Relatório de Análise de Vulnerabilidades

Professor: Jean do Ouro

STATE FARM é um grupo de companhias de seguro e serviços financeiros, localizado nos Estados Unidos, com sede em Bloomington, Illinois. O principal negócio do grupo é o State Farm Mutual Automobile Insurance Company, uma firma seguradora que também comanda as outras empresas da companhia.

Daniel Kevin & Hyan Silva

01/12/2022

ÍNDICE

1. ESCOPO E DEFINIÇÃO DO OBJETIVO DA PESQUISA

SAFE HABOR

Porto Seguro:

Ao conduzir pesquisas de vulnerabilidade de acordo com esta política, consideramos que esta pesquisa é:

Autorizado de acordo com a Lei de Abuso e Fraude de Computador (CFAA) (e/ou leis estaduais semelhantes), e não iniciaremos ou apoiaremos ações legais contra você por violações acidentais e de boa fé desta política;

Isento da Lei de Direitos Autorais do Milênio Digital (DMCA), e não faremos uma reclamação contra você por contornar os controles de tecnologia;

Isento de restrições em nossos Termos e Condições que possam interferir na realização de pesquisas de segurança e renunciamos a essas restrições de forma limitada para o trabalho realizado sob esta política; e

Legal, útil para a segurança geral da Internet e conduzido de boa fé.

Espera-se que você, como sempre, cumpra todas as leis aplicáveis.

Se a qualquer momento você tiver dúvidas ou não tiver certeza se sua pesquisa de segurança é consistente com esta política, pergunte via support@bugcrowd.com antes de prosseguir.

-STATEFARM

NÃO CONFORMIDADE

Se você causou (ou poderia ter causado) danos aos clientes da State Farm, aos negócios da State Farm, aos associados da State Farm ou aos fornecedores da State Farm, você não está em conformidade com esta política.

Exemplos de não conformidade incluem, mas não estão limitados a:

- Divulgação de um problema de Segurança da Informação publicamente (por exemplo, nas mídias sociais) sem o consentimento por escrito da State Farm. Isso inclui metodologia ou código de exploração.
- Divulgação de quaisquer dados (por exemplo, registros de clientes, senhas) publicamente (por exemplo, em uma sala de bate-papo, nas mídias sociais, para seus amigos).
- Criação de registros que são fraudulentos.
- Acessar ou modificar dados em uma conta que não pertence a você.
- Executar ou tentar executar um ataque de “negação de serviço” (DOS / DDOS) de qualquer tipo.
- Engenharia social (por exemplo, phishing, chamada pretexto).
- Usando (por exemplo, upload, e-mail) software malicioso ou ferramentas de segurança.
- Qualquer interação com clientes da State Farm (por exemplo, e-mail não solicitado).
- Qualquer interação (ou seja, comunicações, testes) com fornecedores da State Farm.
- Realização de testes contínuos após a divulgação.

2. OBJETIVO DA PESQUISA

Tratando-se de um exercício universitário, tendo em vista experiências pedagógicas, este documento busca relatar possíveis vulnerabilidades físicas e tecnológicas em uma empresa. Realizando testes de sistema em domínios e subdomínios disponibilizados pela mesma, relatando buscas sobre informações públicas e as reunindo com o intuito de alertar possíveis fraquezas na sua infraestrutura e segurança.

3. TERMO DE RESPONSABILIDADE DOS PENTESTERS

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente, quanto pelo que foi estabelecido pelo orientador Jean Ouro.

As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de “Escopo” e “Objetivos” e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades.

Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.

Neste contexto, embora tenham sido feitos todos os esforços para auditar e avaliar a segurança do ambiente computacional da Unity, este relatório não garante de forma alguma o estabelecimento de um sistema impenetrável. Sendo assim, a FADBA e os pentesters não se responsabilizam por qualquer perda ou dano direto ou indireto causado por qualquer falha ou violação dos sistemas desta da plataforma de viagem.

Por fim, as informações deste relatório têm classificação PÚBLICA e devem ser usadas apenas pela STATEFARM e pela FADBA, sendo de inteira e única responsabilidade de ambas

4. DECLARAÇÃO DE AUTORIZAÇÃO DO CONTRATANTE (MODELO DE CONTRATO COM VALOR) COM TERMO DE PAGAMENTO

A State Farm se dedica a manter a confidencialidade, integridade e disponibilidade dos sistemas e informações da State Farm. Nos preocupamos em proteger nossos clientes e associados dos riscos de segurança da vida cotidiana. Se você notar um problema de segurança da informação em um sistema State Farm ao usar www.statefarm.com ou um aplicativo móvel State Farm, queremos saber sobre isso.

Pedimos que você divulgue problemas de segurança da informação de forma responsável e de acordo com esta Política de Divulgação de Vulnerabilidades. A State Farm trabalhará para resolver o problema em tempo hábil. Contanto que você cumpra esta política ao divulgar questões de segurança da informação para a State Farm, a State Farm não tomará medidas legais contra você ou revogará o acesso aos aplicativos da State Farm.

A State Farm leva a sério a segurança da informação. Reservamo-nos todos os direitos legais em caso de incumprimento.

NOSSO COMPROMISSO (STATEFARM)

Seremos o mais transparentes possível com você. Trabalharemos com você conforme necessário para entender o problema. Se virmos o problema como um falso positivo ou se já soubermos sobre o problema, iremos informá-lo.

Se o problema puder ser validado:

- Descreveremos a prioridade do problema conforme o vemos.
- Sempre que possível, enviaremos atualizações periódicas sobre o status.

5. TERMO DE PAGAMENTO

No que se refere ao pagamento, o programa disponível na bugcrowd não informa os valores de pagamento para o encontro de vulnerabilidades, a empresa escolheu manter de forma privada os valores e não revelou publicamente os valores. A pontuação da bugcrowd também já foi finalizada para este programa.

