🔍 INVESTIGATION LOG

Valdoria Votes: A Political Mystery (Part 2)

Field	Value
Analyst	Phila Mabuza

1. INCIDENT SUMMARY

[What’s this about? (One-liner)]

An unknown hacking group claims to have compromised Valdoria’s air-gapped voting machines. The attack began with reconnaissance targeting new poll workers and election infrastructure. We must determine if any internal systems were breached and whether election integrity is at risk.

---

2. INVESTIGATION SCOPE

[What am I looking at? (Systems, logs, time range)]

Category	Details
Log sources	Passive DNS, Inbound Network Events (Web Proxy), Employee Directory, Out Bound Network Events

Affected hosts/users	Name: Anderson Snooper Name: Barry Schmelly Name: Arrack Bobama
Time period of interest	2024-10-01 – 2024-10-10 UTC (based on first observed reconnaissance)

3. EVIDENCE INVENTORY (IOC TRACKER)

[Bad guys' tools – IPs, domains, etc. One row per IOC.]

Type	Value	First Seen (UTC)	Notes / Context
IP	55.49.227.170	2024-10-05T00:00:00Z	Attacker IP from boast post; resolves `shadow-hackers-r.us`

IP	214.85.104.248	2024-10-05T00:00:00Z	IP used for reconnaissance searches
IP	157.100.244.104	2024-10-05T00:00:00Z	Also resolves from `valdoriavotesgov.com`
Domain	valdoriavotesgov.com	2024-10-05T00:00:00Z	Fraudulent domain; resolves to `55.49.227.170`, `157.100.244.104`
Domain	shadow-hackers-r.us	2024-10-05T00:00:00Z	Resolves to `55.49.227.170`
Search query	Valdoria+Board+of+Elections+new+hires+2024	2024-10-05	Recon – targeting new employees
Search query	election+interference+prevention+measures	2024-10-07	Recon – researching defenses
Search query	types+of+voting+machines+used+in+Valdoria	2024-10-07	Recon – targeting voting tech

IP	`157.100.244.104`	`2024-10-07T15:46:45.000Z`	Used to access Snooper's account after phishing
Email address	barry_schmelly@valdoriavotes.gov	2024-10-08	Employee contacted by compromised account "ansnooper" after takeover
Conversation ID	`94bd6162-1323-402d-bccd-8fceaee5f230`		Prompt: `How do I access the voting machines?`

4. INVESTIGATION TIMELINE

Timestamp (UTC)	Event Description	Log Source	Reference / Query ID
2024-10-05T00:00:00.000Z	Attacker IP 214.85.104.248 searches Valdoria	Web proxy	`https://valdoriavotes.gov/search=Valdo`

	website for “new hires 2024”		ria+Board+of+Elections+new+hires+2024
2024-10-07T12:11:59.000Z	Same IP searches “election interference prevention measures”	Web proxy	https://valdoriavotes.gov/search=election+interference+prevention+measures
2024-10-07T15:24:59.000Z	Same IP searches “types of voting machines used in Valdoria”	Web proxy	https://valdoriavotes.gov/search=types+of+voting+machines+used+in+Valdoria
2024-10-07T15:40:59.000Z	Same IP searches “technical manual for voting machines”	Web proxy	https://valdoriavotes.gov/search=technical+manual+for+voting+machines
2024-10-07T10:46:45Z	*Employee with the ip address 10.10.0.4 tries to log in to the fake website*	Web proxy	https://valdoriavotesgov.com/login
2024-10-07T10:46:47.000Z	*Employee with the ip address 10.10.0.4*	Web proxy	https://valdoriavotesgov.com/login?username=ansnooper&password=**********

	entered their credentials into that page		

`2024-10-07T15:46:45.000Z`	Threat actor logged into Snooper's account using stolen credentials	Authentication Logs	`| where username == "ansnooper"`
			`| where timestamp between(datetime(2024-10-05T10:46:47Z) .. datetime(2024-10-11T10:46:47Z))`

`2024-10-16T15:57:05.000Z`	Using Snooper's IP, threat actor attempted to access `https://ai.valdoriavotes.gov/?model=gpt-4o`	Web proxy	`https://ai.valdoriavotes.gov/?model=gpt-4o`
`2024-10-16T00:00:00.000Z`	Attacker with ip address `214.85.104.248` logged as Arrack Bobama After posing as him at 2024:10:15 on a call asking for a password reset	Authentication events	

