



1. WHOIS query Screenshot
 - a. Domain owner and contact info

 Registrant Contact	
Name:	Domain Administrator
Organization:	State Farm Mutual Automobile Insurance Company
Street:	Three State Farm Plaza R3,
City:	Bloomington
State:	IL
Postal Code:	61710-0001
Country:	US
Phone:	+1.3097357185
Fax:	+1.3097667787
Email:	hone.auto-eisadmin.399n88@statefarm.com

- b. Domain administrator and contact info

 Administrative Contact	
Name:	Domain Administrator
Organization:	State Farm Mutual Automobile Insurance Company
Street:	Three State Farm Plaza R3,
City:	Bloomington
State:	IL
Postal Code:	61710-0001
Country:	US
Phone:	+1.3097357185
Fax:	+1.3097667787
Email:	hone.auto-eisadmin.399n88@statefarm.com

c. The IP ranges that the domain has registered to it (include the CIDR)

Network Resources	
SPRINTLINK (NET-204-94-39-0-1)	204.94.39.0 - 204.94.39.255
SPRINTLINK (NET-205-242-228-0-1)	205.242.228.0 - 205.242.229.255
SPRINTLINK (NET-204-214-51-128-1)	204.214.51.128 - 204.214.51.159
ATT-NET-12-229-168-160 (NET-12-229-168-160-1)	12.229.168.160 - 12.229.168.191
ATT-SFI-NET-2001-1890-12BB-200 (NET6-2001-1890-12BB-200-1)	2001:1890:12BB:200:: - 2001:1890:12BB:2FF:FFFF:FFFF:FFFF:FFFF
STATEFARM (NET-205-166-218-0-1)	205.166.218.0 - 205.166.218.255
STATE-FARM-IPV6-NETWORK-2 (NET6-2620-168-1)	2620:168:: - 2620:168:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SPRINTLINK (NET-199-2-205-128-1)	199.2.205.128 - 199.2.205.255
SPRINTLINK (NET-208-31-160-0-1)	208.31.160.0 - 208.31.160.255
SPRINTLINK (NET-208-31-161-0-1)	208.31.161.0 - 208.31.161.255
SPRINTLINK (NET-208-31-52-0-1)	208.31.52.0 - 208.31.52.255
SPRINTLINK (NET-204-118-102-0-1)	204.118.102.0 - 204.118.102.255
SFI-NET-12-39-28-0 (NET-12-39-28-0-1)	12.39.28.0 - 12.39.29.255
SFI-3 (NET-206-80-128-0-1)	206.80.128.0 - 206.80.143.255

2. DNS Interrogation screenshot

a. Mail server

```
> drill MX statefarm.com
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 62891
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; statefarm.com.      IN      MX

;; ANSWER SECTION:
statefarm.com.  3599    IN      MX      5 mail7.statefarm.com.
statefarm.com.  3599    IN      MX      5 mail6.statefarm.com.
```

```
> drill mail7.statefarm.com
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 32720
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; mail7.statefarm.com. IN      A

;; ANSWER SECTION:
mail7.statefarm.com.  3599    IN      A      206.80.132.156
```

```
> drill mail6.statefarm.com
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 25085
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; mail6.statefarm.com. IN      A

;; ANSWER SECTION:
mail6.statefarm.com.  3599    IN      A      206.80.128.156
```

b. DNS server

```
> drill NS statefarm.com
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 23280
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; statefarm.com.      IN      NS

;; ANSWER SECTION:
statefarm.com.  77034  IN      NS      ns29.statefarm.com.
statefarm.com.  77034  IN      NS      ns31.statefarm.com.
```

```
> drill ns29.statefarm.com
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 54427
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns29.statefarm.com. IN      A

;; ANSWER SECTION:
ns29.statefarm.com.  77230  IN      A      206.80.128.53
```

```
> drill ns31.statefarm.com
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 61068
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns31.statefarm.com. IN      A

;; ANSWER SECTION:
ns31.statefarm.com.  77226  IN      A      206.80.132.53
```