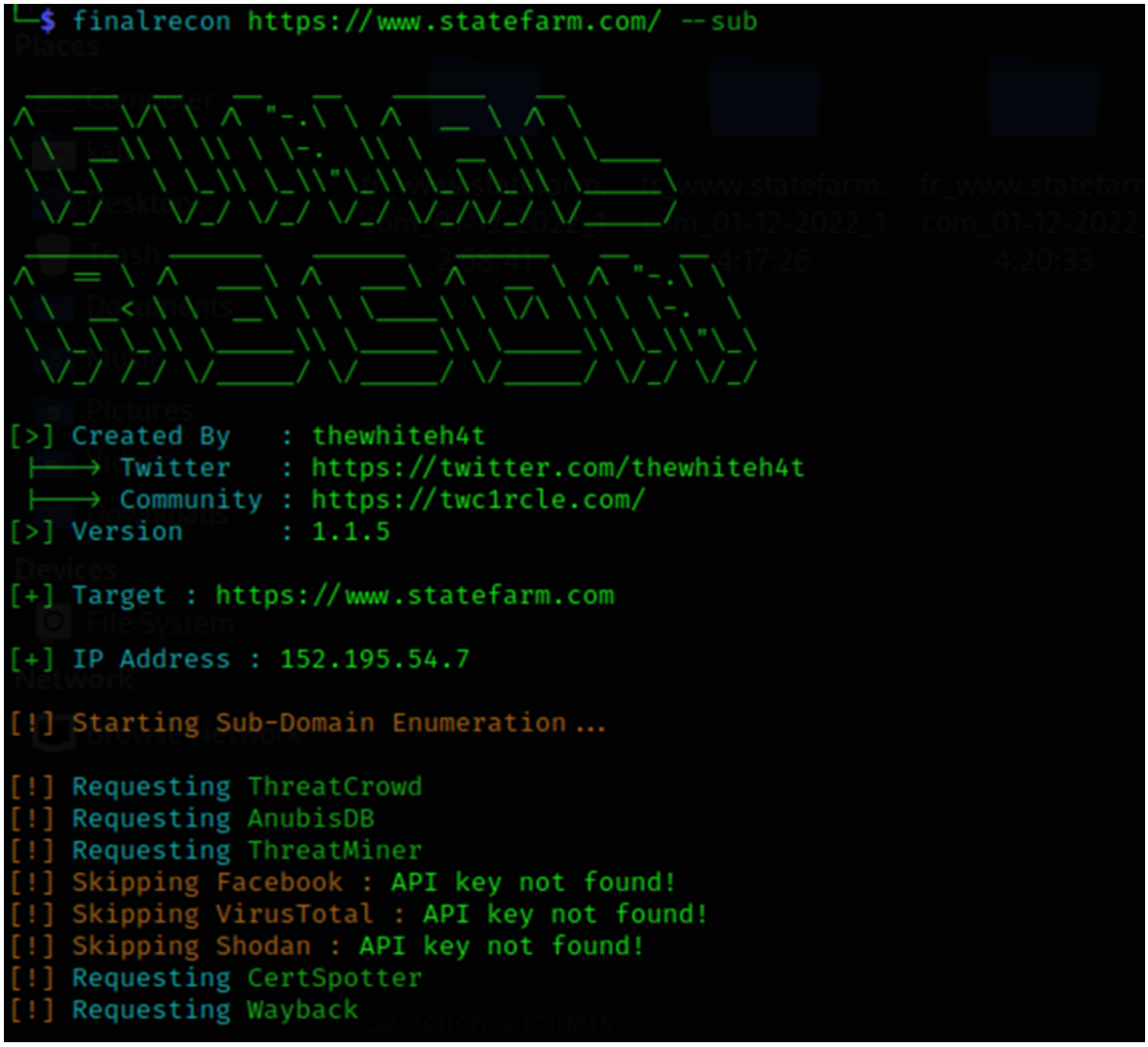
6. DATAS EM QUE OS TESTES FORAM FEITOS

Os testes e buscas por informações foram realizados nos dias 24, 27, 29 e 30 de novembro. Sendo que após esses dias não foram feitas nenhuma pesquisa ou teste.

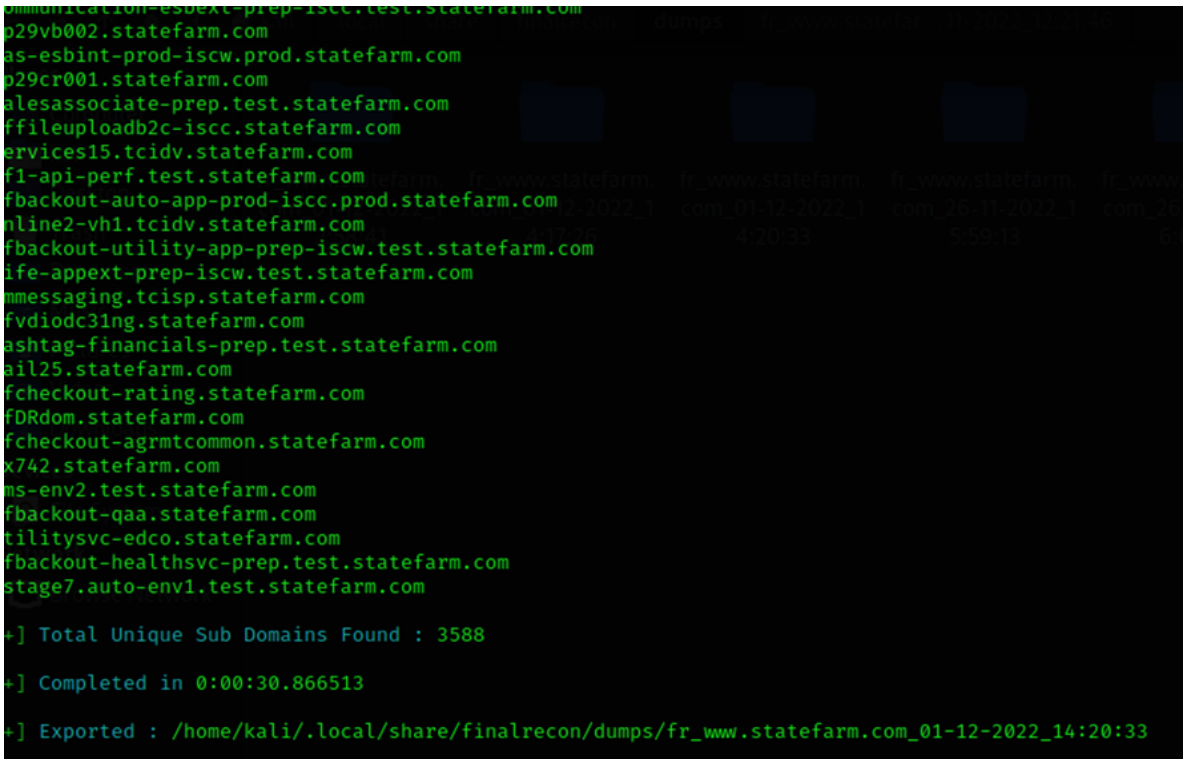
7. DETALHAMENTO DOS DADOS E SUBDOMÍNIOS

7.1 SUBDOMÍNIOS

Usando a ferramenta FinalRecon para a listagem de subdomínios e diretórios obtivemos uma lista muito grande de subdomínios:



Nessa enumeração de subdomínios foram encontrados incríveis 3588:



Se torna inviável colocar todos os 3588 domínios aqui.

