SQLReInjector
Automated Exfiltrated Data Identification

Jason A. Novak
Assistant Director, Digital Forensics
Chicago, IL

Andrea London
Digital Forensic Examiner
Dallas, TX

Overview

STROZ FRIEDBERG

Problem

Historical Solution

SQLReInjector

Demo

Get It!

Questions?

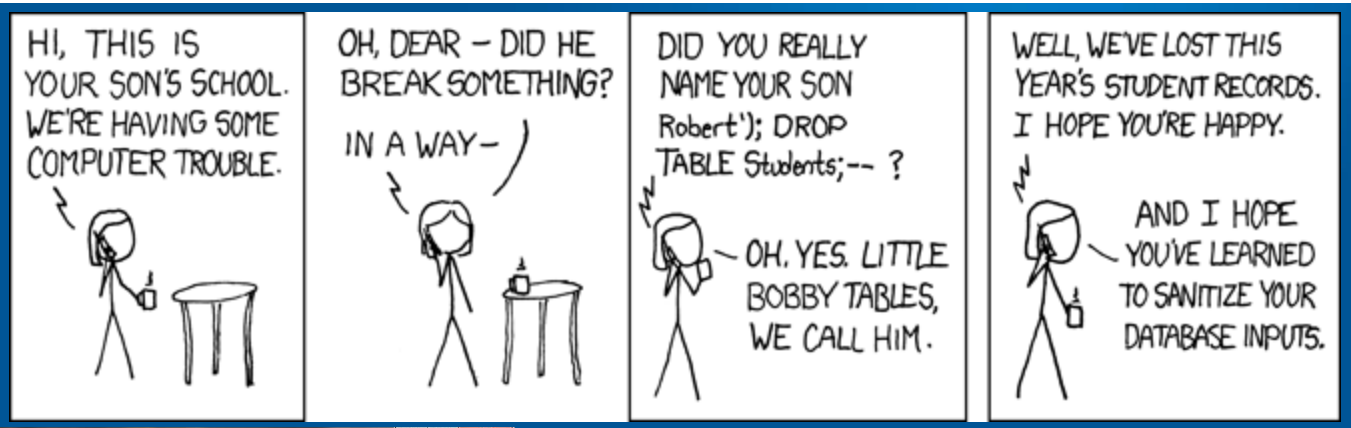
Who We Are

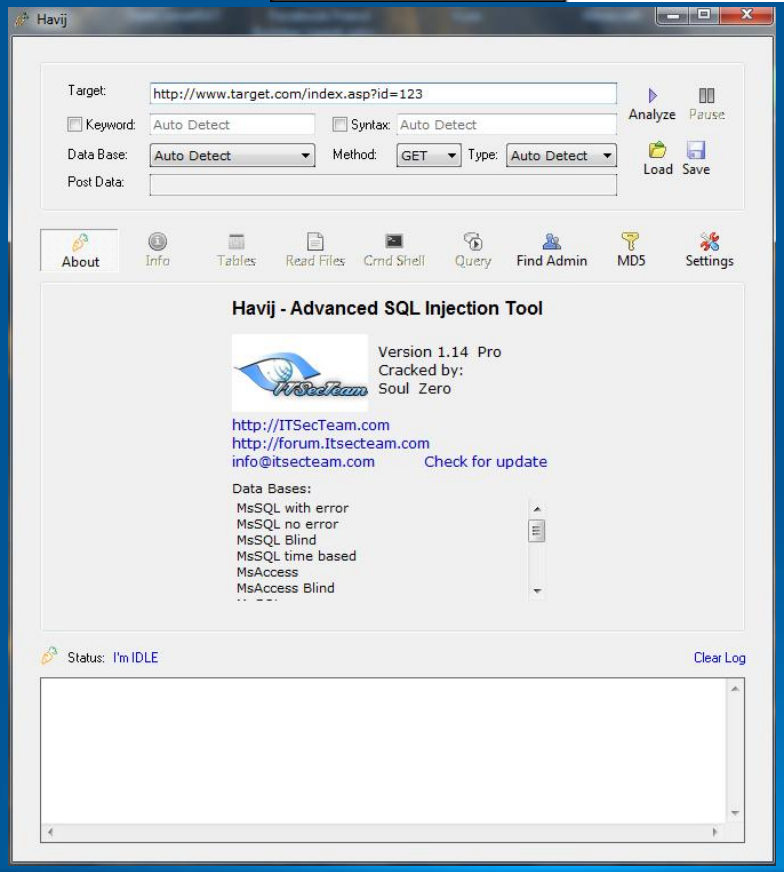
Bibliography

DEF CON

Problem

STROZ FRIEDBERG





sqlmap

Automatic SQL injection and database takeover tool

DEFCON

Problem

STROZ FRIEDBERG

- 97% of data breach cases worldwide involve SQL injection attacks somewhere down the line.

