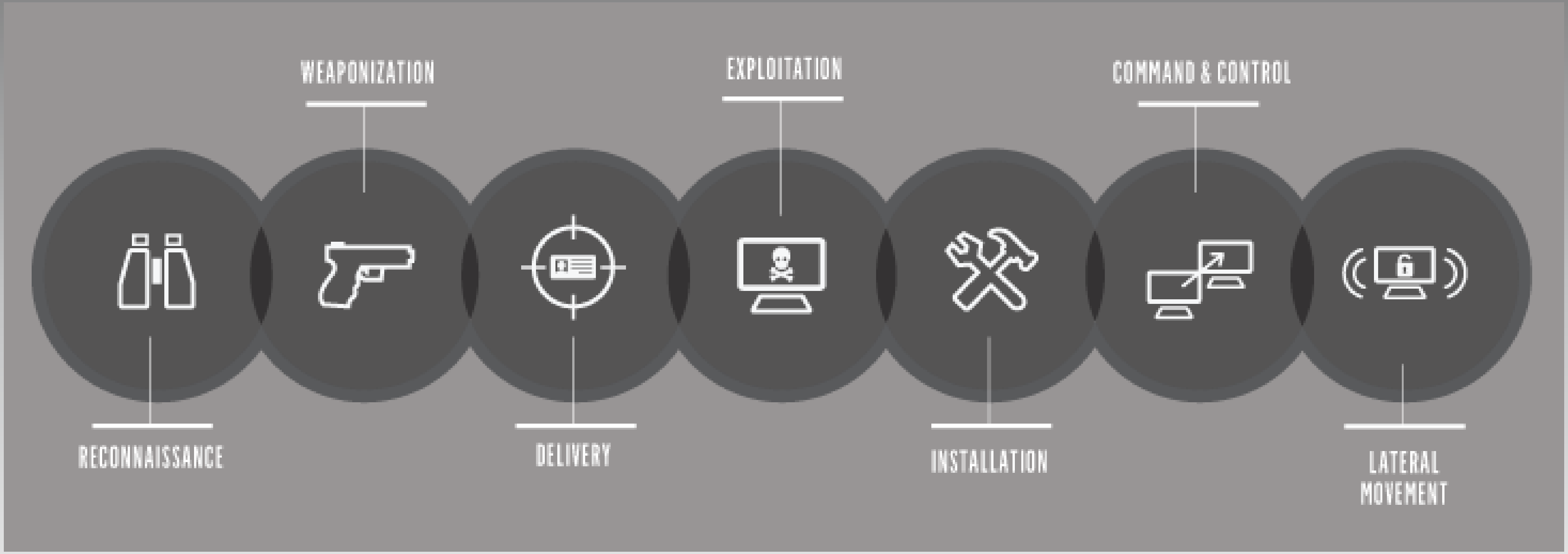
A GLIMPSE INTO TARGETED ATTACKS

Dr. Chris Dietrich

ABOUT ME

- B.Sc. Medieninformatik, FH GE
- M.Sc. Angewandte Informatik
  Institut fuer Internet-Sicherheit if(is), FH GE
- FTE, if(is) WHS/FH GE
- PhD, Uni Mannheim
- CrowdStrike

