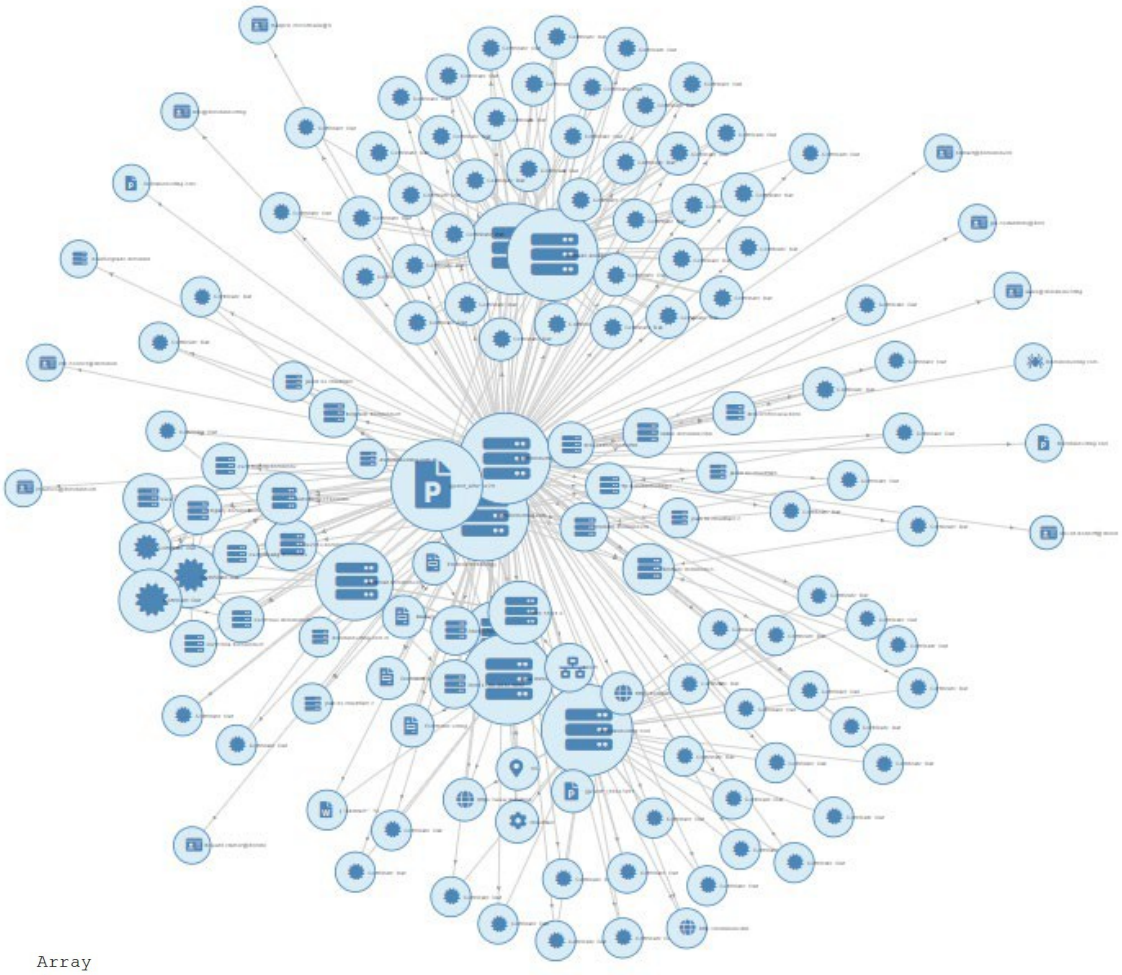
宣言 [redacted] XXX

28 U.S.C. Section 1746に従い、以私の宣言を行う [redacted]。

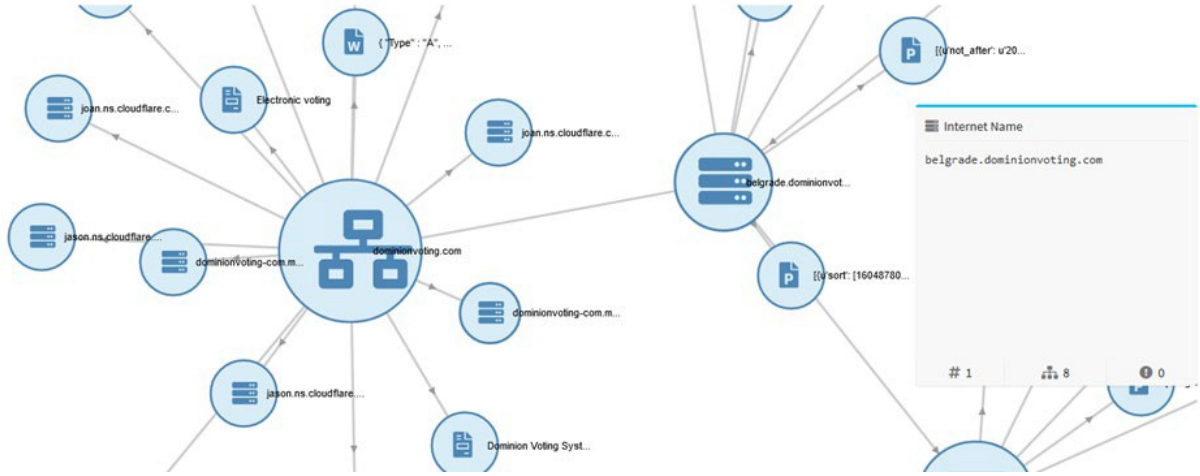
1. 私は21歳以上で、法律上の障害がないために、私は
   この宣言をすることから
2. 私は第305軍事情報部の電子情報アナリストで、SAMミサイルシステムの電子情報を収集した経験があります。私は、世界のトップ選挙の専門家のいくつかによって使用されているホワイトハットハッカーとしての豊富な経験を持っています。私が採用した方法論は、デジタルフォレンジックとOSINTのための業界標準のサイバー操作ツールキットを代表するもので、サーバー、ネットワークノード、およびその他のデジタルプロパティ間の接続を認証し、ネットワークシステムの脆弱性を探るために一般的に使用されています。
3. 私はアメリカ市民で、場所は[redacted]アメリカに住んでいます。
4. ドミニオンとエジソンリサーチのシステムがモノのインターネットに存在するのに対し、これにより、ドミニオン、エジソンリサーチ、および関連するネットワークノード間のネットワーク接続がスキャン可能になります。
5. そして、エジソンリサーチの主な仕事は、集計ソフトから受け取った投票情報の集計結果を報告し、選挙結果を決定本部に提供することであるのに対し、エジソンリサーチの主な仕事は、集計ソフトから受け取った投票情報の集計結果を報告し、決定本部に提供することです。
6. また、SpiderfootとRobtexがネットワークセキュリティとインフラストラクチャを評価するための業界標準のデジタルフォレンジックツールであるのに対し、これらのツールは前述のDominionとEdison
   Researchのシステムのパブリックセキュリティスキャンを実施するために使用されました。
7. 2020-11-
   08日のDominionvoting.comのパブリックネットワークスキャンにより、以下の相互関係が明らかになり、Dominion社員の暗号化されていないパスワードが13個、TORノードで利用可能なハッシュ化されたパスワードが75個明らかになりました。

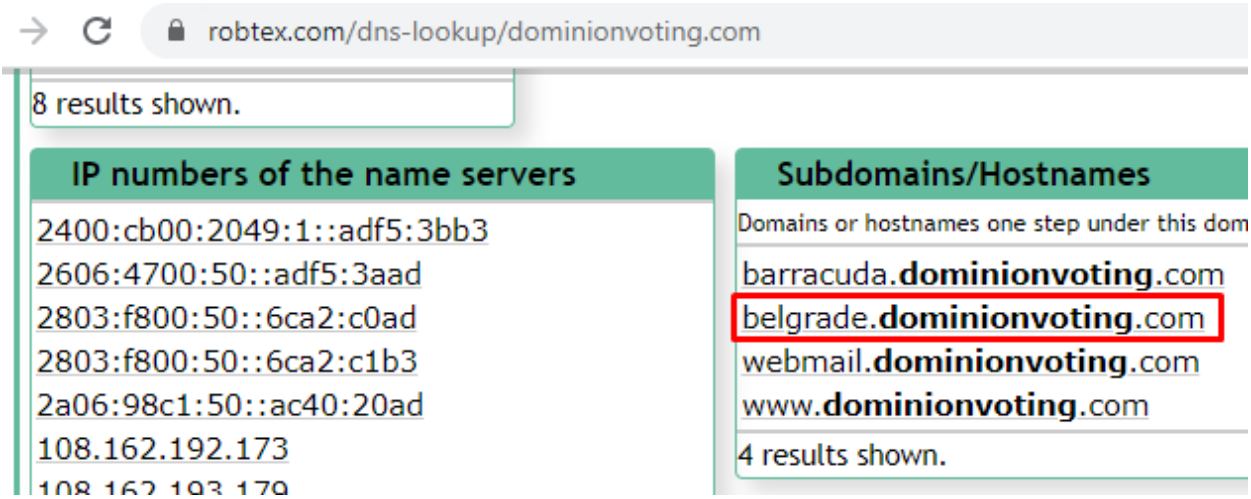


```
Array
(
    [id] => 544167324
    [luser] => ian.macvicar
    [domain] => dominionvoting.com
    [password] => jamley
)

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

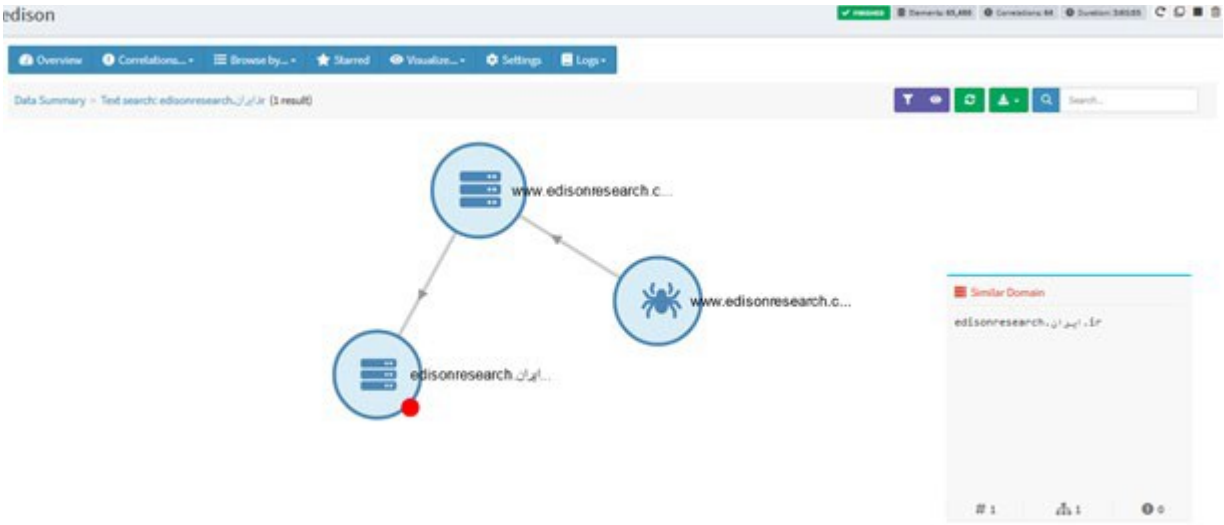
