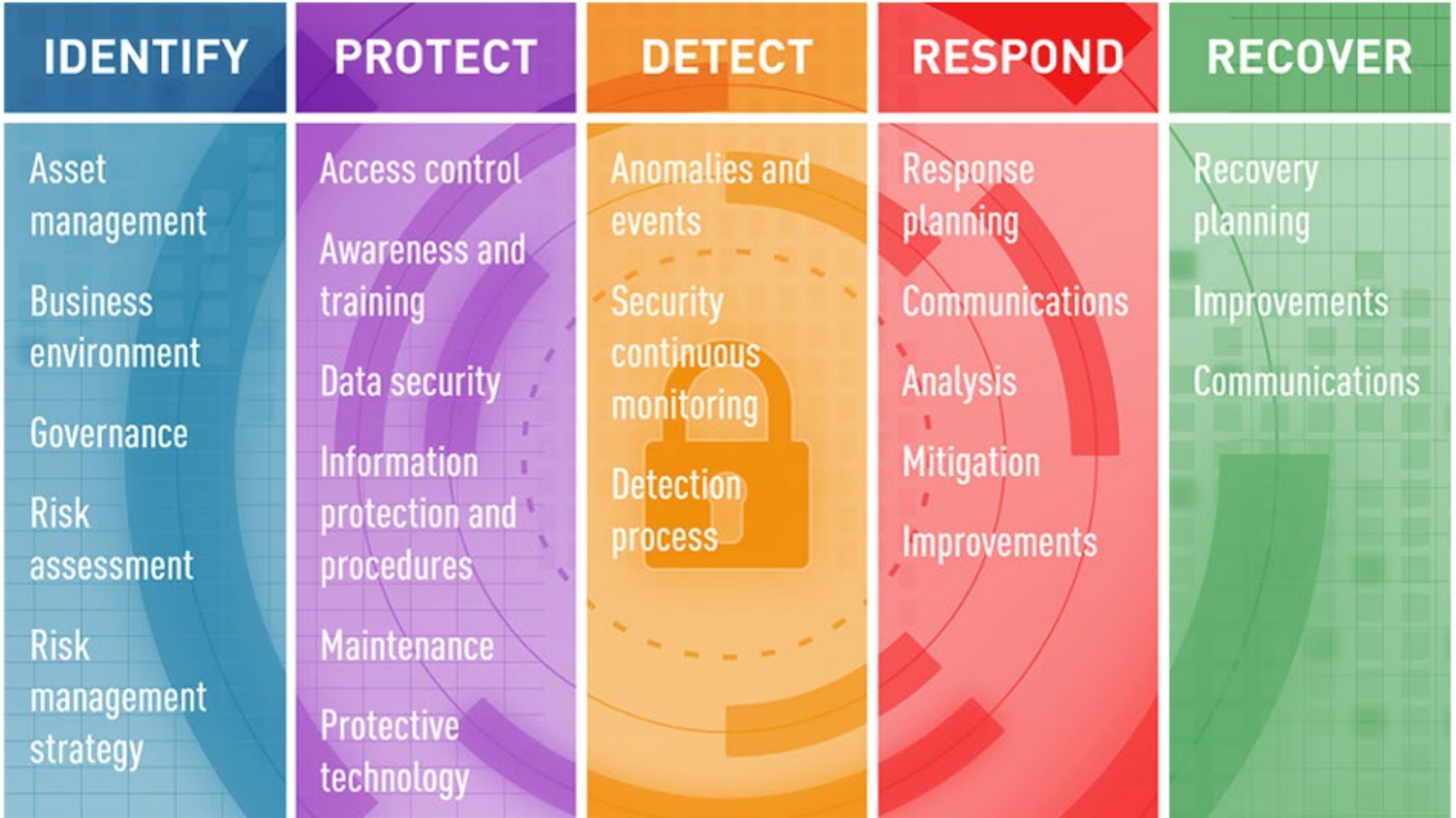

EQUIFAX

EQUIFAX BREACH

ESSENTIALLY, IN THE CYBERWORLD, THIS BREACH WAS A CATEGORY 5 HURRICANE.

- BY AMY LAWLER
- CITC-1351 025
- PRINCIPLES OF INFORMATION ASSURANCE
- SPRING SEMESTER, 2019 PROFESSOR GEORGE MEGHABGHAB


IDENTIFY
Asset management
Business environment
Governance
Risk assessment
Risk management strategy
PROTECT
Access control
Awareness and training
Data security
Information protection and procedures
Maintenance
Protective technology
DETECT
Anomalies and events
Security continuous monitoring
Detection process
RESPOND
Response planning
Communications
Analysis
Mitigation
Improvements
RECOVER
Recovery planning
Improvements
Communications

CRAs

- A **CONSUMER REPORTING AGENCY** is a person or entity that assembles or evaluates consumer credit information or other consumer information for the purpose of furnishing consumer reports to others, which they then sell to other businesses and organizations that use the information to assess or evaluate creditworthiness.
- A **LENDER** uses the information provided to determine whether to offer credit to an individual, the rate of interest to be assigned to the loan, and other terms. of the contract.
- A growing number of entities use information provided by CRAs to help make decisions about individuals' credit worthiness when determining eligibility for insurance, housing, or employment, among other things.
- This information can also be used for other purposes, such as to identify potential customers with specific characteristics for new credit card accounts.
- Equifax provides income and employment verification services using information collected from employers.
- **CRAs** typically use information they collect to generate questions that **FEDERAL AGENCIES** and other entities can use to **test** applicants' knowledge of information in their credit file. These questions and answers are typically the basis for **identity proofing**

EQUIFAX FACTS

CRAs

Equifax is part of the three major credit reporting agencies.

1898

Equifax founders, Cator & Guy Woolford, who are brothers and own a grocery store in **Tennessee**. Would compile lists of customers based on their creditworthiness.

1899

The brothers relocate to Atlanta, GA where they began the **Retail Credit Company**. A book that was filled with compiled credit information, would be sold to merchants in the area. Later they would sell their credit info to life insurance agencies, and then auto liability insurance.

1960's

Data transitioned from written index cards to electronic data systems.

EQUIFAX FACTS…

1971

Retail's credit reporting also began to be governed by the **Fair Credit Reporting Act.** In the early days of the Act, **Equifax was a frequent violator**.

1979

Change their name to EQUIFAX

1980's

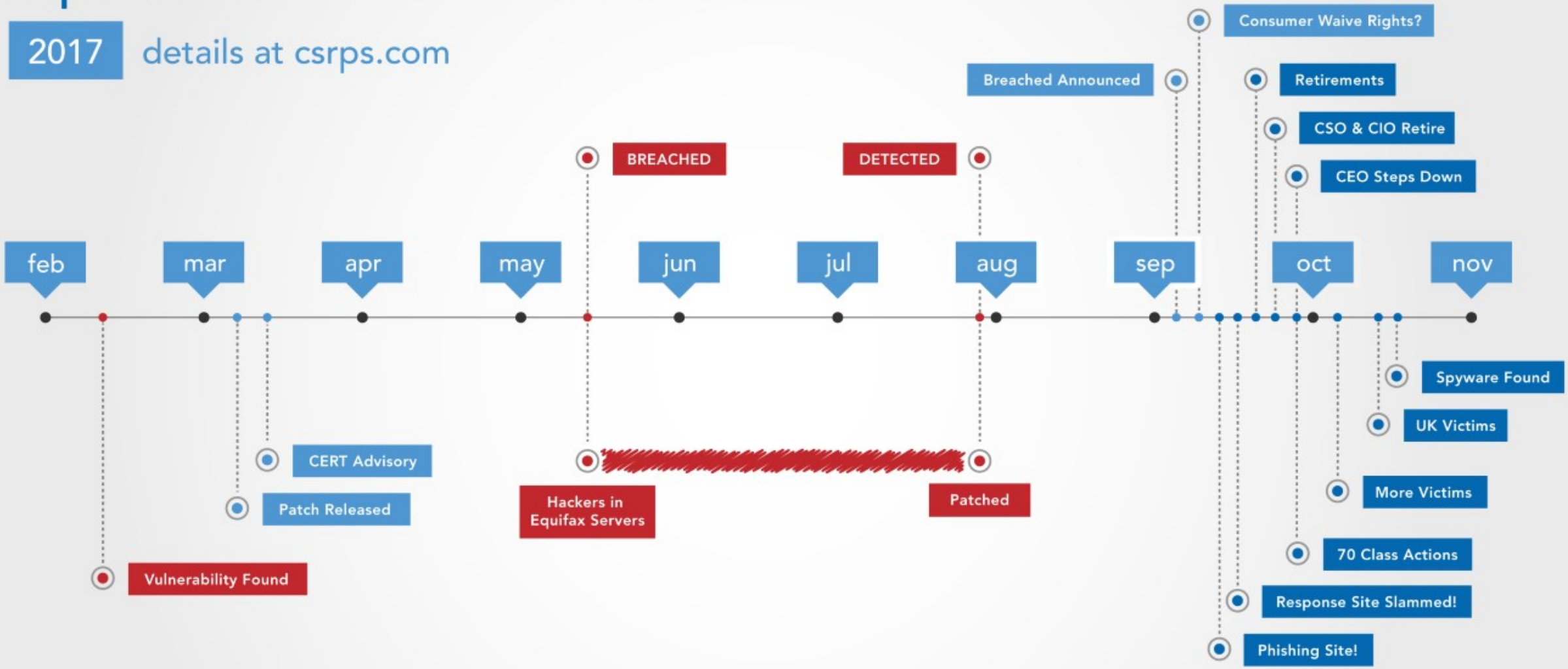
Equifax had data on more than **150 million consumers**, in **all** 50 states, with revenue of **$743 Million.**

