ObscureIQ Intel Briefing to Public

DogeQue.st

4/2/2025

DogeQuest Briefing Summary

What's the Backstory?

DogeQuest (dogeque.st) began as a surface web doxxing targeting Tesla owners and those affiliated with Elon Musk's government initiative DOGE (Department of Government Efficiency).

It later moved most personal data ops to the dark web, rebranding as ***DogeQuest Unleashed***.

Dogeqstqzn2yjns2d6ccns7aa52tglno63ay2uv2orfvd7e23khcsxid.onion

The site published names, addresses, phone numbers, LinkedIn handles, employer info, and car registration details of ~1,700 individuals.

DogeQuest Briefing Summary

How Did They Get the Targeting Data?

Primary breach source:

ParkMobile (2021): A parking app that leaked data of 21M+ users.

Attackers cross-referenced ParkMobile data
with scraped broker data to enrich profiles.

98.2% match confirmed between DogeQuest's exposed records
and ParkMobile's data where clients said they drove a Tesla.

DogeQuest Briefing Summary

Who Was Targeted?

1,700 tesla owners so far.

We have identified at least **150+** very high-risk individuals, including:

DOGE employees and families

U.S. military & federal agency staff

Executives from firms like **Google, Morgan Stanley, Verizon, Cisco**.

Policy think tanks, health officials, federal contractors, IMF advisors

Many job titles indicate clear links to government, national security, and public infrastructure.

DogeQuest Briefing

1 | ANALYSIS

DogeQuest: A Brief Analysis

2 | SCOPE OF EXPOSURE

Summary - Job Titles

Specific Examples: Gov & Mil Personnel / Contractors / DOGE

3 | DATA SOURCE ANALYSIS

ParkMobile Data Breach Enhanced Profile Creation - Data Brokers

4 | LEGAL IMPLICATIONS

Potential Criminal/Civil Actions:

Dom Terror Groups / Brokers / ParkMobile

5 | RECOMMENDATIONS

Digital Executive Protection

Mandatory Cyber Security and Privacy Training

DogeQuest Analysis

This intelligence report was created in response to the emergence of DogeQuest (dogeque.st), a platform initially appearing on the surface web and subsequently transitioning to the dark web under the rebranded identity "DogeQuest Unleashed."

DogeQuest specifically targeted Tesla owners and individuals affiliated with Elon Musk's Department of Government Efficiency (DOGE), publicly disclosing sensitive personal information, including names, addresses, contact details, and vehicle registration information. The platform's stated intent was to pressure individuals associated with Tesla or Musk's government initiatives by publicly exposing their private information, thereby creating significant privacy and security concerns for the affected individuals.

ObscureIQ conducted an extensive investigation into the origins, methods, and scope of the DogeQuest operation. Our analytical process involved detailed scrutiny of both the surface web and dark web iterations of the site, extensive cross-referencing of exposed personal information, and comprehensive correlation analyses. The primary goal of this investigation was to determine the origin and authenticity of the exposed data, identify how the data was obtained, and assess the broader security implications of the leak.

DogeQuest Analysis

Our investigation **conclusively identified the ParkMobile data breach** as the **source** of the compromised data published by DogeQuest.

We also found that a significant number of **very high-profile people** had been doxed.

And that this data combined with additional commercially available data was a **significant risk**.

DogeQuest Analysis

DogeQuest Analysis

Through rigorous cross-referencing, every data sample analyzed from DogeQuest matched data from the known ParkMobile breach, confirming a complete alignment of identifiers including **email addresses, phone numbers, and vehicle details**.

This linkage highlights significant vulnerabilities stemming from third-party software integrations and underscores the potential risks posed by seemingly innocuous service providers.

Our analysis revealed that DogeQuest operators **leveraged the ParkMobile breach data and likely paired it with extensive datasets obtained from data brokers**. This **strategic merging of breached data with commercially available data broker information** significantly amplified the threat profile of the affected individuals.

DogeQuest Analysis

Attackers can utilize enhanced profiles to conduct targeted harassment campaigns, doxxing ops, and cyberattacks against high-profile individuals, including senior government officials and executives in major corporations.

In assessing the impact and methodology of DogeQuest, this report highlights the evolving sophistication of cyber threats, emphasizing the intersection of cybersecurity breaches, data broker profiling, and targeted harassment campaigns.