8. また、同じパブリックスキャンでは、以下のようにベオグラードのグループとの直接のつながりが強調されていました。





9. LinkedInで11/19/2020の「ドミニオン投票」を検索すると、セルビアの多数の従業員がいることが確認された。

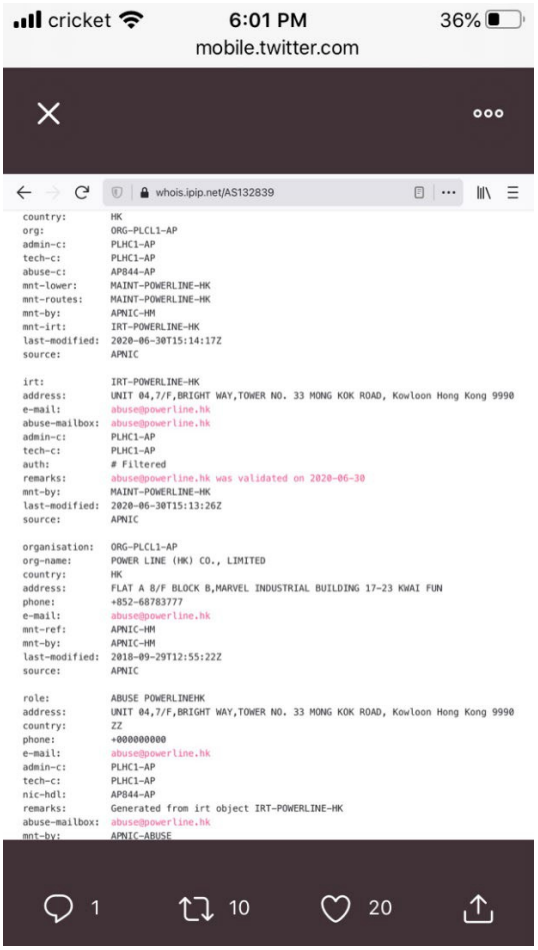
10. 2020-11-
08でエジソンリサーチを追加検索したところ、エジソンリサーチにはイランのサーバーがあることがわかりました。

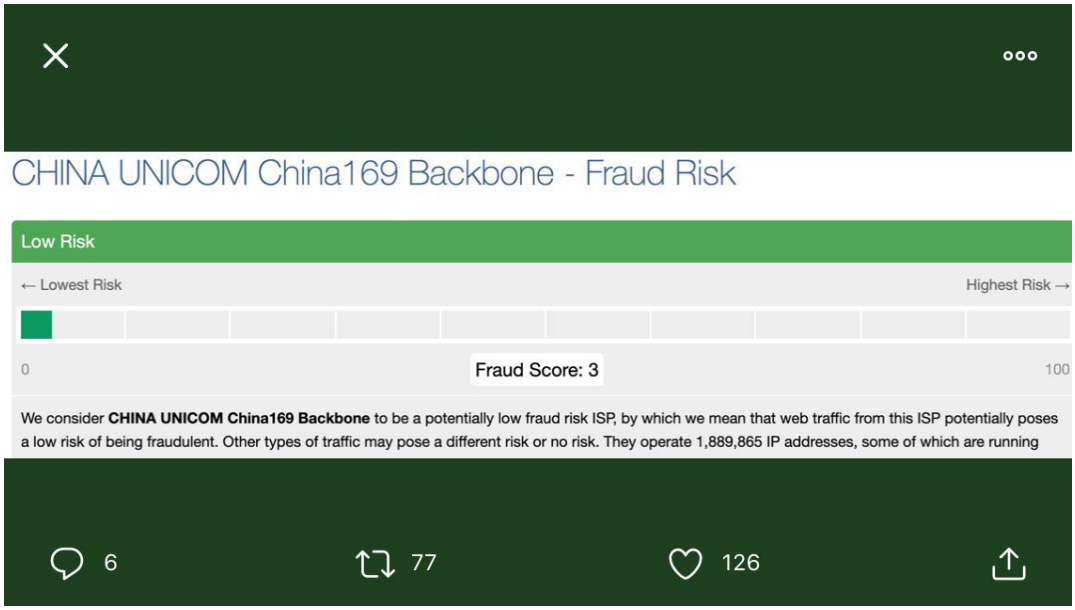


イランのIPをRobtexに入力すると、イランドメインの観点からも"edisonresearch"ホストへの直接接続を確認することができます。つまり、一方向参照の接続であった可能性はないということです。

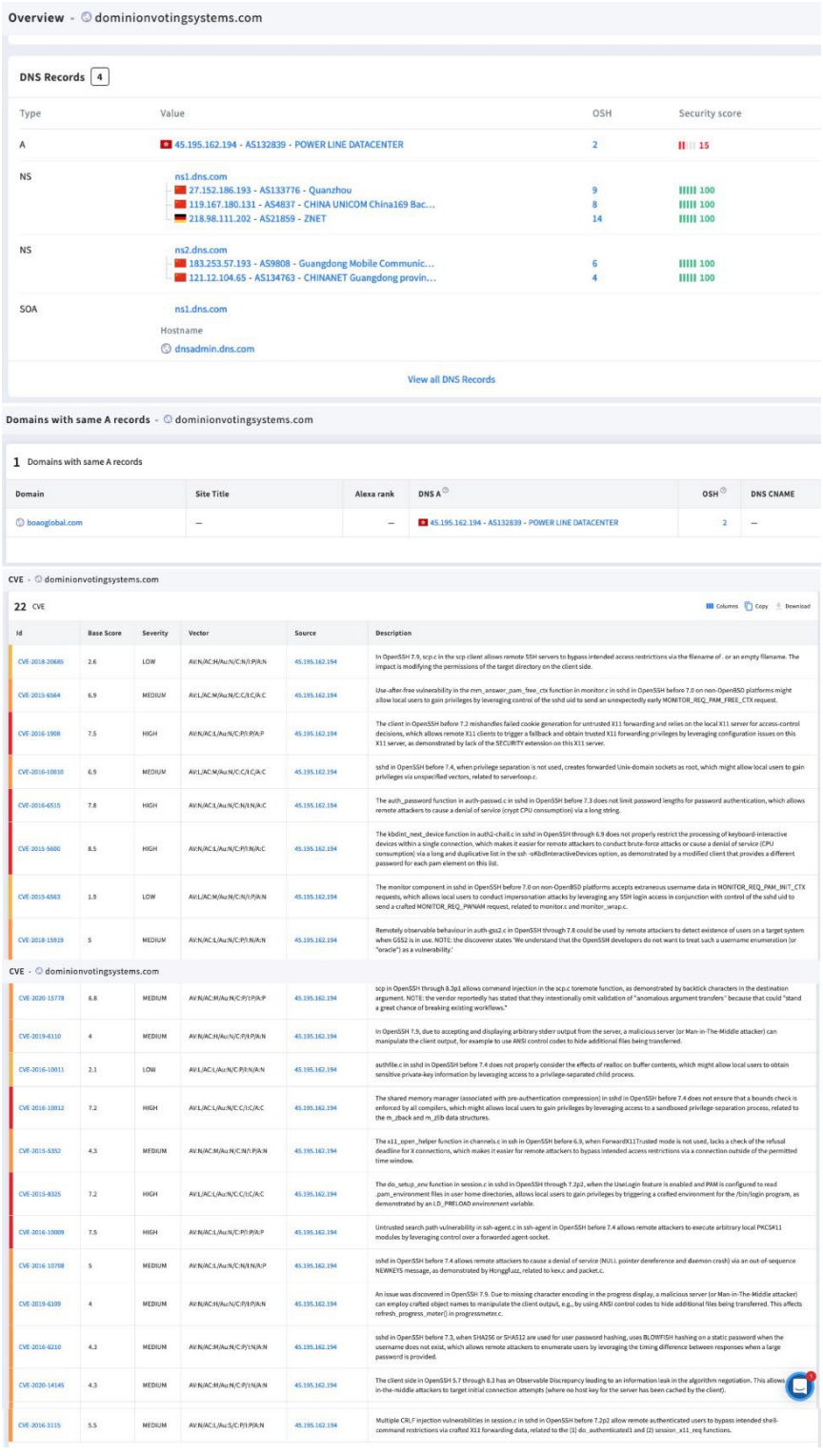
エジソンリサーチ「edisonresearch.com」の所有権を深く検索してみると、BMA Capital Managementとの接続が示されており、shareofear.comとbmacapital.comは、インターネット名の先頭にある「vps」で示されるように、VPSまたは仮想プライベートサーバーを経由してedisonresearch.comに接続されています。

Dominionvotingはdominionvotingsystems.comでもありますが、そのうち中国からのアクセスも含めて他にもたくさんの例があります。中国からのアクセス記録は信頼できるサーバーです。





Domain Name: 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
	218.98.111.202 - 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
boaoglobal.com	–	–	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	–

CVE - dominionvotingsystems.com

22 CVE

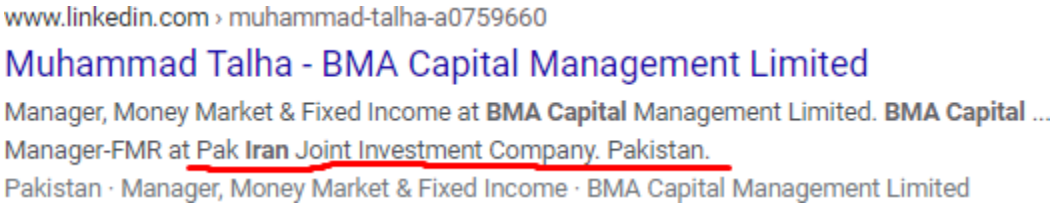
Columns Copy Download

Id	Base Score	Severity	Vector	Source	Description
