iSIGHTPARTNERS℠

Security beyond the edge℠

How to Analyze Drive-by Exploit Frameworks

SANS Malware Analysis Panel

July 8, 2010

Ken Dunham, Director of Global Response

kdunham@isightpartners.com

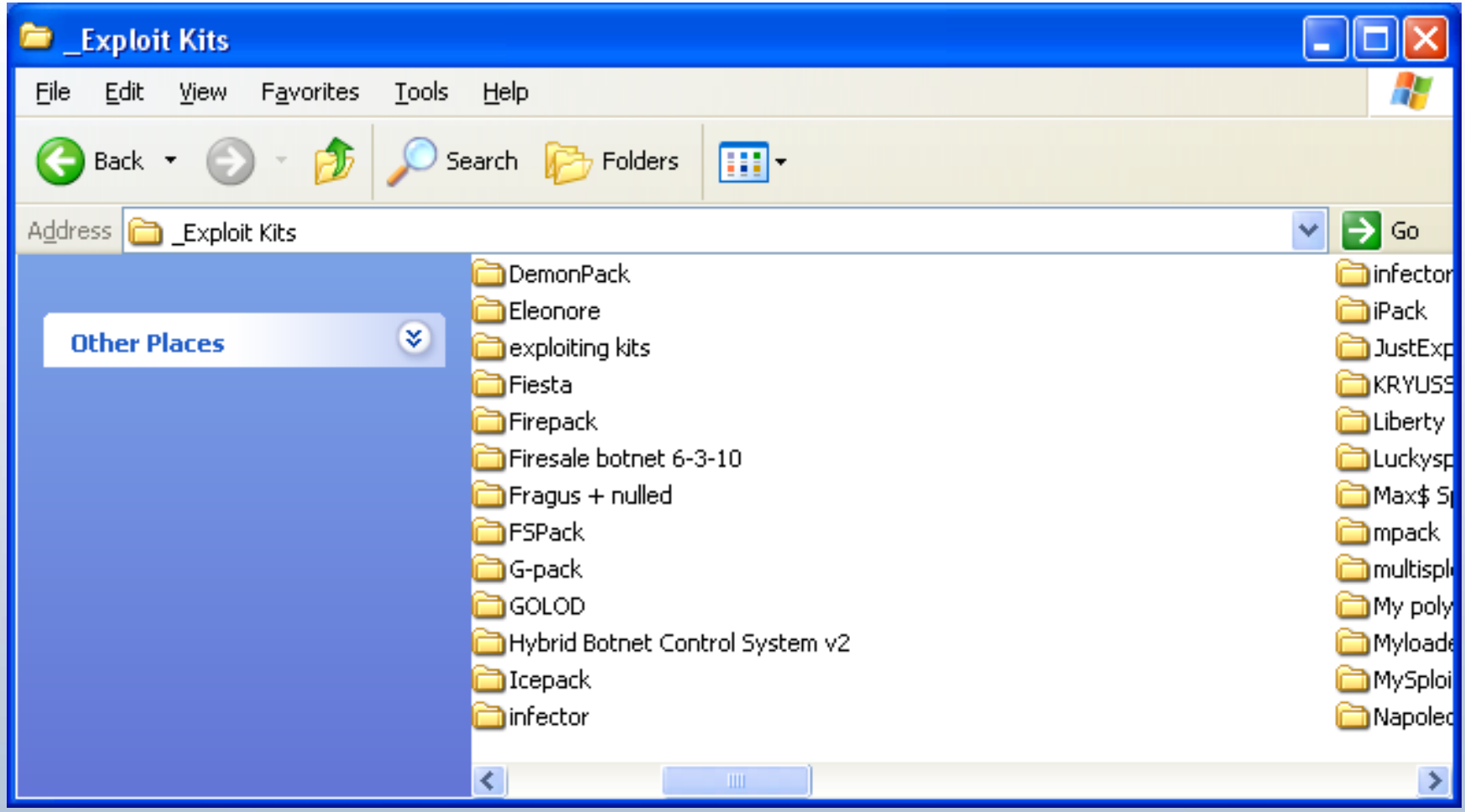
Intro to Ken

- CISSP, GCFA, GCIH Gold (Honors), GSEC, GREM
- Current Director of Global Response for iSIGHT Partners
- Regular brief high level security staff and executives in F100 companies.
- Around 20 years in the industry specializing in incident handling and malcode analysis.
- Author of several books, regular columnist, authored over 5,000 security reports to date.
- Leader of multiple industry collaboration efforts.