c. Find one other server

```
> drill mail.statefarm.com
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57954
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; mail.statefarm.com. IN      A

;; ANSWER SECTION:
mail.statefarm.com.  3458   IN      A      198.245.82.46
```

```
> drill -x 198.245.82.46
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 44943
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 46.82.245.198.in-addr.arpa. IN     PTR

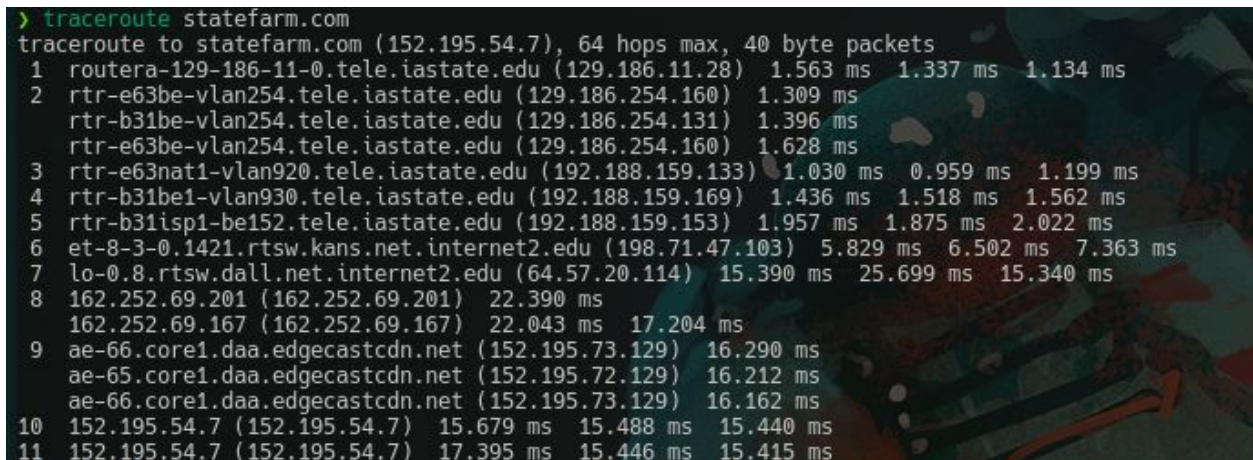
;; ANSWER SECTION:
46.82.245.198.in-addr.arpa.  86399  IN      PTR     reply-mx.s6.exacttarget.com.
```

(Later I also found b2b.statefarm.com)

```
> drill b2b.statefarm.com
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 21839
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; b2b.statefarm.com.  IN      A

;; ANSWER SECTION:
b2b.statefarm.com.  2399   IN      A      206.80.128.141
```

3. Screenshot of traceroutes - include both a visual and textual



```

> traceroute statefarm.com
traceroute to statefarm.com (152.195.54.7), 64 hops max, 40 byte packets
 1  routera-129-186-11-0.tele.iastate.edu (129.186.11.28)  1.563 ms  1.337 ms  1.134 ms
 2  rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  1.309 ms
    rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131)  1.396 ms
    rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160)  1.628 ms
 3  rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133)  1.030 ms  0.959 ms  1.199 ms
 4  rtr-b31be1-vlan930.tele.iastate.edu (192.188.159.169)  1.436 ms  1.518 ms  1.562 ms
 5  rtr-b31isp1-be152.tele.iastate.edu (192.188.159.153)  1.957 ms  1.875 ms  2.022 ms
 6  et-8-3-0.1421.rtsw.kans.net.internet2.edu (198.71.47.103)  5.829 ms  6.502 ms  7.363 ms
 7  lo-0.8.rtsw.dall.net.internet2.edu (64.57.20.114)  15.390 ms  25.699 ms  15.340 ms
 8  162.252.69.201 (162.252.69.201)  22.390 ms
    162.252.69.167 (162.252.69.167)  22.043 ms  17.204 ms
 9  ae-66.core1.daa.edgecastcdn.net (152.195.73.129)  16.290 ms
    ae-65.core1.daa.edgecastcdn.net (152.195.72.129)  16.212 ms
    ae-66.core1.daa.edgecastcdn.net (152.195.73.129)  16.162 ms
10  152.195.54.7 (152.195.54.7)  15.679 ms  15.488 ms  15.440 ms
11  152.195.54.7 (152.195.54.7)  17.395 ms  15.446 ms  15.415 ms