7.2 DIRETÓRIOS

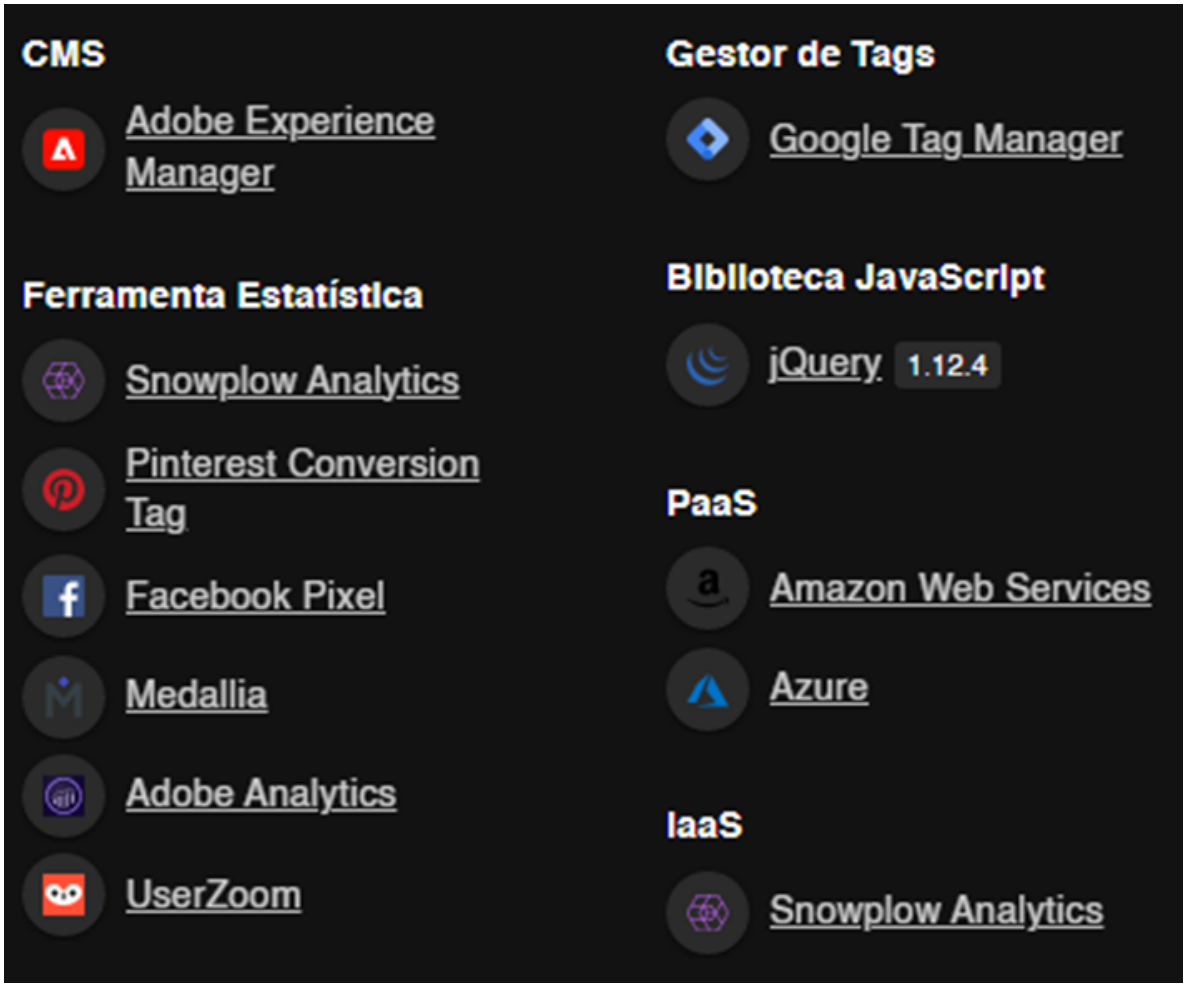
Foram encontrados 30 diretórios no nosso alvo (www.statefarm.com):

Ocorre que, como pode ser visto a estrutura é a seguinte: n° da linha/status/url;

Em todos, o status 403 foi retornado indicando Forbidden acesso não permitido:

Foram feitas várias tentativas de acesso aos diretórios, o que levou a um bloqueio de ip temporário.

8. DETALHAMENTO DOS SOFTWARES INSTALADOS



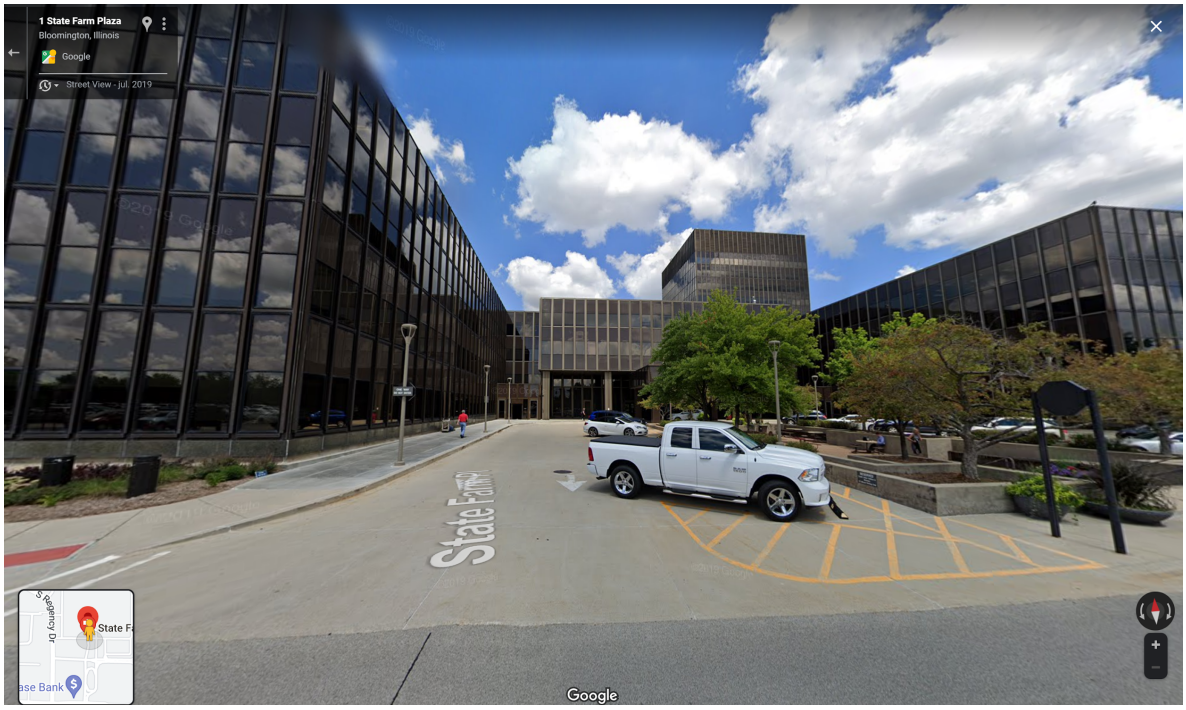
É conhecido várias vulnerabilidades nas bibliotecas do JQuery abaixo da versão 3.5. A encontrada no site sendo usada junto ao DOM pode levar ao tipo de vulnerabilidade de Cross Site Scripting (XSS) *https://owasp.org/www-community/attacks/xss/*.