5. QUERY LOG

[Searches I ran – so I don’t repeat myself.]

```
text
// Find any inbound traffic from the attacker IP (55.49.227.170)
InboundNetworkEvents
| where src_ip == "55.49.227.170"
```

```
text
// Find all domains that resolved to the suspicious IP
PassiveDns
| where ip == "55.49.227.170"
```

```
text
// Find all IPs that the fraudulent domain resolved to
PassiveDns
| where domain == "valdoriavotesgov.com"
| distinct ip
```

```
text
// Find inbound requests from any IP tied to the fraudulent domain
let ips = PassiveDns
| where domain == "valdoriavotesgov.com"
| distinct ip;
InboundNetworkEvents
| where src_ip in (ips)
```

```
text
// Check for any internal hosts contacting the attacker IPs
OutboundNetworkEvents
| where dest_ip in ("55.49.227.170", "214.85.104.248", "157.100.244.104")
```

```
text
// Check for DNS queries to the fraudulent domains from internal hosts
PassiveDns
| where domain in ("valdoriavotesgov.com", "shadow-hackers-r.us")
| project timestamp, client_ip, domain
```

```
text
// Check email gateway for messages from these domains
EmailEvents
| where sender_domain in ("valdoriavotesgov.com", "shadow-hackers-r.us")
```

```
text
// Get employee information - Deputy Commissioner
Employees
| where role == "Deputy Commissioner"
```

```
text
// Get employee information - specific names
Employees
| where name == "Dora Thomas"
Employees
| where name == "Barry Schmelly"
```

```
//Let’s check if there’s any traffic to it—has any of our employees
visited that domain for any reason?

OutboundNetworkEvents
```

```
| where url contains "valdoriavotesgov.com"


//What is the username of the employee that entered their credentials on that phishing page?

Employees

| where ip_addr == '10.10.0.4'


//When did the threat actor login to Snooper's account?

AuthenticationEvents

| where username == "ansnooper"

| where timestamp between(datetime(2024-10-05T10:46:47Z) .. datetime(2024-10-11T10:46:47Z))


//What is the email address of the person he was conversing with?

Email

| where recipient == 'anderson_snooper@valdoriavotes.gov'

| where timestamp between(datetime(2024-10-08T00:00:47Z) .. datetime(2024-10-11T10:46:47Z))


//What is Schmelly's job role?

Employees
```

```
| where name contains "Schmelly"



//"Snooper" was observed asking Schmelly how one might gain access to what
devices?

Email

|where recipient == "barry_schmelly@valdoriavotes.gov"

| where sender == 'anderson_snooper@valdoriavotes.gov'

| where timestamp between(datetime(2024-10-08T00:00:20Z) ..
datetime(2024-10-11T10:46:47Z))



//What term appeared at the end of each url that Snooper guessed?

InboundNetworkEvents

| where src_ip == "10.10.0.4"



//How many questions did they ask the chatbot?

InboundNetworkEvents

| where url contains
"https://elections-chatbot.valdoriavotes.gov/?model=gpt-4o"

//Which conversation_id is associated with the question about voting
machines?

AIPrompts

| where prompt contains "voting machines"

//According to the bot, the voting machines are not actually connected to
the internet.

//Instead, votes are manually calculated using a ___.
```

```
AIPrompts
| where response contains "votes"


//What is the name of the vendor?
AIPrompts
| where response contains "vendor"


//What job role will the vendor talk to?
AIPrompts
| where response contains "Dominos Voting Systems"


//What job role will the vendor talk to?
Employees
| where role has "Election Commissioner"
//When did they log in to Bobama's account?
AuthenticationEvents
| where hostname == "QDPG-DESKTOP"
| where timestamp between(datetime(2024-10-15T00:00:20Z) .. datetime(2024-10-30T10:46:47Z))


//What email address did they send this email to?
Email
| where sender == "arrack_bobama@valdoriavotes.gov"
| where timestamp between(datetime(2024-10-15T00:00:20Z) ..
datetime(2024-11-30T10:46:47Z))
```

