App Protect 2020 Update

PRESENTED BY:
Raymond Pompon
Ray Pompon

director, F5 Labs

20+ years in InfoSec—CISSP

President and founder of the Seattle chapter of InfraGard

28 years in IT

Specialist in Compliance/Audit, Web App Security, and Network Security

Author and Speaker
Application Protection Research Series

Using data to unite tactics and strategy in risk-based security
Application Protection Research Series

2019 Conclusions

- PHP, the weak point of the Internet
- Attack methods follow business models
- Injection, rejuvenated
- Access attacks predominant
- APIs changing the landscape
How Are Applications Targeted?

- Sub domains hosting other versions of the main application site
- Dynamic web page generators
- HTTP headers and cookies
- Web service methods
- Data entry forms
- Web pages and directories
- Events of the application—triggered server-side code
- Cookies/state tracking mechanisms
- Server-side features such as search
- Web pages and directories
- Admin interfaces
- Backend connections through the server (injection)
- Helper apps on client (java, flash)
- Data/active content pools—the data that populates and drives pages
- Apps/files linked to the app
- APIs
- Administrative and monitoring stubs and tools
- Shells, Perl/PHP
- Data entry forms
- Dynamic web page generators
- HTTP headers and cookies
How Can We Organize This Better?

- Sub domains hosting other versions of the main application site
- Server-side features such as search
- APIs
- Administrative and monitoring stubs and tools
- Data/active content pools—the data that populates and drives pages
- Apps/files linked to the app
- Helper apps on client (java, flash)
- Backend connections to the server (injection)
- Data entry forms
- Web service methods
- Cookies/state tracking mechanisms
- Shells, Perl/PHP
- Web pages and directories
- Dynamic web page generators
- HTTP headers and cookies
- Admin interfaces
- Events of the application—triggered server-side code
- Helper apps on client (java, flash)
Breaches by Tier (% of all known-cause breaches)

- API attacks
- Injection
- Malware
- DDoS
- Abuse of functionality
- Cross-site scripting
- Cross-site request forgery
- Man-in-the-middle

- Credential theft
- Credential stuffing
- Session hijacking
- Brute force
- Phishing

Legend:
- APP SERVICES
- ACCESS
Web Attacks Observed Per Day

Approx. 3x growth per year
Avg Web Attacks Per Attacker

- 2017: 4.7
- 2018: 22
- 2019: 25
Methodology & Sources

Baffin Bay Data
2018 Breach Data
2019 Breach Data
F5 SIRT data
Breach Analysis
State Attorney General

761 Cases 2018
87% Had explanations

Submitted Breach Notification Sample

Sample of Notice: Farmgirl Breach Notice Sample.pdf
Organization Name: Farmgirl Flowers, Inc.
Date(s) of Breach (if known): Thursday, April 26, 2018
Sunday, April 29, 2018

Farmgirl FLOWERS
Promoting Center • 1234 MAIN STREET • Austin, TX 78714

May 11, 2018

Re: NOTICE OF DATA BREACH

We are so sorry to inform you that we recently became aware of a data breach that may have compromised your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honesty, trust, and transparency, which is why I'm reaching out personally to let you know about what happened and what we're doing to address it.

What Happened?

On April 29, 2018, at approximately 4:00 p.m. (all times PST), we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between 1:00 p.m. and April 26, 2018, and by April 29, 2018, on that same date. The unauthorized access involved the insertion of rogue code into our checkout page.

What Information Was Involved?

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address, and credit card information including card

XAVIER BECERRA
Attorney General
Breach Analysis
State Attorney General

1025
Cases 2019
85%
Had explanations

State of California Department of Justice
XAVIER BECERRA
Attorney General

Submitted Breach Notification Sample
Sample of Notice: Farmgirl Breach Notice Sample.pdf
Organization Name: Farmgirl Flowers, Inc.
Date(s) of Breach (if known): Thursday, April 26, 2018
Sunday, April 29, 2018

May 11, 2018

Farmgirl FLOWERS

Re: NOTICE OF DATA BREACH

We are so sorry to inform you that we recently became aware of a data breach that may have compromised your personal information. We understand how important your privacy is, and we take the protection of your information very seriously. Our company is built on honesty, trust, and transparency, which is why I’m reaching out personally to let you know about what happened and what we’re doing to address it.

What Happened?

On April 29, 2018, at approximately 4:00 p.m. (all times PST), we learned that there was unauthorized access by electronic means to our data by a person or persons whose identities remain unknown. The unauthorized access occurred sometime between 1:00 p.m. on April 26, 2018, and 3:08 p.m. on that same date. The unauthorized access involved the insertion of rogue code into our checkout page.

The unauthorized access involved the insertion of rogue code into our checkout page.

The unauthorized access involved the insertion of rogue code into our checkout page.

The unauthorized access involved the insertion of rogue code into our checkout page.

The unauthorized access involved the insertion of rogue code into our checkout page.

The unauthorized access involved the insertion of rogue code into our checkout page.