9. INFORMAÇÕES GERAIS DE IP E GEOLOCALIZAÇÃO

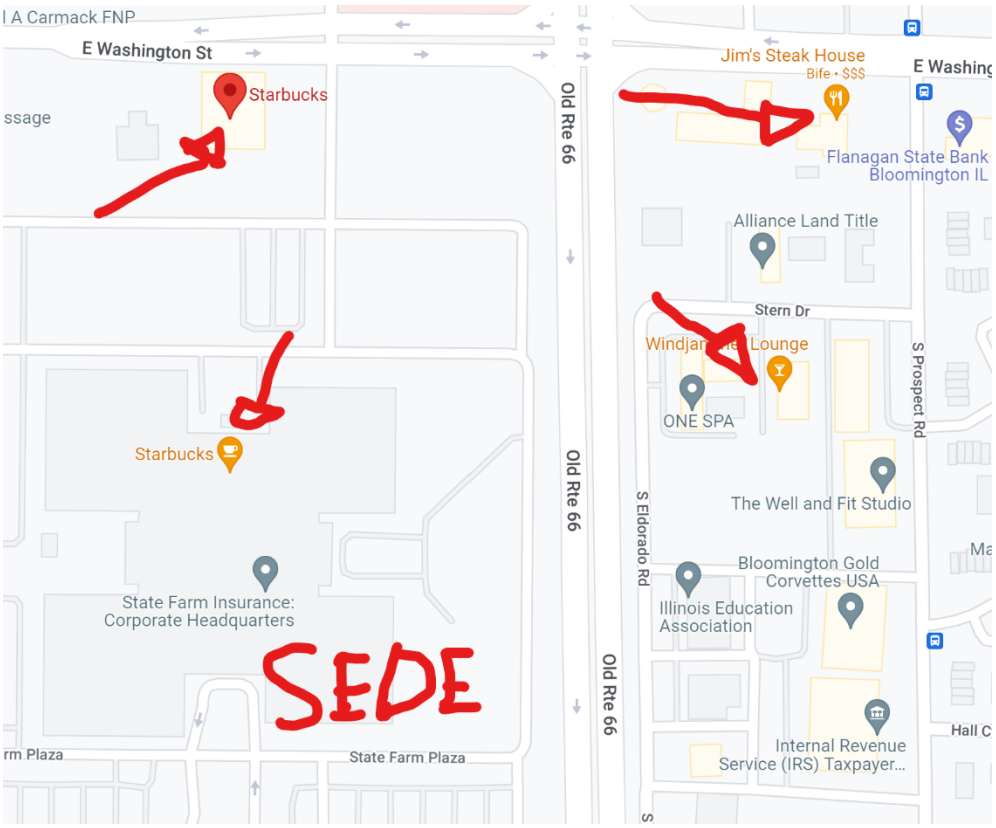
PRINT DO RESULTADO DE BUSCA PELO DOMÍNIO DO STATEFARM NO WWW.WHOIS.COM

```
Registrant Contact Information:
        Name                            Domain Administrator
        Organization                    State Farm Mutual Automobile Insurance Company
        Address                         Three State Farm Plaza R3,
        City                            Bloomington
        State / Province                IL
        Postal Code                     61710-0001
        Country                         US
        Phone                           +1.3097357185
        Fax                             +1.3097667787
        Email                           home.auto-eisadmin.399n00@statefarm.com

Administrative Contact Information:
        Name                            Domain Administrator
        Organization                    State Farm Mutual Automobile Insurance Company
        Address                         Three State Farm Plaza R3,
        City                            Bloomington
        State / Province                IL
        Postal Code                     61710-0001
        Country                         US
        Phone                           +1.3097357185
        Fax                             +1.3097667787
        Email                           home.auto-eisadmin.399n00@statefarm.com

Technical Contact Information:
        Name                            Domain Administrator
        Organization                    State Farm Mutual Automobile Insurance Company
        Address                         Three State Farm Plaza R3,
        City                            Bloomington
        State / Province                IL
        Postal Code                     61710-0001
        Country                         US
        Phone                           +1.3097357185
        Fax                             +1.3097667787
        Email                           home.auto-eisadmin.399n00@statefarm.com

Information Updated: 2022-11-27 17:44:32
```

9.1 STREET VIEW



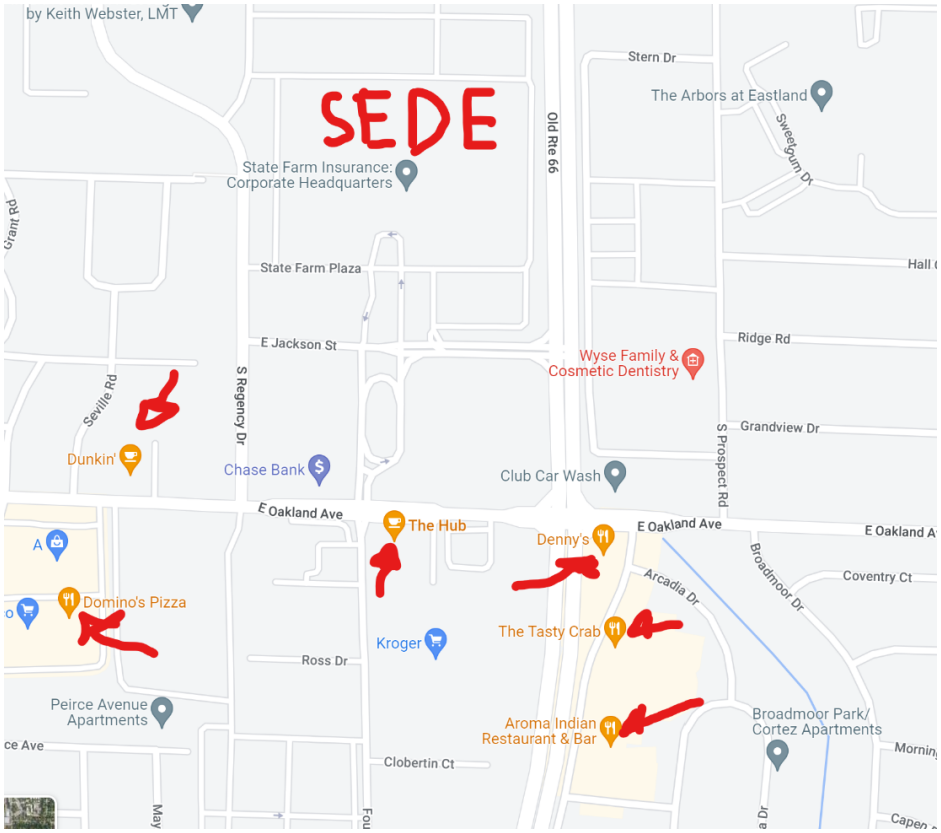
SEDE STATE FARM EM ILLINOIS – BLOOMINGTON



