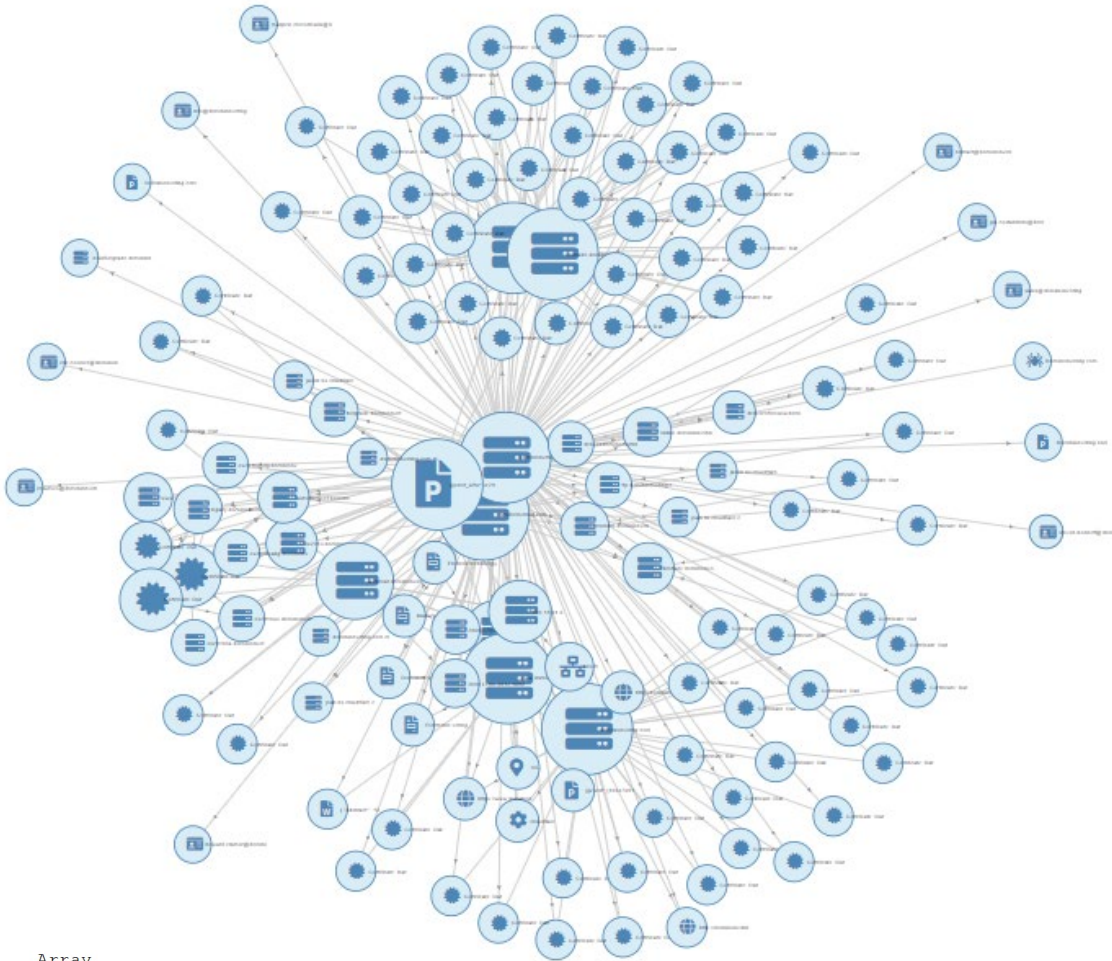


Declaration of [REDACTED]

Pursuant to 28 U.S.C Section 1746, [REDACTED] make the following declaration.