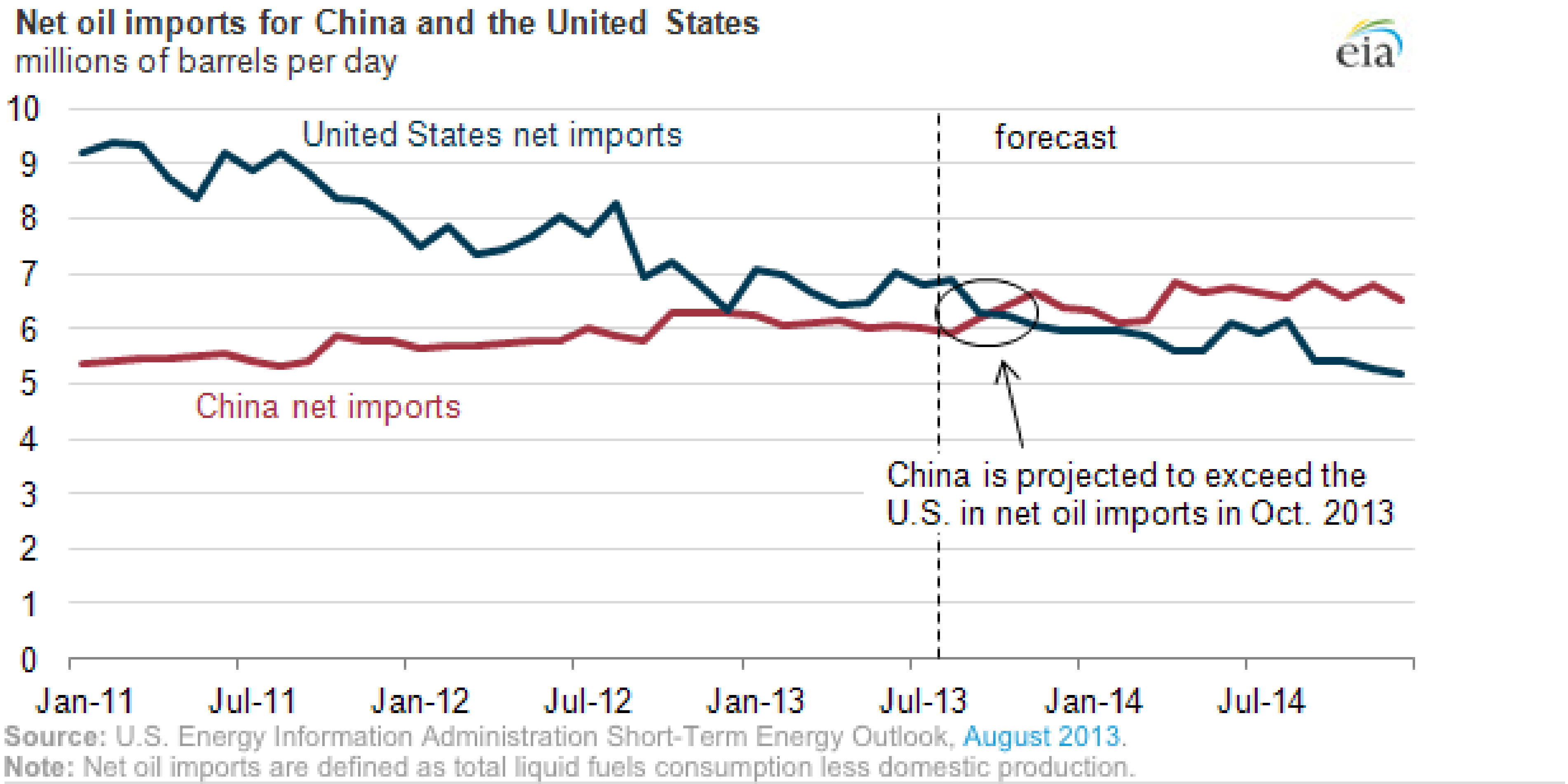

WEAPONIZATION
EXPLOITATION
COMMAND & CONTROL
RECONNAISSANCE
DELIVERY
INSTALLATION
LATERAL MOVEMENT

CASE 1

TARGETING THINK TANKS AND HUMAN RIGHTS ORG

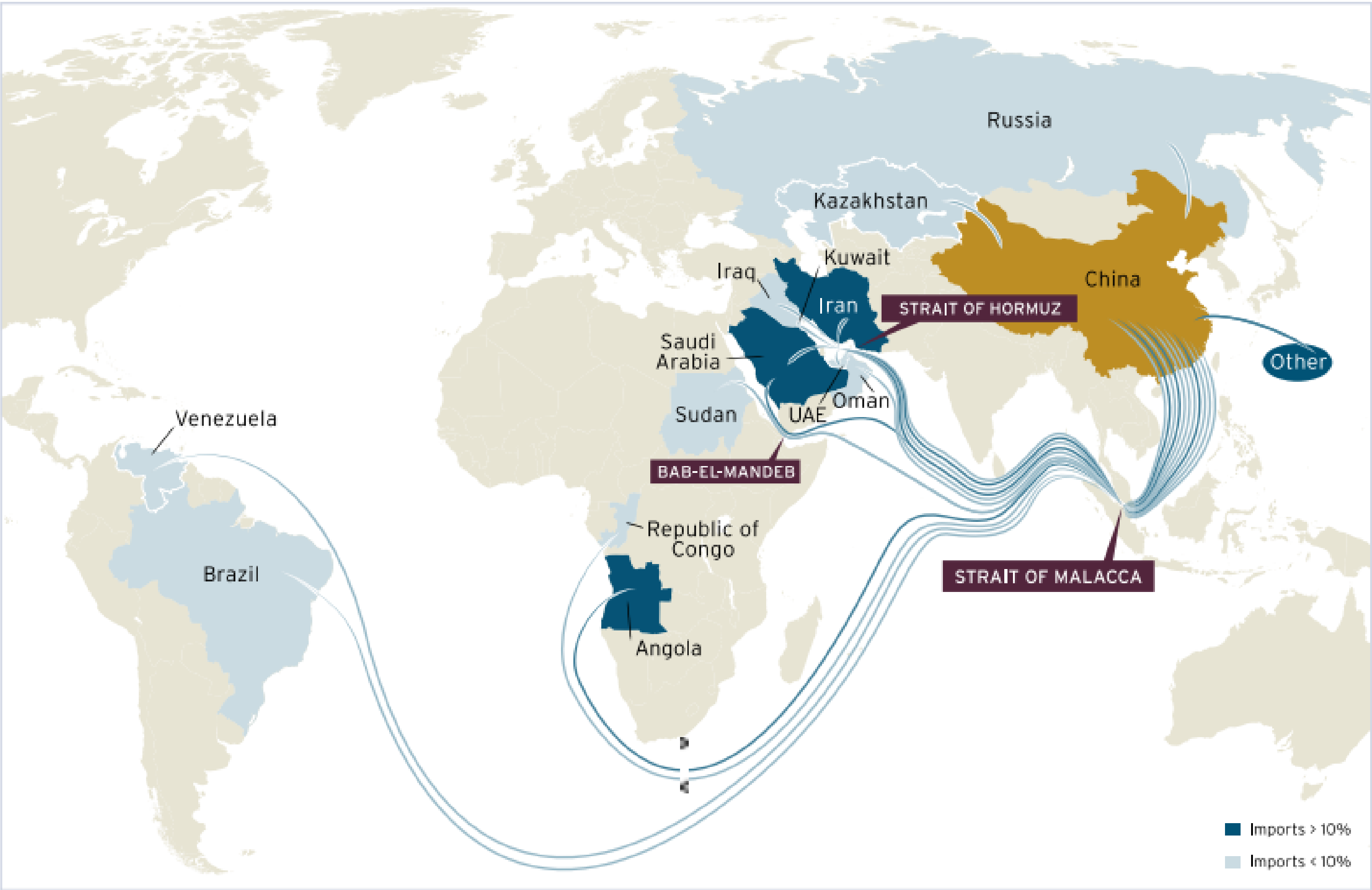
- Former senior government staff
- Suffering from targeted attacks regularly
- Mid-June 2014: Target shift
  - Previously: Far East, Asia/Pacific, China
  - Now: individuals with a tie to Iraq and Middle East issues
- **Why?**

OIL RESOURCE CONSUMPTION



Source: U.S. Energy Information Administration Short-Term Energy Outlook, August 2013.
Note: Net oil imports are defined as total liquid fuels consumption less domestic production.