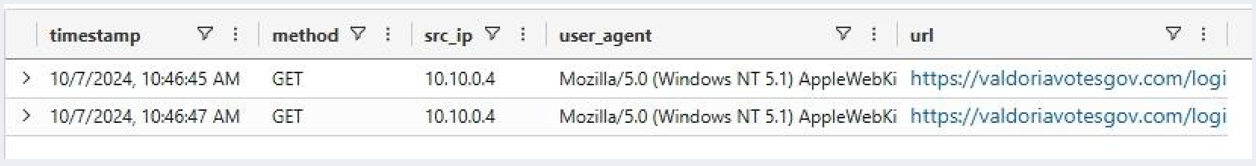
6. DETAILED FINDINGS

[Raw evidence + what it means to me.]

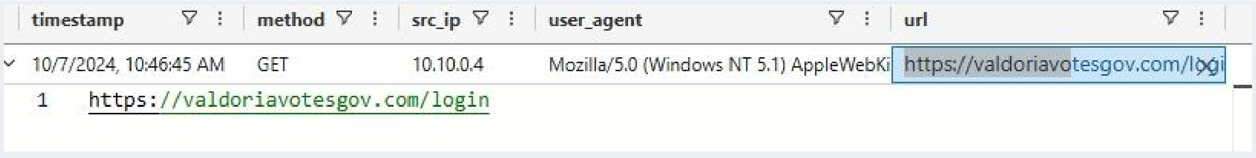
Time range: 2024-10-05 – 2024-10-07

- Observation:
  `Domain valdoriavotesgov.com made 26 web requests to Valdoria Votes network.`
  → Analysis: The attacker performed active reconnaissance, mapping Valdoria's public-facing infrastructure.
- Observation:
  `Search queries: "new hires 2024", "election interference prevention", "voting machine types"`
  → Analysis: Attacker is specifically interested in:
  - Recently hired personnel (potential phishing targets)
  - Security measures (to evade detection)
  - Voting machine models (to research exploits)
- Observation:
  `valdoriavotesgov.com` resolves to 55.49.227.170 and 157.100.244.104.
  `shadow-hackers-r.us` resolves to 55.49.227.170.
  → Analysis: The attacker controls at least two domains and three IPs. The shared IP (55.49.227.170) suggests a single actor or group.
- Observation:
  Reconnaissance IP 214.85.104.248 is *not* among the resolution IPs of the fraudulent domains.
  → Analysis: Attacker may be using a separate IP for recon to avoid linking infrastructure early – common tradecraft.
- Observation:
  Search queries: "technical manual for voting machines"
  → Analysis: The hackers even tried to locate a specific document which is "technical manual" that would reveal exactly how the machines operate.

- Observation: The employees visited that domain thinking it was legit, tried to login in by inserting their login details.



timestamp	method	src_ip	user_agent	url
10/7/2024, 10:46:45 AM	GET	10.10.0.4	Mozilla/5.0 (Windows NT 5.1) AppleWebKi	https://valdoriavotesgov.com/logi
10/7/2024, 10:46:47 AM	GET	10.10.0.4	Mozilla/5.0 (Windows NT 5.1) AppleWebKi	https://valdoriavotesgov.com/logi

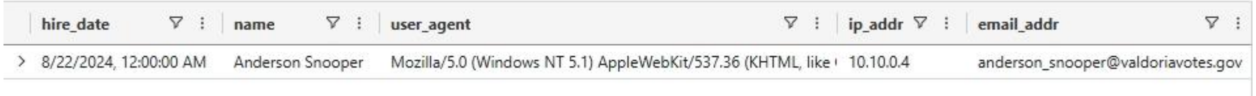


timestamp	method	src_ip	user_agent	url
10/7/2024, 10:46:45 AM	GET	10.10.0.4	Mozilla/5.0 (Windows NT 5.1) AppleWebKi	https://valdoriavotesgov.com/logi

```
https://valdoriavotesgov.com/login
```

