



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Exploit Kits 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.