China Import Countries, 2011



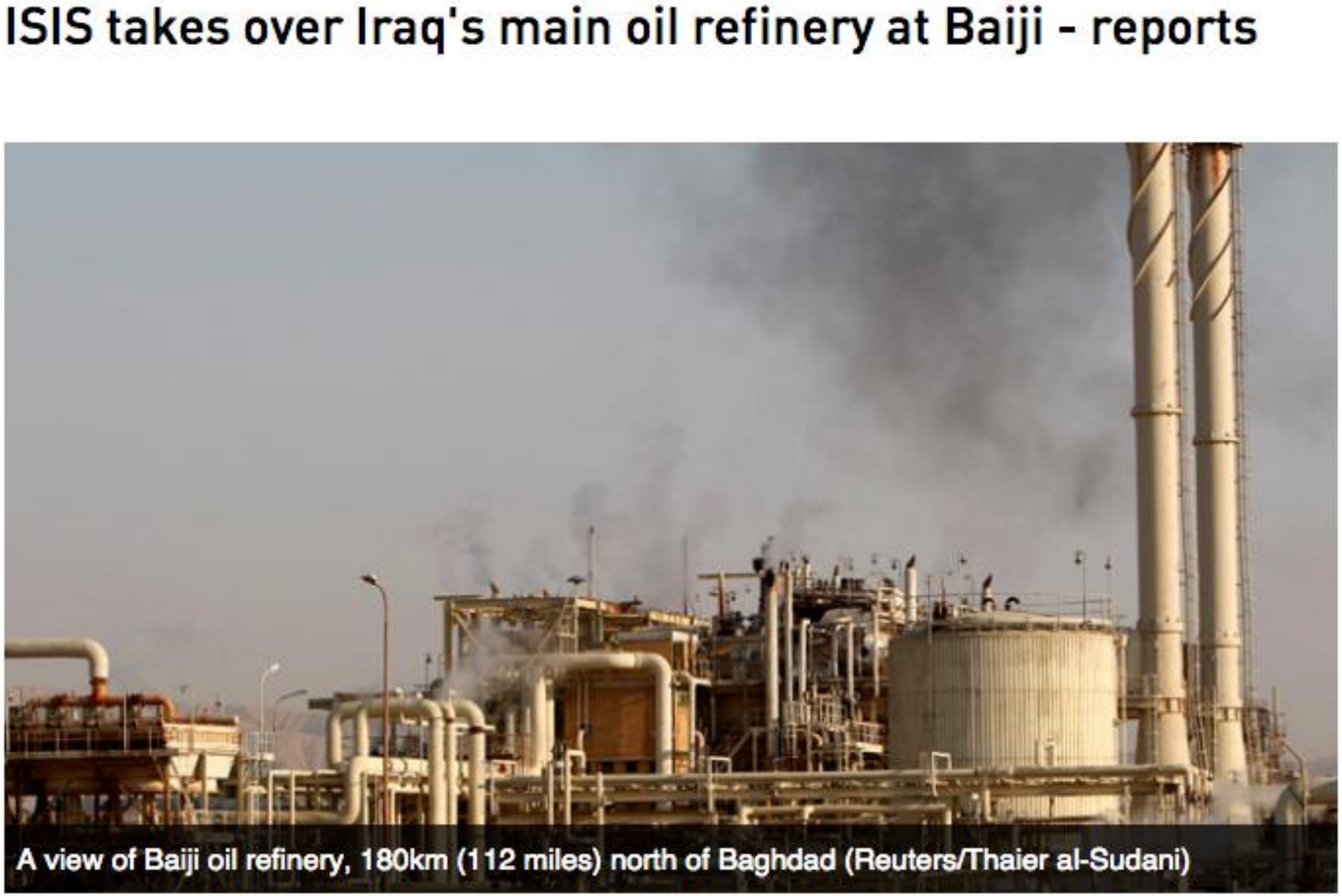
Country	Saudi Arabia	Angola	Iran	Russia	Oman	Iraq	Sudan	Venezuela	Kazakhstan	Kuwait	UAE	Brazil	Republic of Congo	Other
Percentage of Imports	19.8	12.3	10.9	7.8	7.2	5.4	5.1	4.5	4.4	3.8	2.7	2.6	2.2	11.3
Thousand Barrels	366,825	227,395	202,575	144,175	132,495	100,740	94,900	83,950	81,760	69,715	49,275	48,910	41,245	208,780

