Red October Kill Chain High Level LTS

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Actions on Objectives

1 → Target.Identify → 2

MaliciousDoc.Craft → 3.1

MaliciousDoc.Email → 3.2

MaliciousDoc.Receive → 3.3

MaliciousDoc.Open → 4

Zero day exploit (CVE-2009-3129)

Zero day exploit (CVE-2010-3333)

Zero day exploit (CVE-2012-0158)

Zero day exploit (CVE-2011-3544)

ε

MaliciousCode.InitiateSetup → 5

MainComponent.Install.Complete → 6.1

InternetConnection.Check

6.2

Data.Exfiltrate → 7

Modules.Send

OtherTarget.Infect

Target.Lost

SeeminglyBenignDocument.Craft → 8

Legend

1 : Reconnaissance
2 : Weaponization (A)
3 : Delivery
4 : Exploitation
5 : Installation
6 : Command and Control
7 : Actions on Objectives
8 : Weaponization (B)

:= This transition may be made from any of the states which share its color