CVE-2018-20685	2.6	LOW	AV:N/AC:H/Au:N/C:N/I:P/A:N	45.195.162.194	In OpenSSH 7.9, 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-2015-6564	6.9	MEDIUM	AV:L/AC:M/Au:N/C:C/I:C/A:C	45.195.162.194	Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 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/AC:L/Au:N/C:P/I:P/A: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-2016-10010	6.9	MEDIUM	AV:L/AC:M/Au:N/C:C/I:C/A: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-2016-6515	7.8	HIGH	AV:N/AC:L/Au:N/C:N/I: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-2015-5600	8.5	HIGH	AV:N/AC:L/Au:N/C:P/I:N/A:C	45.195.162.194	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 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 -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.
CVE-2015-6563	1.9	LOW	AV:L/AC:M/Au:N/C:N/I:P/A:N	45.195.162.194	The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_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_PWNAM request, related to monitor.c and monitor_wrap.c.
CVE-2018-15919	5	MEDIUM	AV:N/AC:L/Au:N/C:P/I:N/A:N	45.195.162.194	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

CVE - dominionvotingsystems.com

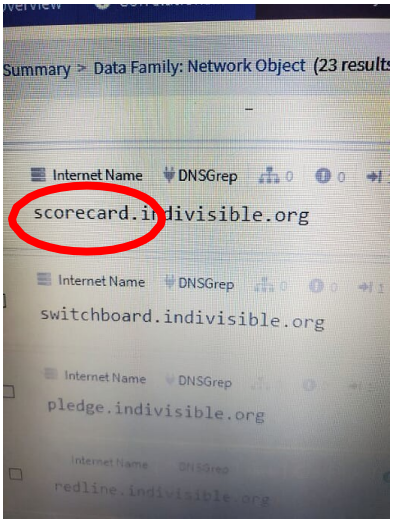
CVE-2020-15778	6.8	MEDIUM	AV:N/AC:M/Au:N/C:P/I:P/A:P	45.195.162.194	scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."
CVE-2019-6110	4	MEDIUM	AV:N/AC:H/Au:N/C:P/I:P/A:N	45.195.162.194	In OpenSSH 7.9, 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-2016-10011	2.1	LOW	AV:L/AC:L/Au:N/C:P/I:N/A:N	45.195.162.194	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2016-10012	7.2	HIGH	AV:L/AC:L/Au:N/C:C/I:C/A: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 compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.
CVE-2015-5352	4.3	MEDIUM	AV:N/AC:M/Au:N/C:N/I:P/A:N	45.195.162.194	The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, 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-2015-8325	7.2	HIGH	AV:L/AC:L/Au:N/C:C/I:C/A:C	45.195.162.194	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, 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-2016-10009	7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A: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-2016-10708	5	MEDIUM	AV:N/AC:L/Au:N/C:N/I:N/A: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/AC:H/Au:N/C:P/I:P/A:N	45.195.162.194	An issue was discovered in OpenSSH 7.9. 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-2016-6210	4.3	MEDIUM	AV:N/AC:M/Au:N/C:P/I: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/AC:M/Au:N/C:P/I: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 (where no host key for the server has been cached by the client).