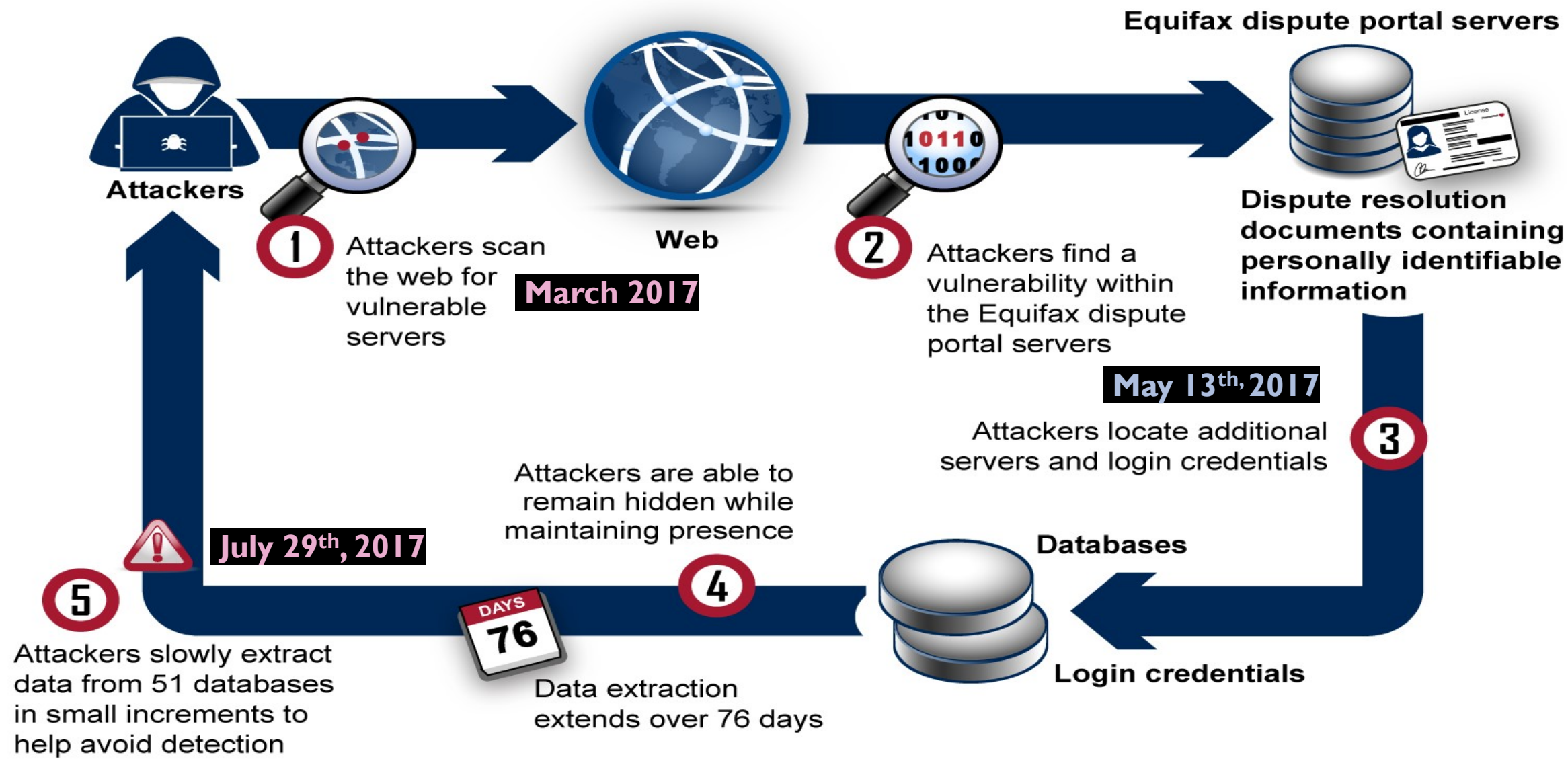
Now!

Equifax has a workforce of about **14,000 employees** throughout **19 countries**, and reports revenue of **$3.14 Billion**.

