Exploit Kits Threat Profile

What Are Exploit Kits?

Exploit kits (EKs) are toolkits that automate the exploitation of vulnerabilities in popular software applications in order to maximize successful infections and serve as a platform to deliver malicious payloads such as Trojans, spyware, ransomware, and other malicious software. Most users will encounter EKs from visiting seemingly legitimate, high-traffic websites that either contain links to EKs embedded within malicious advertising (malvertising) or have malicious code hidden directly within the website itself. Malicious URLs linking to EKs are commonly distributed through spam email and spear-phishing campaigns.

How Exploit Kits Work

There are four key stages to an EK attack.

1. **Contact** - the victim accesses a link that connects to an EK server (i.e. from a malicious ad, compromised website, or email hyperlink).
2. **Redirect** - the victim is filtered based on a set of criteria specified by the EK attacker, such as the IP address or browser type, and redirected to the server that hosts the EK, and then delivers them to the landing page that will determine what vulnerabilities to exploit.
3. **Exploit** - once the vulnerabilities are identified, the EK server downloads the exploit files to target the appropriate applications.
4. **Infect** - once the vulnerabilities are exploited, the attacker downloads and executes malware on the victim’s machine, often a banking Trojan or ransomware.

Mitigation Strategies

The constantly evolving nature of exploit kits underscores the need for a progressive and proactive cybersecurity posture - one that equally addresses the vulnerabilities and exploits of people, processes, and technology. Below are some mitigation strategies to help defend against EKs:

For Applications:

- Keep all operating systems, applications, and essential software up-to-date.
- Update Content Management Systems such as WordPress, Joomla and Drupal running on webservers.
- Update all plugins used by the webserver and disable/remove all unused plugins.
- Whitelist permitted/trusted programs to prevent execution of malicious or unapproved programs including DLL files, scripts, and installers.
- Immediately patch and regularly audit applications, and consider disabling or uninstalling Adobe Flash Player, Internet Explorer, Silverlight, Adobe Reader, and Java if they are not essential to operations.
- Implement a web application firewall and/or File Integrity Monitoring solution.
- Perform monthly vulnerability scans of all public-facing applications and sites.
- Use a browser exploit prevention feature to block the exploit if a user accesses the host URL.
- Utilize web reputation services to ensure that redirection chains are blocked before the malicious payload is downloaded.
- Apply data execution prevention (DEP), address space layout randomization (ASLR), enhanced mitigation experience toolkit (EMET), security-enhanced Linux (SELinux), and Grsecurity.
For Networks:

- Implement a host-based intrusion detection/prevention system (HIDS/HIPS) to identify suspicious behavior in program execution and detect malware not yet identified by anti-virus (AV) vendors.
- Implement deep packet inspection (DPI) technology.
- Segment and segregate networks into security zones to protect sensitive information and critical services.
- Secure backdoors into networks and regularly audit network trust relationships shared with third parties.
- Close all unneeded ports and disable unnecessary services.
- Perform automated, dynamic analysis of email and web content run in a sandbox to detect suspicious behavior and malware not yet identified by AV vendors.

For Users:

- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hyperlinks contained in emails or attachments, especially those from untrusted sources.
- Restrict administrative privileges to operating systems and applications based on user duties (the impact of a compromise is reduced if malware is only run on a low privilege user machine).
- Disable local administrator accounts to help prevent an attacker from propagating through a network.

Reporting

If your organization is the victim of an Exploit Kit attack, or would like to learn more about the NJCCIC, please contact a Cyber Liaison at njccic@cyber.nj.gov or visit www.cyber.nj.gov.

Appendix

**Angler** is one of the most sophisticated EKs used by cybercriminals today and was first observed in 2013. Angler uses malvertising to direct users to its servers, and is known to exploit Adobe Flash Player, Internet Explorer, Microsoft Silverlight, Java, and ActiveX. Angler infects users with Cryptowall 3.0 ransomware or point-of-sale (PoS) malware. It uses various techniques to defeat traditional detection methods including unique obfuscation, antivirus and virtualization software detection, encrypted payload, and fileless infections. Angler is also very quick at integrating new zero-day exploits in its kit, specifically targeting vulnerabilities in Adobe Flash Player. On 28 July 2015, security researchers warned that a malvertising campaign potentially exposed over 10 million users to the Angler EK. In December 2015, Heimdel Security noted Angler was distributing CryptoWall 4.0 ransomware. In February, Angler targeted Skype users through malvertising on its ads. Angler has added many new servers as part of its distribution network, delivering drive-by download attacks through infected websites. According to Palo Alto Networks, as of January 2016, Angler EK has infected more than 90,000 websites, 30 of these are among the 100,000 most visited sites, estimating monthly visits to infected sites may be as high as 11 million.

- Heimdel Security offers a list of resources that provide more technical analyses and IOCs available [here](#).

**Blackhole** became a very popular and preferred exploit kit tool from about 2010 until October of 2013 when its alleged creator, Paunch, was arrested in Russia. Since his arrest, Blackhole EK has sharply declined in use and popularity as its modules haven’t been updated with exploits targeting new vulnerabilities. It was thought to be the end of Blackhole until security firm Malwarebytes noticed a resurfacing of what appeared to be Blackhole EK in drive-by download attacks, exploiting Java and PDF vulnerabilities. It is unlikely, however, to see a significant increase in Blackhole activity as it is probable that the recent sightings were a result of an author simply using the Blackhole EK source code.

- Malwarebytes details the recent Blackhole EK activity available [here](#).
**Fiesta** was first released in 2008 and gained popularity with the decline of Blackhole EK. Fiesta was developed to deliver crypto-ransomware and fake antivirus malware payloads to its victims and exploits vulnerabilities in Flash, Internet Explorer, Adobe Acrobat Reader, and Microsoft Silverlight, and has the capability of terminating running processes and disabling common system tools to make detection and removal more difficult. Two-thirds of Fiesta-related traffic occurred in three countries: United States, Japan, and Australia.