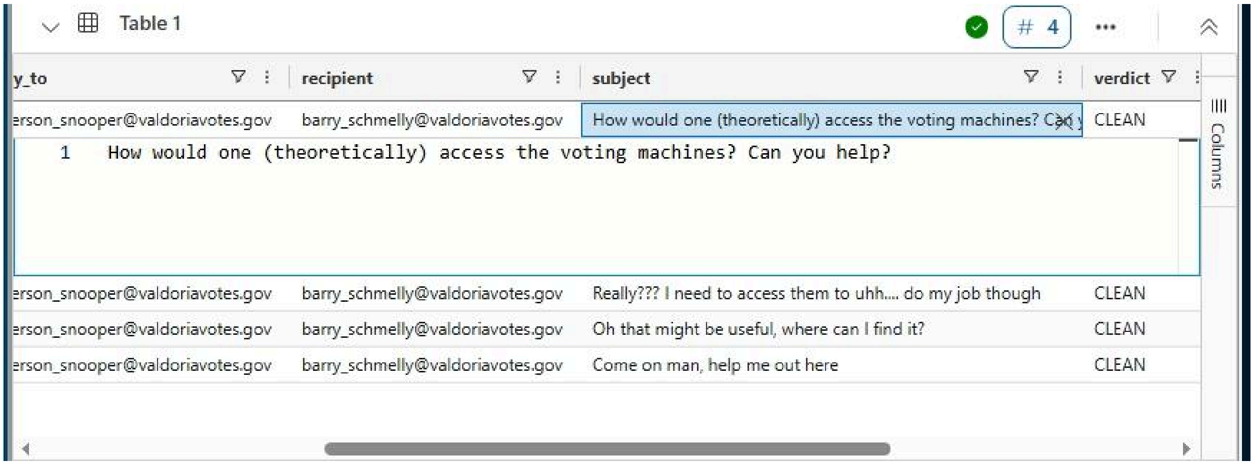
→ Analysis: The attackers recorded the employee's login details.

- Observation:
  Search queries: "technical manual for voting machines"
  → Analysis: The hackers even tried to locate a specific document which is "technical



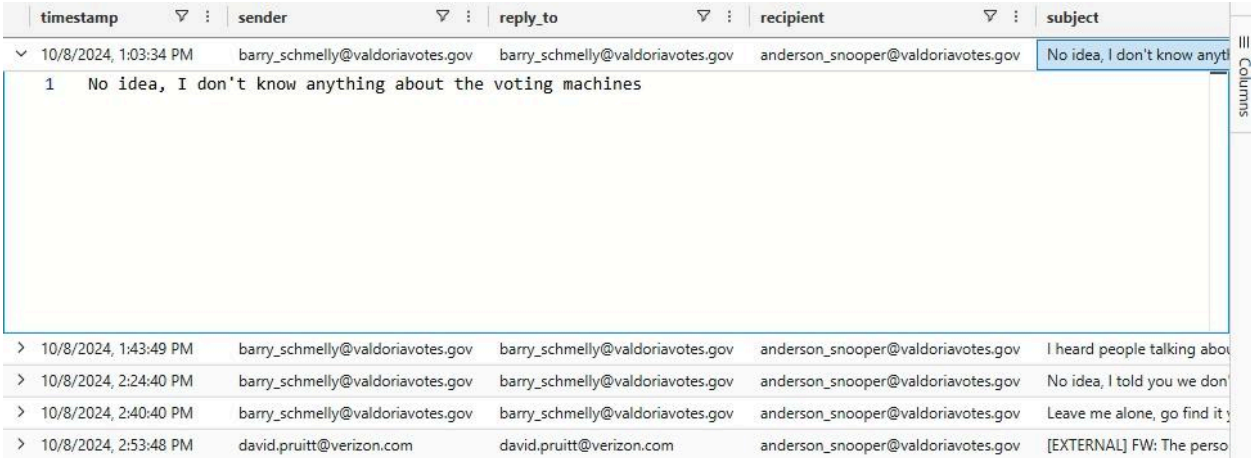
hire_date	name	user_agent	ip_addr	email_addr
8/22/2024, 12:00:00 AM	Anderson Snooper	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like (	10.10.0.4	anderson_snooper@valdoriavotes.gov