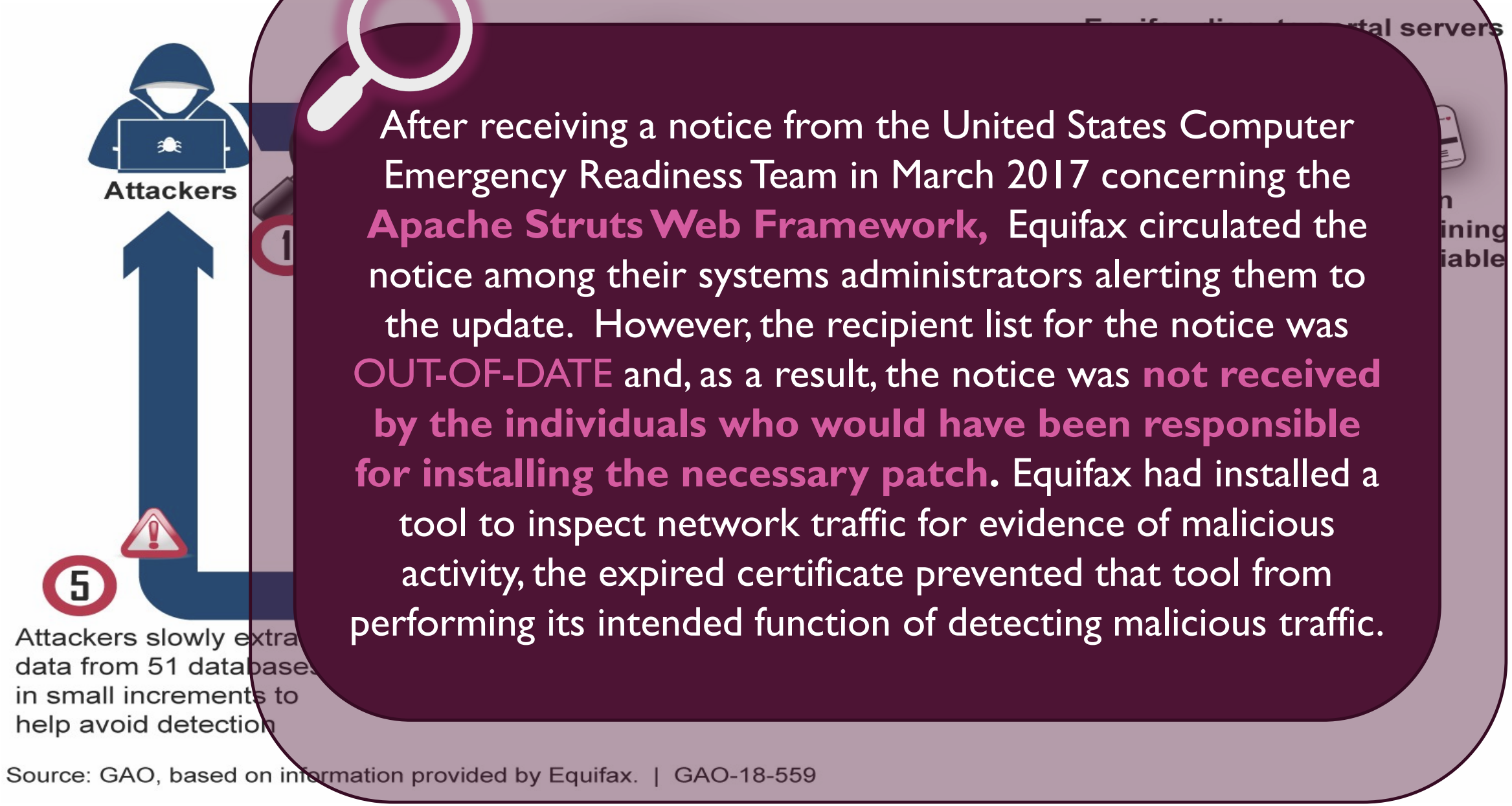
Equifax Data Breach Timeline

2017 details at csrps.com

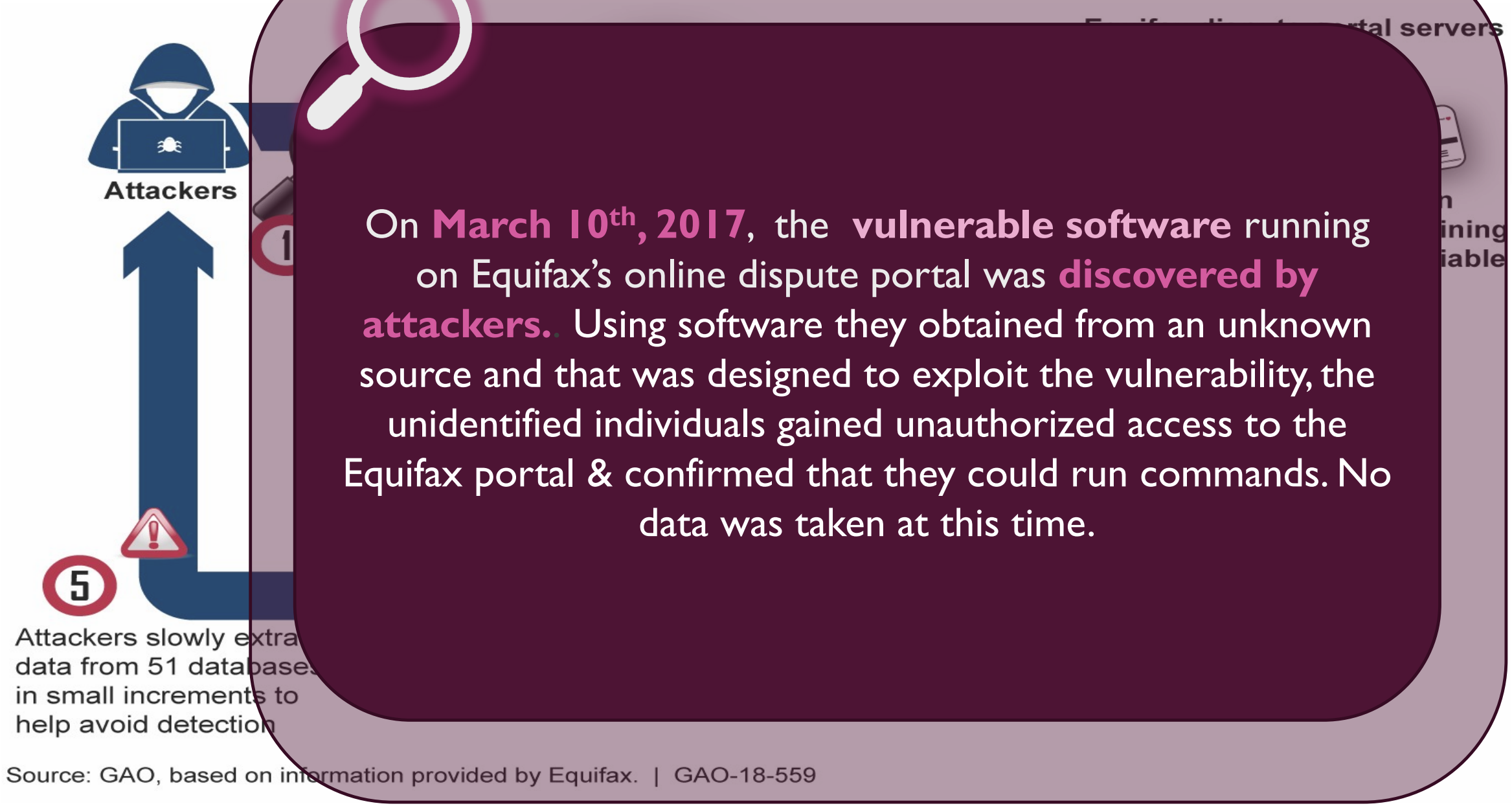




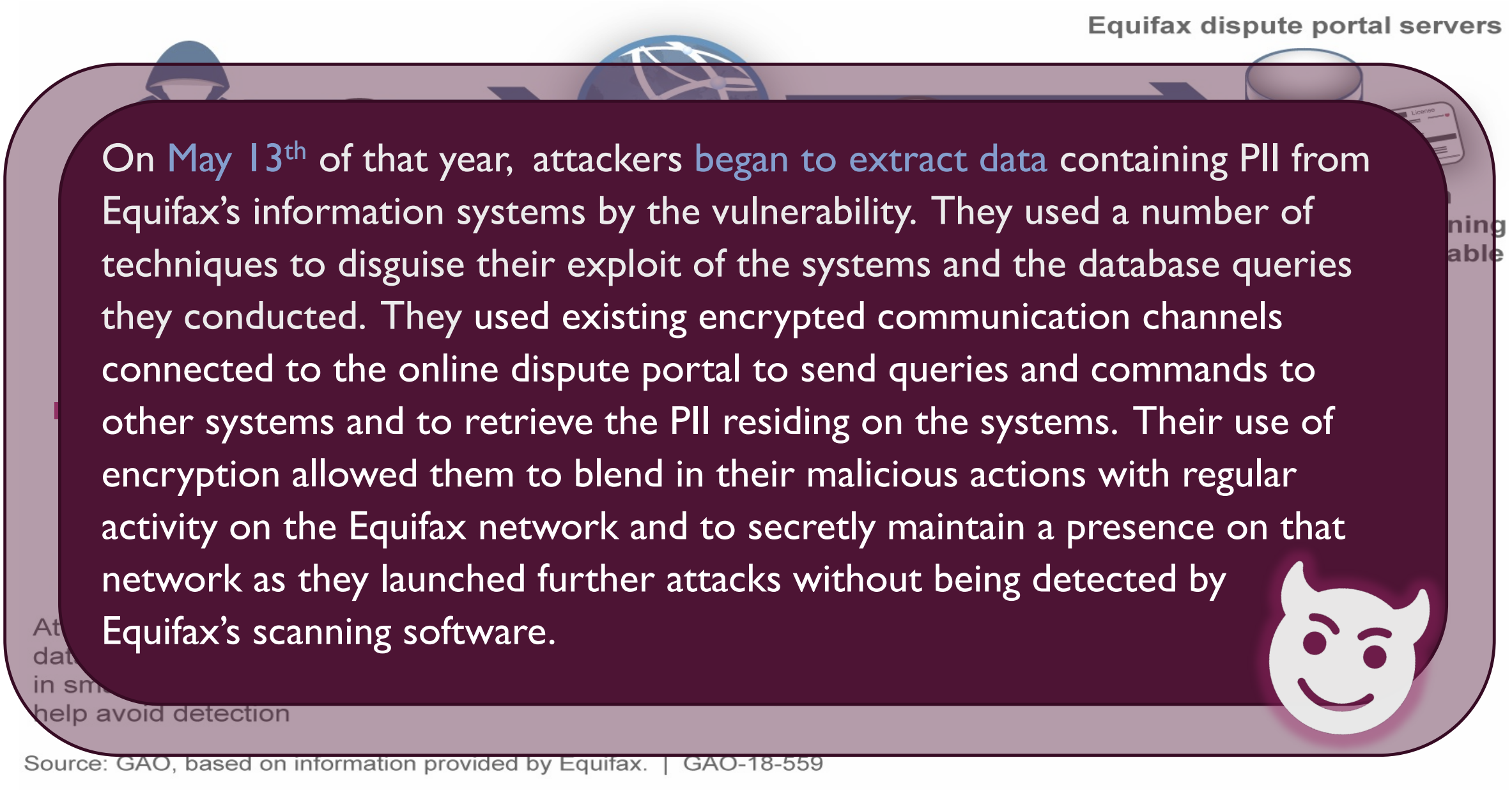
Source: GAO, based on information provided by Equifax. | GAO-18-559