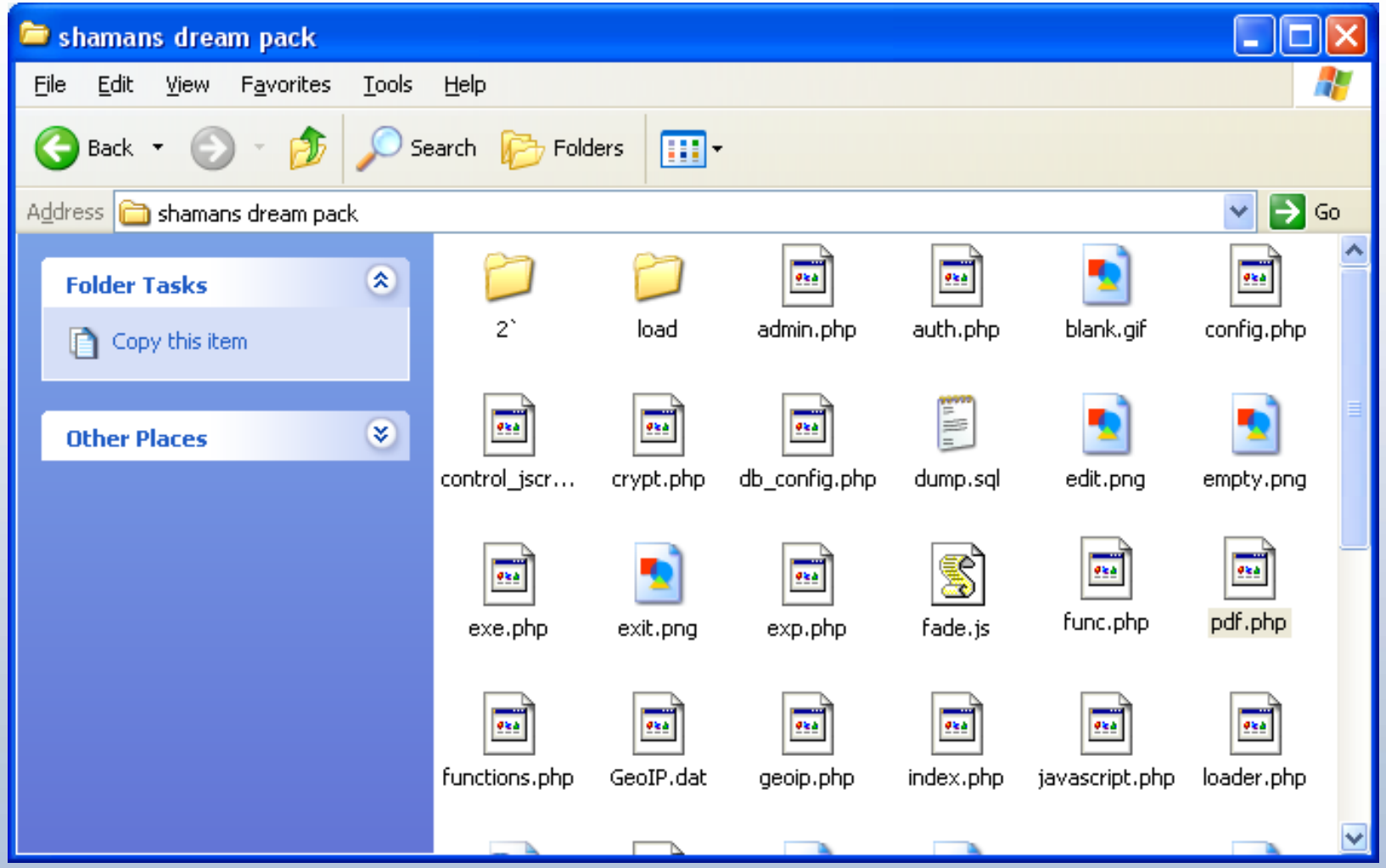
Introduction to Exploit Frameworks

- The threat is remote, attacking vulnerable computers (clients) as users surf the Web.
- They are easy to develop and deploy.
- As a framework it is trivial to update with the latest and greatest exploit vector or client data.
- Scale and automation are serious issues.
- Integration is a greater concern, such as loaders and organized criminal efforts.

A Dime a Dozen



Typical Components



How to Analyze Drive-by Exploit Frameworks?

- Select Challenges Exist for Analysis:
  - Server-side scripts and obfuscation hide the code and/or payloads.
  - Unique IP checks and geo-location conditions may blacklist and/or block analysis of a remote kit.
  - Identification of exploit vectors and payloads can be difficult and time consuming.

Accessing the Framework

- Log files or sites like MDL give clues on hostile URLs and/or administration locations of a kit.
- “Demo” packs are frequently available.
- Other researchers may have a copy.
- Vulnerabilities may exist where select components of a kit may be collected.
- Behavioral testing with careful vulnerability vectors can force specific triggers of interest.