CVE-2016-3115	5.5	MEDIUM	AV:N/AC:L/Au:S/C:P/I:P/A:N	45.195.162.194	Multiple CRLF 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_authenticated1 and (2) session_x11_req functions.

11. BMA Capital
Managementはイランの資本市場へのアクセスを提供する企業として知られており、LinkedInで公開されている直接リンクを使って発見することができます（2020年11月19日にgoogle経由で発見）。

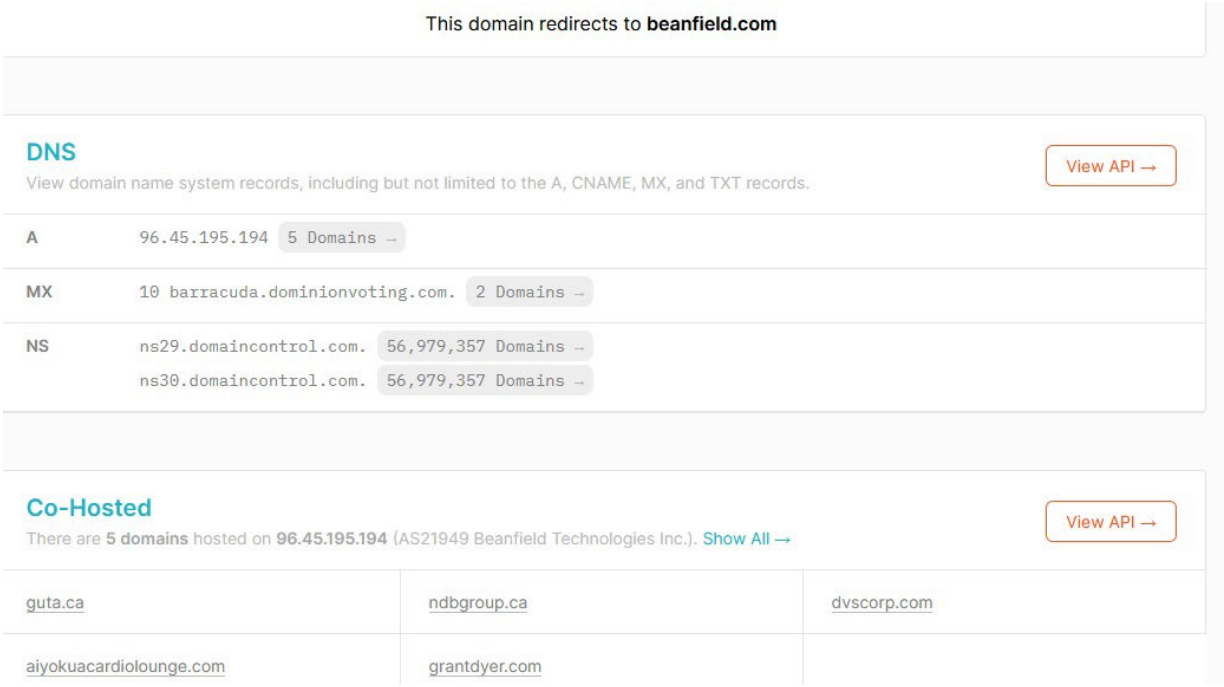


同じRobtexの検索では、イランのアドレスがオランダのサーバーに関連付けられていることが確認されており、イランがオランダをリモートサーバーとして使用しているという既知のOSINTと相関しています(Advanced Persistent Threats: APT33とAPT34を参照)。

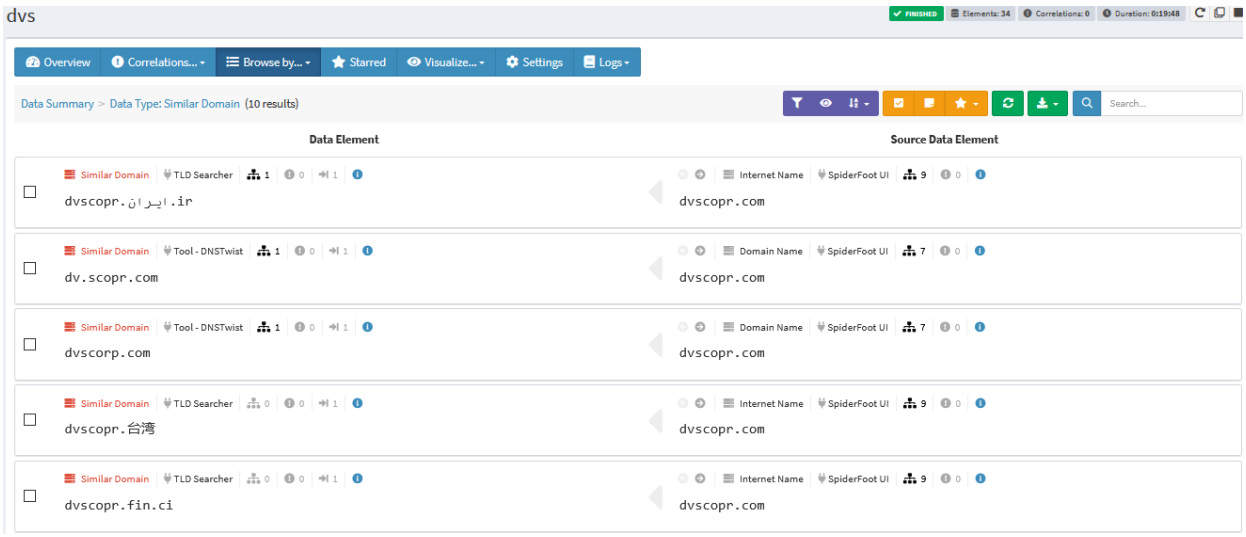
12. indivisible.orgネットワークの検索は、オバマのためのIndivisible(旧ACORN)政治グループの一部として使用されているスコアカード・ソフトウェアの存在を証明するサブドメインを示した。

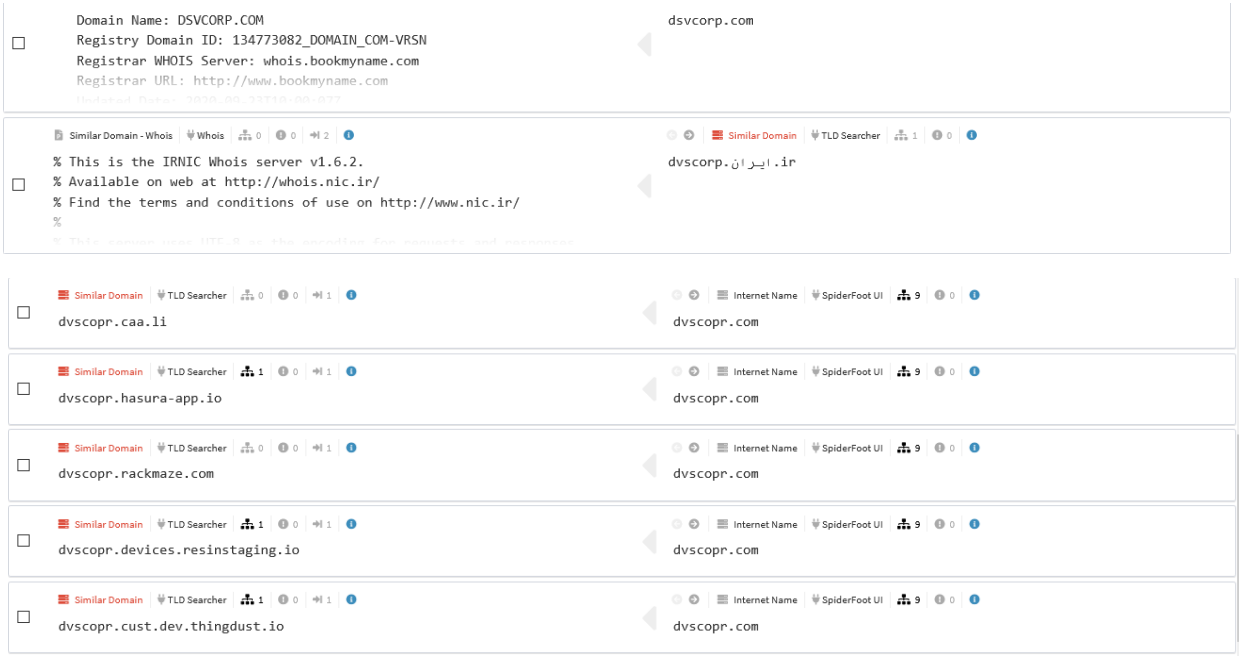


13. 集計ソフト各社には、それぞれ中央報告の「関連会社」があります。エジソンリサーチはドミニオンの関連会社です。
14. カナダのBeanfield.comは、dvscorp.comを含む共同ホスティング関連サイトを介して接続を示しています。

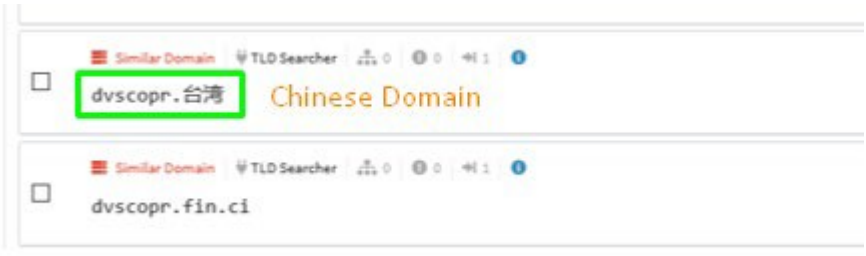