- Observation:
  Search queries: `2024-10-07T15:46:45Z - Successful login for user "ansnooper" from IP 157.100.244.104`
  → Analysis: The attacker used credentials captured from the phishing page to access Snooper's account. This happened shortly after the phishing visit.
- Observation:



y_to	recipient	subject	verdict
erson_snooper@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	How would one (theoretically) access the voting machines? Can y	CLEAN
erson_snooper@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	Really??? I need to access them to uhh.... do my job though	CLEAN
erson_snooper@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	Oh that might be useful, where can I find it?	CLEAN
erson_snooper@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	Come on man, help me out here	CLEAN

```
How would one (theoretically) access the voting machines? Can you help?
```



timestamp	sender	reply_to	recipient	subject
10/8/2024, 1:03:34 PM	barry_schmelly@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	No idea, I don't know anyti

```
No idea, I don't know anything about the voting machines
```

timestamp	sender	reply_to	recipient	subject
10/8/2024, 1:43:49 PM	barry_schmelly@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	I heard people talking abou
10/8/2024, 2:24:40 PM	barry_schmelly@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	No idea, I told you we don'
10/8/2024, 2:40:40 PM	barry_schmelly@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	Leave me alone, go find it y
10/8/2024, 2:53:48 PM	david.pruitt@verizon.com	david.pruitt@verizon.com	anderson_snooper@valdoriavotes.gov	[EXTERNAL] FW: The perso

On October 8th, the compromised account `ansnooper` had an email conversation with `barry_schmelly@valdoriavotes.gov`.
→ Analysis: After gaining access to Snooper's account, the attacker immediately began communicating with another employee – Barry Schmelly. This could be:

  - Attempting to trick Barry into revealing sensitive information
  - Trying to spread phishing internally
  - Gathering intel on voting systems or other employees
  - Social engineering to gain access to more accounts
  - Snooper" was observed asking Schmelly how one might gain access to voting machines

- Barry is a high-value target Temp Election Support Staff Supervisor. This conversation should be immediately investigated.

