Anti-Exploitation Features

Cyber attackers want access to your sensitive information or intellectual property for strategic advantage, or more commonly, for monetary gain. They commonly attempt to exploit vulnerabilities in your computer system and network by using malware delivered via email or web servers. Avoiding all potential avenues of attack is impractical in today's dynamic cyber environment; however, anti-exploitation features are an effective way to prevent these attacks.

The Exploit Problem

Exploitation is generally the first step before an attacker can deliver a payload (malicious code or executable program) to a target system. Depending on motive and method, attackers may launch exploitation attempts against many users or, conversely, craft malware against a specific user or system of interest. Figure 1 illustrates a typical exploitation sequence in which an attacker exploits a system via a web browser. If financially motivated, the attacker will usually install adware or "ransomware," for which he gets a monetary payoff. If exfiltration of information is the goal, the malware will usually be more covert, and may establish a longer term foothold in the system.

Anti-Exploitation Features

An anti-exploitation feature provides protection against exploits in a broad, generic manner. This is in contrast to antivirus or signature-based detection, which looks for known-bad pieces of code or malicious files. An example of an anti-exploitation feature is Data Execution Prevention (DEP), which stops an exploit by disrupting the methods by which an attacker can inject code into a running program.

Anti-exploitation features are especially effective against common attacks meant for mass infection, such as drive-by download sites, malicious iframes, and phishing campaigns. They also help mitigate zero-day vulnerabilities - previously unknown vulnerabilities with no available patches or fixes.

Many anti-exploitation features are built into modern operating systems and simply need to be enabled. The most common features are DEP and Address Space Layout Randomization (ASLR). These features work in tandem to stop typical buffer overflows and other memory corruption exploits. Traditionally, the responsibility has been on the software developers to opt their programs into these anti-exploitation features, but it is highly recommended to have these features enabled by default. Mobile operating systems already have many anti-exploitation features enabled by default.

For Microsoft Windows® systems, Microsoft's Enhanced Mitigation Experience Toolkit (EMET) provides DEP and ASLR protection in addition to several other anti-exploitation features[1]. EMET is a free tool that can configure per-application enforcement of anti-exploitation features, even if the software does not natively support the features. At a minimum, configure EMET to protect all applications that typically ingest data from the Internet, such as web browsers and document readers.

Several antivirus programs are also beginning to add anti-exploitation features to their antivirus suites or Host Intrusion Prevention Systems (HIPS).

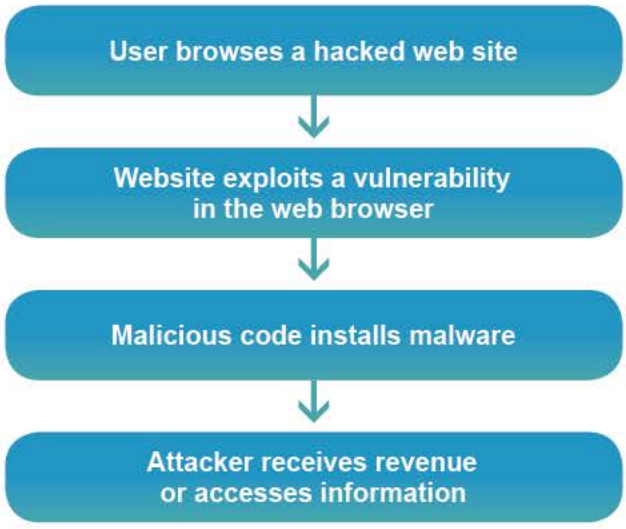

Figure 1: Exploit sequence

Application Compatibility with Anti-Exploitation Features

If application authors use modern development best practices, most current applications should be compatible with anti-exploitation features. However, application compatibility, especially with older and third-party applications, can be a problem when enabling anti-exploitation features. As these features become more widespread, developers will feel compelled to fix incompatibility issues. Vendors of anti-exploitation tools often log and publish a list of incompatible applications, which you should view before enabling the features in your network.

Since many of the anti-exploitation features can be configured on a per-application basis, protection features can be disabled for an incompatible application while still being enabled for and protecting other applications on the system. When available as an option, anti-exploitation features should be configured system-wide as opt-out protections with specific incompatible applications exempted.

As with all security features, anti-exploitation is not a cure-all, and should be part of a comprehensive network security program. However, attackers would prefer to go after less secure systems rather than expend the additional cost and effort to exploit hard targets protected with anti-exploitation capabilities.

Additional Information

- Mitigation Monday #2:
  Defense against Drive-By Downloads
  http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf
- Data Execution Prevention (DEP):
  http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf
- Microsoft EMET:
  http://support.microsoft.com/kb/2458544

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**

[1] Microsoft Windows® is a registered trademark of Microsoft Corp.