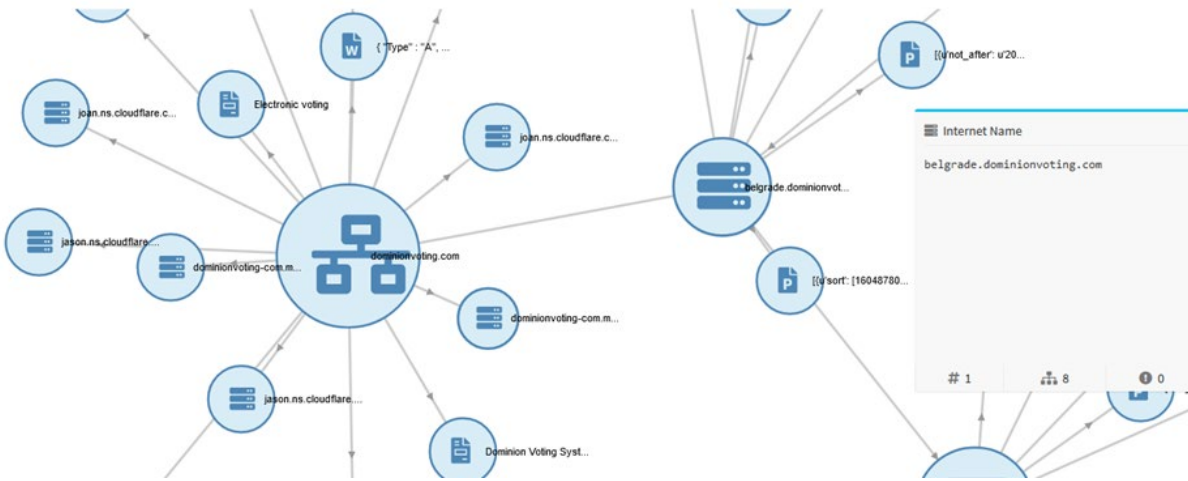
1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside [REDACTED] location in the United States of America.
4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,
7. A public network scan of Dominionvoting.com on 2020-11-08 revealed the following inter-relationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:



```
Array  
(  
  [id] => 544167324  
  [luser] => ian.macvicar  
  [domain] => dominionvoting.com  
  [password] => jamley  
)
```

```
7  
Array  
(  
  [id] => 599400504  
  [luser] => jelena.tanaskovic  
  [domain] => dominionvoting.com
```

8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:



→ robtex.com/dns-lookup/dominionvoting.com

8 results shown.

IP numbers of the name servers	Subdomains/Hostnames
2400:cb00:2049:1::adf5:3bb3	Domains or hostnames one step under this dom
2606:4700:50::adf5:3aad	barracuda.dominionvoting.com
2803:f800:50::6ca2:c0ad	belgrade.dominionvoting.com
2803:f800:50::6ca2:c1b3	webmail.dominionvoting.com
2a06:98c1:50::ac40:20ad	www.dominionvoting.com
108.162.192.173	4 results shown.
108.162.193.170	

9. A cursory search on LinkedIn of “dominion voting” on 11/19/2020 confirms the numerous employees in Serbia:

Vukašin Đorđević • 3rd
Software Developer at Dominion Voting Systems
Serbia

Edvan Sabanovic • 3rd
Senior Full-stack Web Developer
Belgrade, Serbia
Past: Senior Web Developer at Dominion Voting Systems

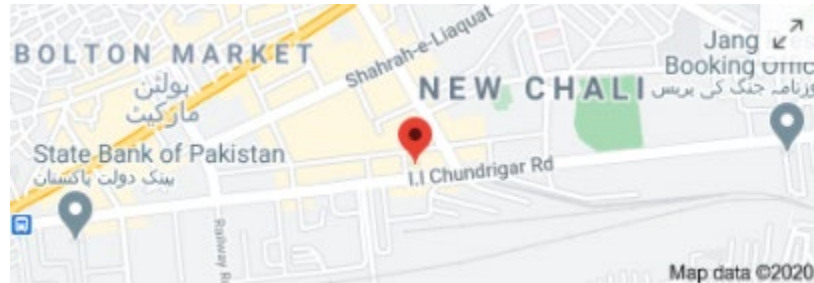
10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:



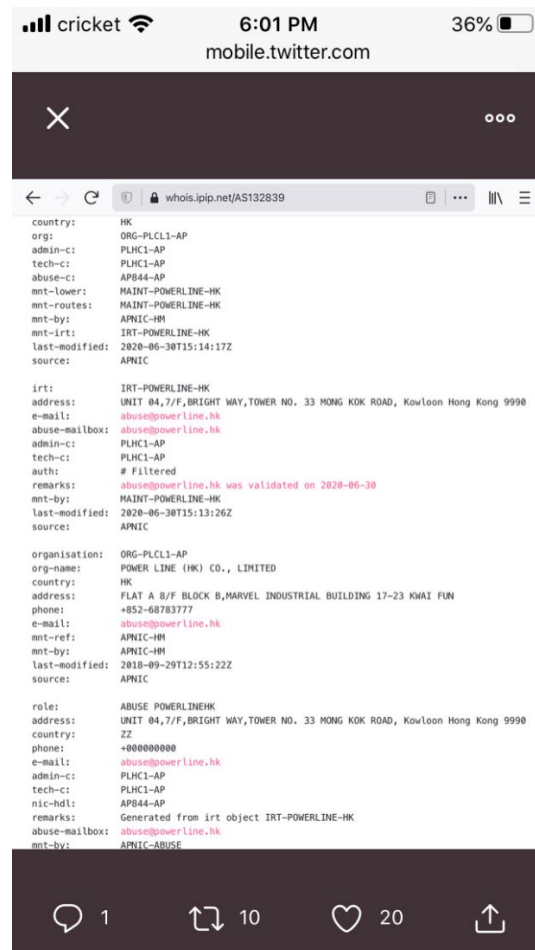
Inputting the Iranian IP into Robtex confirms the direct connection into the “edisonresearch” host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.



A deeper search of the ownership of Edison Research “edisonresearch.com” shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the “vps” at the start of the internet name:



Dominionvoting is also dominionvotingsystems.com, of which there are also many more examples, including access of the network from China. The records of China accessing the server are reliable.



CHINA UNICOM China169 Backbone - Fraud Risk

Low Risk

← Lowest Risk Highest Risk →

0 Fraud Score: 3 100

We consider **CHINA UNICOM China169 Backbone** to be a potentially low fraud risk ISP, by which we mean that web traffic from this ISP potentially poses a low risk of being fraudulent. Other types of traffic may pose a different risk or no risk. They operate 1,889,865 IP addresses, some of which are running

6 77 126

Domain Name: [dominionvotingsystems.com](http://www.dominionvotingsystems.com)
 Registry Domain ID: 2530599738_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.godaddy.com
 Registrar URL: <http://www.godaddy.com>
 Updated Date: 2020-05-26T15:48:58Z
 Creation Date: 2020-05-26T15:48:57Z
 Registrar Registration Expiration Date: 2021-05-26T15:48:57Z
 Registrar: GoDaddy.com, LLC
 Registrar IANA ID: 146
 Registrar Abuse Contact Email: abuse@godaddy.com
 Registrar Abuse Contact Phone: +1.4806242505
 Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
 Domain Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
 Domain Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
 Domain Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
 Registrant Organization:
 Registrant State/Province: Hunan
 Registrant Country: CN
 Registrant Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
 Admin Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
 Tech Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
 Name Server: NS1.DNS.COM
 Name Server: NS2.DNS.COM
 DNSSEC: unsigned

Overview - [dominionvotingsystems.com](#)

DNS Records 4

Type	Value	OSH	Security score
A	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	15
NS	ns1.dns.com 27.152.186.193 - AS133776 - Quanzhou	9	100
	119.167.180.131 - AS4837 - CHINA UNICOM China169 Bac...	8	100
	218.96.111.202 - AS21859 - ZNET	14	100
NS	ns2.dns.com 183.253.57.193 - AS9808 - Guangdong Mobile Communic...	6	100
	121.12.104.65 - AS134763 - CHINANET Guangdong provin...	4	100
SOA	ns1.dns.com Hostname dnsadmin.dns.com		

[View all DNS Records](#)

Domains with same A records - [dominionvotingsystems.com](#)

1 Domains with same A records

Domain	Site Title	Alexa rank	DNS A	OSH	DNS CNAME
boanglobal.com	-	-	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	-

CVE - [dominionvotingsystems.com](#)