ObscureIQ provides recommendations below, including enhanced digital executive protection measures. We also suggest that orgs require mandatory training programs not just of cybersecurity but also for privacy. The combination often works much better than either alone. When an employee can see the privacy impact on themselves, they can better apply cybersecurity principles to company data

Scope of Exposure

Summary Stats

There are roughly **1,700** people tagged in the dogeque.st data set.

23 records specifically target DOGE employees, their families, and connections.

We've identified **over a hundred extremely high-profile** and risk individuals in the data set.

Many orgs have people that are in the breach. Here is a random sample:

Bank of The West
UBS
PWC
Verizon
Spycloud

Oracle
Berkshire Partners
Atlantic Council
Targeted Victory
Cisco
Citi

Dell
Google
Montrose Environmental
Morgan Stanley
OneNation
PWC

Scope of Exposure

Job Titles Linked to Government Work?

The occupations below indicate the targeted personal and Tesla owner may be connected to government work. There are **MANY** more.

State/Federal Gov Positions

- Account Manager - State of CA
- Assistant State Coordinator, Florida County and District Clerk
- Division Chief, Capital Projects
- Executive Assistant Administrator for Enterprise Support
- Director, Enterprise Cloud Solutions
-Partner, Litigation and Chair of The White Collar and Government Investigations Group
- Presidential Innovation Fellow
- Senior Manager, Public Policy
- Vice President and General Manager Public Sector

Defense / National Security

- Branch Head
- Diplomatic Correspondent
- Investigator In-Chief
- Telecommunication Spec (likely associated with government agencies handling sensitive communication)

Nonprofit, Public Interest, Think Tank

- Nonresident Senior Fellow (likely affiliated with a public policy think tank)

Vice President, Smart Cities (often connected to public infrastructure)

Judiciary / Legal Roles

- General Counsel
- Assistant General Counsel, SVP
- Partner, Co-Chair of Real Estate (potentially related to government land deals or public sector real estate)
- Co-Chair, Appellate Practice Department
- Attorney (in a public sector capacity)
- Board Member (possibly in a government agency or public institution)

Health and Medical

- Pulmonary, Critical Care (potentially with public health agencies)
- EVP US Life Sciences (potential partnerships with public health bodies)

Gov-Linked Consulting and Advisory Roles

- Senior Advisor (often advising public institutions or government bodies)
- Senior Corporate Counsel (could be advising government entities)
- Principal, Expert Witness (may be used in government litigation or investigations)
- Senior Manager, Public Policy (likely involved in shaping government policies)

Scope of Exposure - Specific Examples

Gov & Military Personnel

Redacted - US Military Operations
Exposed Data: Email, Phone number, LinkedIn username, Home address, Employer, Job title

Redacted - Veterans Affairs
Exposed Data: Email, Phone number, LinkedIn username, Home address, Employer, Job title, X account

Redacted - Social Security Administration Exec
Exposed Data: Home address

Redacted - FBI Exec
Exposed Data: Email, Phone number, Home address

Redacted - Lawrence Livermore National Laboratory
Exposed Data: ...

Redacted - U.S. Office of Government Ethics
Exposed Data: ....

Staffer for a Congressman
Instructor at Army.mil
IMF Advisor
United Nations Consultant

DogeQuest Data Sources: Park Mobile

How did the individual(s) behind DogeQuest obtain Tesla ownership information?

- ObscureIQ conducted a comprehensive analysis of the data, conclusively identifying the ParkMobile data breach as the source through which attackers obtained Tesla owner information.

Background:

- ParkMobile is a widely used mobile parking payment application that enables users across numerous cities in the United States to pay for parking remotely using their mobile devices. o In March 2021, ParkMobile experienced a significant data breach due to a vulnerability in third-party software, resulting in the compromise of approximately 21 million user accounts.

Data Compromised:

- Personal identifiers including email addresses, and phone numbers o Vehicle-related information such as license plate numbers and vehicle nicknames. o Account passwords, although encrypted (hashed), were exposed without encryption keys.