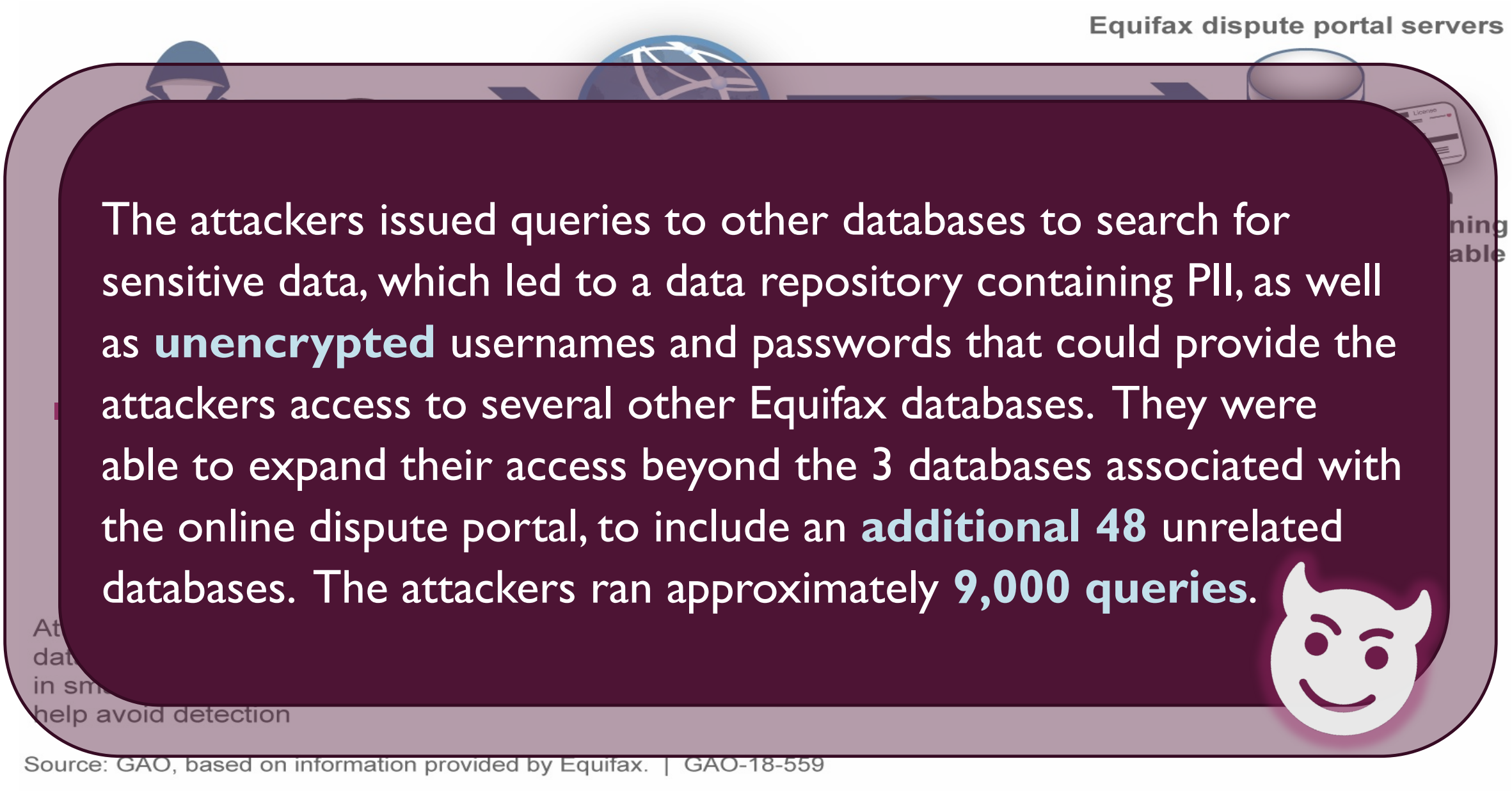
After receiving a notice from the United States Computer Emergency Readiness Team in March 2017 concerning the **Apache Struts Web Framework,** Equifax circulated the notice among their systems administrators alerting them to the update. However, the recipient list for the notice was OUT-OF-DATE and, as a result, the notice was **not received by the individuals who would have been responsible for installing the necessary patch.** Equifax had installed a tool to inspect network traffic for evidence of malicious activity, the expired certificate prevented that tool from performing its intended function of detecting malicious traffic.



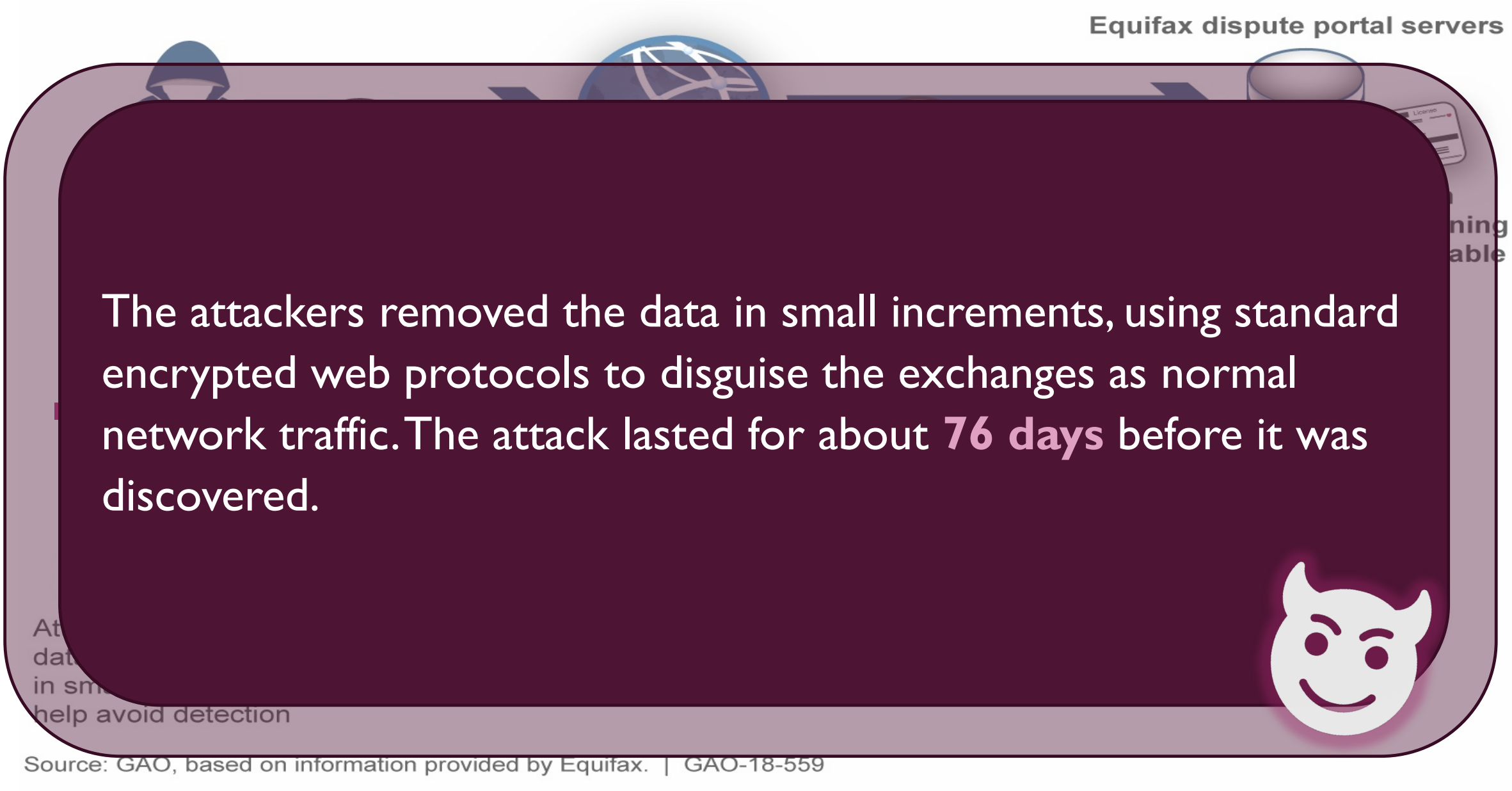
On **March 10th, 2017**, the **vulnerable software** running on Equifax's online dispute portal was **discovered by attackers.**. Using software they obtained from an unknown source and that was designed to exploit the vulnerability, the unidentified individuals gained unauthorized access to the Equifax portal & confirmed that they could run commands. No data was taken at this time.



