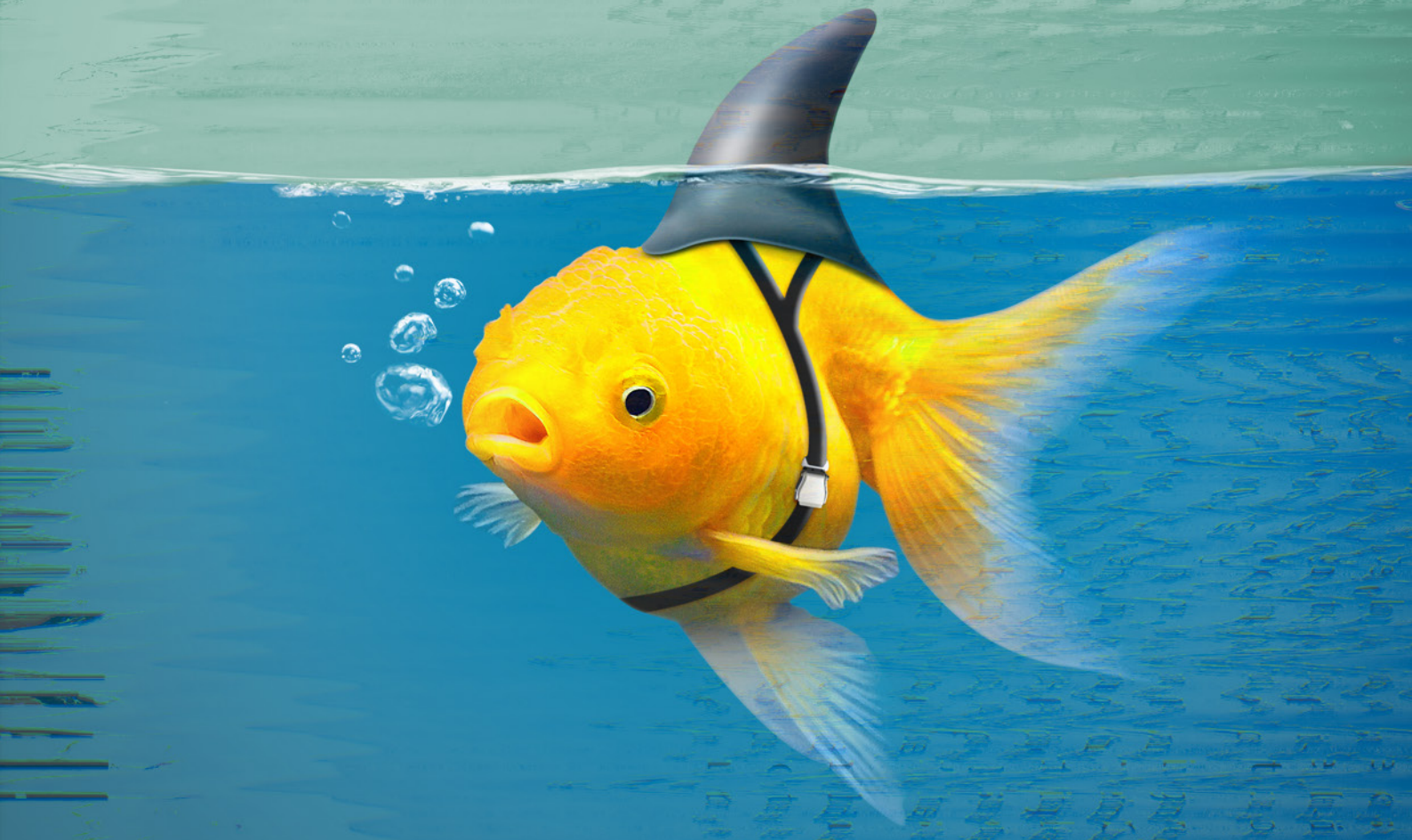
WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