Created by Marcia Underwood of the Brookings Institution with data compiled from the U.S. Energy Information Agency's China Country Report 2012. http://www.eia.gov/countries/cab.cfm?fips=CH.

Iraq

- 5.4% of oil imports
- Ranked 6th

JUNE 18TH 2014

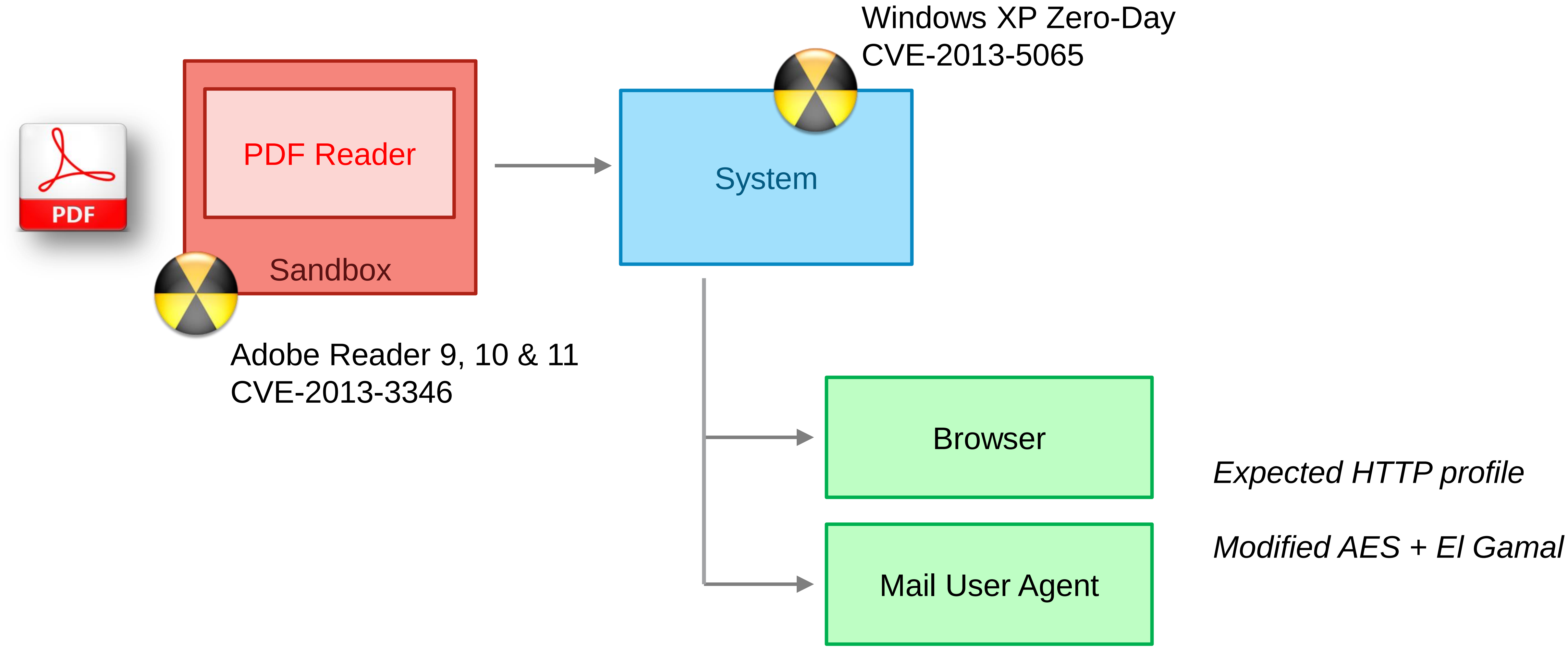


ISIS takes over Iraq's main oil refinery at Baiji - reports

A view of Baiji oil refinery, 180km (112 miles) north of Baghdad (Reuters/Thaier al-Sudani)

CASE 2