On May 13th of that year, attackers began to extract data containing PII from Equifax's information systems by the vulnerability. They used a number of techniques to disguise their exploit of the systems and the database queries they conducted. They used existing encrypted communication channels connected to the online dispute portal to send queries and commands to other systems and to retrieve the PII residing on the systems. Their use of encryption allowed them to blend in their malicious actions with regular activity on the Equifax network and to secretly maintain a presence on that network as they launched further attacks without being detected by Equifax's scanning software.

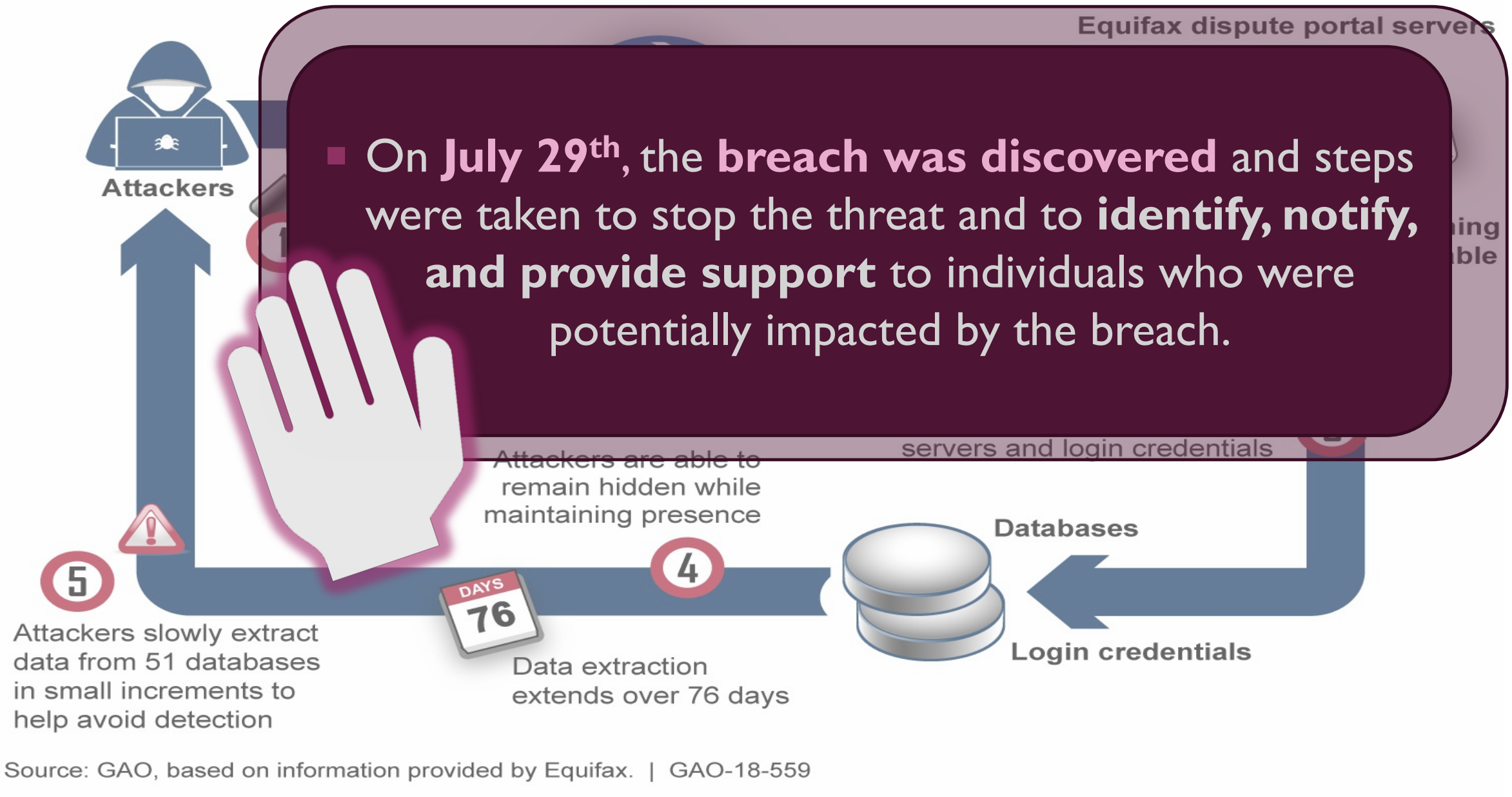


The attackers issued queries to other databases to search for sensitive data, which led to a data repository containing PII, as well as **unencrypted** usernames and passwords that could provide the attackers access to several other Equifax databases. They were able to expand their access beyond the 3 databases associated with the online dispute portal, to include an **additional 48** unrelated databases. The attackers ran approximately **9,000 queries**.