WHITE PAPER

CEO Impersonation: A Look into the Top 100 CEOs of 2021



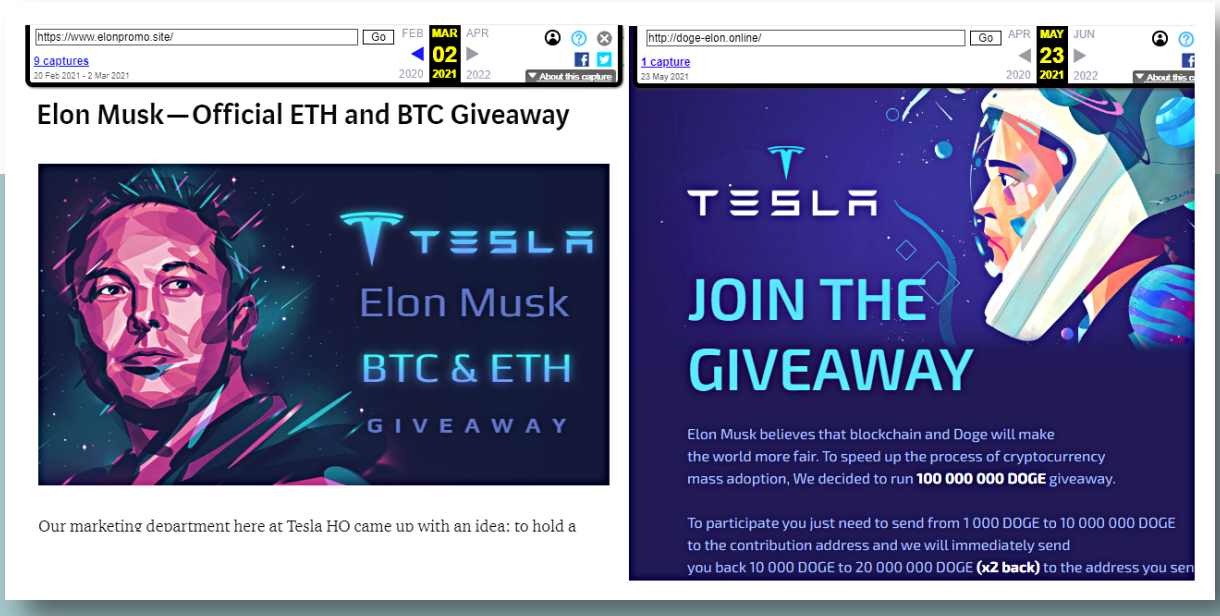
Contents

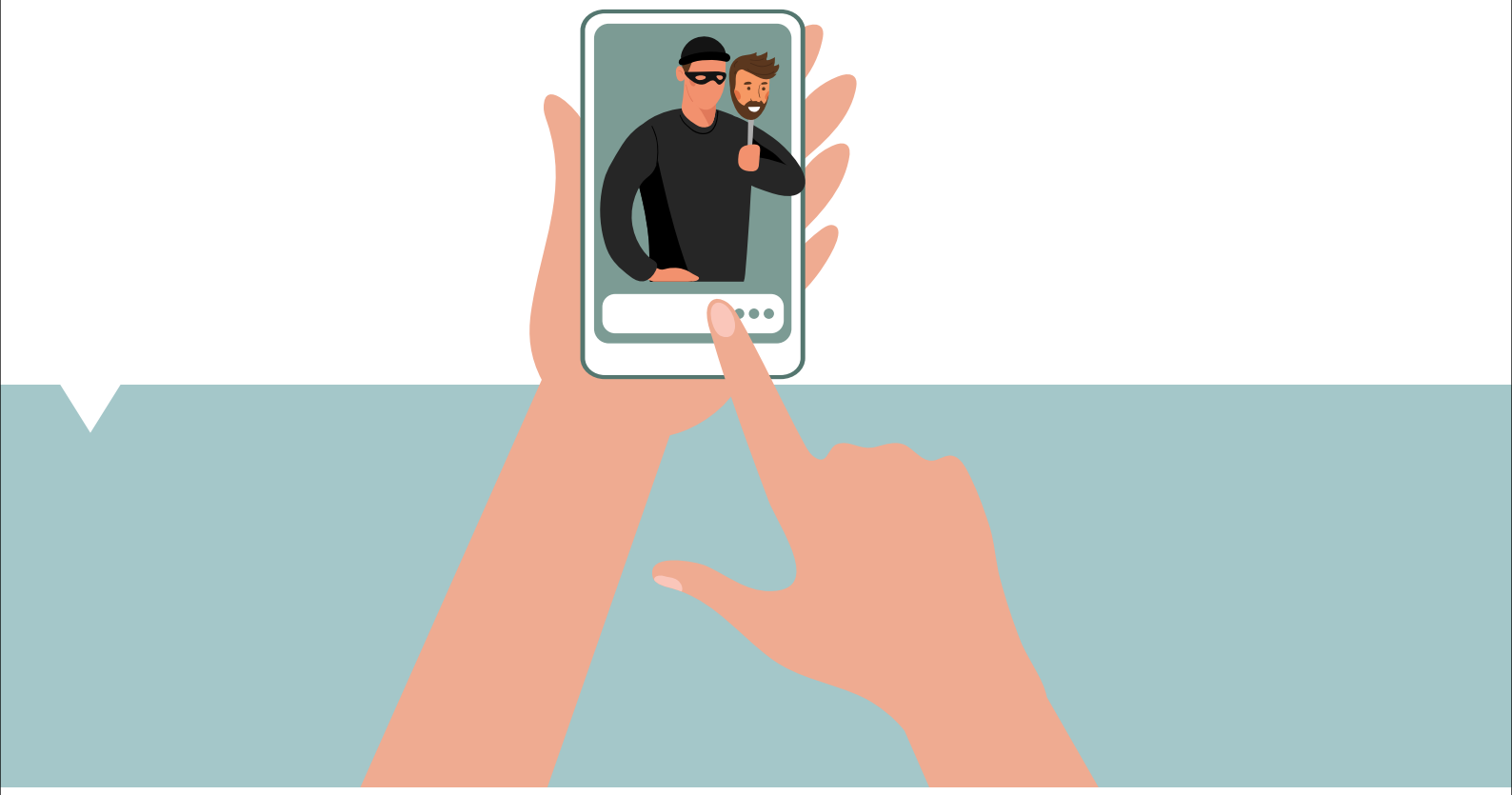
CEO Impersonation: A Look into the Top 100 CEOs of 2021

