Cybercrime Kill Chain vs. Effectiveness of Defense Layers

Dr. Stefan Frei & Francisco Artés

@stefan_frei    @franklyfranc

NSS Labs
Trusted Advice. Measured.
Undetected Exploits

Undetected exploits

Exploits that bypass our defense layers (IPS, NGFW, Antivirus, ..)

Sadly enough, these exploits exist and are plentiful ..
Exploits for prevalent programs

Exploits that hit popular programs with large market share

Exploits for prevalent & vulnerable programs

Exploits that bypass our defense layers (IPS, NGFW, Antivirus, ..)

Exploits for popular programs are a dangerous beast ..
Proven and readily available exploits

Undetected exploits

Exploits that bypass our defense layers (IPS, NGFW, Antivirus, ..)

Exploits that hit popular programs with large market share

Exploits that are readily available in crimeware kits or penetration testing tools

Exploits available in crimeware kits

Prevalent & vulnerable programs

Make them readily available for everyone with a criminal mid calls for disaster!
Failure of the security industry

- Undetected exploits
- Prevalent & vulnerable programs
- Exploits available in crimeware kits

Security products failing to detect these exploits are hardly acceptable
Undetected Exploits vs. Metasploit

Correlation of exploits not detected by IPS/NGFW with exploits available in Metasploit

Many publicly available and easy to use exploits bypass detection

26% of 866 Metasploit exploits are not detected by at least one IPS/NGFW