```

```


traceroute to statefarm.com (152.195.54.7), 64 hops max, 40 byte packets 1
routera-129-186-11-0.tele.iastate.edu (129.186.11.28) 1.402 ms 1.183 ms 1.272 ms 2
rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160) 1.268 ms
rtr-b31be-vlan254.tele.iastate.edu (129.186.254.131) 1.293 ms
rtr-e63be-vlan254.tele.iastate.edu (129.186.254.160) 1.268 ms 3
rtr-e63nat1-vlan920.tele.iastate.edu (192.188.159.133) 1.013 ms 1.511 ms 1.179 ms 4
rtr-b31be1-vlan930.tele.iastate.edu (192.188.159.169) 1.667 ms 1.531 ms 1.501 ms 5
rtr-b31isp1-be152.tele.iastate.edu (192.188.159.153) 1.706 ms 2.106 ms 2.150 ms 6
et-8-3-0.1421.rtsw.kans.net.internet2.edu (198.71.47.103) 5.640 ms 5.934 ms 5.801 ms 7
lo-0.8.rtsw.dall.net.internet2.edu (64.57.20.114) 15.458 ms 15.209 ms 18.995 ms 8
162.252.69.201 (162.252.69.201) 16.663 ms 15.941 ms 162.252.69.167 (162.252.69.167)
22.831 ms 9 ae-65.core1.daa.edgecastcdn.net (152.195.72.129) 55.015 ms 16.199 ms
ae-66.core1.daa.edgecastcdn.net (152.195.73.129) 22.130 ms 10 152.195.54.7 (152.195.54.7)
15.187 ms 15.405 ms 15.335 ms 11 152.195.54.7 (152.195.54.7) 37.690 ms 52.176 ms 15.334
ms

```


4. Geolocation of host(s) screenshot

a. What country

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2021-2-1)

Domain Name	Country	Region	City
statefarm.com	United States of America 	Virginia	Ashburn
ISP	Organization	Latitude	Longitude
ANS Communications Inc	Not Available	39.0341	-77.4885

Geolocation data from [DB-IP](#) (Product: Full, 2021-2-1)

Domain Name	Country	Region	City
statefarm.com	United States 	New York	New York
ISP	Organization	Latitude	Longitude
Verizon Communications	ANS Communications, Inc	40.7128	-74.006

b. Which ISP

There are a few other entries than the ones above, and they give a mix of ANS and Verizon as both the organization and ISP.

c. Who is providing the hosting of the website?

d. Who is providing the target's DNS?

MarkMonitor for both

Where is this site hosted	Who is hosting this website
Domain Name	statefarm.com
Registry Domain ID	1207177_DOMAIN_COM-VRSN
Registrar WHOIS Server	whois.markmonitor.com
Registrar URL	http
Updated Date	2020-04-21T02
Creation Date	1995-05-24T00
Registrar Registration Expiration Date	2022-05-22T00
Registrar	MarkMonitor, Inc.

5. Sensitive information on public website - screenshots and description of why useful
- a. Employee rosters and email addresses

<https://www.statefarm.com/agent/us>

Browse Nearby Insurance Agents in Your State

United States		
Alabama	Kentucky	North Dakota
Alaska	Louisiana	Ohio
Arizona	Maine	Oklahoma
Arkansas	Maryland	Oregon
California	Massachusetts	Pennsylvania
Colorado	Michigan	Rhode Island
Connecticut	Minnesota	South Carolina
Delaware	Mississippi	South Dakota
District of Columbia	Missouri	Tennessee
Florida	Montana	Texas
Georgia	Nebraska	Utah
Hawaii	Nevada	Vermont
Idaho	New Hampshire	Virginia
Illinois	New Jersey	Washington
Indiana	New Mexico	West Virginia
Iowa	New York	Wisconsin
Kansas	North Carolina	Wyoming