ANATOMY OF AN ATTACK



PDF Reader

Sandbox

Adobe Reader 9, 10 & 11
CVE-2013-3346

System

Windows XP Zero-Day
CVE-2013-5065

Browser

Mail User Agent

Expected HTTP profile

Modified AES + El Gamal

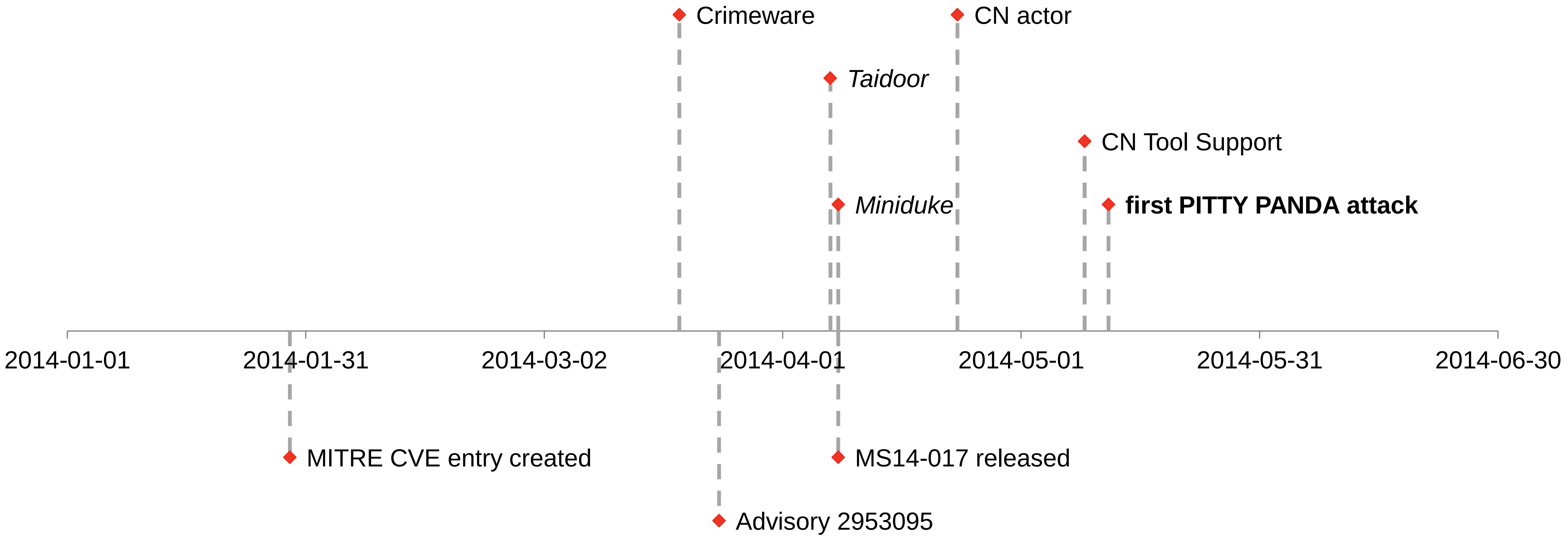
EXPLOIT CLIENT-SIDE SOFTWARE

- Exploit vulnerabilities in client-side software
  - Microsoft Office (Word, Excel, Powerpoint)
  - Email/communication software
  - PDF readers
  - OS components
- Specifically crafted exploit documents