What Information Was Involved?

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address and credit card information including card

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address and credit card information including card

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address and credit card information including card

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address and credit card information including card

The information that was accessed without authorization could have included your name, billing address for a credit card, telephone number, email address and credit card information including card
Caveats for Public Breach Notifications

• Small $n$
• Limited detail
• Reductive categories
• Reductive causes
• US Only
2018 US Breaches by Cause (%)

- Access-related: 47.0%
- Web: 17.3%
- Accidental: 14.0%
- Physical security: 9.0%
- Malware: 5.0%
- Insider: 4.0%
- Phishing (no details): 2.1%
- Third-party compromised: 1.6%
2019 US Breaches by Cause (%)

- Access related: 51.8%
- Web: 18.9%
- Accidental: 13.0%
- Physical: 6.1%
- Malware: 6.6%
- Insider: 3.1%
- Third-party compromised: 0.5%
2019 Breach Root Causes

<table>
<thead>
<tr>
<th>Industry</th>
<th>Government</th>
<th>Manufacturing</th>
<th>Tech</th>
<th>Non-profit</th>
<th>Health</th>
<th>Education</th>
<th>Services</th>
<th>CPA*</th>
<th>Finance</th>
<th>Retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web (mostly injection)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>26.7%</td>
<td>36.5%</td>
<td>18.8%</td>
<td>10.8%</td>
<td>2.4%</td>
<td>3.8%</td>
<td>11.8%</td>
<td></td>
<td>2.7%</td>
<td>82.4%</td>
</tr>
<tr>
<td>Access (mostly phishing and email)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>46.7%</td>
<td>32.7%</td>
<td>59.4%</td>
<td>56.8%</td>
<td>57.6%</td>
<td>67.3%</td>
<td>62.5%</td>
<td>84.0%</td>
<td>62.3%</td>
<td>9.3%</td>
</tr>
</tbody>
</table>
Web Attacks:

Don’t fix it if it ain’t broke
2017 Application Attacks
Injection → PHP & SQL

- Login: 1%
- Affiliates: 1%
- Admin: 2%
- Betablock: 2%
- Cart: 3%
- Comments: 4%
- Exchweb: 6%
- SQL: 56%
- PHP: 58%
2018 Application Attacks
Injection → PHP

- Affiliates: 0%
- Betablock: 0%
- Cart: 0%
- Exchweb: 0%
- ASP: 1%
- Comments: 2%
- Admin: 3%
- SQL: 8%
- PHP: 81%
Card Stealing Web Injects

Stolen data exfiltrated via HTTPS to a drop server

Targeted Site

Malicious PHP Code

Payment Card Info Breached

Injects usually due to weak input filters common in PHP, JS, CMS sys

Can add fake fields to page

Targeted Site

Fake fields to page
A typical shopping site

Third party widgets/content

All linked off main app site but hosted elsewhere...
Access Attacks:
Primary cause of breach

- Brute force
- Credential Stuffing
- Phishing
2018 Access Attacks Broken Down

- 20.0% Email cited as cause
- 19.6% Phishing gain access to email
- 4.0% Access creds stolen
- 2.2% Access cred stuffing and brute
2019 Access Attacks Broken Down

- 32.8% Email cited as cause
- 14.2% Phishing gain access to email
- 1.9% Access creds stolen
- 2.2% Access cred stuffing and brute
Brute Force attacks by industry from reported 2018 F5 SIRT incidents

- Telecom: 22.2%
- Retail: 23.1%
- Tech: 23.5%
- Service: 25.0%
- Education: 27.3%
- Health: 41.7%
- Finance: 47.8%
- Public: 50.0%
Brute Force attacks by industry from reported 2019 F5 SIRT incidents

- Telecom: 6.5%
- Retail: 6.5%
- Tech: 9.7%
- Manufact: 9.7%
- NonProfit: 3.2%
- Health: 6.5%
- Finance: 32.3%
- Public: 6.5%
2018 Brute Force incidents reported to F5 SIRT

41.7% Canada
33.3% USA
0.0% LATAM
43.5% EMEA
9.5% APAC
2019 Brute Force incidents reported to F5 SIRT

- **72.7%** N. Amer
- **18.2%** EMEA
- **4.5%** APAC
- **4.5%** LATAM
Breach Data Conclusions

- Access attacks predominant
- Retail breaches increasingly dominated by formjacking
- Breach modes driven more by business model and application architecture than by traditional sector
- Third-party enfilade attacks make niche providers risky (more on this in 2020)
Mitigation Recommendations

- **Program maturity**
  - Inventory
  - Vulnerability management
  - Change control
  - Access control
  - Training
  - Monitoring and Logging

- **Multifactor Authentication**
- **WAF / WAAP**
Primary External Partners for This Briefing

36 months of global attack web app data

Data Analysis & Statistical Analysis
F5Labs.com

Tell us what you want to read about
@F5Labs

Twitter  LinkedIn  Email Updates  RSS