Insurance Agents in Ames, Iowa

 <p>Pat Brown RICP®, CLU® Lic: IA-684000 1112 Buckeye Ave PO Box 2204 Ames, IA 50010-8063 515-233-1295 Agent Website Email agent</p>	 <p>Mark Doyle CPCU® Lic: IA-6857955 2701 Stange Rd. Suite 110 Ames, IA 50010-3959 515-232-8090 Agent Website Email agent</p>	 <p>Scott Richardson RICP® Scott Richardson Ins Agcy Inc Lic: IA-1002221834 101 Main Street Ames, IA 50010-6359 515-232-0030 Agent Website Email agent</p>
--	---	--

<https://github.com/{insert username}>

Rex Bennett
rexb1971

Follow

...

1 follower · 0 following · 0

@StateFarmlns

Champaign, Illinois

rex.bennett.jefz@statefarm.com

Ryan Regal
rreegz

Follow

...

1 follower · 2 following · 2

ryan.regal.qjzc@statefarm.com

Highlights

* Arctic Code Vault Contributor

The first site contains an entire set of all State Farm agents and takes us to their own webpages. They don't give direct email information but rather allow you to email from a textbox on the page. The other two users are State Farm developers pages on github. This shows off how they format the email address as first.last.4_random_chars@statefarm.com. As well, we now have some potential targets to phish who work in IT, and all the agents if we figure out their emails.

- b. Technical documents (how to use services/login/etc)
- <https://jobs.statefarm.com/main/jobs/12821?lang=en-us>
- <https://jobs.statefarm.com/main/jobs/12551?lang=en-us>

The pictures below are some jobs postings I found that are currently open. On these it shows all sorts of information based on what qualifications they are looking for. It shows that they have Cisco router and use splunk, Apache/Tomcat servers, and RHEL7. These help us get a feel for what they are using on their network for web hosting as well as intrusion detection.

Business Skills:

- Communicates well by phone and in writing
- Understanding of ITIL and EOM Principles
- Self-directed, team player
- High technical aptitude
- Customer service mindset

Technical Skills:

- Practical work experience desired Cisco certification desired, but not required
- IT Networking degree desired, but not required
- Experience with Telecommunications cable/hardware installation, termination and testing
- Understanding of Cisco Unified Communications
- Understanding of Cisco routers and switches
- Softphone technology including Cisco Jabber
- Experience with Network Automation is desired but not required

Qualifications

- 5 years professional software development experience
- Hands on experience in DevOps including CI/CD pipelines using GIT/Jenkins.
- Hands on development experience in one or more of the following languages:
 - Java
 - Python
 - or similar with willingness to learn
- API development
- Salesforce platform experience and cloud native tools
- Familiarity with SRE principles.
- Proven track record of deploying reliable solutions
- Experienced Developer (Java, Groovy) Scripting languages (Python/ Perl /Shell) Lightweight web development (HTML/CSS/JavaScript/jQuery/PERL CGI).
- Web frameworks (Node.js/Ember/Angular/Knockout.js/Bootstrap).
- Web services (SOAP/REST) & data formats (XML/JSON).
- Source Code Repository & Integration Solutions (Git/Puppet/Jenkins).
- Linux (RHEL7)/Apache/Tomcat & other open source technologies. Knowledge of SQL/database query languages.
- Experience integrating 3rd party software & enterprise automation solutions.
- Splunk Power User - Splunk dashboards, reports, and development.
- Software Architecture experience or knowledge.
- Willingness & ability to learn new technologies Strong technical problem solving skills & ability to apply critical thinking when making decisions
- Understanding of agile & willingness to adhere to best practices Understanding of coding standards & best practices Understanding of DevOps, Continuous Integration/Continuous Delivery and importance of automation
- Well versed in ITIL concepts and tooling

6. Recent happenings in the news - screenshots and description of why useful

a. Business Partner: (originally mergers)

