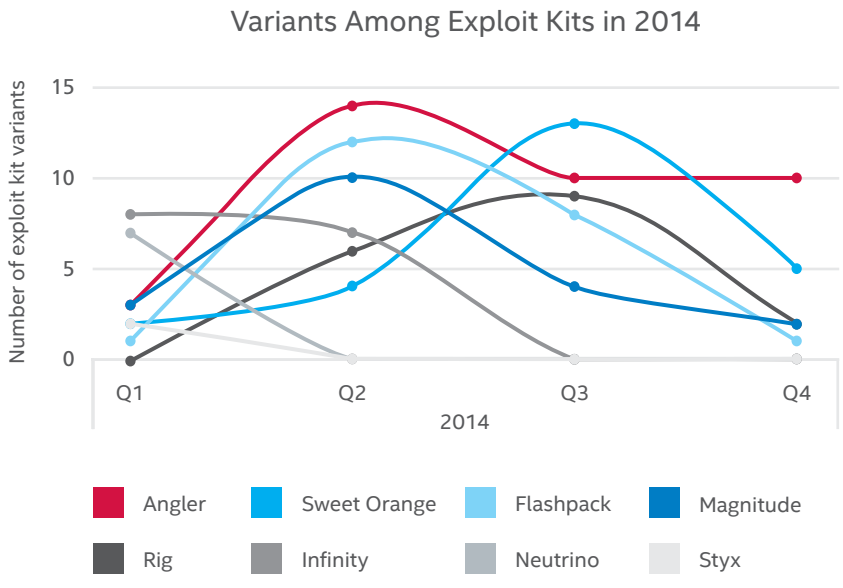
Solution Brief

# Defeating the Angler Exploit Kit

An exploit kit is an off-the-shelf software package containing easy-to-use packaged attacks on known and unknown (zero-day) vulnerabilities. These toolkits exploit client-side vulnerabilities, typically targeting the web browser and applications that can be accessed by the web browser. Exploit kits can also track infection metrics and have robust control capabilities.

## What is the Angler Exploit Kit?

The Angler exploit kit is discussed in depth in the **McAfee® Labs Threats Report: February 2015**. Angler grew in prevalence and notoriety in the second half of 2014 because of its features such as fileless infection (memory injection), virtual machine and security product detection, and its ability to deliver a wide range of payloads including banking Trojans, rootkits, ransomware, CryptoLocker, and backdoor Trojans. In addition, Angler does not require technical proficiency to use effectively, and its availability on online "dark" markets has led to its high growth:




Source: McAfee Labs, 2015.

intel Security

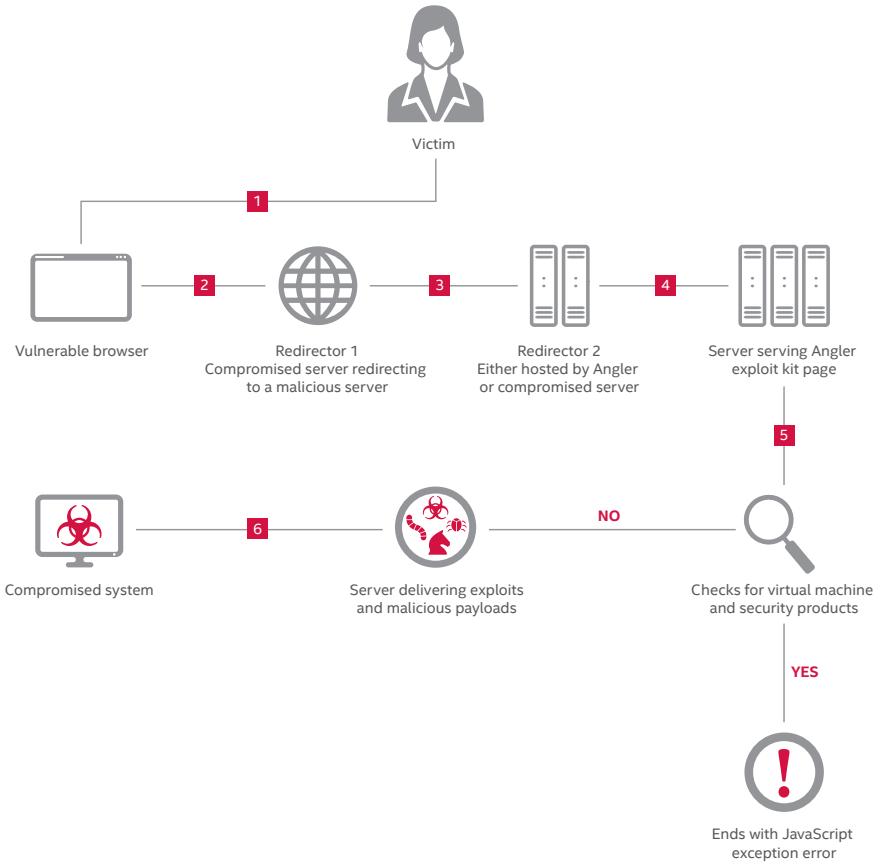
Angler frequently changes its patterns and payloads to hinder the ability of security products to detect the active exploit kit. Angler performs several evasive actions to avoid detection:

- Uses two levels of redirectors before reaching the landing page.
- Compromised web servers hosting the landing page can be visited only once from an IP. The attackers are clearly actively monitoring the hosts.
- Detects the presence of virtual machines and security products in the system.
- Makes garbage and junk calls to be difficult to reverse engineer.
- Encrypts all payloads at download and decrypts them on the compromised machine.
- Uses fileless infection (directly deployed in memory).

