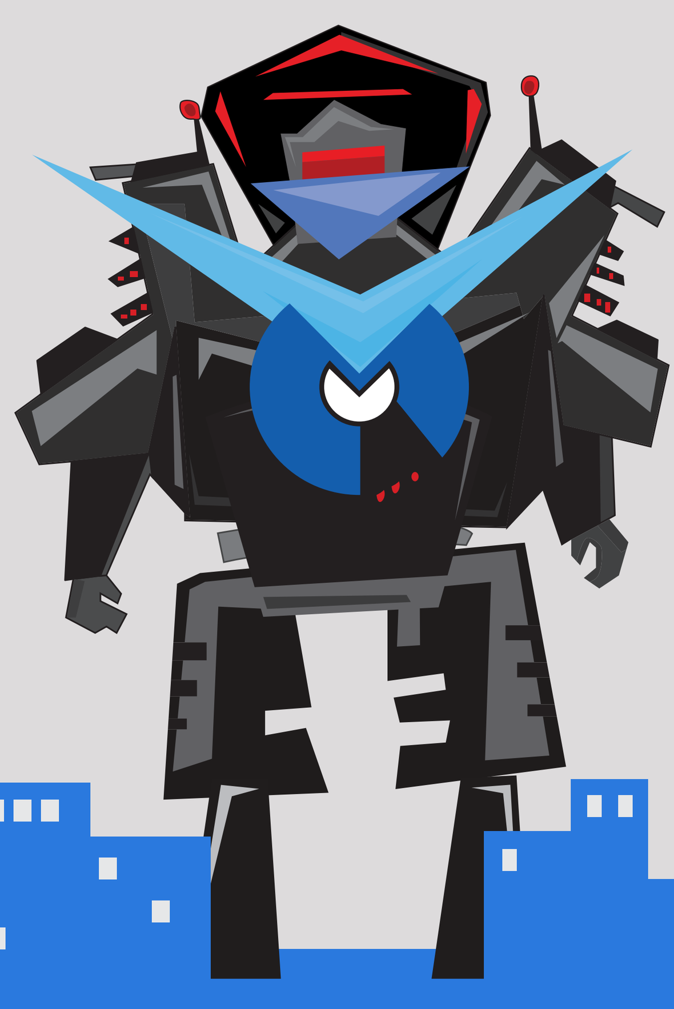

Understanding EXPLOIT KITS

Exploit Kits are small packages of malicious code that hide in dark corners of the internet, used to infect computers with viruses, malware, and more. They can hide anywhere—even huge, trusted sites—and they're exploding in popularity. Learn what they are, and how to stop them.

What do they do?

Spread Criminal Code
Clusters of criminal code hide on high-traffic sites or even within an ad on that site.

Find Vulnerabilities
The Exploit Kit builds a picture of what software you frequently use and what vulnerabilities they have.

Infect Your Computer
Using pre-built "exploit" code, the Exploit Kit creates a hole and forces it wide open, leaving your computer at the mercy of the attacker.

How common are they?

6,000 INFECTIONS / .5 HOUR
Recent research saw a single exploit kit on a well-visited site infect 6,000 people in half an hour.

2 BIL VISITORS / MONTH
In the last year, even sites with a combined traffic load of around 2 billion visitors per month were observed serving Exploit Kits at one time or another.

60%
About 60% (and growing) of all new malware comes from Exploit Kits.

2010 — OUTDATED SOFTWARE CAN BE INFECTED FOR 5 YRS
Exploit Kits are still infecting users through holes in outdated software that are nearly 5 years old.

Which sites are vulnerable?

In short, all of them. Even trusted, commonly-visited websites–without any clicks, downloads, or popups–can infect users. That's exactly why they're exploding in popularity among cyber criminals.

Most commonly affected software

These are the top five softwares most commonly abused by online criminals. Look familiar? We thought so. And unfortunately, these are only a handful of the most dangerous Exploit Kits – this list is constantly growing and changing as new ones emerge and old ones adapt to the latest vulnerabilities.

Internet Explorer · Flash · Silverlight · Adobe Reader · Java

MOST INFECTED → LEAST INFECTED

Top Exploit Kits	Internet Explorer	Flash	Silverlight	Adobe Reader	Java
RIG	☠	☠	☠		☠
FLASH	☠	☠			
ASTRUM	☠	☠	☠	☠	
NULL HOLE	☠	☠			
SWEET ORANGE	☠	☠			
NUCLEAR	☠	☠		☠	
ANGLER	☠	☠	☠		
FIESTA	☠	☠	☠	☠	
NEUTRINO	☠	☠			
NITERIS	☠	☠			
DAGONG	☠	☠			
TOP EXP	☠	☠			
ARCHIE	☠	☠			
HAN JUAN	☠	☠			

How do Exploit Kits attack?

EXPOSURE
The user simply browses to a compromised website or a site displaying a malicious ad.

REDIRECTION
A silent redirection takes place, without the user's knowledge.

WHICH KIT FITS?
The user is sent to one of many Exploit Kits that are suited to their location and software.

VULNERABILITIES ARE DETERMINED
An Exploit Kit landing page tests the browser for appropriate vulnerabilities.

THE PAYLOAD
Once the machine has been cracked open by the exploit, the payload is sent in the form of malware that can steal your bank account, take your machine hostage and more.

What can you do about it?

1 Keep your computer up to date

By keeping your computer and software up to date you drastically cut the chances of any exploits working, because you'll benefit from patches to all known vulnerabilities.

2 Use browser add-ons

An effective way to thwart malicious redirections is to use browser add-ons that can block Flash or disable scripts.

3 Security Software

Layering your protection with antivirus and Malwarebytes Anti-Malware for Business is a convenient and effective solution. Malwarebytes Anti-Exploit for Business addresses exploits and zero-day threats is also recommended for total peace of mind.

Malwarebytes

malwarebytes.com