Locating Live Kits

- SANS and security sites that alert users of ongoing attacks; IDS/IPS log files and incident response.
- http://www.malwaredomainlist.com/mdl.php
- http://www.malwareurl.com/listing-urls.php
- http://malc0de.com/database/

NOTE: Search for terms like "Fragus", "Eleonore", "Pack", "exploit", "kit", or similar terms.

Tools

Virtualized test system such as VMware, Qemu, or similar solutions. Native operating systems can also be made using tools like Acronis for rapid restoration of images. A LAMP server is key to analyzing interactively a PHP/MySQL exploit framework.

Translations

Many kits involve foreign language. Specifically, Russian is quite common. Cyrillic characters may require decoding first, from a site like http://2cyr.com/decode/?lang=en, before translating with the Google engine or others.

WAMP/LAMP Servers Introduction

Exploit frameworks typically require a server, MySQL database, and PHP. For this reasons a Windows or Linux computer with an Apache server, MySQL database, and PHP installed is required to test any copies of kits that may be obtained for analysis.

WAMP servers are easier to set up then a Linux build. WAMP configurations are also beneficial since local testing of the exploit payload/infection can be performed on the same test computer.

WAMP Server (Windows•Apache•MySQL•PHP)

WampServer.com, at http://www.wampserver.com/en/download.php makes it easy to install a compatible set of packages on a Windows computer. Simply download, run, and follow the instructions. Once installed right-click and left-click on the taskbar icon to work with the server and the wamp server directory for files/server. Other tools may also be helpful such as Malzilla, Cygwin for Perl/Python and Linux tools inside of Windows, Ollydbg, and more.

LAMP Server (Linux•Apache•MySQL•PHP)

Ubuntu is one of several options. Below are a few packages that can easily be installed within Ubuntu:

Synaptic Package Manager Installs:

- apache2
- php5
- phpmyadmin
- mysql-server

Additional installations that may be helpful:

- PDF Print Solution (CUPS) for printing web pages to PDF files (sudo apt-get install cups-pdf)
- Proxy solutions
- Firefox Extension *Live HTTP Headers* for rapid triage of HTTP headers in packets from local tests.

Local Kit Configuration Pointers

1. Locate the configuration file and review for database credentials/setup required.
2. Change permissions on the kit directory if necessary to enable access/read/write.
3. Look for install.php or similar files that are then used to install the kit.
4. Universalize usernames and tables within your WAMP/LAMP server and change kit configurations to speed up localized testing of new kits.
5. Use snapshots within VMware to save loaded kits for faster referencing and update checks.