The Angler exploit kit performs several steps to successfully infect systems:

- Victim accesses a compromised web server through a vulnerable browser.
- Compromised web server redirects to an intermediate server.
- Intermediate server redirects to a malicious web server hosting the exploit kit's landing page.
- Landing page checks for the presence of vulnerable plug-ins (Java, Flash, and Silverlight) and their version information.
- When a vulnerable browser or plug-ins is found, the exploit kit delivers the proper payload and infects the machine.

The Angler Exploit Kit Infection Chain



## Safeguarding against the Angler Exploit Kit

Here are some recommended ways to protect systems against the Angler exploit kit:

- Use a security-conscious Internet service provider that implements strong antispam and antiphishing procedures.
- Enable automatic operating system updates, or download operating system updates regularly, to keep operating systems patched against known vulnerabilities. Install patches from other software developers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan and spyware attacks.
- Use great caution when opening attachments. Configure antivirus software to automatically scan all email and instant-message attachments. Make sure email programs do not automatically open attachments or automatically render graphics, and ensure that the preview pane is turned off. Never open unsolicited emails, or unexpected attachments—even from known people.
- Beware of spam-based phishing schemes. Don't click on links in emails or instant messages.
- Use a browser plug-in to block the execution of scripts and iframes.

## How Intel Security Can Help Protect against the Angler Exploit Kit

### McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in trusted websites are just some of the attack methods used to deliver the Angler exploit kit. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway anti-malware engine**: Signatureless intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protects against zero-day and targeted attacks. The McAfee Gateway Anti-Malware Engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee Global Threat Intelligence (McAfee GTI)**: Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

### McAfee VirusScan® Enterprise

Detecting and cleaning malware such as those delivered by Angler is simple with **McAfee VirusScan Enterprise**. McAfee VirusScan Enterprise uses the award-winning McAfee scanning engine to protect your files from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks**: Integrates antimalware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in applications.
- **Unbeatable malware detection and cleaning**: Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques including port blocking, filename blocking, folder/directory lockdown, file share lockdown, and infection trace and block.
- **Real-time security with McAfee GTI integration**: Protection against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in the market.

**McAfee Advanced Threat Defense**

**McAfee Advanced Threat Defense** is a multilayered malware detection solution that combines multiple inspection engines. By combining multiple inspection engines that apply signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing, McAfee Advanced Threat Defense will protect against prevalent exploit kits such as Angler and the malware it deploys.

- **Signature-based detection**: Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledge base is created and maintained by McAfee Labs, and currently includes more than 150 million signatures including Angler and its variants.
- **Reputation-based detection**: Looks up the reputation of files using the McAfee GTI network to detect newly emerging threats.
- **Real-time static analysis and emulation**: Provides real-time static analysis and emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.
- **Full static-code analysis**: Reverse-engineers file code to assess all its attributes and instruction sets, and fully analyze source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by the specific malware.
- **Dynamic sandbox analysis**: Executes file code in a virtual runtime environment and observes the resulting behavior. Virtual environments can be configured to match your company's host environments, and support custom OS images of Windows 7 (32-/64-bit), Windows XP, Windows Server 2003, Windows Server 2008 (64-bit), and Android.

**McAfee Network Security Platform**

**McAfee Network Security Platform** is designed to perform deep inspections of network traffic. McAfee Network Security Platform combines advanced inspection techniques—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent both known and zero-day attacks on the network.

- **Comprehensive malware defense**: Combines file reputation from McAfee GTI, deep file analysis with JavaScript inspection, and signatureless, advanced malware analysis to detect and defeat zero-day threats, custom malware, and other stealthy attacks.
- **Leverages advanced inspection techniques**: Includes full protocol analysis, threat reputation, and behavior analysis to detect and prevent both known and zero-day attacks on the network.
- **Integration with McAfee GTI**: Combines real-time file reputation, IP reputation, and geolocation feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.
- **Security Connected**: Actionable integration with McAfee Advanced Threat Defense enables McAfee Network Security Platform to submit suspect files found in monitored traffic to McAfee Advanced Threat Defense, and deny or allow them based on findings from McAfee Advanced Threat Defense.

**McAfee Threat Intelligence Exchange**

Having an intelligence platform that can adapt over time to suit your environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks, thanks to its visibility into immediate threats, such as unknown files or applications being executed in the environment.

- **Comprehensive threat intelligence**: Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation**: McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from execution in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Visibility**: McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process's actions from initial install to the present enables faster response and remediation.
- **Indicators of compromise (IoCs)**: Import known bad files hashes and McAfee Threat Intelligence Exchange can immunize your environment against these known bad files through policy enforcement. If any of the IoCs trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the IoC.

The growing prevalence of easy-to-use exploit kits such as Angler is a sobering reminder that the threat landscape is always changing. Intel Security technology can help your company proactively protect itself against threats like the Angler exploit kit on both the endpoint and network.



**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com