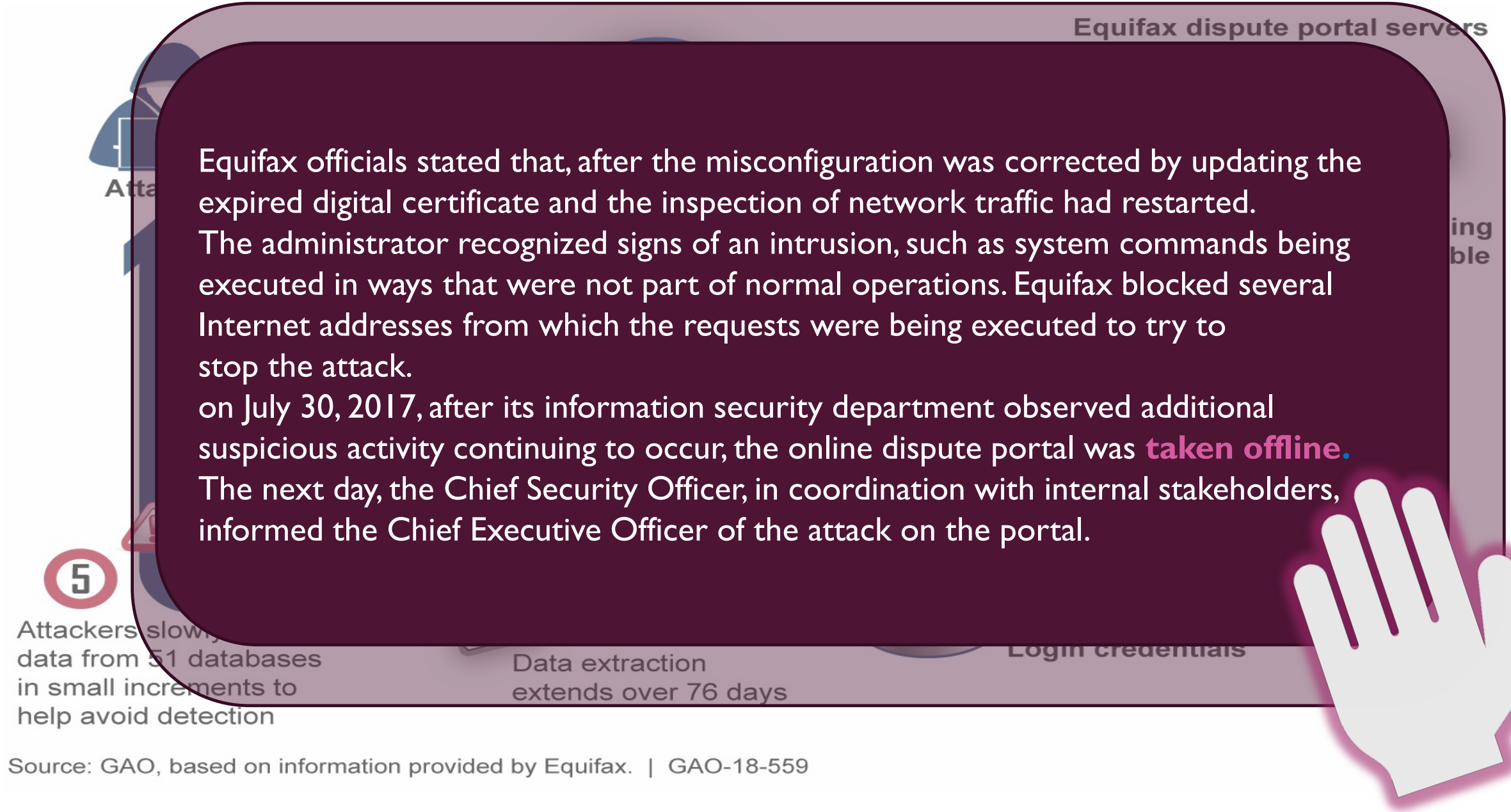


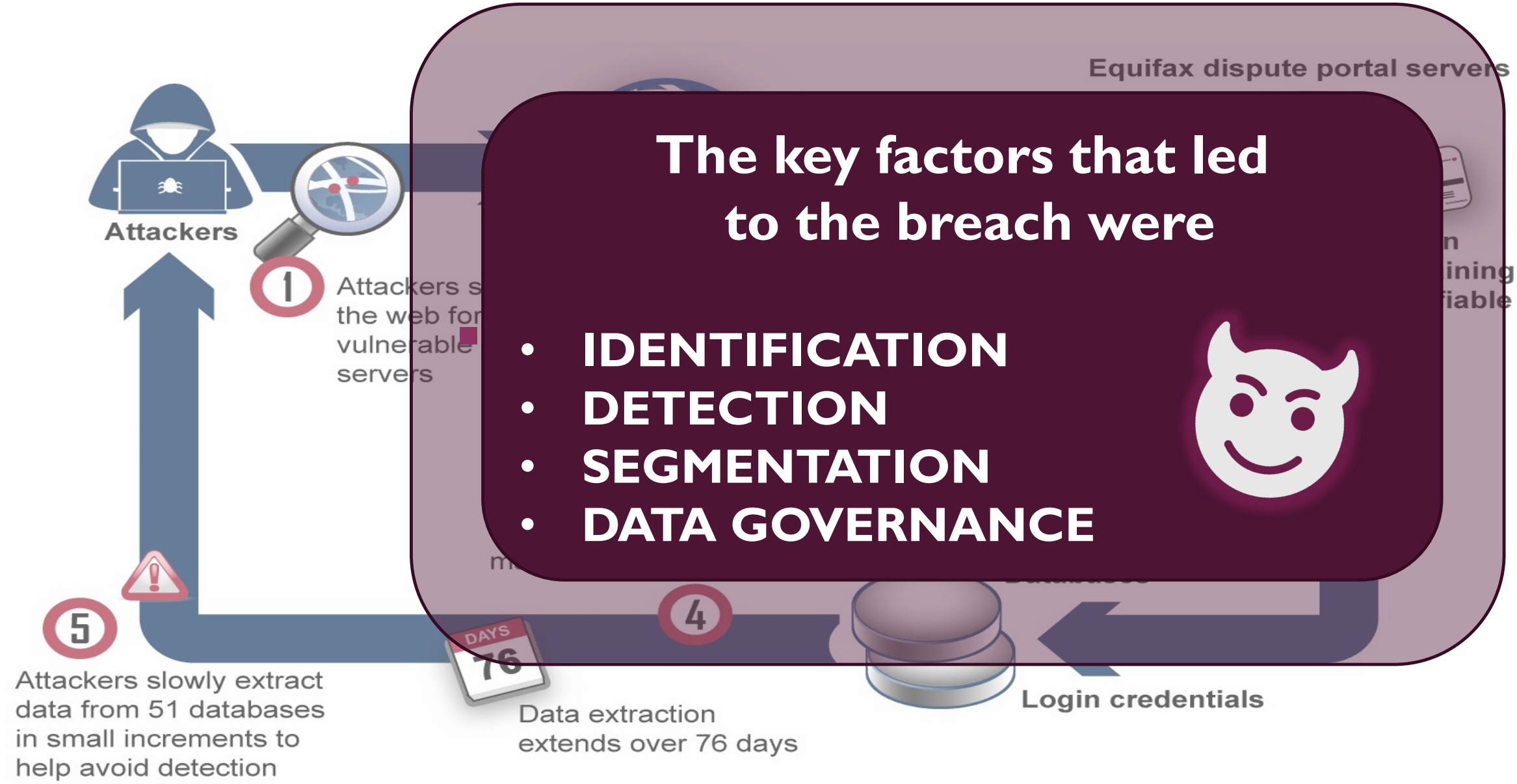
The attackers removed the data in small increments, using standard encrypted web protocols to disguise the exchanges as normal network traffic. The attack lasted for about **76 days** before it was discovered.

- On **July 29th**, the **breach was discovered** and steps were taken to stop the threat and to **identify, notify, and provide support** to individuals who were potentially impacted by the breach.



Source: GAO, based on information provided by Equifax. | GAO-18-559


Equifax dispute portal servers
Equifax officials stated that, after the misconfiguration was corrected by updating the expired digital certificate and the inspection of network traffic had restarted.
The administrator recognized signs of an intrusion, such as system commands being executed in ways that were not part of normal operations. Equifax blocked several Internet addresses from which the requests were being executed to try to stop the attack.
on July 30, 2017, after its information security department observed additional suspicious activity continuing to occur, the online dispute portal was taken offline.
The next day, the Chief Security Officer, in coordination with internal stakeholders, informed the Chief Executive Officer of the attack on the portal.
5
Attackers slowly
data from 51 databases
in small increments to
help avoid detection
Data extraction
extends over 76 days
Login credentials
Source: GAO, based on information provided by Equifax. | GAO-18-559



Source: GAO, based on information provided by Equifax. | GAO-18-559

WHAT THEY FOUND?

A network administrator conducting routine checks, discovers that a **MISCONFIGURED PIECE OF EQUIPMENT** allowed attackers to **communicate with compromised servers and steal data without detection.**

This **misconfiguration** allowed encrypted traffic to pass through the network **without being inspected**. Equifax says, the misconfiguration was due to an **EXPIRED digital certificate,** and had expired about **10 MONTHS BEFORE** the breach occurred.

At least **145.5 million consumers** in the U.S.

Nearly **1 million consumers** outside of the U.S were effected **AND….**

EQUIFAX

FEDERAL AGENCIES SUCH AS:

- Internal Revenue Service (IRS)
- Social Security Administration (SSA)
- U.S. Postal Service (USPS)

- The **IRS**, **SSA**, and **USPS** use Equifax's identity verification services, conducted assessments of the company's security controls, which identified a number of lower-level technical concerns that Equifax was directed to address.
- The agencies also made adjustments to their contracts with Equifax, such as **modifying notification requirements** for future data breaches.
- In the case of **IRS**, one of its contracts with Equifax was **terminated**.
- **The Department of Homeland Security** offered assistance in responding to the breach; however, Equifax reportedly **declined** the assistance because it had already retained professional services from an external cybersecurity consultant.
- The Bureau of Consumer Financial Protection and the Federal Trade Commission, which have regulatory and enforcement authority over consumer reporting agencies (CRAs) such as Equifax, initiated an investigation into the breach and Equifax's response in September 2017.

INVESTIGATION

The GAO (United States Government Accountability Office) was asked by the Congressional Requesters to conduct an analysis and report on the Equifax breach. The GAO analyzed documentation generated by Equifax and its cybersecurity consultant in response to the breach, such as the report summarizing the results of the consultant's forensic analysis of the Equifax systems. In addition, they conducted a site visit and interviewed relevant company officials and observed the organization's physical security measures. The GAO also conducted a performance audit from November 2017 to August 2018 in accordance with generally accepted government auditing standards.

RESPONSE

- Equifax stated that they implemented a new endpoint security tool to detect misconfigurations, evaluate potential indications of compromise, and automatically notify system administrators of identified vulnerabilities.
- Equifax officials reported that the company has implemented a new governance structure to regularly communicate risk awareness to Equifax's board of directors and seniors.