このDominionパートナードメイン"dvscorp"には、新しいネットワークデバイスが自動的にシステムに接続される自動発見機能も含まれています。次の図は、関連するdvscopr.com のマッピングの一部を示していますが、これは Dominion のインフラストラクチャを模倣したもので、名前の明らかなタイポ派生です。タイポ派生は、リダイレクトトラフィックをキャッチするために一般的に購入され、時にはハニーポットとして使用されることもあります。図は、インフラストラクチャが方法論として複数の異なるサーバーにまたがっていることを示しています。





上の図では、これらのドメインがイランなどとのつながりも示していますが、その中には以下のような中国のドメインも含まれていて、ハイライトされています。



15. 自動検出機能により、プログラマーはインターネットに接続されている間はどのようなシステムでも、それがデバイスのコンステレーションの一部になってしまえばアクセスできるようになります（オリジナルのSpiderfootグラフを参照）。
16. 2019年のDominion Voting Systems Corporationは、同社の特許の多くを中国に売却した（カナダのHSBC銀行経由）。

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

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date recorded	Pages
050500/0236	Sep 25, 2019	Sep 26, 2019	7
Conveyance: SECURITY AGREEMENT			
Assignors	Correspondent		Attorney docket
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020		
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

特に興味深いのは、認証に関する特許の性質を示す文書の一節です。

Patent assignment 050500/0236

