Exploit Kits: A Prevailing Vector for Malware Distribution

August 5, 2015

TLP: WHITE | Since first appearing around 2006, exploit kits (EK) have evolved into one the most prevalent web-based vectors for malware distribution and a threat facing nearly all internet users. An EK is a malicious toolkit designed to distribute different malware variants by exploiting common vulnerabilities found in outdated or unpatched software applications, such as web browsers and plugins. EKs are increasingly automated, sophisticated, and effective at infecting user machines due to the abundance of exploitable vulnerabilities that often go unpatched for weeks or even months. Additionally, the software applications targeted by EKs are present on a large majority of endpoints in the U.S., including Adobe Flash Player, Internet Explorer, Java and Microsoft Silverlight. The criminal developers responsible for creating these malicious toolkits are able to deploy updates that exploit the most current vulnerabilities, such as multiple Adobe Flash zero-day vulnerabilities discovered in January and July of 2015. Although the overall number of new and active EKs has decreased from a peak in 2012-2013, the NJCCIC assesses EK infections will continue to increase throughout 2015 as malicious actors capitalize on the window of opportunity between when vulnerabilities are discovered and software patches are released and implemented. The NJCCIC recommends that organizations and home users immediately apply updates to operating systems, content management systems, web browsers, and plugins; consider uninstalling or disabling applications and plug-ins that are not essential to daily operations; and regularly educate users on the latest tactics used in malicious emails and advertising.

Threat Overview

EKs automate the exploitation of client-side vulnerabilities in popular software applications in order to maximize successful infections and serve as a platform to deliver payloads such as Trojans, spyware, ransomware, and other malicious software. A key characteristic of EKs is the ease of use and affordability, making it possible for a novice hacker with limited resources to launch a successful and profitable malware campaign. Malicious actors have a variety of EKs from which to choose, as they are widely available for rent or purchase through black-market websites. An EK typically provides a user-friendly graphical user interface (GUI) and the capability of monitoring the infection rate, as well as remotely controlling the exploited system. EKs are often developed in one country, sold in another, and used in a third to attack a fourth – making it difficult to attribute malicious activities to threat actors or country of origin.

- As of January 2015, EKs delivered more than two-thirds of all malware observed by anti-malware software company Malwarebytes. Additionally, Malwarebytes reported that two billion mainstream website visitors were redirected to critical servers in a one month period, and a single EK on a high-traffic site can infect 6,000 users within a half hour. The sustained success of these toolkits over the last several years, combined with user-friendly interfaces and low technical barriers, have made EKs an attractive option for profit-motivated cybercriminals. According to Microsoft, individual EKs can yield up to $50,000 in a single day for an attacker.

- Analysis by Trend Micro revealed that the U.S. was the target of 57% of all exploit kit attack activity in 2014. While EK activity has primarily been attributed to criminal actors, the security firm Symantec observed the use of EKs among cyberespionage groups in 2014 and posed the possibility of EKs designed to target critical infrastructure through exploiting Industrial Control Systems (ICS).

- EKs pose a threat that requires a multifaceted mitigation strategy encompassing both web-based detection as well as behavior and file-based detection solutions. The first line of defense, however, is the timely patching of systems. Although EKs have recently targeted zero-day vulnerabilities, the majority of exploits are targeting known vulnerabilities with existing patches for applications such as Adobe Reader, Java, and Internet Explorer. In their annual Data Breach Investigation Report, Verizon underscored the risk organizations accept by not updating their systems, reporting that 99.9% of exploited vulnerabilities in 2014 were compromised more than a year after the Common Vulnerability and Exposure, commonly referred to as CVE, was published.
**How Exploit Kits Work**

Most users will encounter EKs from visiting seemingly legitimate, high-traffic websites where links to EKs are embedded in malicious advertising or malicious code is injected into the website, often by exploiting vulnerabilities in content management systems (CMS). Links to EKs are also commonly sent in spam email or during spear phishing campaigns.

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 set of criteria specified by the EK attacker, such as IP address or browser type, and redirected to the server that hosts the EK and 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.

**Exploit Kit Variants**

The following is a list of EKs currently available for rent or purchase by malicious cyber actors, the majority of which require only a basic understanding of computer networking to operate.

**Note:** See the appendix for full descriptions of these EKs as well as links to additional resources with technical details and Indicators of Compromise (IOCs).

- **Angler** is one of the most sophisticated EKs used by cybercriminals today, and is known to exploit Adobe Flash Player, Internet Explorer, Microsoft Silverlight, Java, and ActiveX.
- **RIG** was discovered in 2014 and remains one of the most active EKs today. On 3 August 2015, Trustwave reported an updated variant, labeled RIG 3.0, targeting in Java, Internet Explorer, Flash, and Silverlight.
- **Nuclear** dates back to 2010 but was updated with new exploits in 2013 and remains one of the most widely used EKs. Nuclear exploits vulnerabilities in Active X, Flash, Internet Explorer, Java, PDF, and Silverlight.
- **Sweet Orange** emerged in 2012 and filled the void left behind by the Blackhole EK after its author was arrested. It quickly rose in popularity and was very active in 2014 exploiting Internet Explorer, Flash, Java, and Firefox.
- **Fiesta** was identified in 2013 as an updated version of the NeoSploit EK. Fiesta exploits Flash, Internet Explorer, Adobe Acrobat Reader, and Silverlight, and over one-third of attacks targeted the U.S.
- **Neutrino**, also identified in 2013, remains active exploiting vulnerabilities in all Java versions up to Java 7 Update 11.
- **Magnitude** appeared in 2013 when it began exploiting Java and Flash to deliver malicious payloads such as the Zeus Trojan. On 29 June 2015, Magnitude began exploiting the recent Flash zero-day vulnerability.

**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 web servers.
- 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 malicious advertising (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-days 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.

- The Talos Group from Cisco offers more information on Angler EK variants, including IOCs, found [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 the RIG’s source code after being banned from a hacker forum for trying to scam customers. However, on 3 August 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 malicious advertisements on web pages. Although it has mainly been observed distributing a spam bot to infected machines, it also has been used to distribute ransomware as well.

- The Trustwave report on RIG 3.0 can be found [here](#).
- Additional information on the RIG exploit pack from Kahu Security can be found [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 systems infected by this EK have spiked up to 12,500 and the top three countries affected are Japan, the United States, and Australia.

- For more information, the Talos Group details the evolution of the Nuclear EK [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, like 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 promoted as having the capability of redirecting 150,000 unique visitors to the malicious payload.

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

**Fiesta** was first released in 2008 but also gained some popularity with the decline of Blackhole, and was developed to deliver crypto-ransomware and fake antivirus malware payloads to its victims. Fiesta 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 EK related traffic occurred in three countries: United States, Japan, and Australia.

- More information about the Fiesta EK can be found [here](#).
Neutrino was discovered in 2012 remains active, exploiting vulnerabilities in all Java versions 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 a server. Neutrino developers often purchase iframe traffic in order to generate additional revenue. Neutrino EKs are available for rent at about $40 per day or $450 per month.24

- The Internet Storm Center provides Neutrino technical details 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, Zasy, and Ngrbot. Magnitude was also 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.25 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. The top victims of Magnitude include the United States, Iran, and Vietnam; however, the success rate varied greatly with the highest success rate being 68% in Vietnam while only having a 9% success rate in the US.26

- TrendMicro provides details on the Magnitude EK’s exploitation of the Adobe vulnerability here.
Sources