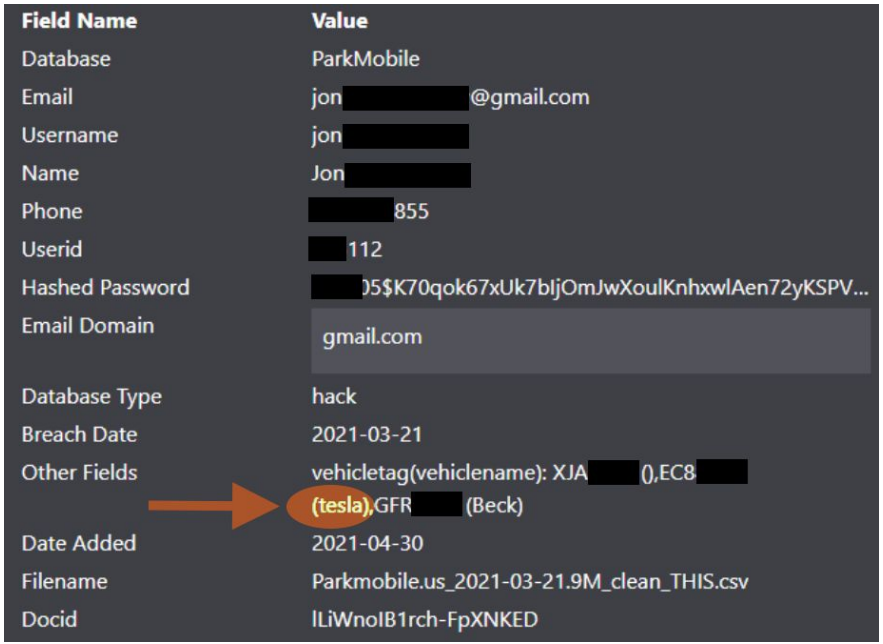
Aftermath & Ongoing Risks:

- Initially sold on dark web forums, the compromised data eventually became publicly available for free o Significantly increases the risk of: Doxxing, ID theft, Phishing, Targeting

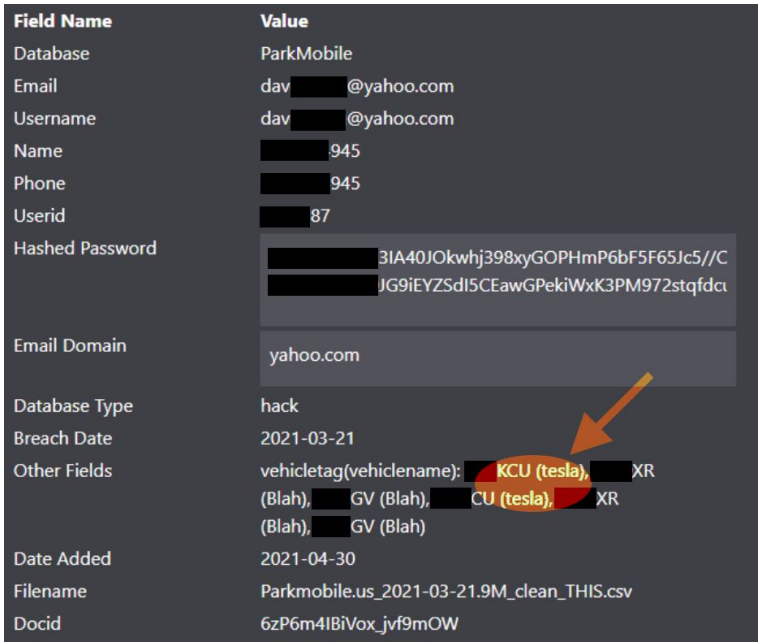
DogeQuest Data Sources: Park Mobile

Data Compromised:

- Vehicle nicknames in the Park Mobile breach were used to ID likely Tesla owners.



Field Name	Value
Database	ParkMobile
Email	jon[redacted]@gmail.com
Username	jon[redacted]
Name	Jon[redacted]
Phone	[redacted]855
Userid	[redacted]112
Hashed Password	[redacted])5$K70qok67xUk7bIjOmJwXoulKnhxwlAen72yKSPV...
Email Domain	gmail.com
Database Type	hack
Breach Date	2021-03-21
Other Fields	vehicletag(vehiclename): XJA[redacted](),EC8[redacted] (tesla),GFR[redacted] (Beck)
Date Added	2021-04-30
Filename	Parkmobile.us_2021-03-21.9M_clean_THIS.csv
Docid	lLiWnoIB1rch-FpXNKED



Field Name	Value
Database	ParkMobile
Email	dav[redacted]@yahoo.com
Username	dav[redacted]@yahoo.com
Name	[redacted]945
Phone	[redacted]945
Userid	[redacted]87
Hashed Password	[redacted]3IA40JOkwhj398xyGOPHmP6bF5F65Jc5//C[redacted]JG9iEYZSdI5CEawGPekiWxK3PM972stqfdcu
Email Domain	yahoo.com
Database Type	hack
Breach Date	2021-03-21
Other Fields	vehicletag(vehiclename): [redacted]KCU (tesla),[redacted]XR (Blah),[redacted]GV (Blah),[redacted]CU (tesla),[redacted]XR (Blah),[redacted]GV (Blah)
Date Added	2021-04-30
Filename	Parkmobile.us_2021-03-21.9M_clean_THIS.csv
Docid	6zP6m4IBiVox_jvf9mOW

DogeQuest Data Sources: Park Mobile

How can we be sure that ParkMobile was the Source of the Tesla Owner data?