CEO fraud, spear-phishing, or business email compromise (BEC)—CEO impersonation has often been called by these names. This type of cybercrime almost always falls under the social engineering category as threat actors try to manipulate their victims' way of thinking. The underlying motives could vary, ranging from corporate espionage to financial gain. But we often see more of the latter in the stories we hear and read.

The impersonation of Elon Musk in several crypto giveaway scams is one example of such scams. Scammers pretending to be Elon Musk are believed to have stolen more than US$2 million from several people. In one investigation, WhoisXML API cybersecurity researchers uncovered several domains that share the same registrant email domain as elonpromo[.]site, one of the domains used in a fake crypto giveaway campaign.

Captures from the Wayback Machine provide some perspective. The content hosted on elonpromo[.]site in March 2021 looked similar to one of the domains uncovered by the researchers.





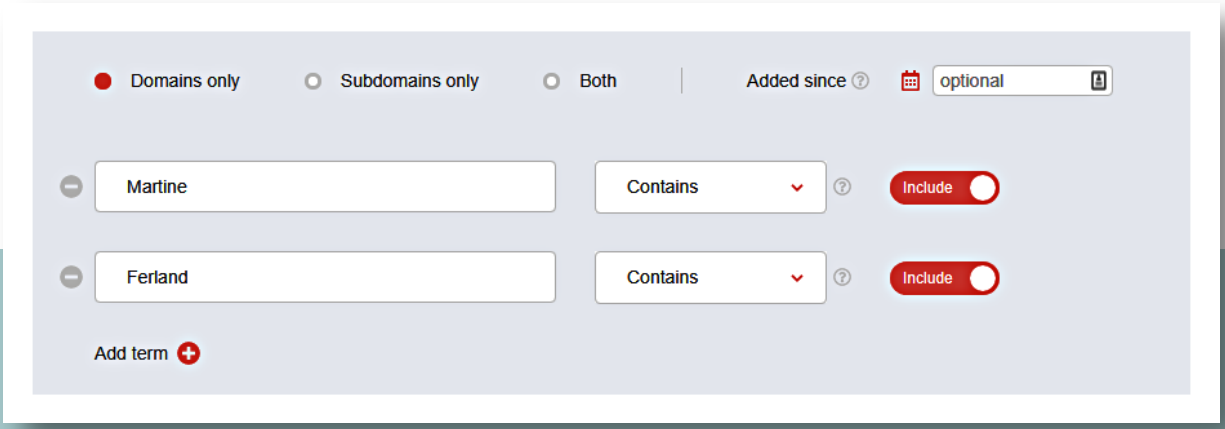
Whatever the motive, attack vectors tend to remain the same. Threat actors would use the names of CEOs and top executives and attempt to lure victims to their specially crafted websites. Verizon's 2021 Data Breach Investigations Report (DBIR) noted as much, saying that in BEC scams, email addresses with CEO names often appeared in their datasets.

When it comes to domain names and subdomains, what could CEO impersonation look like? Do companies defensively register domains that use their CEOs' names? To answer these questions and more, WhoisXML API researchers took the names of Glassdoor's 2021 Top 100 CEOs and extensively searched for domain names and subdomains that contain their names. A summary of the findings are as follows:

- More than 2,000 domains and subdomains contain the CEOs' names.
- Their names appear in more than 600 subdomains.
- 92% of the domains had redacted WHOIS records.
- Only 2% can be publicly attributed to their respective organizations.
- Screenshot analyses reveal some suspicious redirects.
- Some domains have been reported "malicious."

Methodology and Tools

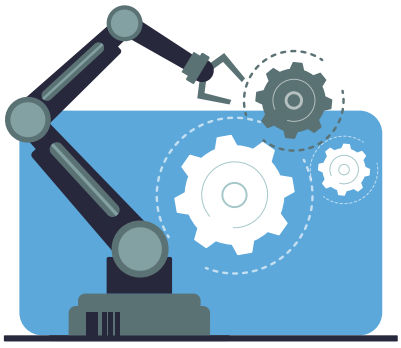
Obtaining the domain footprint of the top 100 CEOs required the researchers to use their names as query strings on Domain Research Suite (DRS) Domains and Subdomains Discovery. In most instances, the first and last names were separate search terms, as shown in the image below.