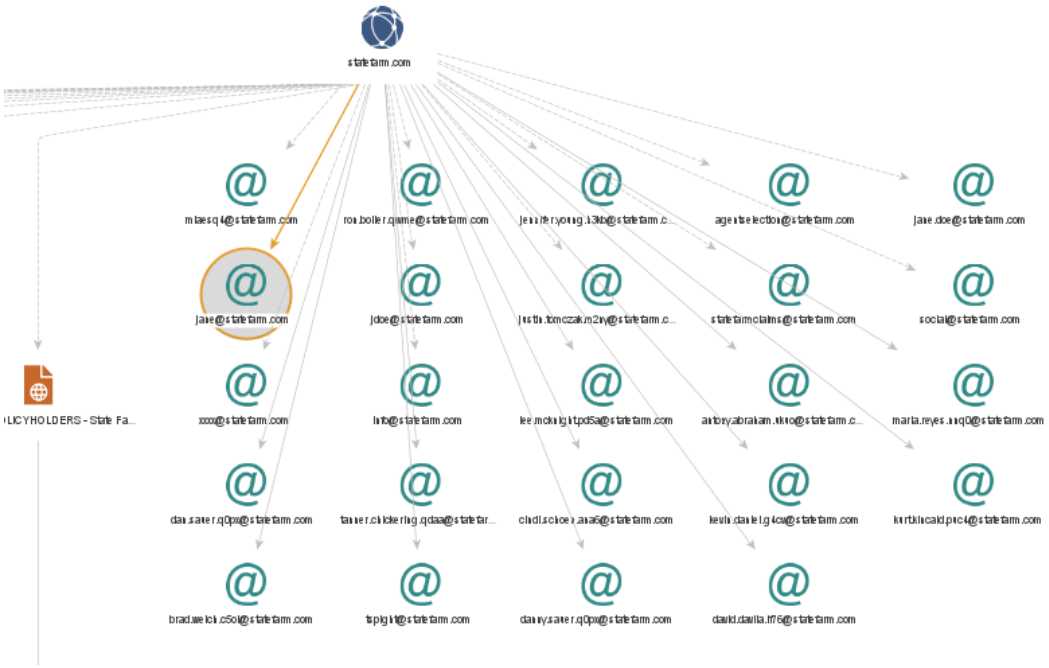
Lugares sociais são pontos estratégicos para o uso da engenharia social, pois lá existe a oportunidade de encontrar funcionários da empresa, e eventualmente realizar uma coleta de informação.

Uma boa medida para que esse comportamento não aconteça, é instalar cafeterias e restaurantes dentro da própria empresa.

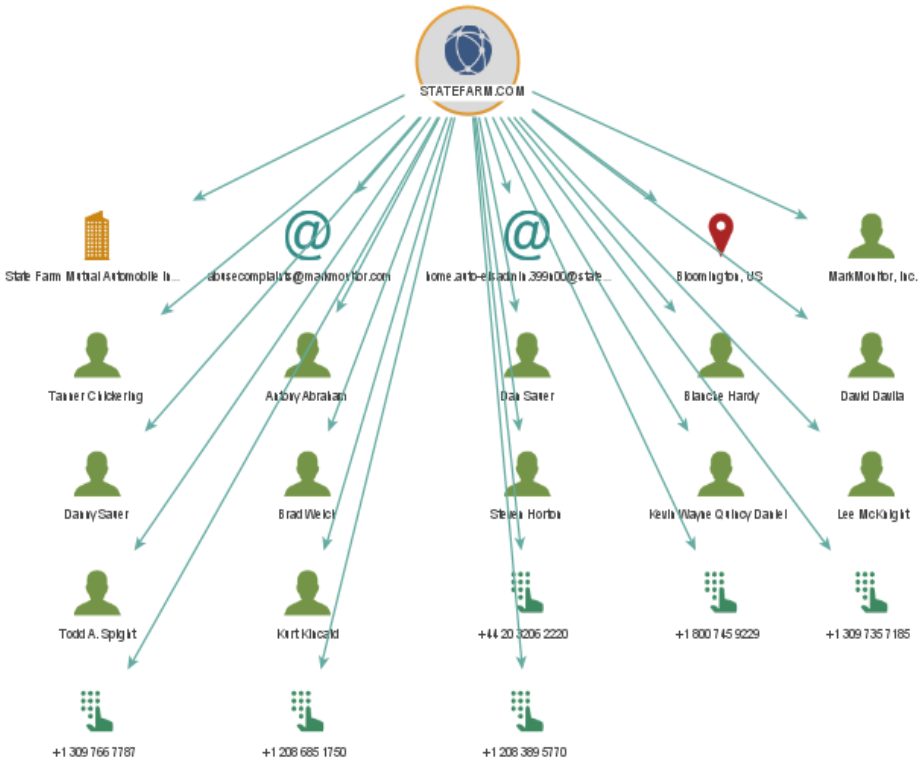
E treinamentos específicos para que não divulguem informações.



EMAIL DE FUNCIONARIOS E LEAKS (RELATORIO DO MALTEGO)

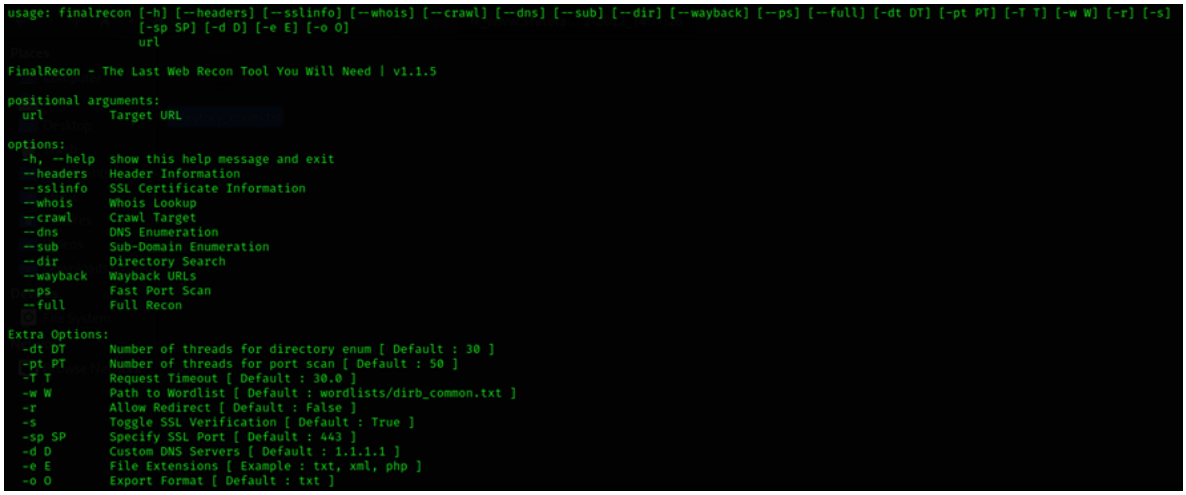


PESSOAS LIGADAS A STATEFARM (MALTEGO)



10. SOFTWARE USADO E RESULTADOS E VULNERABILIDADES RELATADA

10.1 FinalRecon e suas funções:



O funcionamento dele é focado na obtenção não agressiva de dados, sendo essa uma característica que adotamos nos testes.

