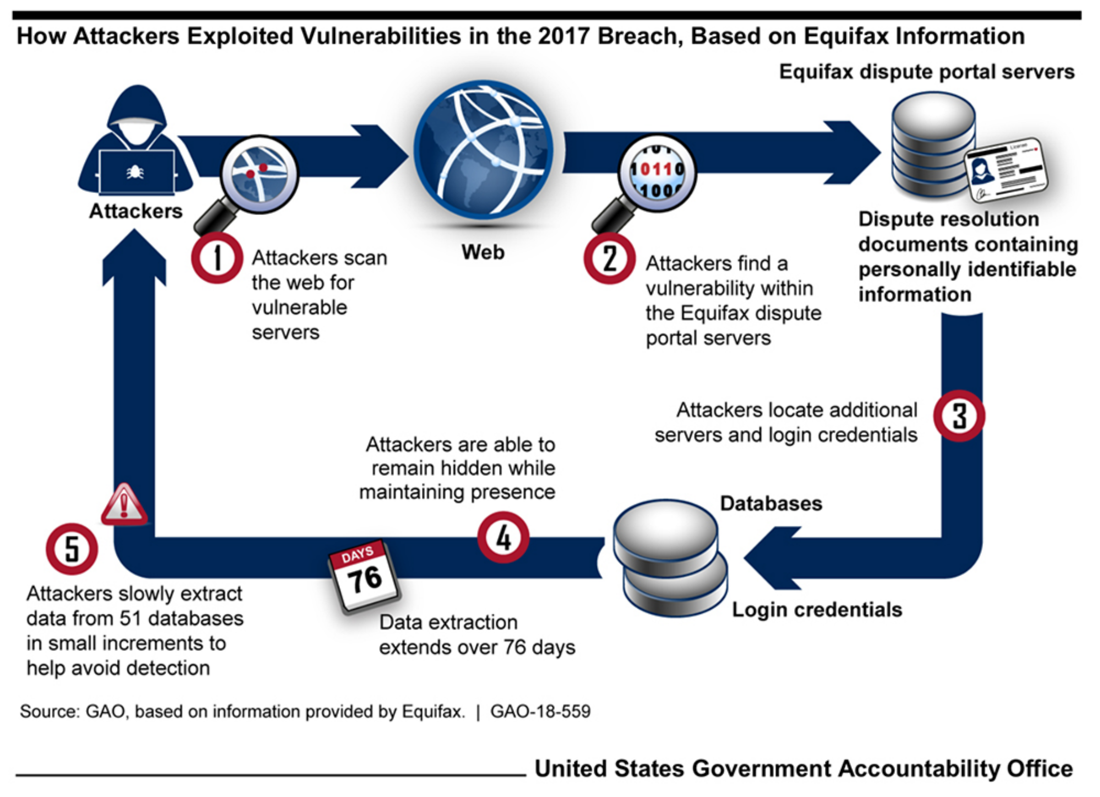
Security Newsletter

17 Februari 2020

Subscribe to this newsletter

Learn From How Others Get Breached: Equifax Edition



How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information

Equifax dispute portal servers
Attackers
Web
1 Attackers scan the web for vulnerable servers
10110 100
2 Attackers find a vulnerability within the Equifax dispute portal servers
Dispute resolution documents containing personally identifiable information
3 Attackers locate additional servers and login credentials
Databases
Login credentials
4 Attackers are able to remain hidden while maintaining presence
DAYS 76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

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

United States Government Accountability Office

The goal here is not blame, but rather to highlight specific missteps by an organization so that others can avoid making the same mistakes, hopefully making them less likely to fall victim to attacks. On to Equifax, which suffered a breach in 2017 that U.S. prosecutors say resulted in the theft of personally identifiable information for 145 million Americans. On Monday, the Justice Department unsealed an indictment charging four officers of the Chinese People's Liberation

The short version of what went wrong is that beginning in March 2017, hackers found and then exploited an unpatched, critical Apache Struts flaw, using it to gain a beachhead inside Equifax's network. Along the way, they found plaintext credentials being stored in text files, giving them administrator-level access to numerous databases. Over the course of 76 days, attackers ran 9,000 queries against 51 databases, using encrypted communications to exfiltrate data, as well as their own remote desktop protocol and web shell software, together with leased Swiss servers as a staging area so that IP addresses didn't trace back to China.