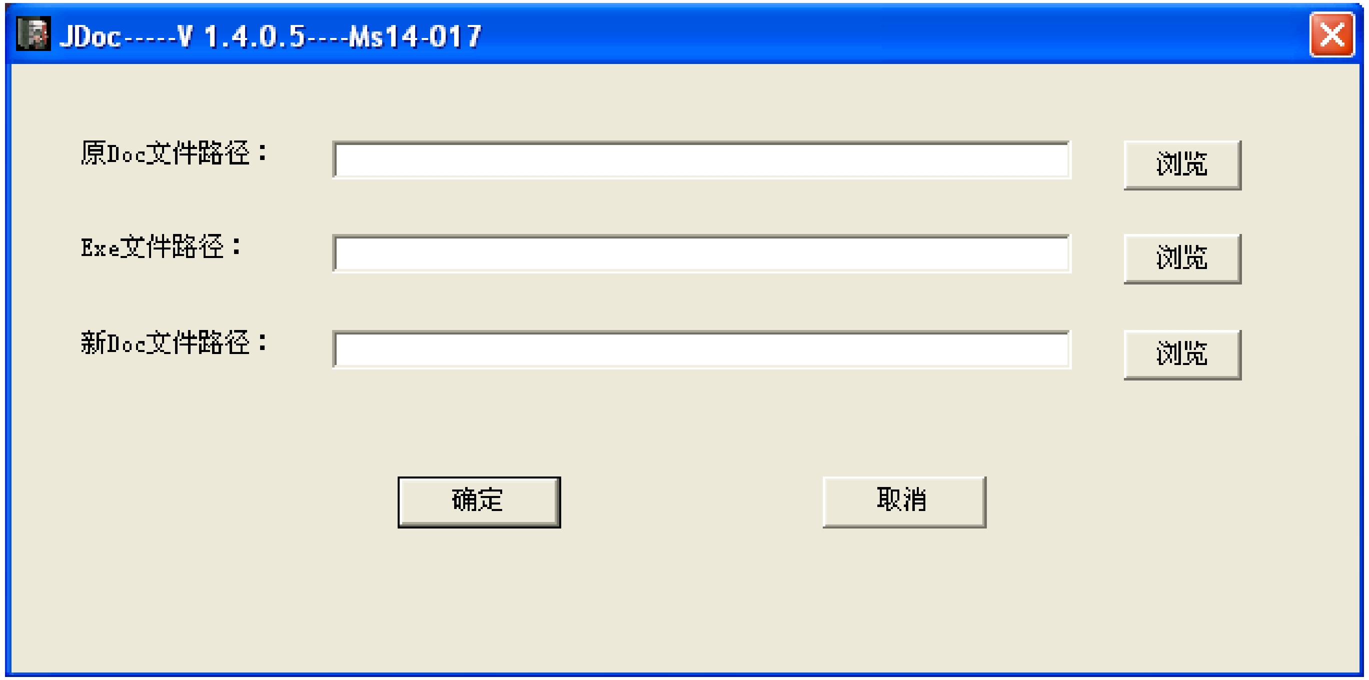
CVE-2014-1761 – KEY FACTS

- Initially discovered by Google Security Team
- RTF Parser Memory Corruption Vulnerability
- Affects Microsoft Word versions 2003 to 2013
- Popular among targeted attack actors in Q2 2014

PROLIFERATION OF CVE-2014-1761 – TIMELINE



PROLIFERATION OF CVE-2014-1761



- Adversary tool support
- Automatically create exploit documents for CVE-2014-1761
- Input
  - Arbitrary Word decoy document
  - Arbitrary malware binary

THANK YOU.