SECURITY AGREEMENT

Date recorded	Reel/frame	Pages
Sep 26, 2019	050500/0236	7

Assignors
DOMINION VOTING SYSTEMS CORPORATION

Execution date
Sep 25, 2019

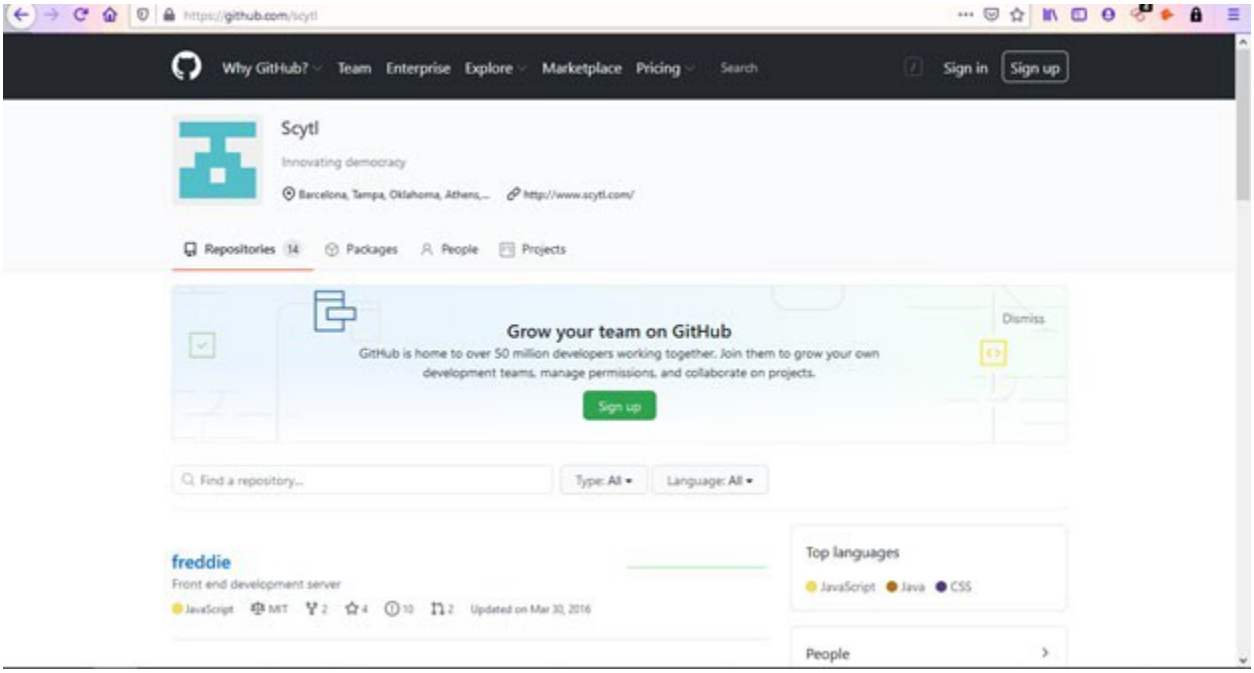
Assignee
HSBC BANK CANADA, AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET
TORONTO M5J 1S9
CANADA

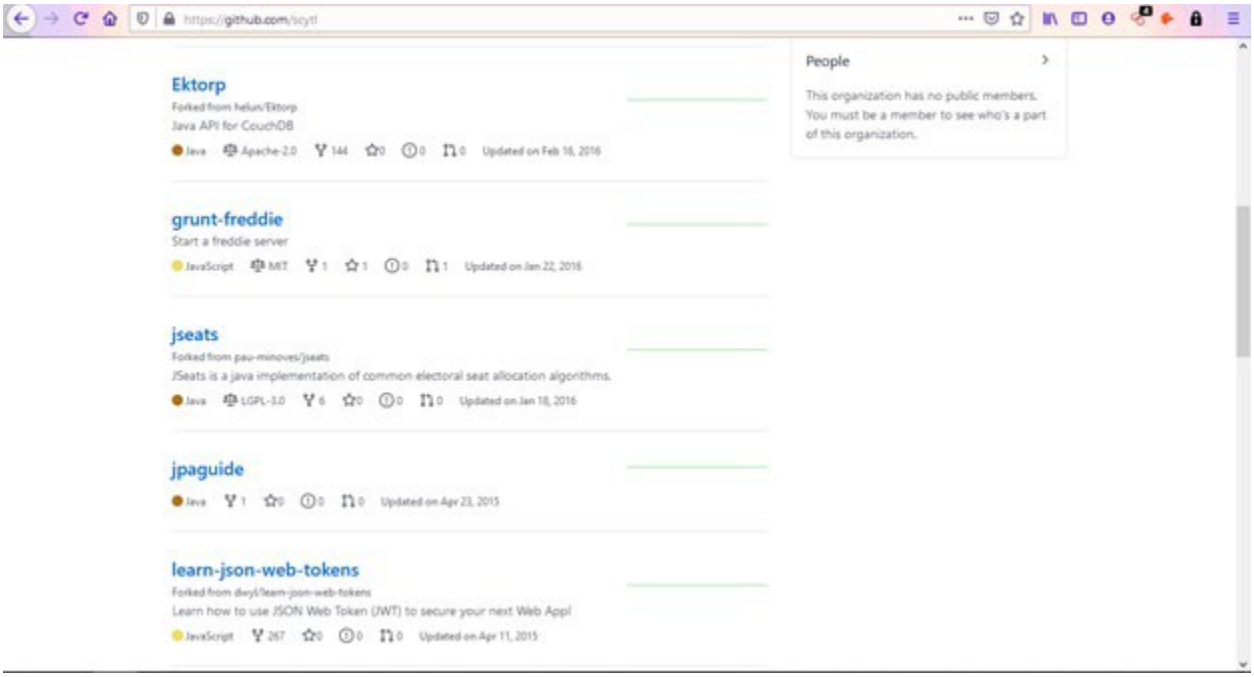
Correspondent
CHAPMAN & CUTLER LLP
1270 AVENUE OF THE AMERICAS, 30TH FLOOR
ATTN: SOREN SCHWARTZ
NEW YORK, NY 10020

Properties (18 total)

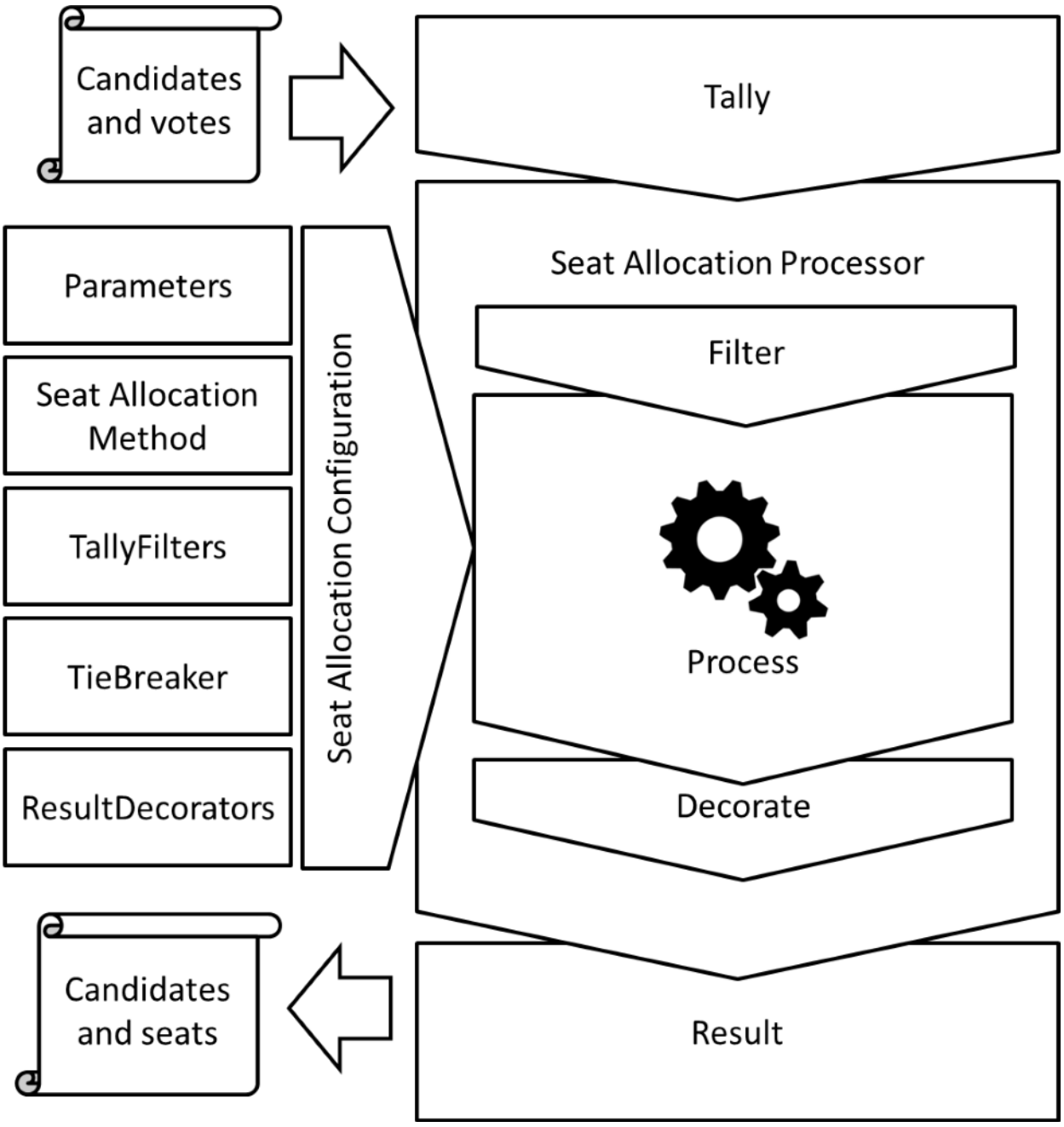
Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE 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はバックボーン（クラウドのようなもの）を作ります。SCYTLは選挙システム内のセキュリティを担当しています。

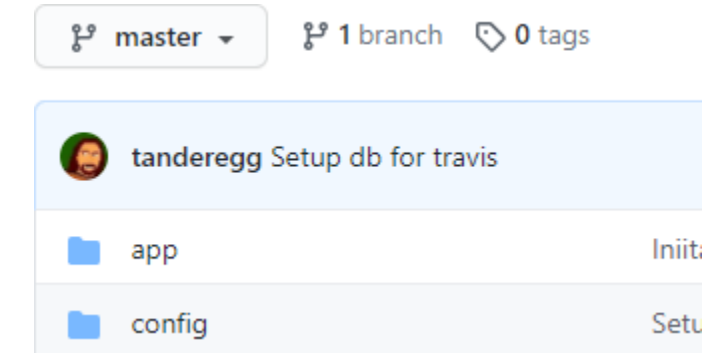




18. ScytlのGitHubアカウントでは、Scytl Jseatsは、データを平滑化するデコレータ処理を含む、より広範な選挙タイプをサポートするために必要なプログラミングをいくつか持っています。