This method ensures that aside from the typical first and last name sequence (e.g., sundarpichai[.]com, michaeldowling[.]us, and timpierce[.]com), other sequences would also be returned (e.g., pichaisundar[.]com, dowlingmichael[.]com and piercehtims[.]com).

For some names that include common terms, the researchers used the first and last name as a single search string. This method was used in seven names, which would have returned hundreds of false positives otherwise. For example, putting Tim Cook as two separate query strings returned about 1,500 domains that have nothing to do with Tim Cook, Apple's CEO. Some examples are "cooktime," "cookietime," "timetocook," "ecooktime," "theultimateoutdoorcookingexperience," and "bestelectricpressurecookertestimonials," to name a few.

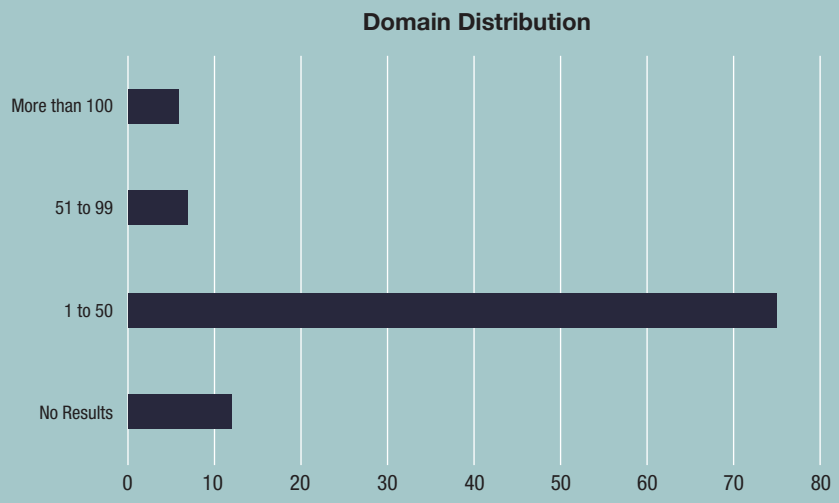
The WHOIS records of the domains and subdomains were then obtained using Bulk WHOIS Lookup. The researchers also analyzed the screenshots of the domains via Screenshot API. Lastly, the Threat Intelligence Platform (TIP) was used to see if any of the domains have been reported as malicious.



Data Analysis

WhoisXML API researchers analyzed 2,157 domains and 652 subdomains after looking up domains and subdomains containing the names of the top 100 CEOs using the method specified in the previous section.

Of the 100 names, 12 didn't return any result. The majority (75 names) returned between one and 50 domains and subdomains.



Seven names returned 51–99 domains and subdomains, while six names had 100 results or more. These six CEOs took up 53% of the total number of results. The table below shows the distribution of results among the top 6 CEOs.

CEO Name	Company Name	Number of Domains and Subdomains Found
Kevin Murphy	Ferguson Enterprises	490
Rene F. Jones	M&T Bank	279
Tim Cook	Apple	266
Tim Ryan	PwC	229
Marc Benioff	Salesforce	121
Ben Peterson	Blue Raven Solar	100

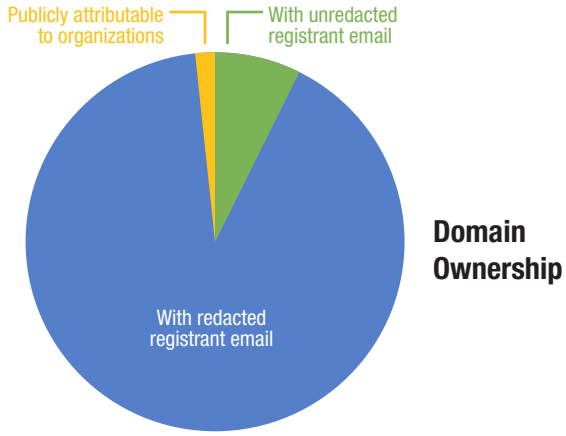
Domain Ownership: Do the Domains Belong to the Names' Rightful Owners?

When it comes to personal names, the idea of domain ownership could be complicated and obscure. After all, anyone with the same name can claim ownership. However, the CEOs included in this study are among the most prominent ones. When searching the Internet for "Tim Cook" or "Ted Mathas," the first few results are always attributed to Apple and New York Life, respectively. The same holds true for most of the top 100 CEOs.

While prominence doesn't make one the only rightful and legitimate owner of a domain that uses a person's name, it can be argued that most people would associate such domains with the most prominent individuals. Furthermore, the World Intellectual Property Organization (WIPO) recognizes that there could be an offense in "the registration of personal names as domain names by parties unconnected with the persons in question."

To determine whether the domains in this study belong to the CEOs in question or their respective organizations or not, the researchers analyzed the domain queries' Bulk WHOIS Lookup results.