BUSINESS IMPACT

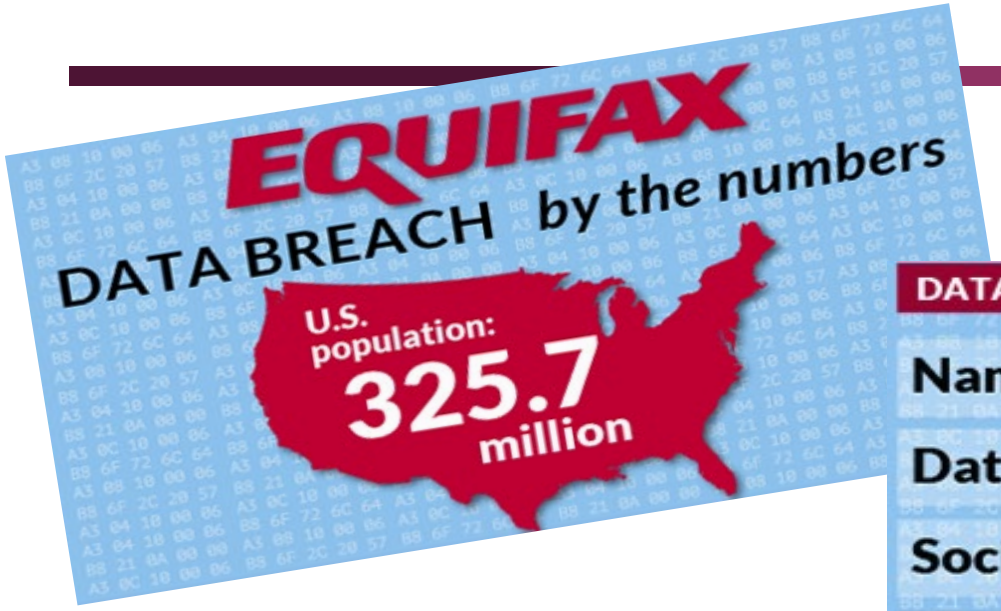
- Equifax took steps to identify what data had been lost and the number of individuals affected so that it could fulfill its responsibility to notify affected individuals.
- Much of the stolen data consisted of **incomplete records**. Some data sets included information that could be matched to more than one known individual. Multiple types of PII had been compromised, including individuals' names, Social Security numbers, birth dates, addresses, and driver's license numbers. Because many of the records were incomplete, not all of the types of PII had been compromised for all affected individuals.
- After Equifax completed its initial analysis of the datasets, it estimated that approximately **145.5 million U.S. consumers had been affected by the breach**.
- Equifax determined that credit card numbers for approximately **209,000 consumers** and certain dispute documents, which had included PII for approximately **182,000 consumers**, had been accessed.
- Equifax recreated the attackers' database queries on a separate system and ran the queries at high speed, allowing Equifax to generate its estimate in a relatively short period of time. Equifax staff then worked to reconstruct queries against the data tables to identify which queries had successfully extracted data and which individuals were associated with that data.

EQUIFAX THEN…..

- provided written notification to all **U.S. state attorneys general** regarding the approximate number of potentially affected residents in each state and its plans for consumer remediation. The notification included steps individuals could take to determine if they were affected by the breach and to help protect against misuse of their personal information.
- issued a press release to the public providing information about the breach and the types of PII that had been compromised.
- set up a dedicated website to help individuals determine if their information might have been stolen in the breach. However, the website experienced several technical issues, including excessive downtime and inaccurate data.

EQUIFAX THEN…..

- expanded its call center operations.
- provides several services to all U.S. consumers, regardless of whether their information had been compromised, free of charge. These services were offered to consumers from September 7, 2017 until January 31, 2018.
- announced a new service called "Lock & Alert." This new service allows consumers to use their smartphone or computer to lock and unlock their Equifax credit report. Equifax announced that it was making this service available to all consumers at no cost.



DATA ELEMENT STOLEN	IMPACTED U.S. CONSUMERS
Name	147 million
Date of birth	147 million
Social Security Number	146 million
Address	99 million
Gender	27 million
Phone number	20 million
Driver's license number	18 million
Email address	2 million
Credit card number	209,000
Tax ID	97,500
Driver's license state	27,000

252,063,800 - Adults in the US
-147,000,000 - Breach Victims

105,063,800 - not effected

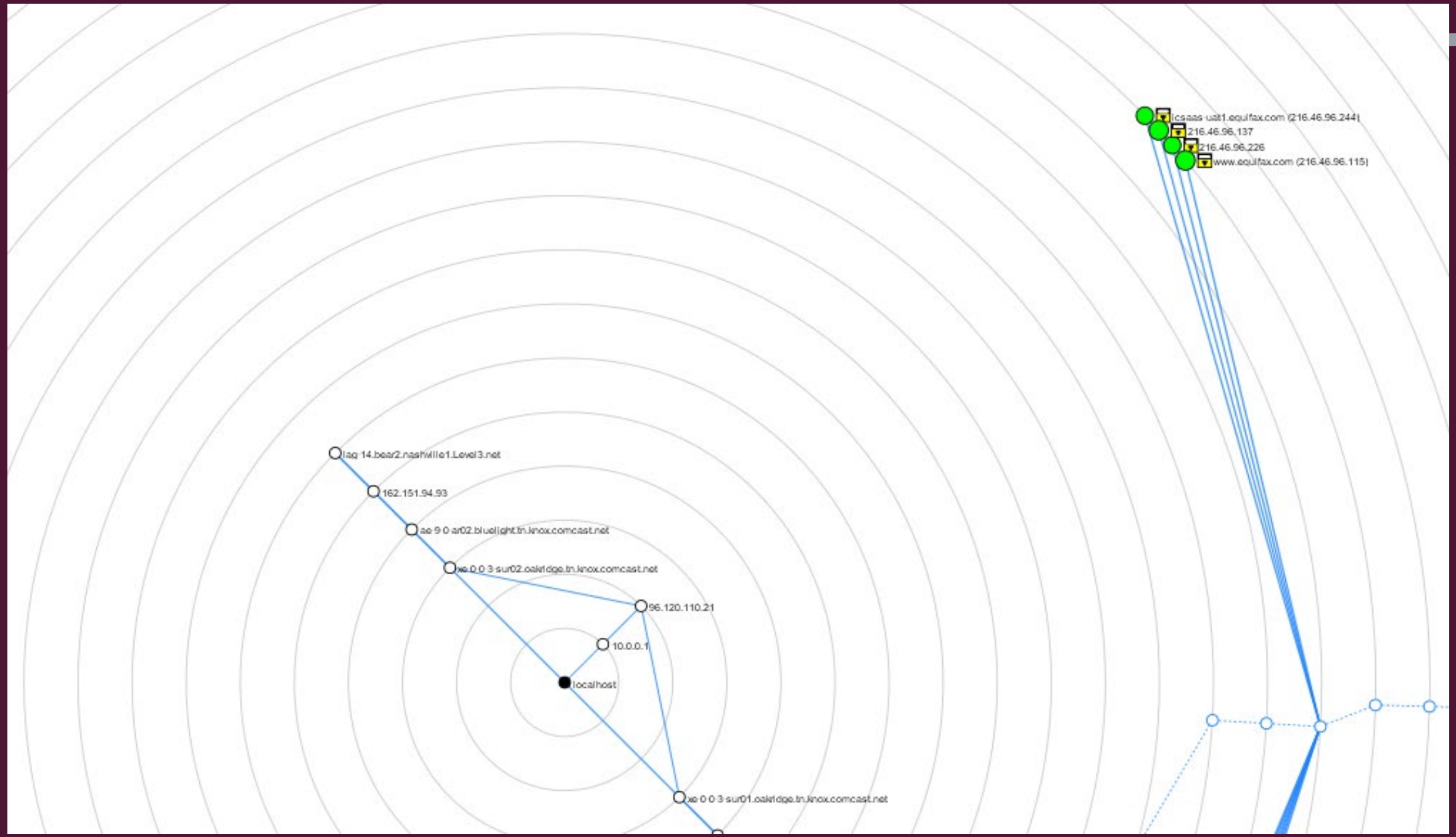
Well over half of the adult US population were violated.