19. 関係ないですが、CTCL（Center for Tech and Civic Life）はMark Zuckerbergが出資しています。彼らのgithubページ（https://github.com/ctcl）では、プログラマーの一人が政府の役職に就いている。Bipcoopのレポには、開発者の一人としてtanderegが掲載されており、彼は消費者金融保護局で働いている。



20. AA20-304A-
と題された同梱の文書に記載さ
れているように
サイバースセキュリティと2020年10月30日の指定日にAA20-304AのプロダクトIDを持つCISA(Infrastructure Security Agency)とFBIは、イランのAPTチームがウェブサイトスキャンソフトウェアACUTE NIXを使用して、選挙会社のウェブサイト内の脆弱性を見つけるために使用されていることが確認され、私が個人的にキャプチャし、より高い当局に報告した押収されたクラウドストレージを購入していたと報告しています。これらのスキャン行動は、侵略国の外国人エージェントが米国の有権者リストにアクセスしていたことを示しており、最近になってそれを行っていました。
21. 私の専門的な意見としては、この宣誓供述書は、Dominion Voter SystemsとEdison Researchがイランや中国などの不正な行為者によってアクセスされ、確実に危険にさらされていたことを示す明確な証拠を提示しています。不正な行為者と敵対的な

外国の影響力を持つサーバーや従業員を使用し、簡単に発見できる多数の漏洩した資格情報を組み合わせることで、これらの組織は外国の敵対者がデータにアクセスできるようにしていました。

選挙を監視し 選挙を操作するために

意図的にインフラへのアクセスを提供しました

直近の2020年の選挙も含めてですこれは、基本的なサイバーセキュリティを提供する義務を完全に怠ったことを表しています。これは技術的な問題ではなく、むしろガバナンスと基本的なセキュリティの問題である。この問題が是正されなければ、米国およびそれ以降の将来の選挙は安全ではなくなり、市民は選挙結果に自信を持てなくなる。

私は偽証罪の罰則の下に宣言します

私の知る限り真実であり正しいことを2020年11月23日に執行