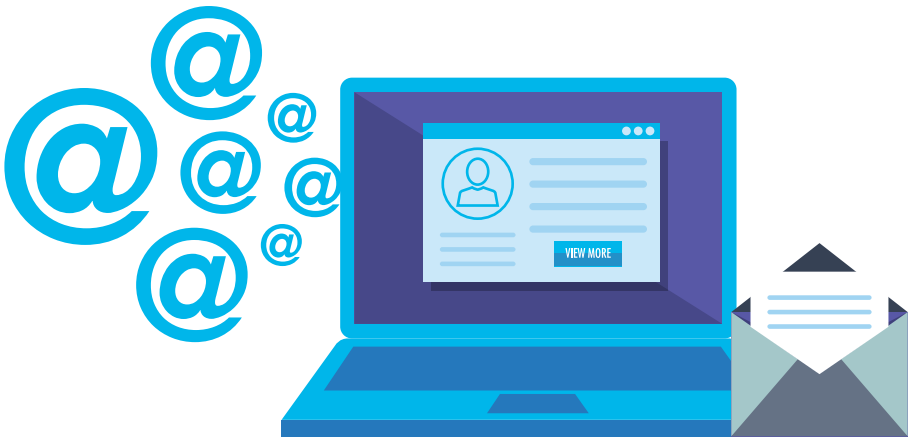
Out of 2,157 domains, 1,526 had WHOIS records. The rest probably did not resolve for various reasons, including possibly nonrenewal of registration.



Of the domains that did resolve, 92% had redacted or privacy-protected WHOIS records, specifically registrant email addresses. CEOs or organizations could have opted to keep them that way after gaining ownership of the domains. However, from a cybersecurity standpoint, privacy redaction makes it difficult to establish a domain name's authenticity and legitimacy, especially when it is used in official communications.

Around 8% of the domains had unredacted registrant email addresses. These used email providers, such as:

- Hotmail
- Gmail
- MSN
- 163.com
- Outlook



Some unredacted records also used corporate email addresses, but only 2% could be attributed to the organizations the CEOs belong to. Among the publicly attributable domains are those containing these CEO names:

CEO Name	Company Name	Registrant Organization	Examples of Domains Found
Alan Scnitzer	Travelers	The Travelers Indemnity Company	alan-schnitzer[.]com | alandschnitzer[.]com
Brian Moynihan	Bank of America	Bank of America	briantmoynihan[.]com | brianmoynihanblows[.]net
Richard Fairbank	Capital One	Capital One Services, LLC	richardfairbanksux[.]net | richardfairbanksucks[.]net
Jane Fraser	Citi	CitiBank, N.A.	janefraser[.]com | janefraser[.]us
Todd Graves	Raising Cane's	Raising Cane's LLC	toddbgraves[.]us | toddgraves[.]us
Ted Mathas	New York Life	New York Life Insurance Company	tedmathas[.]com
Pat Gelsinger	Intel Corporation	Intel Corporation	patgelsinger[.]net | patrickgelsinger[.]com

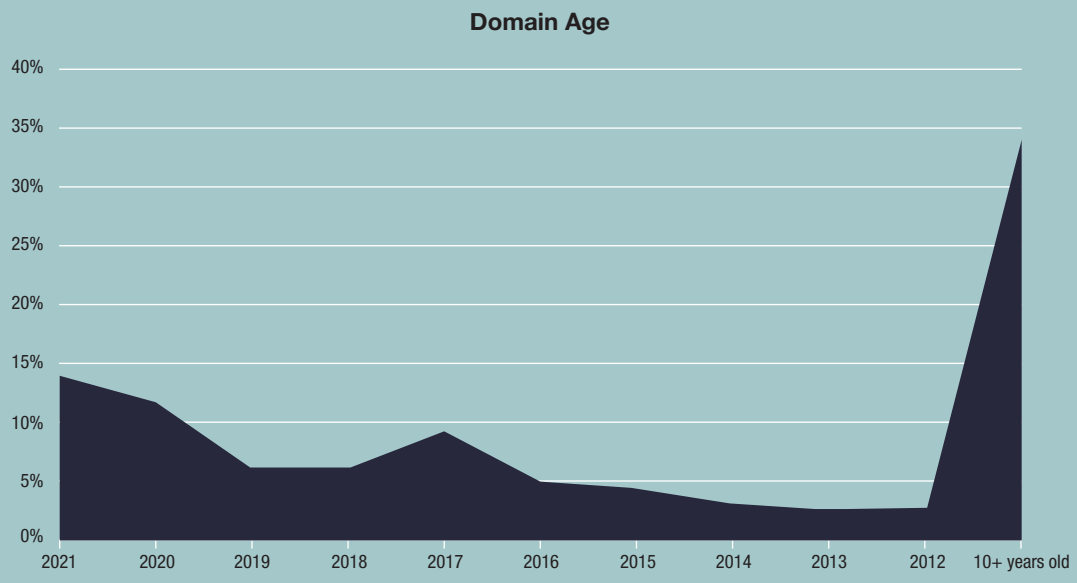
It's interesting to note that the top 6 CEOs with the biggest domain and subdomain footprints are not found in the list of attributable domains.

