THE SEVEN STAGES of Advanced Threats
Understanding the cyber attack kill chain.

01 | STAGE ONE
RECON
Cybercriminals peruse personal, professional and social media websites to create seemingly trustworthy “lures” that link to compromised websites under their control.

02 | STAGE TWO
LURE
Using information collected in the recon stage, cybercriminals create innocuous-looking email, social media or other “lures” to fool users into clicking links to compromised websites.

03 | STAGE THREE
REDIRECT
In their lures, cybercriminals may use links that “redirect” users to compromised websites that contain exploit kits, exploit code or obfuscated scripts.

85% of malicious links are found on comprised hosts.

04 | STAGE FOUR
EXPLOIT KIT
Once a user clicks on a link to compromised site, an exploit kit scans the victim’s system to find unpatched or zero-day vulnerabilities — the first step toward further infiltration.

When malware called home last year, ½ the time it installed one or more dropper files.

05 | STAGE FIVE
DROPPER FILE
Once the exploit kit finds an opening, the cybercriminal delivers a “dropper file” to infect the victim’s system.

06 | STAGE SIX
CALL HOME
Once the dropper file infects the target system, it “calls home” to a command-and-control server to download additional programs, tools or instructions.

07 | STAGE SEVEN
DATA THEFT
The end-game of most modern cyber attacks, the data theft stage completes the threat kill chain. Cybercriminals steal intellectual property, personally identifiable information or other valuable data.

www.websense.com/sevenstages