<https://newsroom.statefarm.com/pet-medical-insurance-trupanion/>

The screenshot shows the State Farm newsroom page for the article "State Farm® Unleashes Medical Insurance for Pets through Trupanion®". The page features a large image of a dog and the Trupanion logo. The article is dated BLOOMINGTON, Ill., August 07, 2020. The headline reads: "State Farm® Unleashes Medical Insurance for Pets through Trupanion® Helping the pets we love get the best veterinary care". The article text discusses how State Farm has partnered with Trupanion to provide medical coverage for pets, highlighting the benefits for pet owners and the quality of care provided by Trupanion. It also mentions that the insurance is available in 50 states and the District of Columbia.

b. Acquisitions: <https://newsroom.statefarm.com/state-farm-to-acquire-gainsco/>

The screenshot shows the State Farm newsroom page for the article "State Farm® to Acquire GAINSCO". The page features a large image of the State Farm logo and the GAINSCO logo. The article is dated BLOOMINGTON, Ill., January 04, 2021. The headline reads: "State Farm® to Acquire GAINSCO". The article text discusses the acquisition of GAINSCO by State Farm, highlighting the benefits for both companies and the customers. It also mentions that the transaction is expected to close in early 2021, subject to regulatory approvals and shareholder approval.

Both Trupanion and Gainsco are “working” with State Farm. Gainsco is becoming a subsidiary of them and thus being integrated into State Farm. This could mean a whole lot of a tech side. Like “combining” networks and setting up accounts for Gainsco. Trupanion, on the other side, is simply handling veterinary insurance for State Farm customers. This would mean that the two need to handle claims from one another and need to set up ways to communicate seamlessly.

- c. Where do you believe vulnerabilities may lie?

Interbusiness communications.

Are there login portals for other businesses to make claims / go through StateFarm for insurance? Trupanion and Statefarm will have claims together dealing with insurance, and Gainsco is now a subsidiary of State Farm.

7. Vulnerable web apps

- a. Can you find any vulnerable web apps using Google Dorks against your target?

<https://b2b.statefarm.com>

https://b2b.statefarm.com/b2b/CS23186/forms/System_Access_Agreement.pdf

Business to business web page and the agreement with using it, which tells us it connects to their network. As well, there are many logins using claim numbers.

<https://proofing.statefarm.com/login-interceptor/login?agentAssociateId=VXFGJ8PP6GE>

proofing.statefarm.com comes back with a 404 page not found error.