Diretórios encontrados:

403, https://www.statefarm.com/.git/HEAD

403, https://www.statefarm.com/.htaccess

403, https://www.statefarm.com/_config

403, https://www.statefarm.com/.htpasswd

403, https://www.statefarm.com/.svn

403, https://www.statefarm.com/.svn/entries

403, https://www.statefarm.com/.hta

403, https://www.statefarm.com/.bash_history

403, https://www.statefarm.com/_mmserverscripts

403, https://www.statefarm.com/~adm

403, https://www.statefarm.com/~admin

403, https://www.statefarm.com/~administrator

403, https://www.statefarm.com/~apache

403, https://www.statefarm.com/~amanda

403, https://www.statefarm.com/~guest

403, https://www.statefarm.com/~bin

403, https://www.statefarm.com/~http

403, https://www.statefarm.com/~ftp

403, https://www.statefarm.com/~logs

403, https://www.statefarm.com/~httpd

403, https://www.statefarm.com/~log

403, https://www.statefarm.com/~lp

403, https://www.statefarm.com/~mail

403, https://www.statefarm.com/~operator

403, https://www.statefarm.com/~nobody

403, https://www.statefarm.com/~sysadm

403, https://www.statefarm.com/~sys

403, https://www.statefarm.com/~webmaster

403, https://www.statefarm.com/~tmp

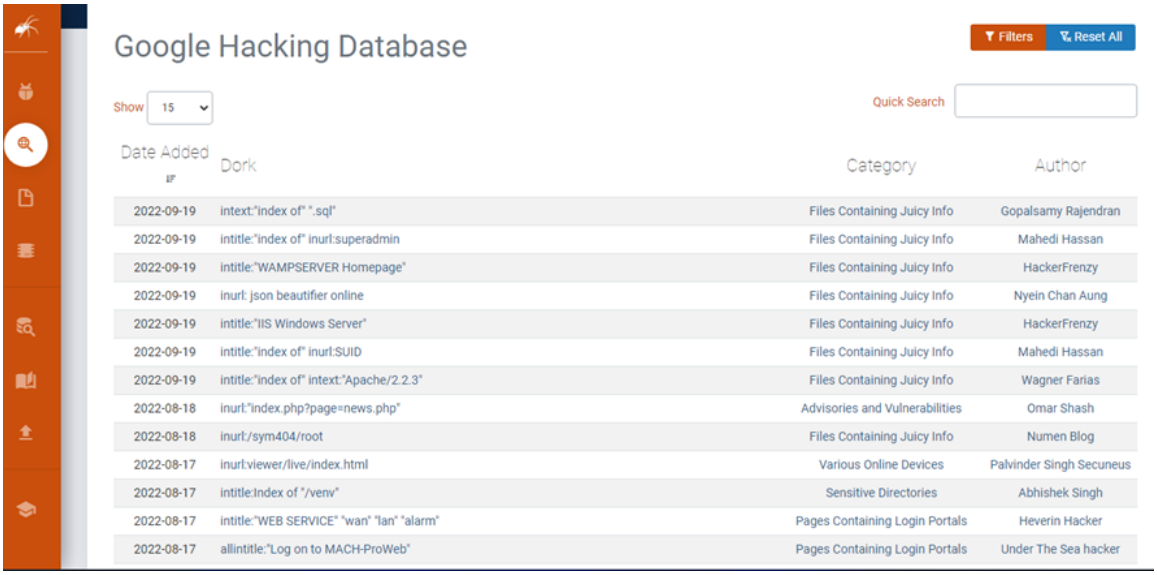
403, https://www.statefarm.com/~www

200, https://www.statefarm.com/

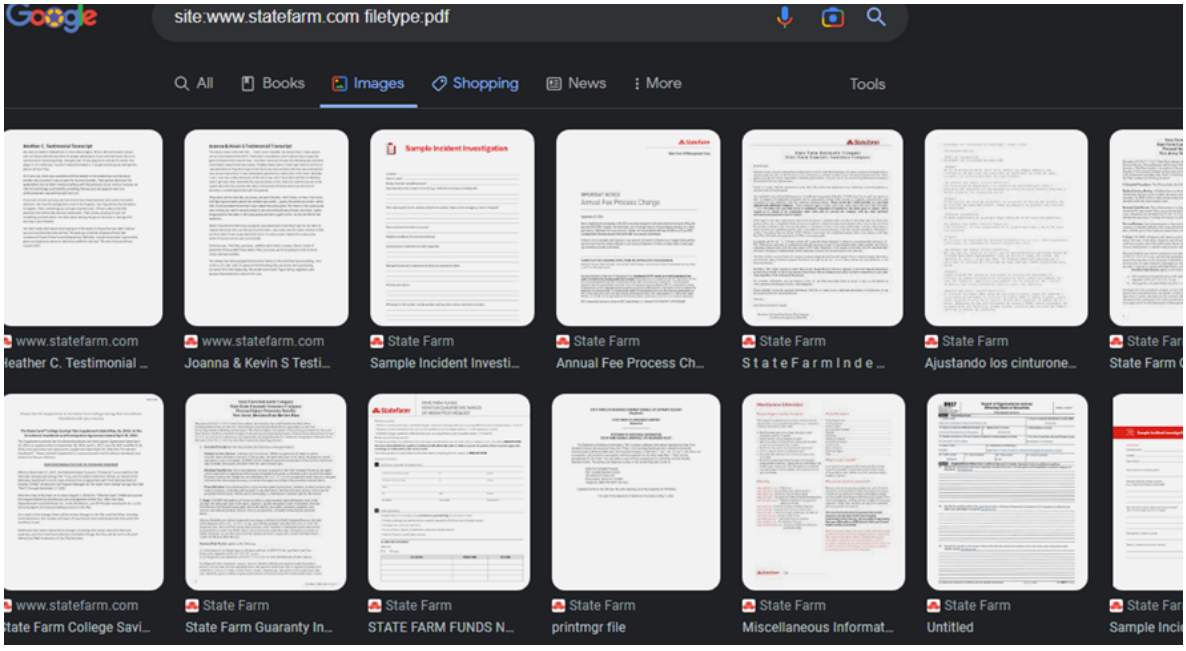
Subdomínios encontrados: Se torna inviável colocar os subdomínios aqui;