22 CVE

ID	Base Score	Severity	Vector	Source	Description
CVE-2018-20685	2.6	LOW	AV:N/A/C/M:N/C/N:P/N	45.195.162.194	In OpenSSH 7.8, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of, or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2019-4564	6.9	MEDIUM	AV:N/A/C/M:N/C/C/C/C	45.195.162.194	Use-after-free vulnerability in the mkn_ansvar_pam_base_ctx function in monitor.c in sshd in OpenSSH before 7.8 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.
CVE-2016-1908	7.5	HIGH	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.
CVE-2016-19010	6.9	MEDIUM	AV:N/A/C/M:N/C/C/C/C	45.195.162.194	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.
CVE-2016-6155	7.8	HIGH	AV:N/A/C/M:N/N/A/C	45.195.162.194	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2015-5680	8.5	HIGH	AV:N/A/C/M:N/C/N/A/C	45.195.162.194	The libidn2_init_device function in auth2-chall.c in sshd in OpenSSH through 6.8 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh-askpassInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.
CVE-2015-4843	1.9	LOW	AV:N/A/C/M:N/C/N/P/N	45.195.162.194	The monitor component in sshd in OpenSSH before 7.8 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_UNT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PAM_UNT request, related to monitor_auth.c.
CVE-2018-15819	5	MEDIUM	AV:N/A/C/M:N/C/N/N/A/N	45.195.162.194	Remotely observable behaviour in auth_gss.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSSAPI is in use. NOTE: the discover status. We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.
CVE-2020-15778	6.8	MEDIUM	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	scp in OpenSSH through 8.3p1 allows command injection in the scp.c:tomore function, as demonstrated by backslash characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."
CVE-2019-6130	4	MEDIUM	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	In OpenSSH 7.8, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-the-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
CVE-2016-19011	2.1	LOW	AV:L/A/C/M:N/C/N/P/N	45.195.162.194	auth2.c in sshd in OpenSSH before 7.4 does not properly consider the effects of malloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2016-19013	7.2	HIGH	AV:L/A/C/M:N/C/C/C/C	45.195.162.194	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all variables, which might allow local users to gain privileges by leveraging access to a standardized privilege separation process, related to the m_block and m_sib data structures.
CVE-2013-5352	4.3	MEDIUM	AV:N/A/C/M:N/C/N/P/P	45.195.162.194	The x11_open_helper function in channel.c in ssh in OpenSSH before 6.8, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.
CVE-2011-8225	7.2	HIGH	AV:L/A/C/M:N/C/C/C/C	45.195.162.194	The do_setup_env function in session.c in sshd in OpenSSH through 7.3p1, when the UseLogin feature is enabled and PAM is configured to read pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
CVE-2016-19009	7.5	HIGH	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent socket.
CVE-2016-12708	5	MEDIUM	AV:N/A/C/M:N/C/N/P/P	45.195.162.194	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
CVE-2019-6109	4	MEDIUM	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	An issue was discovered in OpenSSH 7.8. Due to missing character encoding in the progress display, a malicious server (or Man-in-the-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2016-6220	4.3	MEDIUM	AV:N/A/C/M:N/C/P/N/A/N	45.195.162.194	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2020-14145	4.3	MEDIUM	AV:N/A/C/M:N/C/P/N/A/N	45.195.162.194	The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows in-the-middle attackers to target initial connection attempts (before no host key for the server has been cached by the client).
CVE-2016-3115	5.5	MEDIUM	AV:N/A/C/M:N/C/P/P/P	45.195.162.194	Multiple CVE injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated() and (2) session_x11_req functions.

11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

This domain redirects to **beanfield.com**

DNS

View domain name system records, including but not limited to the A, CNAME, MX, and TXT records. View API →

A	96.45.195.194	5 Domains →
MX	10 barracuda.dominionvoting.com.	2 Domains →
NS	ns29.domaincontrol.com.	56,979,357 Domains →
	ns30.domaincontrol.com.	56,979,357 Domains →

Co-Hosted

There are **5 domains** hosted on **96.45.195.194** (AS21949 Beanfield Technologies Inc.). Show All → View API →

guta.ca	ndbgroup.ca	dvscorp.com
aiyokuacardioulounge.com	grantdyer.com	

This Dominion partner domain “dvscopr” also includes an auto discovery feature, where new in-network devices automatically connect to the system. The following diagram shows some of the related dvscopr.com mappings, which mimic the infrastructure for Dominion and are an obvious typo derivation of the name. Typo derivations are commonly purchased to catch redirect traffic and sometimes are used as honeypots. The diagram shows that infrastructure spans multiple different servers as a methodology.