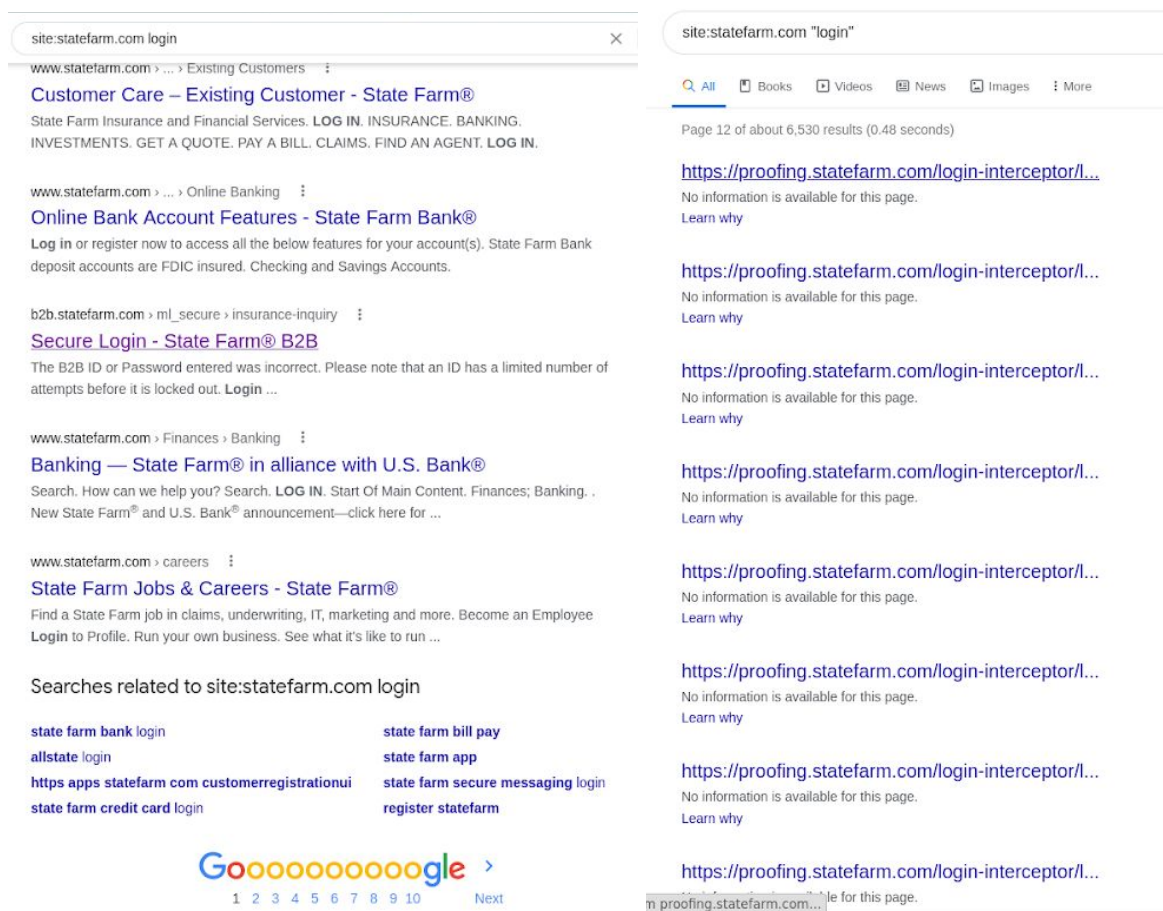
However, this login seems to exist even though proofing doesn't?

b. Provide list of google queries you tried

I tried:

- site:statefarm.com filetype:htm
 - This showed some of the proofing login pages
 - And some unused sites that probably shouldn't be up (old info)
- site:statefarm.com filetype:php
 - Nothing
- site:statefarm.com login
 - This gave a link with secure login for the b2b login page
 - This also has more interceptor pages
- site:statefarm.com login -agent -proofing
 - I was getting the agent's and proofing pages but just got more b2b

Also the b2b page seems to say I entered a user/password incorrectly despite never trying to log in. As well, the login interceptor's URL says an "agents associate id". (I saw another ID like this inspecting the html of agents webpages, and I think it was within the send email button.)



8. Similar Domains

a. Can you find any domains similar to the target for sale?

Yes there are many.

b. Are there domains that might benefit an attacker, should they be purchased?

I think .agency, .expert, and .com.co are better ones if you want to try social engineering a people and trick them onto a fake webpage.

thestatefarm.net	\$19.99 \$14.99^⑦ for the first year	Add to Cart
statefarm.world	\$41.99 \$1.99^⑦ for the first year	Add to Cart
statefarm.one	\$12.99^⑦ Same price next year	Add to Cart
statefarm.digital	\$42.99 \$3.99^⑦ for the first year	Add to Cart
statefarmus.net	\$19.99 \$14.99^⑦ for the first year	Add to Cart
statefarm.zone	\$42.99 \$9.99^⑦ for the first year	Add to Cart
statefarm.expert	\$69.99 \$9.99^⑦ for the first year	Add to Cart
statefarmusa.net	\$19.99 \$14.99^⑦ for the first year	Add to Cart
statefarm.agency	\$27.99 \$4.99^⑦ for the first year	Add to Cart
statefarm.com.co	\$19.99^⑦ Same price next year	Add to Cart

Fun fact: State Farm also has st8fm.com as a domain, and it contains transcripts to commercials, JS code used on many of their web pages, and a bunch of random files for filing claims. Plus there is stuff like this out on the internet: <https://www.statefarm.com/robots.txt>