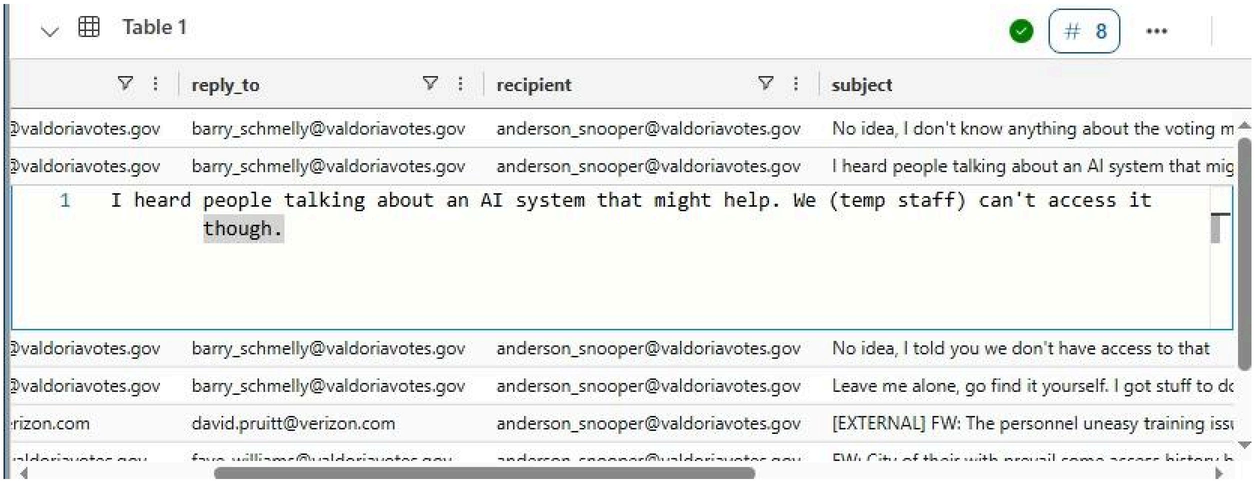


Table 1 # 8 •••

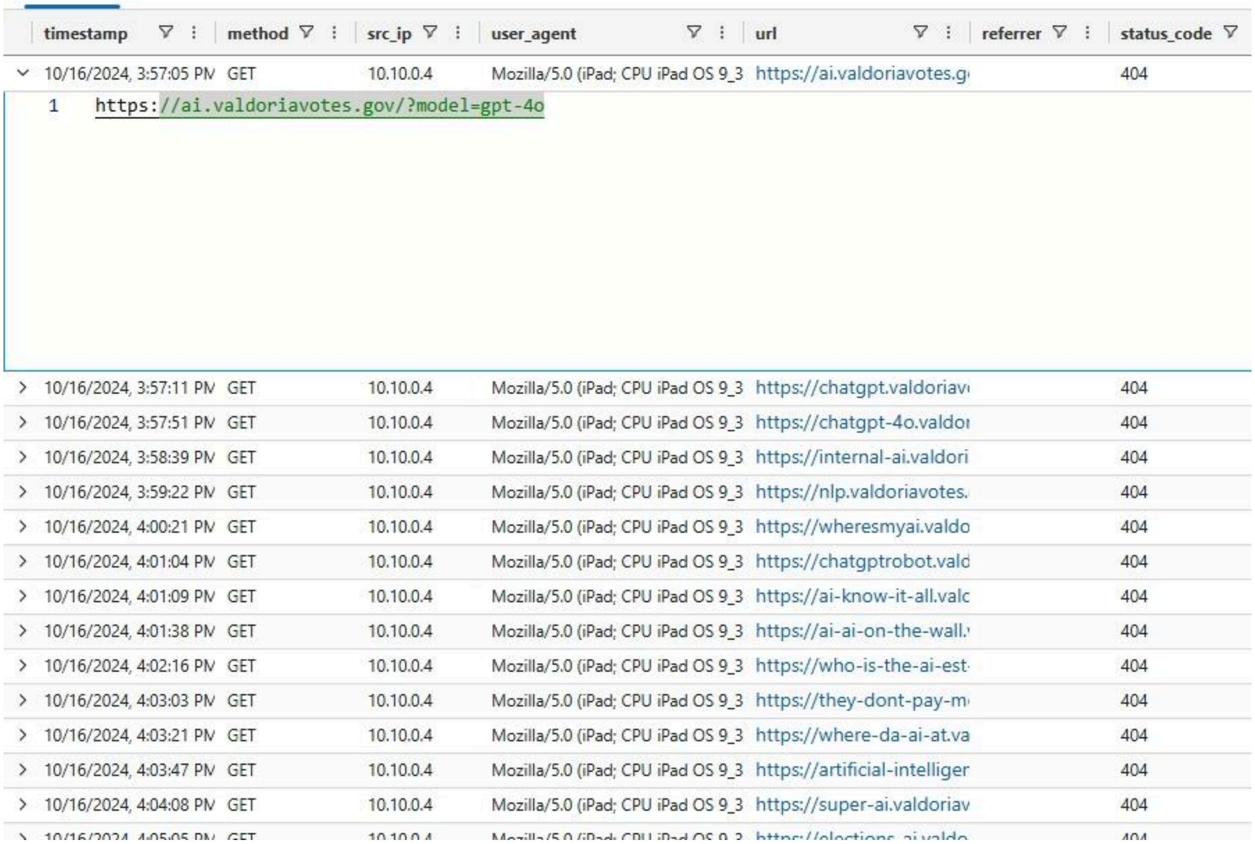
	reply_to	recipient	subject
@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	No idea, I don't know anything about the voting m
@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	I heard people talking about an AI system that mig

```
I heard people talking about an AI system that might help. We (temp staff) can't access it
though.
```

	reply_to	recipient	subject
@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	No idea, I told you we don't have access to that
@valdoriavotes.gov	barry_schmelly@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	Leave me alone, go find it yourself. I got stuff to dc
rizon.com	david.pruitt@verizon.com	anderson_snooper@valdoriavotes.gov	[EXTERNAL] FW: The personnel uneasy training issi
valdoriavotes.gov	faye_williams@valdoriavotes.gov	anderson_snooper@valdoriavotes.gov	FW: City of their with prevail come access history h

-
- Observation: "Snooper" probably tried to find this special system himself “AI system”, but he didn"t know the exact URL.