Large corporations usually make their WHOIS records public, as in the cases of the sample domains in the table above. The zero-trust approach dictates that we only trust resources that we can validate. As such, 98% of domains in this study whose WHOIS records cannot be publicly attributed to legitimate companies warrant further scrutiny.

How Old Are the Domains?

Around 34% of the domains are more than 10 years old, while the domain registration of the remaining domains seems to be on an increasing trend for the past four years.

To be exact, 6% of the domains were created in 2018, while another 6% in 2019. But domain registration doubled in 2020 at 12%. Halfway through 2021, 14% of the domains have already been created.



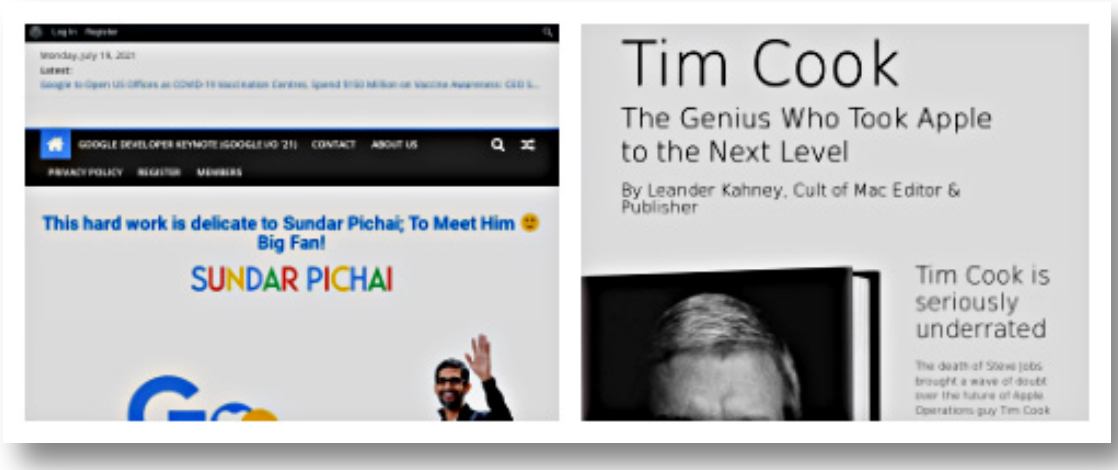
This domain registration trend is consistent with reports about the significant increase in BEC scams and other cybercrime incidents in 2020. One study cited a 3,000% increase in phishing and BEC scams last year, mostly related to the COVID-19 pandemic.

While the number of CEO-related domain registrations is not as high as that of coronavirus-themed domains, they still showed significant growth. As cybersecurity professionals continue to focus on coronavirus-related threats, threat actors could also be cooking up CEO impersonation fraud campaigns.

What Do the Domains Look Like?

Screenshot API reveals the appearance of the websites the queried domains point to. Around 70% of the domains were resolvable, and the majority are parked. Most of them are up for sale, a likely indication that their current owners are not the CEOs of their respective companies.

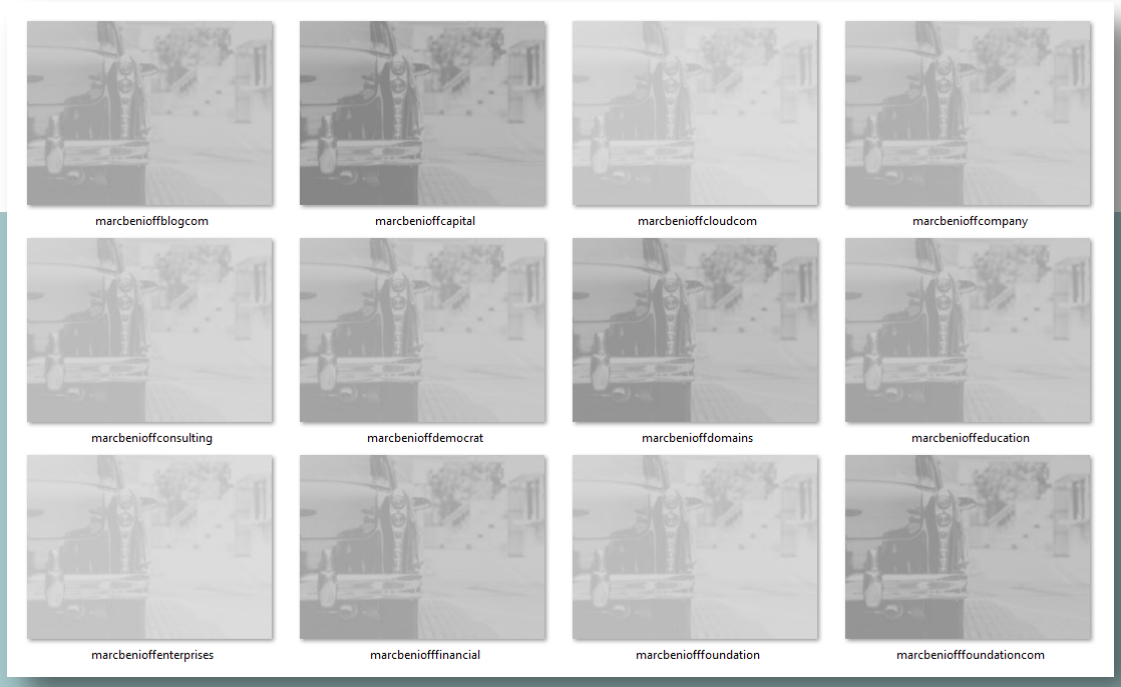
Some websites appear to have been created by fans, such as those that feature Sundar Pichai and Tim Cook.