The screenshot shows a network analysis tool interface with the following details:

- Page Title:** dvs
- Navigation:** Overview, Correlations, Browse by, Starred, Visualize, Settings, Logs.
- Data Summary:** Data Type: Similar Domain (10 results)
- Table:**

Data Element	Source Data Element
Similar Domain TLD Searcher 1 0 1 0 dvscopr.ايران.ir	Internet Name SpiderFoot UI 9 0 0 1 dvscopr.com
Similar Domain Tool - DNSTwist 1 0 1 1 0 dv.scopr.com	Domain Name SpiderFoot UI 7 0 0 1 dvscopr.com
Similar Domain Tool - DNSTwist 1 0 1 1 0 dvscorp.com	Domain Name SpiderFoot UI 7 0 0 1 dvscopr.com
Similar Domain TLD Searcher 0 0 0 1 1 0 dvscopr.台湾	Internet Name SpiderFoot UI 9 0 0 1 dvscopr.com
Similar Domain TLD Searcher 0 0 0 1 1 0 dvscopr.fin.ci	Internet Name SpiderFoot UI 9 0 0 1 dvscopr.com

<input type="checkbox"/> <p>Domain Name: DSVCORP.COM Registry Domain ID: 134773082_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.bookmyname.com Registrar URL: http://www.bookmyname.com Updated Date: 2020-09-13T10:00:07Z</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain - Whois Whois 0 0 2 1 % This is the IIRNIC Whois server v1.6.2. % Available on web at http://whois.nic.ir/ % Find the terms and conditions of use on http://www.nic.ir/ % % This server uses HTTP 8 as the protocol for requests and responses</p>	dsvcorp. ایران
<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 1 dsvcorp.caa.li</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 1 dsvcorp.hasura-app.io</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 1 dsvcorp.rackmaze.com</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 1 dsvcorp.devices.resinstaging.io</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 1 dsvcorp.cust.dev.thingdust.io</p>	dsvcorp.com

The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:

<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 1 dsvcorp.台湾 Chinese Domain</p>
<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 1 dsvcorp.fin.ci</p>

15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame 050500/0236	Execution date Sep 25, 2019	Date recorded Sep 26, 2019	Pages 7
Conveyance SECURITY AGREEMENT			
Assignors DOMINION VOTING SYSTEMS CORPORATION	Correspondent CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020		Attorney docket
Assignee HSBC BANK CANADA, AS COLLATERAL AGENT 4TH FLOOR, 70 YORK STREET TORONTO M5J 1S9 CANADA			

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

[View all](#)

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function—the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Release 2.0.0 | [Release Notes](#) | [Send Feedback](#) | [Legacy Patent Assignment Search](#) | [Legacy Trademark Assignment Search](#)

Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:

Patent assignment 050500/0236

SECURITY AGREEMENT [🔗](#)