- Cisco outlines details of the Fiesta EK available [here](#).

**Magnitude** made itself known in October of 2013 when it breached the servers of PHP.net, a popular scripting language development website, and redirected the site’s visitors to its landing page using a compromised JavaScript file. It then exploited vulnerabilities in Java and Flash to deliver malicious payloads like Zeus, Andromeda, Necurs, Zsy, and Ngrbot. Magnitude was later used in an attack against Yahoo and WordPress website users. Magnitude operates as a pay-per-campaign model and its customers are responsible for generating traffic to the kit’s landing pages. The sellers of the Magnitude EK require 5-20% of the user’s malicious traffic in order to turn a profit and stand to make nearly $3 million solely by maintaining infrastructure. On 29 June 2015, ThreatPost reported that Magnitude included exploits for the recently patched zero-day vulnerability found in Adobe Flash Player and was delivering CryptoWall ransomware to Windows 7 computers running Internet Explorer 11. In 2015, the top victims of Magnitude included the United States, Iran, and Vietnam; however, the success rate varied greatly with the highest success rate being 68% in Vietnam and only a 9% success rate in the US. According to Malwarebytes, in 2016, Magnitude EK has been infecting victims with CryptoWall 4.0 ransomware by exploiting vulnerabilities in older versions of Adobe Flash Player. Magnitude EK is spreading through malvertising on pop-under ads, ads that appear behind the main browser window and remains open until the user manually closes them.

- TrendMicro provides details on the Magnitude EK’s exploitation of the Adobe vulnerability available [here](#).

**Neutrino** was discovered in 2012 and remains active, exploiting vulnerabilities in all Java versions at least up to Java 7 Update 11. Neutrino downloads a ransomware variant on the victim’s machine when it successfully finds a vulnerable target. It features a user-friendly control panel, continuously monitors the status of present antivirus software, filters network traffic, and encrypts stolen information before sending it back to the server. Neutrino developers often purchase iframe traffic in order to generate additional revenue. Neutrino EK is available for rent at about $40 per day or $450 per month. Neutrino EK is now equipped with Cryptolocker 2 and CryptoWall 4.0 ransomware and variants of the Kovter malware – click-fraud malware that resides in registry, evading detection. Neutrino EK exploits Flash vulnerabilities including CVE-2015-7645, and uses Google SEO poisoning. Recently, Neutrino has been seen using Microsoft Office macros malware as a vector to spread through spear-phishing emails.

- The Internet Storm Center provides Neutrino technical details available [here](#).
- Neutrino IOCs reported by Heimdel Security are available [here](#).

**Nuclear** dates back to 2009 and remains one of the most widely used EKs. It exploits vulnerabilities in ActiveX, Flash, Internet Explorer, Java, PDF, and Silverlight, and disseminates malware and ransomware. Nuclear can detect if antivirus software is running and, if found, it terminates the associated process as well as antivirus driver files. Security researchers at Trend Micro estimate the number of daily infected users spiked to 12,500 in May 2015 and the top three countries affected are Japan, the United States, and Australia. In November 2015, Nuclear EK was the first exploit kit found infecting victims with CryptoWall 4.0. In the same month, Nuclear EK was also discovered delivering malware that could subsequently download the Kelihos Trojan onto the victim’s device.

- The Talos Group details the evolution of the Nuclear EK available [here](#).
RIG was discovered in 2014 and remains one of the most active exploits kits today. In February 2015, a security researcher from MalwareTech reported that an underground reseller leaked RIG’s source code after being banned from a hacker forum for trying to scam customers. However, on August 3, 2015, Trustwave reported that the author of the original RIG EK released an updated version, labeled RIG 3.0, which maintains the exploitation percentage of the previous version while vastly increasing the number of times it exposes victims to its landing page. After monitoring RIG 3.0 over a six-week period, Trustwave SpiderLabs researchers observed an average infection rate of 27,000 machines per day, totaling over 1.3 million infections worldwide. RIG 3.0 targets vulnerabilities in Java, Internet Explorer, Flash, and Silverlight, and spreads through malvertisements on web pages. According to Heimdel Security, more than 50 percent of Windows 7 devices running Internet Explorer 9 are exploited by RIG EK through two Flash vulnerabilities (CVE-2015-5119 and CVE-2015-5122). RIG EK has recently been seen spreading through drive-by attacks using Google search engine optimization (SEO) poisoning and malvertising. In December 2015, Cyphort discovered RIG was infecting victims with Radamant ransomware.

- Cisco’s Talos group assessment of the RIG EK available [here](#).
- Cyphort’s assessment and information on IOCs are available [here](#).

Sweet Orange emerged in 2012 to fill the void left behind by the Blackhole EK after its author was arrested and it quickly rose in popularity among cybercriminals. Sweet Orange contains many of the same features as other variants, including a database that records a list of successful infections, statistics about various current exploits, and regular malware updating. It is also capable of evading and disabling sandboxes. Much like the author of Blackhole attempted to do, the Sweet Orange authors have devised ways to prevent the security community from obtaining the kit’s source code by minimizing advertising and brokering only to trusted buyers. Client-side exploits found in the kit include Java, Internet Explorer, and Firefox. Sweet Orange is advertised as having the capability of redirecting 150,000 unique visitors to the malicious payload. As of 2015, Sweet Orange EK is also spread TeslaCrypt ransomware. The Internet Crime Complaint Center considers TeslaCrypt as the most current and significant ransomware threat targeting U.S. individuals and businesses.

- Webroot provides screenshots and details of the Sweet Orange EK available [here](#).