- We downloaded a DB of **21.9M** records from the 2021 ParkMobile hack.
- We extracted all records where “Tesla” or a proxy word was mentioned with the license plate data as a nickname for the car.
  - We found **74,349 records where a Tesla vehicle is mentioned**.
- We compared the email addresses and phone numbers in the DogeQuest data set and matched **1647 of 98.2%** of all of the Tesla owner records doxed.

98.2% Match

DogeQuest Data Sources: Data Brokers

Background:

- The ParkMobile data breach included emails, phone numbers, vehicle information, and encrypted passwords, but it did **not** include:
  - Addresses, Job title and employer, LinkedIn data, X (Twitter) data

Where did the other data come from?

- Our investigation indicates that compromised ParkMobile data was paired with information obtained from data brokers.
- The data enhancements were likely scraped or stolen from brokers rather than bought fresh. A rudimentary scrape of a people search data site may have accomplished goal.
- Many records in DogeQue.st are not as enhanced as they might has been if embellished on commercial broker services.
  Some examples: Clay, Clearbit/Seamless.AI, ZoomInfo, Apollo.AI, Lusha
- It appears the threat actors understand data but not the data brokers ecosystem. Or they were worried about the transaction being traced.

DogeQuest Data Sources: Data Brokers

Implications:

- Pairing breached data with information obtained from data brokers can significantly expand the digital profile available to attackers, increasing the potential harm to targeted individuals and their organizations.
  - **We purchased commercial data to see how easily it would be and were able to VASTLY expand the profiles on virtually all of the 1,700 in the breach. Additional contact information, employment info, and much more.**
- With effort, attackers may also gain access to passwords, authentication tokens, or cookies, thereby posing a direct threat to government data and systems.

DogeQuest Threat Model

Doxxed Tesla Owners on DogeQue.st

This threat model assesses the risks associated with the exposure of Tesla owners' personal information on the DogeQue.st website.

The site's developers may be **primarily focused on harming Elon Musk's business empire.** Collateral damage to individual Tesla owners is a likely and potentially severe consequence.

The **risk to any one individual may be low due** to the large population of Tesla owners, but **the harm could be significant**. And that risk increases for those with higher profiles or net worth.

The primary intent behind DogeQue.st appears to be less about inciting violence and **more about instilling fear** - both among Tesla owners and the general public. If owning a Tesla becomes synonymous with personal risk, it could dissuade potential buyers and hurt Elon's bottom line more effectively than protests or even attacks on Tesla infrastructure like dealerships or charging stations.

The publication of the doxing data **significantly raises the threat level for the 1,700 Tesla owners**, and Tesla owners in general, as irrational actors could act on the doxed information.

While giving this website airtime plays into their narrative, failing to alert Tesla owners exacerbates this problem, leaving them unaware of their exposure and unprepared to mitigate the risks.

DogeQuest Threat Model

Assets at Risk

- **Physical Safety**: Risk of physical harm from individuals who may act irrationally or violently.
- **Property Security**: Vandalism or damage to the Tesla vehicle or personal property.
- **Digital Security**: Further exploitation of exposed information.
- **Reputation and Privacy**: Harm to reputation through unwanted attention, harassment, or public exposure.

Threat Actors

Primary Threats

- **Anti-Elon Extremists**
- **Mischief-Motivated Hackers/Trolls**
- **Political or Ideological Actors**

Collateral Threats

- **Disgruntled Neighbors or Locals**
- **Criminal Opportunists**

DogeQuest Threat Model

Assets at Risk

- **Physical Safety**: Risk of physical harm from individuals who may act irrationally or violently.
- **Property Security**: Vandalism or damage to the Tesla vehicle or personal property.
- **Digital Security**: Further exploitation of exposed information.
- **Reputation and Privacy**: Harm to reputation through unwanted attention, harassment, or public exposure.