- On average the cost of data breach response and remediation is between $194 - $222 per record.

- As of July 9th, privacyrights.org cites 330 breaches in 2012 effecting 18.6 million records.

(datalossdb.org reports much higher at 723 breaches thus far)

DEFCON

Problem

STROZ FRIEDBERG

Historical response is costly

Fly a bunch of consultants to a data center

They image the server

Analyze the logs

Determine what was exfiltrated from reviewing those logs.

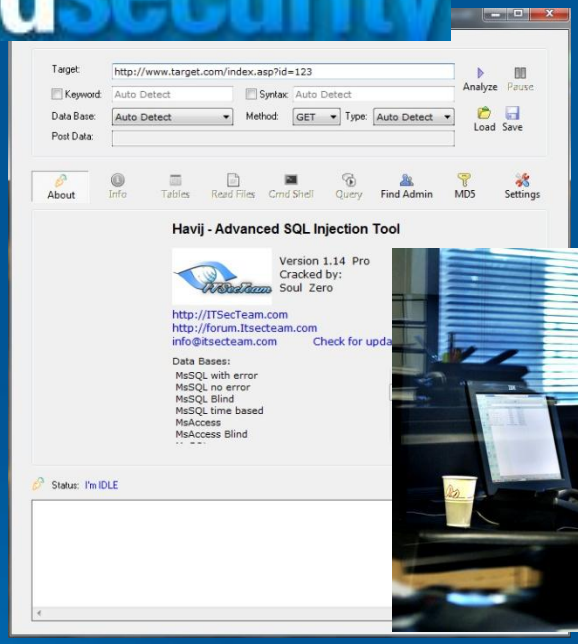
Typically running SQL commands against SQL server