10.1 SPIDERFOOT

10.2 GOOGLE HACKING DATABASE (GHDB)

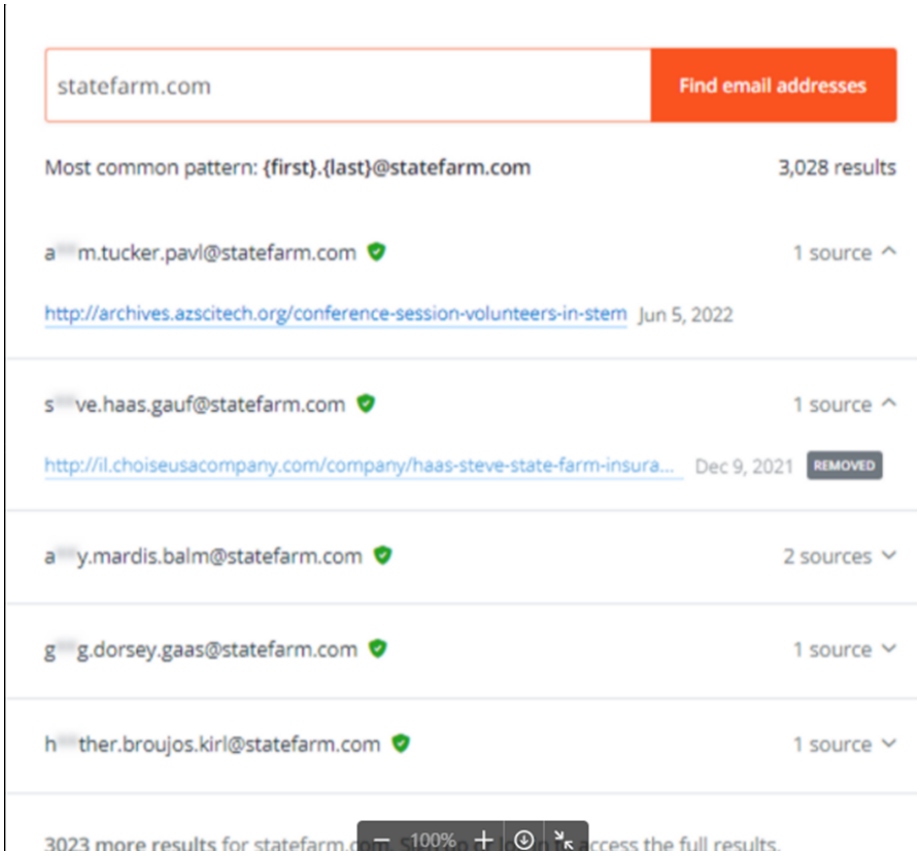


Foi feito buscas por arquivos :XLS, DOC, PDF, SQL, PHP, TXT, DB e SH.

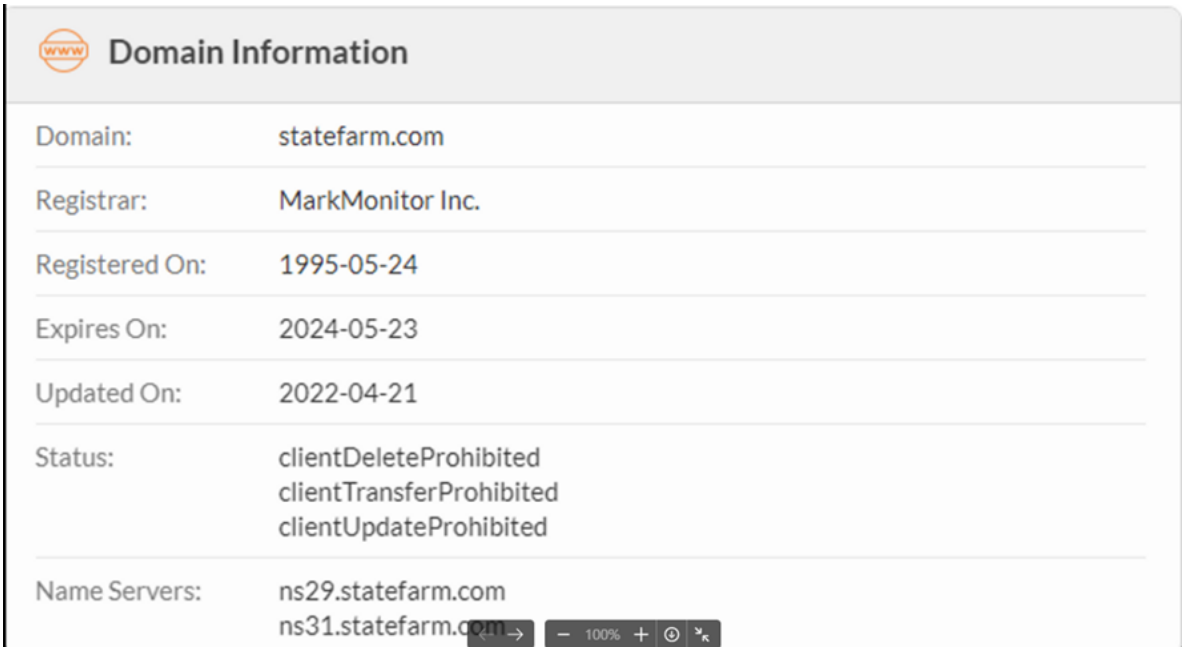


A imagem acima é um exemplo de busca por esses arquivos. Nessa busca, fazendo uso das ferramentas do GHDB não foi encontrado dados sensíveis ou comprometedores.

10.3 HUNTER.IO



10.4 WHO IS



10.5 HAVEIBEENPWNED

As imagens relacionadas ao uso do programa está sendo mostradas no tópico onze. Onde foi verificado se os e-mails haviam sido vazados ou alguma informação referente ao usuário.

11. LISTA DE E-MAILS QUE JÁ TEM A SUA SENHA EXPOSTA

home.auto-eisadmin.399n00@statefarm.com – o domínio foi registrado em uma empresa que gerencia portfólios de domínios (MarkMonitor). Esse e-mail que está listado no Who.is como registro está registrado em quatro vazamentos de dados;

Adam Tucker, Software Developer, State Farm, adam.tucker.pavl@statefarm.com – Foram encontrados seis vazamentos:

Adapt: In November 2018, security researcher Bob Diachenko identified an unprotected database hosted by data aggregator "Adapt". A provider of "Fresh Quality Contacts", the service exposed over 9.3M unique records of individuals and employer information including their names, employers, job titles, contact information and data relating to the employer including organisation description, size and revenue. No response was received from Adapt when contacted.

Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles

Apollo: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

Data & Leads: In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator. Upon further investigation, the data was linked to marketing company Data & Leads. The exposed Elasticsearch instance contained over 44M unique email addresses along with names, IP and physical addresses, phone numbers and employment information. No response was received from Data & Leads when contacted by Bob and their site subsequently went offline.