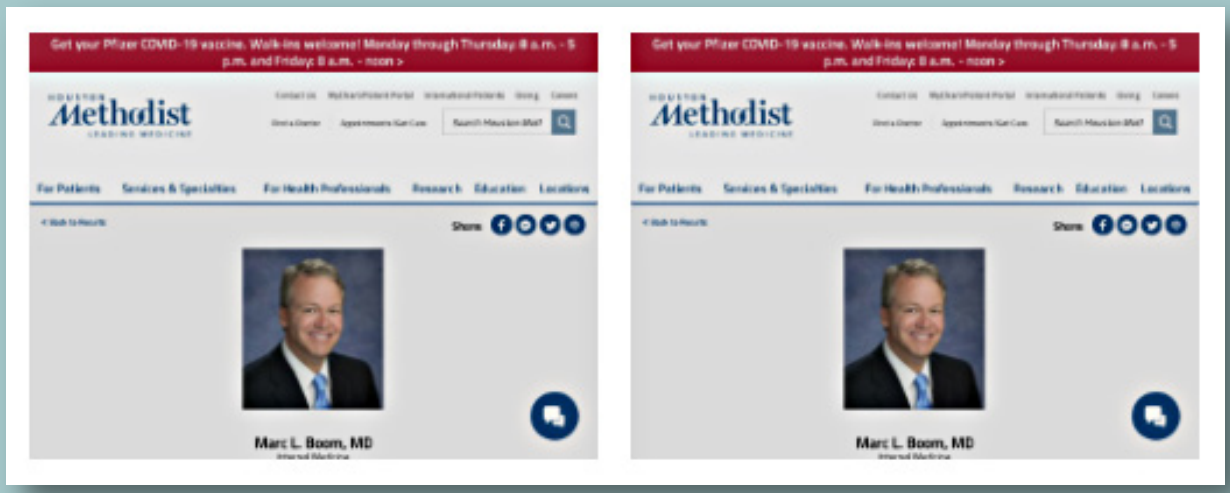
sundarpichaiin timcookbookcom

Reserved and Redirected: In the Name of Brand Protection

Some organizations use third-party brand management providers. Examples are those related to Marc Benioff, Salesforce's CEO. More than 30 of the domains are under Trakk, NameCorp's corporate domain management service. Their screenshot results look like these:



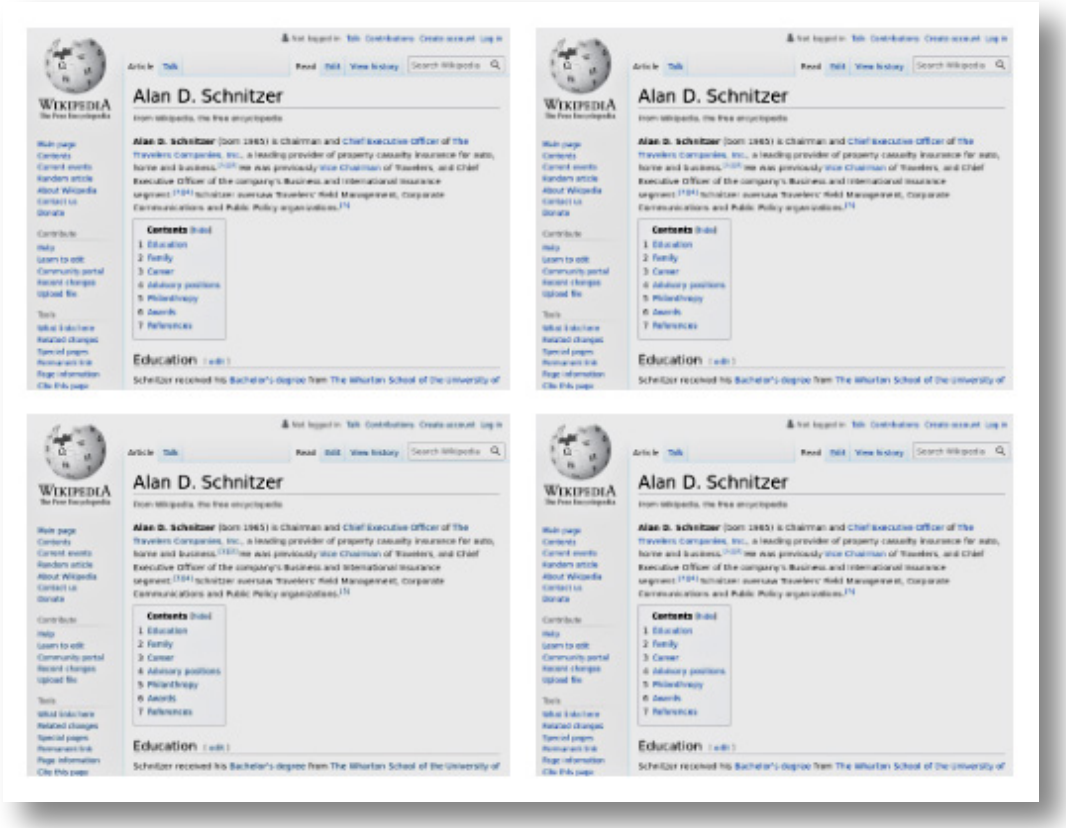
Other companies keep their CEOs' names safe by redirecting related domains to their legitimate websites. Domains associated with Marc Boom, CEO of Houston Methodist, for instance, are redirected to houstonmethodist[.]org/doctor/marc-boom.