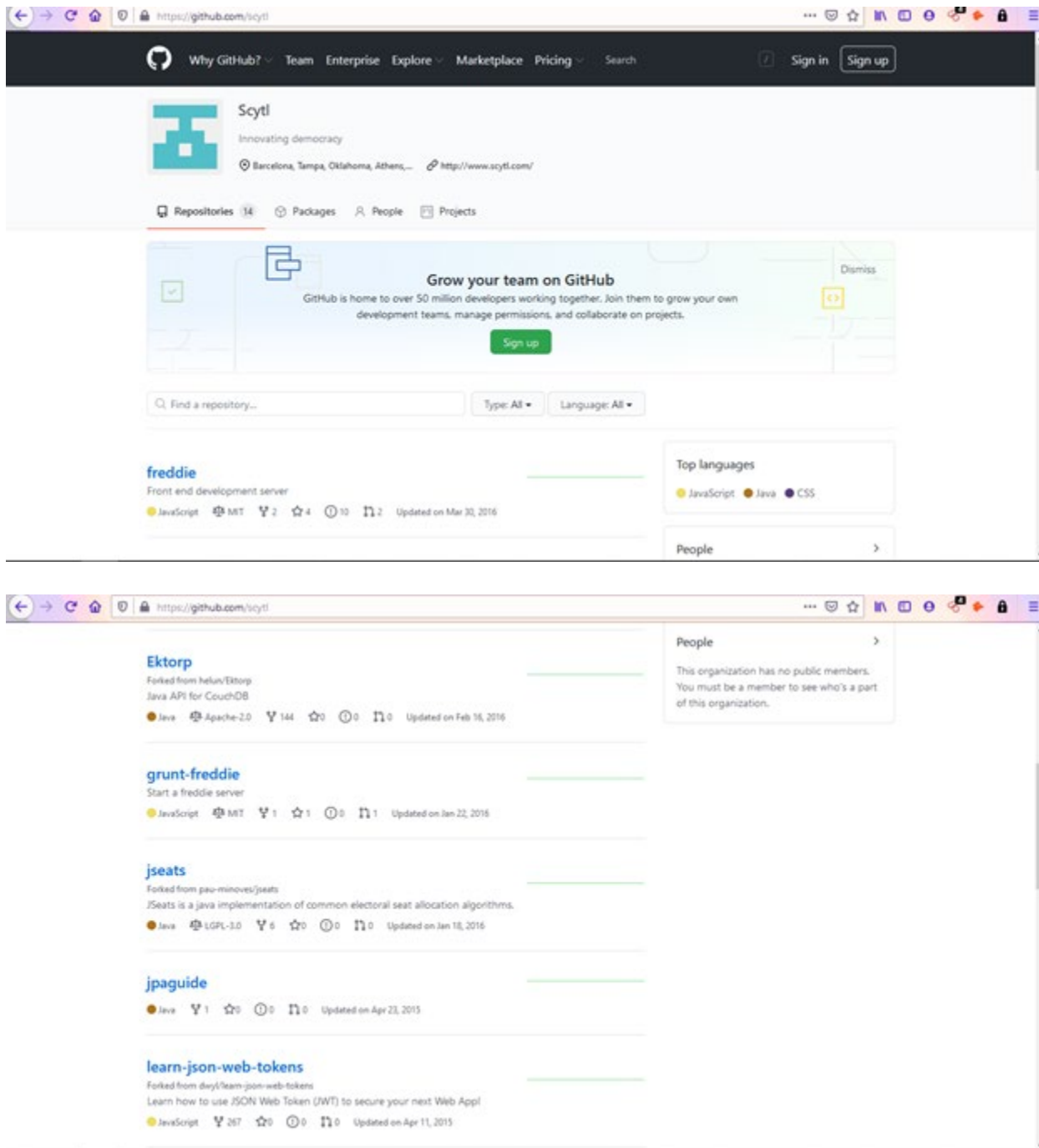
Date recorded Sep 26, 2019	Reel/frame 050500/0236	Pages 7
Assignors DOMINION VOTING SYSTEMS CORPORATION	Execution date Sep 25, 2019	
Assignee HSBC BANK CANADA, AS COLLATERAL AGENT 4TH FLOOR, 70 YORK STREET TORONTO M5J 1S9 CANADA	Correspondent CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020	

Properties (18 total)