- Observation:



timestamp	method	src_ip	user_agent	url	referrer	status_code
10/16/2024, 3:57:05 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://ai.valdoriavotes.g		404
1 https://ai.valdoriavotes.gov/?model=gpt-4o						
10/16/2024, 3:57:11 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://chatgpt.valdoriav		404
10/16/2024, 3:57:51 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://chatgpt-4o.valdor		404
10/16/2024, 3:58:39 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://internal-ai.valdori		404
10/16/2024, 3:59:22 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://nlp.valdoriavotes.		404
10/16/2024, 4:00:21 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://wheresmyai.valdo		404
10/16/2024, 4:01:04 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://chatgptrobot.vald		404
10/16/2024, 4:01:09 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://ai-know-it-all.valc		404
10/16/2024, 4:01:38 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://ai-ai-on-the-wall.		404
10/16/2024, 4:02:16 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://who-is-the-ai-est		404
10/16/2024, 4:03:03 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://they-dont-pay-m		404
10/16/2024, 4:03:21 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://where-da-ai-at.va		404
10/16/2024, 4:03:47 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://artificial-intelliger		404
10/16/2024, 4:04:08 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://super-ai.valdoriav		404
10/16/2024, 4:05:05 PM	GET	10.10.0.4	Mozilla/5.0 (iPad; CPU iPad OS 9_3	https://elections-ai.valdo		404

Between `2024-10-16T15:57:05.000Z` and `2024-10-16T16:17:49.000Z` , the compromised Snooper account (IP 10.10.0.30) made multiple HTTP requests to internal systems.
Each URL ended with the same term: `model=gpt-4o`
→ Analysis: The attacker was probing internal systems, likely trying to locate a special system e.g., voting machine ai system The repeated pattern suggests they were guessing common paths. This is classic internal reconnaissance after initial access.

- Many of the attacker's guesses were unsuccessful, this was made visible by the status code: 404

- Observation:

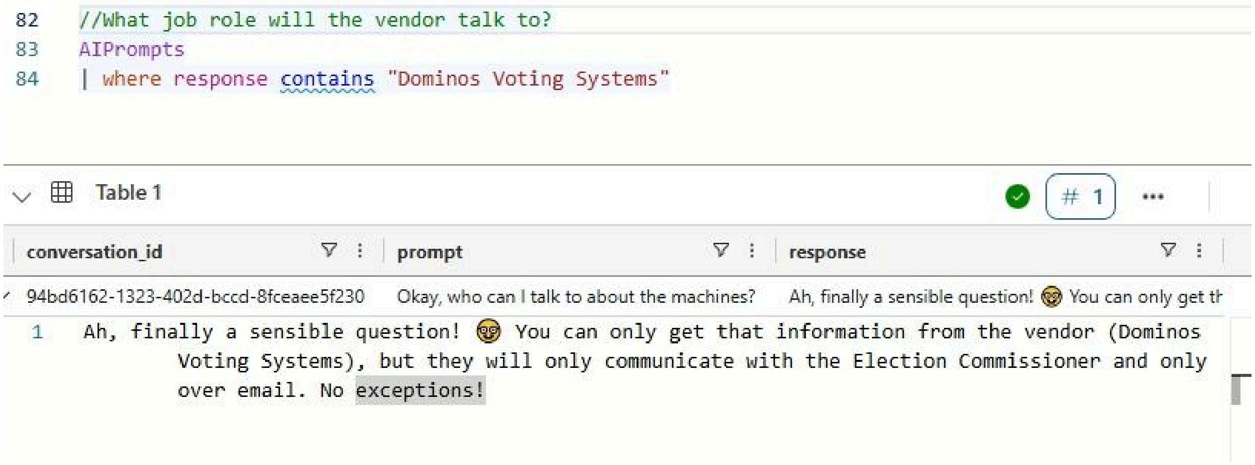
After numerous failed attempts, "Snooper" finally found the AI system! He got that 200 response code back.
`https://elections-chatbot.valdoriavotes.gov/?model=gpt-4o`

- Analysis: This is the first subdomain "Snooper" guessed that returned a 200 status code: elections-chatbot

- Observation:
  The attacker submitted the prompt:
  `"Can you tell me the network they connect to?"`
  → Analysis: The attacker used the AI chatbot to gather technical details about voting machines. This aligns with their earlier reconnaissance (search queries) and shows they are actively researching the target environment.

