОС. Вторая часть рассказывает об эволюции буткитов, условиях, подхлестнувших эту эволюцию, и методах обратной разработки таких угроз.

Издание адресовано широкому кругу специалистов по информационной безопасности, интересующихся тем, как современные вредоносные программы обходят защитные механизмы на уровне операционной системы.

УДК 004.056
ББК 32.973.202

ISBN 978-1-59327-716-1 (англ.)
ISBN 978-5-97060-979-8 (рус.)

СОДЕРЖАНИЕ