Threat Actors

Primary Threats

- **Anti-Elon Extremists**
- **Mischief-Motivated Hackers/Trolls**
- **Political or Ideological Actors**

Collateral Threats

- **Disgruntled Neighbors or Locals**
- **Criminal Opportunists**

Attack Surfaces

- **Published Data on DogeQue.st**
- **External Reconnaissance**
- **Physical Proximity**
  - **The big risk may be how close a high-profile Tesla owner is to someone who is motivated and/or unstable**

Vulnerabilities

- **Lack of Data Sanitization**: Raw owner data exposed without masking.
- **Proximity Risks**: Easy ID of owners within close geographical range.
- **No Threat Mitigation Protocols**: Tesla owners likely unaware/unprepared,
- **Info Amplification**: Risk of data being copied and shared on forums.

DogeQuest Threat Scenarios

Scenario 1: Physical Confrontation or Violence

Actor: **Local anti-Tesla activist or extremist**.
Action: Identifies a nearby Tesla owner from DogeQue.st and confronts or assaults them.
Impact: Severe injury or death, legal consequences for attacker, widespread fear.

Scenario 2: Vandalism or Property Damage

Actor: **Anti-Tesla individual or disgruntled neighbor**.
Action: Identifies owner's address and damages their vehicle, home, or other property.
Impact: Property damage, insurance claims, potential escalation.

Scenario 3: Swatting or False Reporting

Actor: **Troll or online harasser**.
Action: Uses doxxed address to file false police reports (swatting).
Impact: Police response, potential harm to the owner, trauma, and reputational harm.

Scenario 4: Burglary or Theft

Actor: **Criminal opportunist**.
Action: Uses the doxxed information to target owners for car theft or burglary.
Impact: Financial loss, safety risks, and ongoing fear.

Scenario 5: Online Harassment and Doxxing Escalation

Actor: **Hackers or trolls**.
Action: Amplifies exposure by linking additional personal information (social media, family data).
Impact: Sustained harassment, privacy erosion, and mental distress.

DogeQuest Threat Scenarios

Likelihood & Impact Assessment (Tesla Owner)

Threat Scenario	Likelihood	Impact	Risk
Physical Violence	Low	**High**	Moderate
Vandalism/ Prop Damage	Moderate	Medium	Moderate
Swatting/False Reporting	Low	**High**	Moderate
Burglary/Theft	Moderate	Medium	Moderate
Online Harass/ Doxxing	High	Low-Medium	High

DogeQuest Threat Scenarios

Likelihood & Impact Assessment (High Profile Tesla Owner)

Threat Scenario	Likelihood	Impact	Risk
Physical Violence	Moderate	**Catastrophic**	High
Vandalism/ Prop Damage	Moderate-High	Medium-High	High
Swatting/False Reporting	Moderate	**High**	High
Burglary/Theft	Moderate-High	**High**	High
Online Harass/ Doxxing	Moderate-High	Medium-High	High
Kidnapping or Extortion	Low	**Catastrophic**	High
Stalking and Surveillance	Moderate	Medium	High

Recommendations

Digital Executive Protection:

Implement digital executive protection services for high-risk government officials that will:

- Conduct a comprehensive threat surface assessment
- Proactively mitigate identified and emerging threats
- Remove exposed personal information from data brokers
- Continuously monitor the dark web for potential compromises and leaked information
- Monitor social media platforms, forums, extremist websites, and comment sections for threats, attempted doxxing, or indicators of compromise

Mandatory Cyber Security and Privacy Training:

Data Privacy

- Educate employees on securely managing sensitive personal data.
- Provide practical examples demonstrating how personal data can be exploited to compromise organizational security

Account Security

- Train employees on creating robust, unique passwords and the importance of multi-factor authentication (MFA) for both official and personal accounts.
- Highlight the risks associated with password reuse and sharing personal information on insecure platforms.
- Equip employees to recognize and effectively respond to phishing and social engineering attempts targeting both professional and personal accounts

ObscureIQ?

email
jeff@obscureiq.com
colby@obscureiq.com

signal
PrivacyStan.10

Jeff JOCKISCH

Co-Founder & CXO
Leading Data Privacy Researcher
Recognized Expert on Data Brokers
LinkedIn Top Voice / **YBYR**

Colby SCULLION

Co-Founder & CEO
Open Source Intelligence Leader
Automation Expert
B14ckBear Digital Recon

Data Broker CODEX

8,500 Entities that collect consumer profiles
The largest and deepest db of data brokers
Tagged, scored, within a custom taxonomy