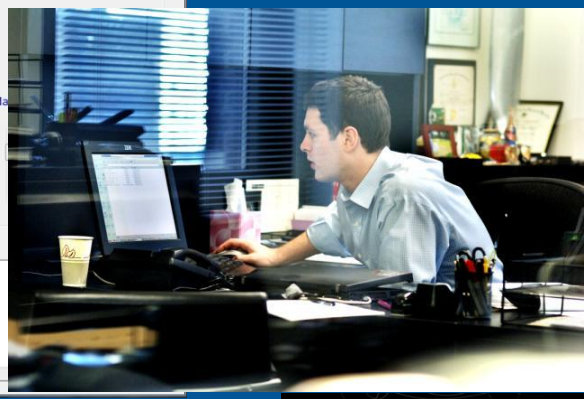
Only going to get costlier

DEF CON

Problem

STROZ FRIEDBERG

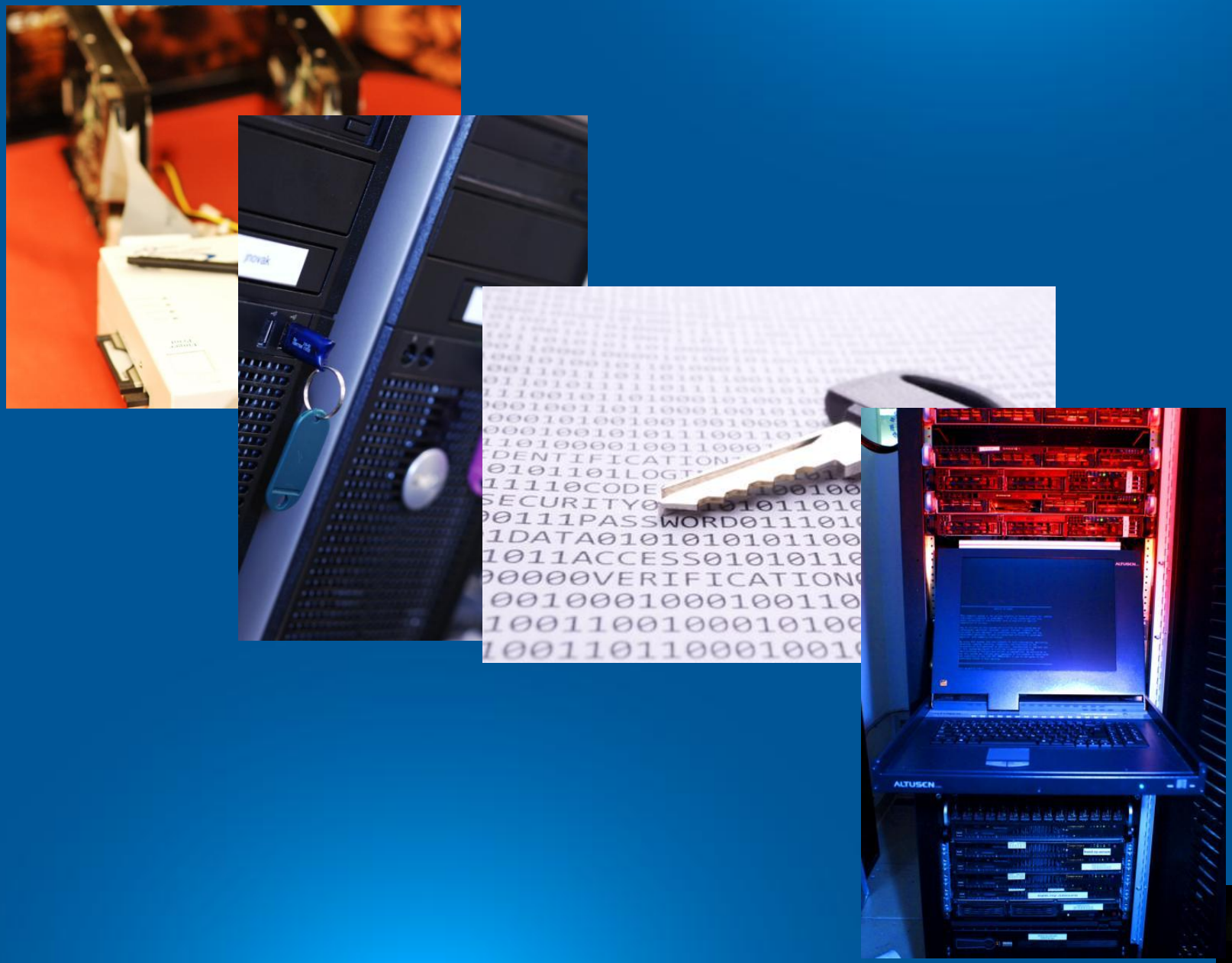




DEFCON

SQLReInjector

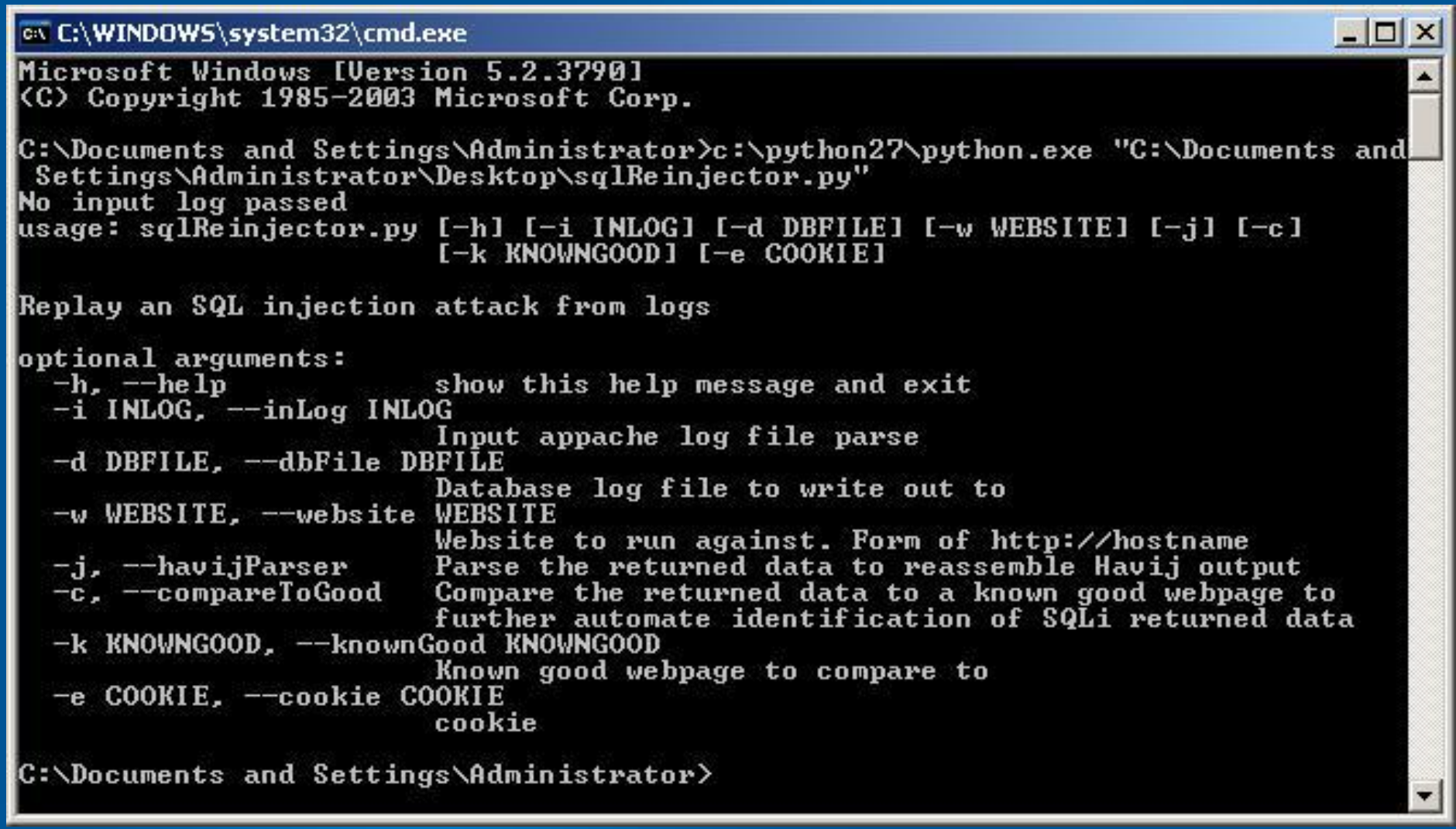
STROZ FRIEDBERG



DEFCON

SQLReInjector

STROZ FRIEDBERG



DEFCON

Demo Time

Where to Get It

STROZ FRIEDBERG

github.com/strozfriedberg

DEFCON

QUESTIONS?

Bibliography and Thanks

STROZ FRIEDBERG

- Exploits of a Mom / Little Bobby Tables by Randall Munroe
  - http://xkcd.com/327/
- sqlmap by Bernardo Damele A.G. and Miroslav Stampar
  - http://sqlmap.org/
- DVWA by RandomStorm
  - http://www.dvwa.co.uk/
- Apache Log Parsing
  - apachelog Python Module, http://code.google.com/p/apachelog/, hfuecks@gmail.com;
  - Apache-LogRegex Module, search.cpan.org/dist/Apache-LogRegex/, Peter Hickman;
- Virtualization of Forensic Images
  - LiveView, http://liveview.sourceforge.net/, CERT Software Engineering Institute
- Replaying SQL Injection Attacks
  - Bret Padres, http://cyberspeak.libsyn.com
- Injection Attack and Data Theft Statistics
  - Neira Jones, Barclay Card http://news.techworld.com/security/3331283/barclays-97-percent-of-data-breaches-still-due-to-sql-injection/

- Thanks to:
  - Erin Nealy Cox
  - Cheri Carr
  - Scott Brown

DEFCON

Who We Are

STROZ FRIEDBERG

Over 270 employees in 11 U.S. and 1 U.K. Offices

Who We Are

STROZ FRIEDBERG

Jason A. Novak
Assistant Director, Digital Forensics
Chicago, IL
jnovak@strozfriedberg.com

Andrea London
Digital Forensic Examiner
Dallas, TX
alondon@strozfriedberg.com

www.StrozFriedberg.com

DEFCON