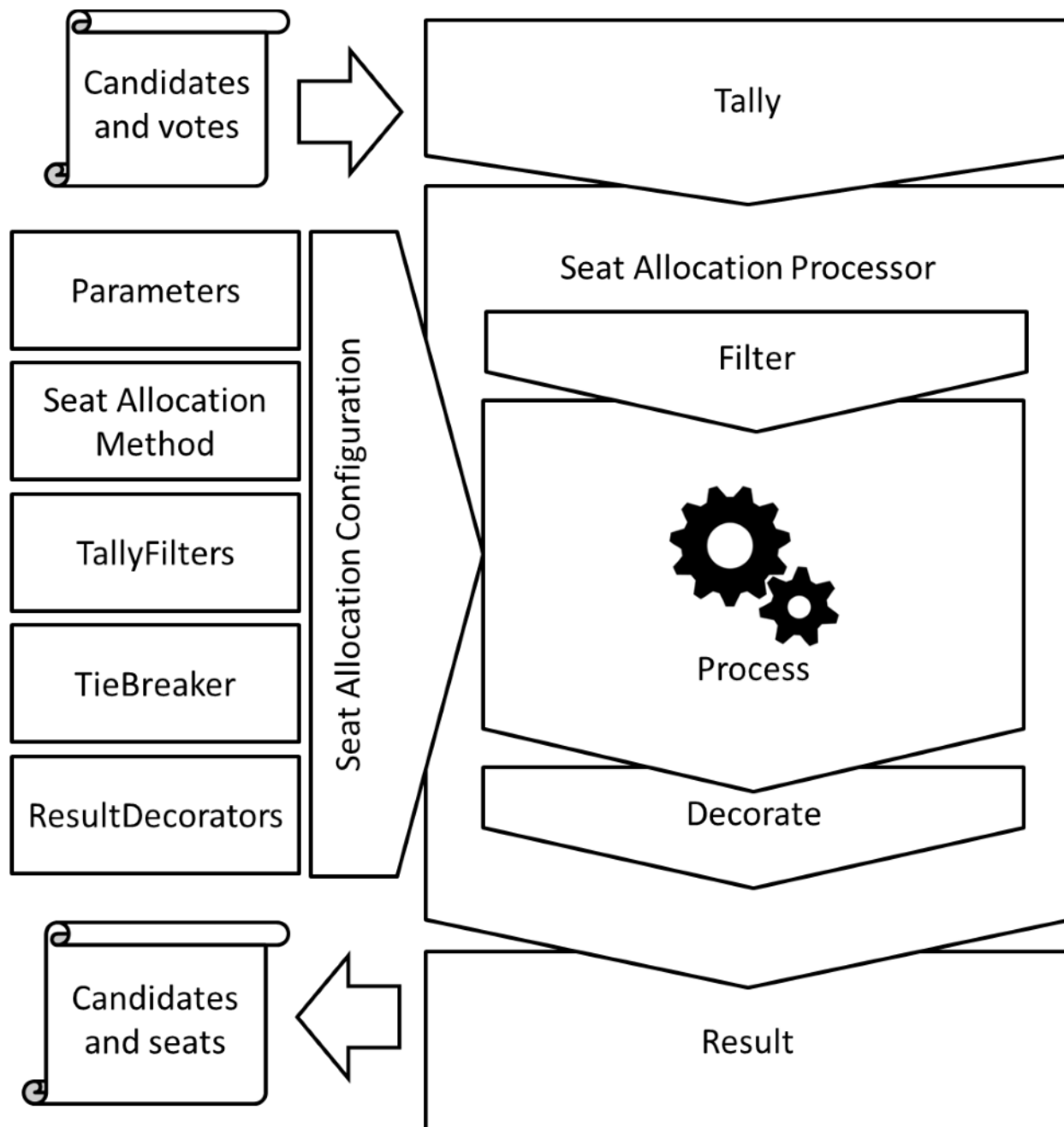
Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN POULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC		
8195505 Jun 5, 2012	20050247783 Nov 10, 2005	11121997 May 5, 2005
3. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7422151 Sep 9, 2008	20070012767 Jan 18, 2007	11526028 Sep 25, 2006
4. BALLOT LEVEL SECURITY FEATURES FOR OPTICAL SCAN VOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION Inventors: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN		



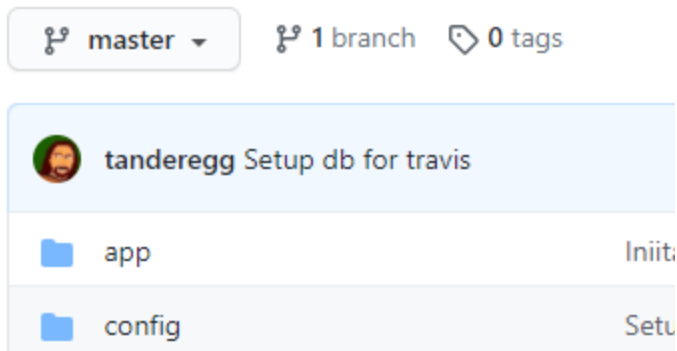
17. Smartmatic creates the backbone (like the cloud). SCYTL is responsible for the security within the election system.



18. In the GitHub account for ScytI, ScytI Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. Unrelated, but also a point of interest is CTCL or Center for Tech and Civic Life funded by Mark Zuckerberg. Within their github page (<https://github.com/ctcl>), one of the programmers holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



Tim Anderegg

tanderegg

Follow

...

38 followers · 23 following · 133

Consumer Financial Protection Bureau

Washington DC

20. As seen in included document titled

“AA20-304A-

Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data” that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.

21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 23th, 2020.