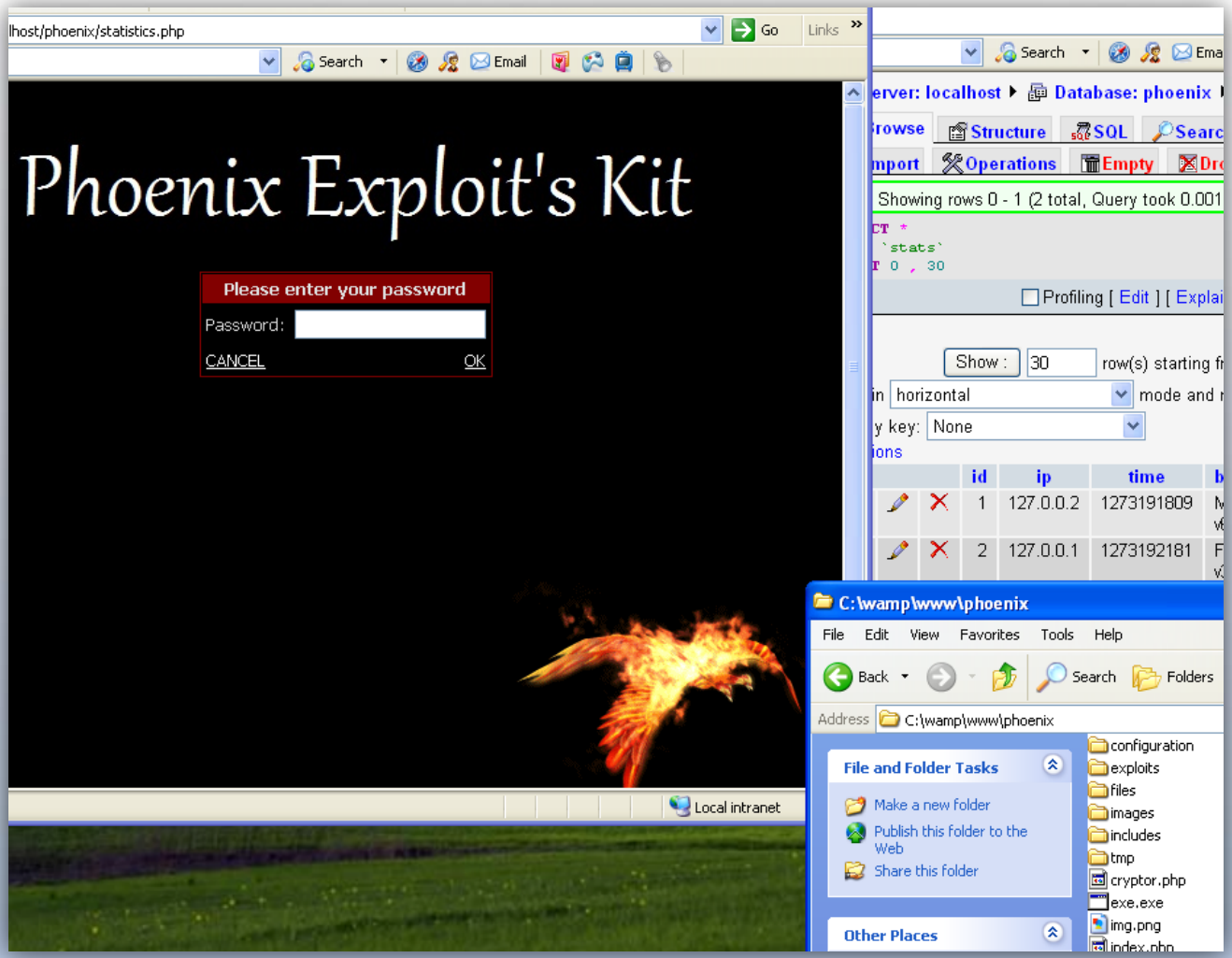
LAMP/WAMP Servers • Local Tests

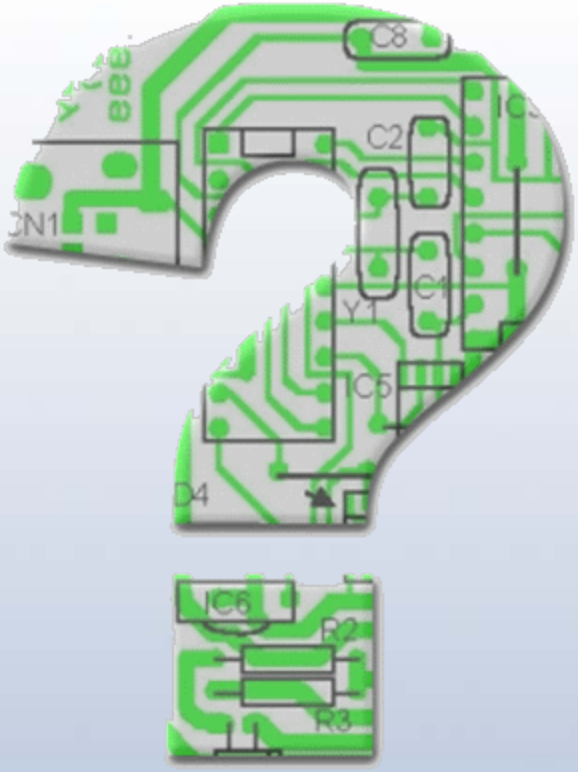
- Requires some setup (*see handout*)
- Localized testing removes unique IP and geolocation checks that may exist in a remote attack server.
- Interactive MySQL/PHP testing.
- Local exploitation triggers and analysis.

Detailed Analysis of the Kit

- Script analysis, de-obfuscation/de-zending.
- Analysis of netflow data from local and remote kits.
- Correlation to limited exploit vector tests and/or abuse intel.
- CLSID and exploit string correlation.
- Follow-up limited exploit vector tests.

Phoenix Kit Example





kdunham@isightpartners.com

iSIGHTPARTNERS
Security beyond the edge