Compromised data: Email addresses, Employers, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

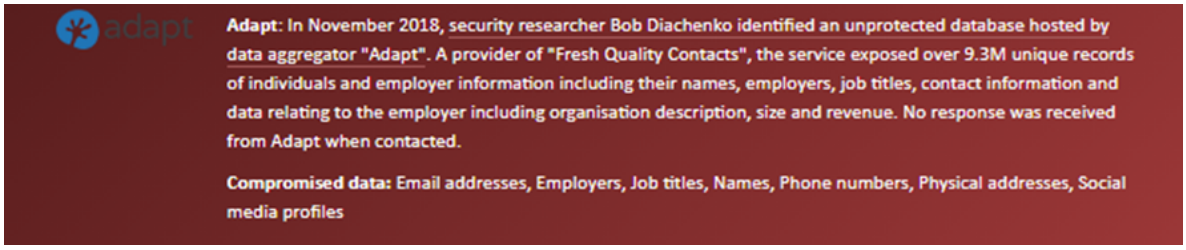
Elasticsearch Instance of Sales Leads on AWS: In October 2018, security researcher Bob Diachenko identified multiple exposed databases with hundreds of millions of records. One of those datasets was an Elasticsearch instance on AWS containing sales lead data and 5.8M unique email addresses. The data contained information relating to individuals and the companies they worked for including their names, email addresses and company name and contact information. Despite best efforts, it was not possible to identify the owner of the data hence this breach as been titled "Elasticsearch Sales Leads".

Compromised data: Email addresses, Employers, Names, Physical addresses

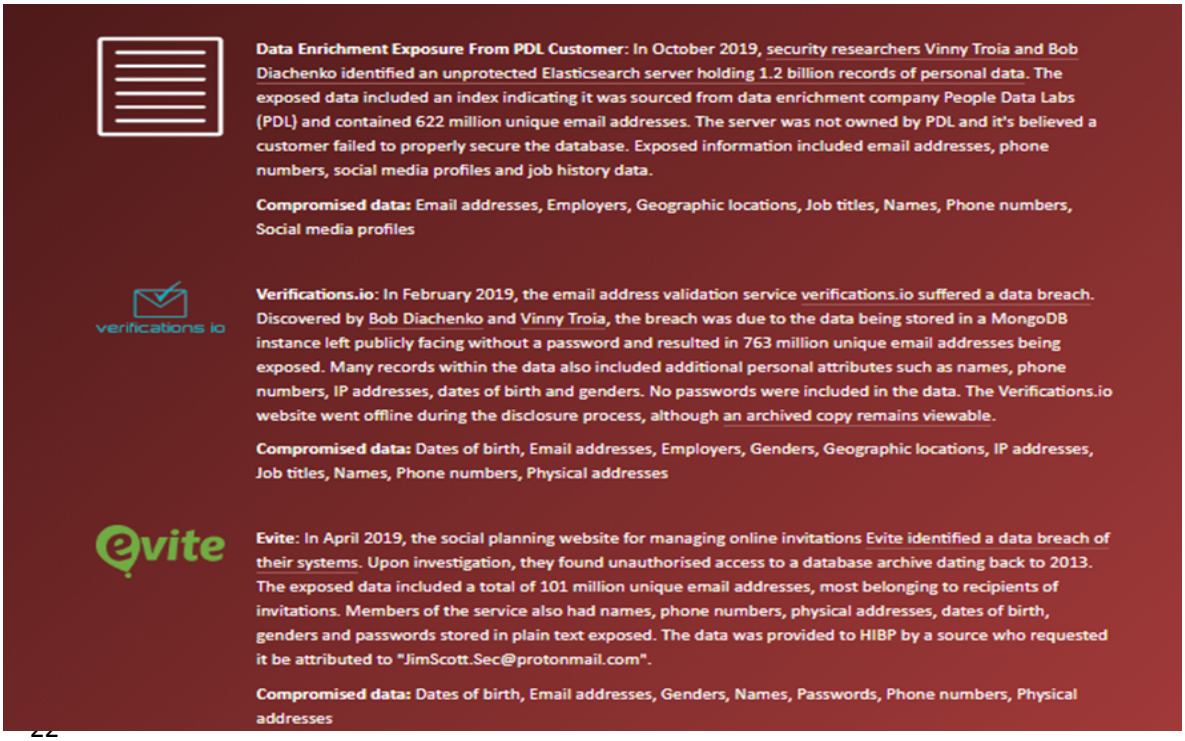
Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io

lisa.huth.a4pb@statefarm.com - foram encontrados dois vazamentos.

andy.mardis.balm@statefarm.com – Foi encontrado apenas um vazamento.



greg.dorsey.gaas@statefarm.com – Foram encontrados três vazamentos.



12. ALERTA DE VULNERABILIDADE DOS INDICADORES QUE DEMONSTRAM PREOCUPAÇÃO POR GRAU DE SEVERIDADE

GRÁFICO OBTIDO PELO SPIDERFOOT

2022-11-27 19:34:02	Host potencialmente obsoleto/não mantido: www.statefarm.com	Um host parece estar obsoleto com base em vários indicadores, como códigos HTTP malsucedidos, certificados SSL expirados, mensagens de erro, vulnerabilidades e arquivos indesejados encontrados. Esses hosts podem não ser mantidos, expondo o alvo a riscos de segurança.	ALTO	7
2022-11-27 19:34:03	Múltiplos códigos HTTP de falha encontrados em www.statefarm.com	Códigos de erro HTTP sem sucesso foram encontrados. 401 e 403 não estão incluídos, pois se referem a falhas de autenticação/autorização.	BAIXO	2
2022-11-27 19:34:03	Várias vulnerabilidades médias/baixas encontradas em www.statefarm.com	Várias vulnerabilidades classificadas como MÉDIAS ou BAIXAS foram encontradas em um host. Essas vulnerabilidades representam um risco menor para o alvo, porém, em conjunto, podem ser uma indicação de que o host não está bem mantido.	MÉDIO	4

13. QUADRO SWOT DA SEGURANÇA DO SITE (FORÇAS, 10. FRAQUEZAS, OPORTUNIDADES E AMEAÇAS)

CONCLUSÃO

14. SUGESTÕES PARA O CONTRATANTE

14.1 VERIFICAR ATUALIZAÇÕES DOS FRAMEWORKS, SISTEMAS OPERACIONAIS E FERRAMENTAS DE TRABALHO

Devido a boa Política de segurança que a empresa adotou, não se faz necessária grandes intervenções, mas deve-se destacar a utilização indevida de um HOST OBSOLETO nas dependências do servidor.

Sugerimos que haja uma verificação no host mencionado e a partir disso conclui se sua exclusão ou manutenção, para evitar possíveis vazamentos. Assim como da verificação das atualizações das ferramentas e frameworks.

14.2 INVESTIR EM TREINAMENTOS

Apenas o investimento em hardware e processos não podem garantir a segurança, a parte mais vulnerável das empresas são as pessoas, por isso, investir em treinamentos para noções de segurança da informação reconhecimento de ataques como phishing, spams e outras formas de tentativas de engenharia social

15. POLÍTICA DE SENHA

A senha deve possuir no mínimo 8 caracteres, números e letras MAIÚSCULAS e minúsculas e caracteres especiais (., #, $). Além disso não é permitido que a mesma contenha o nome ou sobrenome da pessoa

16. Número de tentativas sem restrições (LOCK OUT)

Perante a realização de scans em alguns momentos o ip de nossas máquinas foram bloqueados na realização dos testes, apontando um bom uso de medidas protetivas.