PROTEUS TECHNOLOGIES

Outsmart.

CyberVigilance™

A PROTEUS TECHNOLOGIES CYBER SOLUTION

#ACTB4URHACKD

RESEARCH REMEDIATE RESPOND

“Weakness and vulnerability – these things will always be exploited” - Z. Smith

An Exploit Kit is a malicious tool with pre-written code used by cyber criminals to target computers for nefarious purposes. Most exploit kits are created by a small number of sophisticated cyber criminals but they can be purchased and used by lower skilled criminals who have little technical knowledge.

Exploitation Comes In Many Forms

With a 75% jump in activity observed in 2015, Exploit Kit usage is on the rise and will most likely continue to rise as ransomware has become a lucrative business enterprise with large financial rewards for cyber criminals. Currently the Magnitude, Neutrino, and Nuclear exploit kits are the most popular but the Angler is by far the largest threat.

Angler uses a process known as a drive-by download combined with other aggressive tactics to direct unsuspecting users to its servers and proceeds to exploit security holes in outdated or insecure software applications such as Adobe Flash Player, Internet Explorer, Microsoft Silverlight, Java, and ActiveX. It uses various techniques to defeat traditional detection methods including unique obfuscation, antivirus and virtualization software detection, encrypted payload, and fileless infections.

Act Before You’re Hacked

Modern exploit kits are becoming harder to catch as they maneuver to avoid detection by security researchers and Angler is arguably one of the most sophisticated and prolific exploit kits currently on the market today. Contact PROTEUS at CV@proteuseng.com to find out how our CyberVigilance™ services can help YOU protect your infrastructure from exploit kits or other security threats.

PROTEUS TECHNOLOGIES

Outsmart.