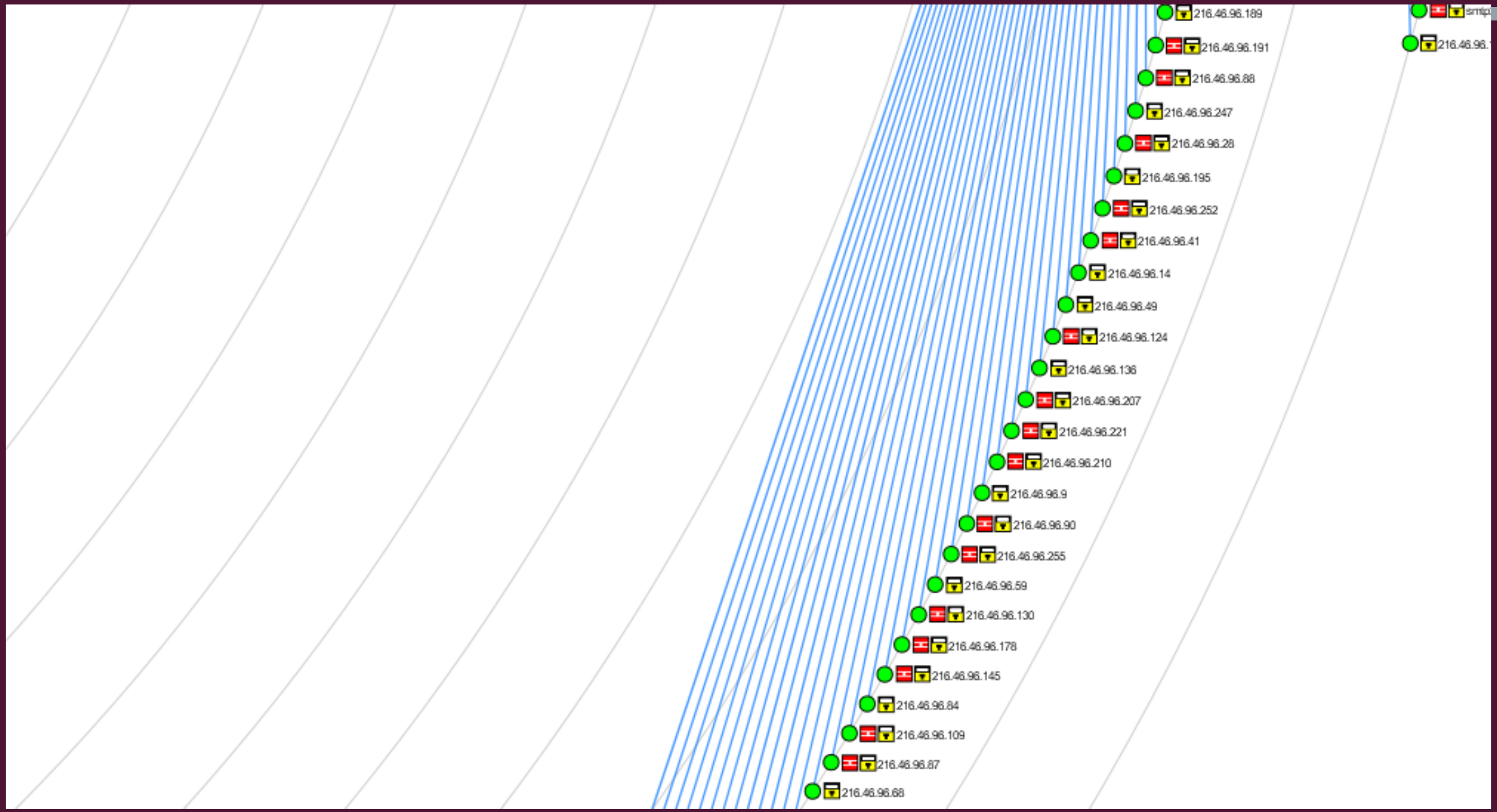
NMAP NEWS.EQUIFAX.COM - 216.46.96.115

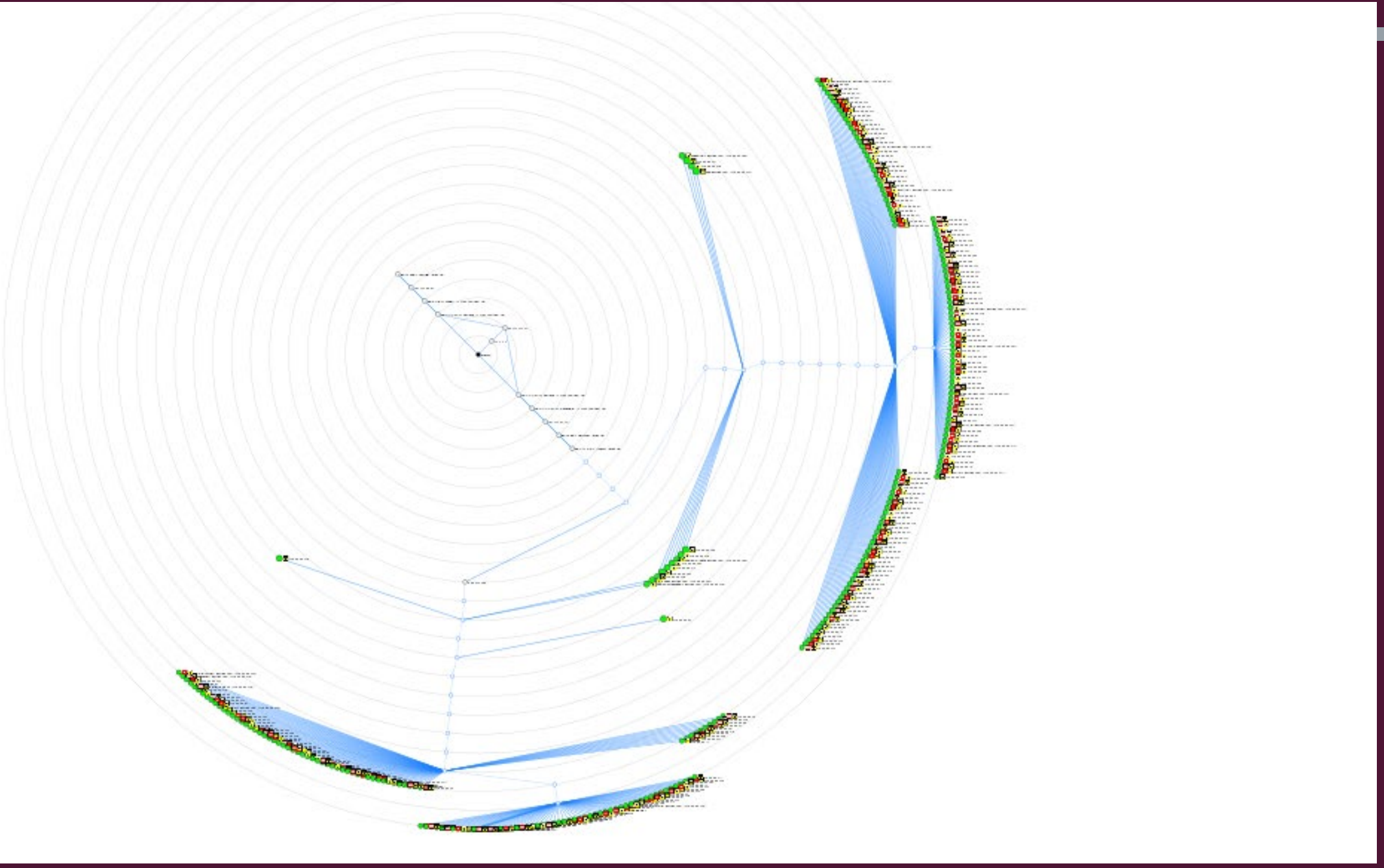
Nmap scan report for

www.equifax.com

PORT	STATE	SERVICE
80/tcp	open	http
113/tcp	closed	ident
443/tcp	open	https
2000/tcp	open	cisco-sccp
5060/tcp	open	sip
8008/tcp	open	http


icsaas uat1.equifax.com (216.46.96.244)
216.46.96.137
216.46.96.226
www.equifax.com (216.46.96.115)
lag-14.bear2.nashville1.Level3.net
162.151.94.93
ae-9-0-ar02.bluelight.tn.knox.comcast.net
xe-0-0-3-sur02.oakridge.tn.knox.comcast.net
96.120.110.21
10.0.0.1
localhost
xe-0-0-3-sur01.oakridge.tn.knox.comcast.net


216.46.96.189
216.46.96.191
216.46.96.88
216.46.96.247
216.46.96.28
216.46.96.195
216.46.96.252
216.46.96.41
216.46.96.14
216.46.96.49
216.46.96.124
216.46.96.136
216.46.96.207
216.46.96.221
216.46.96.210
216.46.96.9
216.46.96.90
216.46.96.255
216.46.96.59
216.46.96.130
216.46.96.178
216.46.96.145
216.46.96.84
216.46.96.109
216.46.96.87
216.46.96.68



RESOURCES

https://keycreditrepair.com/brief-history-equifax/

https://datacenter.kidscount.org/data/tables/99-total-population-by-child-and-adult#detailed/1/any/false/871,870,573,869,36,868,867,133,38,35/39,40,41/416,417

https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07

https://beta.grafiti.io/facts/13189