TOP DATA BREACHES

VOLUME I, EDITION 3 AS REPORTED FOR **WEEK OF AUGUST 4, 2014**

4 TOP DATA BREACHES REPORTED THIS WEEK

NOW WHAT?

This week's top reported incidents have one thing in common:
They leave numerous questions unanswered.

CYBERVOR

1.2 BILLION
PEOPLE IMPACTED

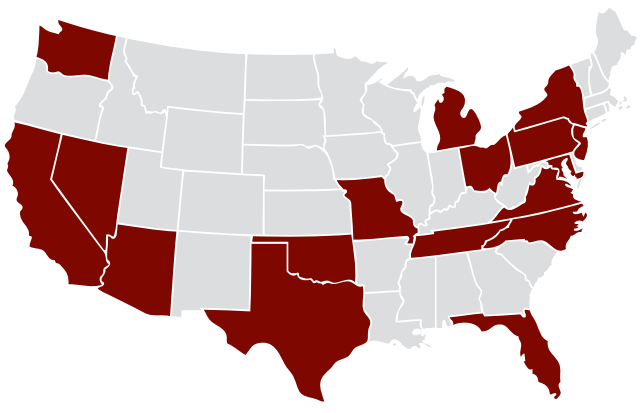
THE ANNOUNCEMENT

Security firm Hold Security says a Russian cyber gang has breached more than 420,000 Web and FTP sites to pilfer over 1.2 billion credentials.

QUESTIONS RAISED

- Which Web and FTP sites were compromised, and when?
- Are the 1.2 billion credentials linked to unannounced incidents, or are they compromises from previous incidents?
- Are impacted organizations being notified by the security firm about the breach?
- What motivated Hold Security to make its announcement the week of the Black Hat USA and Def Con conferences?

P.F. CHANG'S CHINA BISTRO®



33 STORES
AFFECTED NATIONWIDE

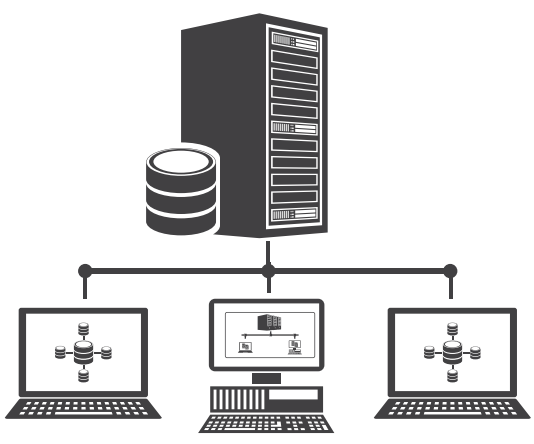
THE ANNOUNCEMENT

The restaurant chain offers an update on its investigation of a data breach, saying that 33 of its 210 U.S. locations were impacted, resulting in the potential theft of customer payment card information.

QUESTIONS RAISED

- Why were only 33 of its 210 U.S. locations affected?
- What do these sites have in common?
- How did the chain deduce the specific range of times for each impacted location?

USIS®



THE ANNOUNCEMENT

The company, which conducts background checks for the Department of Homeland Security and other agencies, says it has identified a cyber-attack on its corporate network, which "has all the markings of a state-sponsored attack."

QUESTIONS RAISED

- What information was compromised in the attack?
- When did the compromise occur?
- How many government agencies are impacted?
- Why does the firm believe this was a "state-sponsored attack?"

SNOWDEN 2.0?
ANOTHER INSIDER LEAK

THE ANNOUNCEMENT

U.S. officials have confirmed the existence of a new leaker exposing national security documents, CNN reports. The leak apparently involves documents prepared by the National Counterterrorism Center.

QUESTIONS RAISED

- Are government officials aware of who the leaker is?
- Where did the leaker work?
- Has the leaker been apprehended?
- Does the leaker, like Edward Snowden, have access to other information that could be disclosed?

Data Sources:
Hold Security, P.F. Chang's, U.S. Investigations Services, Office of Personnel Management, CNN, The Intercept

View this infographic online
http://www.databreachtoday.com/top-breaches-raise-questions-a-7174

ISMG Network Sources

http://www.databreachtoday.com/5-facts-about-cybervor-report-a-7163
http://www.databreachtoday.com/pf-changs-breach-33-locations-hit-a-7153
http://www.databreachtoday.com/background-check-firm-hit-by-breach-a-7168
http://www.databreachtoday.com/report-new-government-leaker-confirmed-a-7159

Data Breach Prevention. Response. Notification. TODAY