CERIAS

the center for education and research in information assurance and security

Web-Based Malware Propagation

James E. Goldman, Cory Q. Nguyen
Computer and Information Technology Department

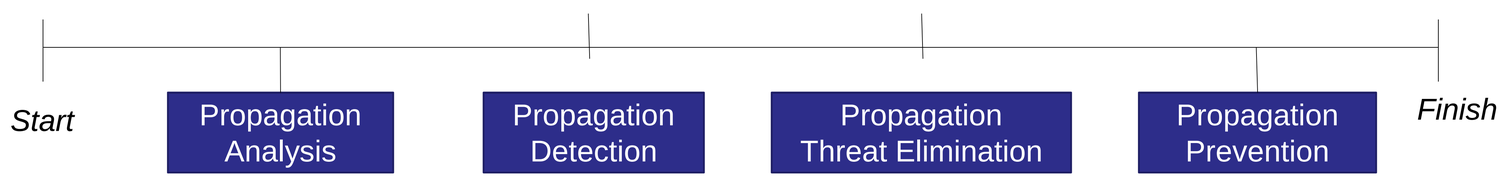
Abstract

The Internet is becoming an increasingly popular attack vector used by cyber criminals to infect computers for malicious purposes. It is estimated that over 10% of legitimate websites are infected with malware. The purpose of studying web-based malware is to understand how malware propagates through the web and the techniques and tools cyber criminals use to successfully infect computers. By understanding the varying attack vectors, the appropriate detection and prevention mechanisms can be employed to eliminate or reduce the threat of malware infections.

Successful web-based malware propagation consists of three elements: *Propagation Vector, Propagation Apparatus, and Propagation Technique*. For malware to propagate, it requires an infrastructure or "pipeline" that would allow the malware propagation vehicle to travel through. The malware propagation vehicle is made up of the tools and techniques that would get a victim to the malicious site to successfully infect their computer. The absences of any one of these three elements would render the web-based malware impotent.

The ultimate goal of this study is to eliminate and prevent the successful propagation of web-based malware. However, currently standing, cyber criminals have the advantage due to the lack of detection tools and understanding of web-based malware propagation.

Web-Based Malware Analysis Timeline



Web-Based Malware Propagation

Vector	Vehicle					Detection	Prevention/ Elimination
	Technique				Apparatus/Tool		
Email	Phishing (Active)				All Used in Websites Vector	Anti-Phishing	Training
	Drive-by-Download				Active-X, Java Applet, Certificates, & etc..		Virtual Web-Browser
Websites	Phishing (Passive)	Redirect	Automatic	Search Engine Manipulation (Meta Tagging)	HTML	Anti-Phishing	Virtual Web-Browser Block/Disable Script
				HTTP Refresher Header	• HTML • JavaScript • CGI • PHP • Ajax	Anti-Phishing	Virtual Web-Browser Block/Disable Script
			Server-Side Scripting		• .htaccess • HTTP3xx Status Code	Anti-Phishing	Virtual Web-Browser
			Manual Redirect		HTML	Anti-Phishing	Training Virtual Web Browser
		Iframe			HTML	Not Yet Determined	Virtual Web Browser
		Pop-Up			• HTML • JavaScript • PHP • Actionscript • CGI • JSP • ASP (C#/VBScript)	Pop-Up Blockers	Training Virtual Web Browser Pop-Up Blockers
		Flash			Actionscript 1.0/2.0/3.0	Web-Content Filtering	Virtual Web Browser Block/Disable Script
		Widget			• Actionscript 1.0/2.0/3.0 • Ajax • JavaScript	Not Yet Determined	Virtual Web Browser Block/Disable Script
		Streaming Media	Audio		• Windows Media Player • Apple QuickTime Player • RealPlayer	Web-Content Filtering	Virtual Web Browser Block/Disable Script
			Video				
Social Networking Sites	Phishing (Active)				All Used in Websites Vector	Web-Content Filtering	Training Virtual Web Browser Block/Disable Script
Peer-2-Peer	Drive-by-Download				Limitless	Anti-Virus Anti-Spyware	Security Policy Anti-Malware
Worms	Self-Replicating				Limitless	Network IDS Host IDS	Network IPS Host IPS
Web-Browser	Vulnerability Exploit				Limitless	Anti-Virus Anti-Virus	Virtual Web-Browser Patch System

Successful Web-Based Malware Propagation depends on three things:

Propagation Vector + Propagation Apparatus + Propagation Technique

Pipeline (Infrastructure)

Vehicle (To get victim from point A to B)

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center