Before the breach began, Equifax had allowed eight SSL certificates to expire, meaning that a tool it had for analyzing encrypted communications was not working. Once the security team renewed the certificates in August 2017, alarms began sounding, highlighting the malicious activity. If there's one thing that every organization should learn from the Equifax breach, it's about patching.

Continuous vulnerability assessment and remediation is one of the cornerstones of the top 20 critical security control areas identified by the SANS Institute. "And for good reason, as unpatched critical flaws often offer a malicious actor a trivial route to gain a foothold," Stubley tells me. "Without assurance activity focused on ensuring that patches have been applied in a timely manner, organizations are leaving themselves open and increasing the likelihood of a successful breach."

Read More on BankInfoSecurity

Apple joins FIDO Alliance, commits to getting rid of passwords

We all use passwords. We also all suck at using them. 81% of all hacking-based security breaches can be traced back to poor passwords. So, it is that the FIDO Alliance has been seeking to replace password-only logins with secure and fast login experiences across websites and apps using the emerging standard WebAuthn Their efforts have been supported by nearly all major technology and e-commerce companies with one major exception: Apple. Now, Apple has joined FIDO.

Currently, there is full FIDO support in three major platforms: Google Android and Chrome, Microsoft Windows and Edge, and Mozilla Firefox." While third-party security and authentication programs, such as the Nok Nok S3 Suite, supported WebAuthn logins on mobile Apps on iOS and Apple Watch Apps, "some organizations have been hesitant to deploy FIDO because there was no [major] public commitment from Apple to FIDO. Now with the addition of Apple, all major platform vendors in the FIDO Alliance prove that the world is finally ready for this technology.

Hopefully, now that Apple, a major player in the mobile space, has committed publicly to supporting FIDO and WebAuthn, we can finally start taking a step forward in putting passwords into the grave. Their day as a serious way of securing your information is long done.

Read More on ZDNet

More #News

- Official: Puerto Rico govt loses $2.6M in phishing scam
- The SSO Wall of Shame
- U.S. Store Chain Rutter's Hit by Credit Card Stealing Malware
- Google to force Nest users to turn on 2FA
- Microsoft Urges Exchange Admins to Disable SMBv1 to Block Malware
- Google removes 500+ malicious Chrome extensions from the Web Store
- FBI: BEC Losses Totaled $1.7 Billion in 2019
- FBI: Cybercrime losses tripled over the last 5 years
- Coding Flaw Exposes Voter Details for 6.5 Million Israelis
- Software error exposes the ID numbers for 1.26 million Danish citizens
- Enterprise companies struggle to control security certificates, cryptographic keys
- Emotet trojan evolves to spread via WiFi connections

#Patch Time!

- Microsoft Patch Tuesday, February 2020 Edition
- Adobe Releases the February 2020 Security Updates
- SweynTooth Bug Collection Affects Hundreds of Bluetooth Products
- Siemens Patches Serious DoS Vulnerabilities in Several Products
- WordPress Cookie Consent Plugin Fixes Critical XSS Flaw for 700K Users
- IE zero day and heap of RDP flaws fixed in February Patch Tuesday
- Firefox 73 Released With Security Fixes, New DoH Provider, Mor

#Tech and #Tools

- Broxy: An HTTP/HTTPS intercept proxy written in Go.
- Introducing BloodHound 3.0
- Deep Dive into Real-World Kubernetes Threats
- FIDO2 deep dive: attestations, trust model and security
- Episode 3-Defeating IDS and Firewalls: An Intro to Shell Strategy
- Forging SWIFT MT Payment Messages for fun and pr... research!
- Down the Rabbit Hole of Harvested Personal Data
- Pytm – A Pythonic Framework For Threat Modeling
- Advanced Binary Deobfuscation course
- How to set up secure ldap for active directory
- Tutorial on privilege escalation and post exploitation tactics in Google Cloud Platform environments
- Jenkins servers can be abused for DDoS attacks
- Kubernetes rollouts: 5 security best practices
- An In-Depth Technical Analysis of CurveBall (CVE-2020-0601)

Kindred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us