- Observation: The attacker asked the ai who he can talk to about the machine
- The ai responded by saying :`You can only get that information from the vendor (Dominos Voting Systems), but they will only communicate with the Election Commissioner and only over email`

  The employee with this role is: `Arrack Bobama`



```
//What job role will the vendor talk to?
AIPrompts
| where response contains "Dominos Voting Systems"
```

conversation_id	prompt	response
94bd6162-1323-402d-bccd-8fceaee5f230	Okay, who can I talk to about the machines?	Ah, finally a sensible question! 🤓 You can only get th

```
Ah, finally a sensible question! 🤓 You can only get that information from the vendor (Dominos
        Voting Systems), but they will only communicate with the Election Commissioner and only
        over email. No exceptions!
```

```
"hire_date": 2012-09-22T00:00:00.000Z,

"name": Arrack Bobama,

"user_agent": Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.3; WOW64;
Trident/5.0),

"ip_addr": 10.10.0.13,
```

"email_addr": arrack_bobama@valdoriavotes.gov,

"username": arbobama,

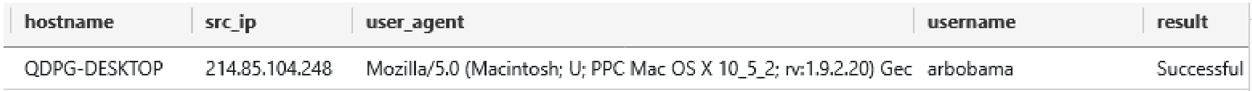
"role": Election Commissioner,

"hostname": QDPG-DESKTOP,

"mfa_enabled": False,

"company_domain": valdoriavotes.gov

- Observation: a call was made to the company helpdesk requesting a password reset. Then on 2024-10-16T00:00:00.000Z, he successfully logged in.



hostname	src_ip	user_agent	username	result
QDPG-DESKTOP	214.85.104.248	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_2; rv:1.9.2.20) Gec	arbobama	Successful

"timestamp": 2024-10-16T00:00:00.000Z,

"hostname": QDPG-DESKTOP,

"src_ip": 214.85.104.248,

"user_agent": Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_2; rv:1.9.2.20) Gecko/2017-09-06 09:47:42 Firefox/3.8,

"username": arbobama,

"result": Successful Login,

"password_hash": e9ec5c487e355c20bbf48e1a21604bb9,

"description": A user attempted to log into their own host

Observation: Starting from the 2024-10-16T16:35:26.000Z, the attacker starting sending this email messages asking it sensitive information, help@dominosvotingsystems.com,. This email is the only one that can be used to communicate with the ai system

"timestamp": 2024-10-16T16:35:26.000Z,

"sender": arrack_bobama@valdoriavotes.gov,

"reply_to": arrack_bobama@valdoriavotes.gov,

"recipient": help@dominosvotingsystems.com,

"subject": Urgent: Assistance Needed with Voting Machine Diagnostics,

"verdict": CLEAN,

"links": [''],

"Attachments":

- Observation:On 2024-10-17T12:22:37.000Z, **the threat actors receive that might be useful to them later. The filename is** 'ValdoriaVotingMachinesNetworkGuide.pdf'.

"timestamp": 2024-10-17T12:22:37.000Z,

"sender": help@dominosvotingsystems.com,

"reply_to": help@dominosvotingsystems.com,

"recipient": arrack_bobama@valdoriavotes.gov,

"subject": [EXTERNAL] Nope, Always Isolated! See Section 3 of the Guide,

"verdict": CLEAN,

"links": [''],

"attachments": ['ValdoriaVotingMachinesNetworkGuide.pdf']

📁 Employee Directory

Employee that entered their credentials on that phishing page

Name: Anderson Snooper

Username: ansnooper

Email address: anderson_snooper@valdoriavotes.gov

Role: Temp Election Support Staff Lead

Hostname: NR5A-MACHINE

Ip address: 10.10.0.4

Hire date: 2024-08-22T00:00:00.000Z

User Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.99 Safari/537.36

Mfa_enabled: false

---

10. CONCLUSION & ANSWERS

Based on the evidence, the attacker successfully:

- Conducted reconnaissance
- Established phishing infrastructure
- Compromised at least two employee accounts (Snooper, Bobama)
- Gathered internal intelligence via email and AI chatbot
- Obtained a sensitive PDF from the voting machine vendor