marcboomnet **drmarcboomnet**

Alan Schnitzer's domains, on the other hand, are redirected to the Traveler CEO's Wikipedia page (en[.]wikipedia[.]org/wiki/Alan_D._Schnitzer).

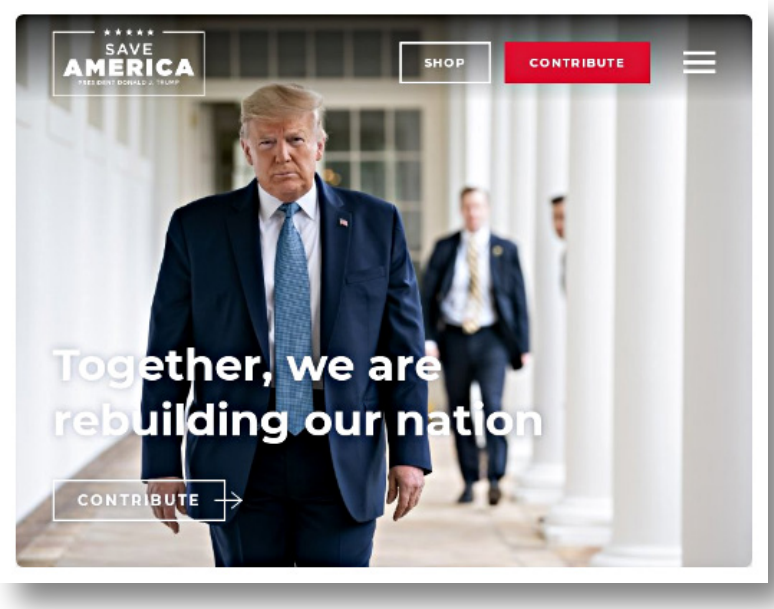
alandschnitzercom alanschnitzercom



alandschnitzerme alanschnitzerorg

Not All Redirects Could Be Logical or Safe

More domains are similarly set up as redirects. However, some screenshot results seem suspicious or, at the very least, confusing. An example is dougpalladini[.]com. For some reason, the domain using the name of Vans CEO redirects to donaldjtrump[.]com

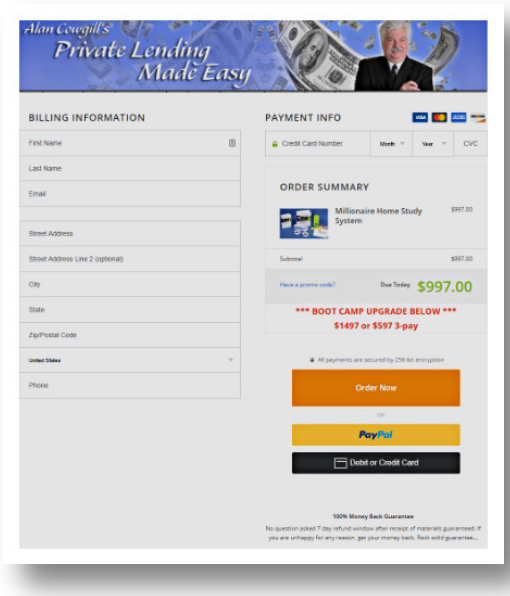


dougpalladini.com website screenshot

A more suspicious redirect was detected for one of the domains using the name of Apple's CEO. The domain timcook[.]club redirects to a checkout page with the URL

https://m254[.]infusionsoft[.]app/app/orderForms/35f7b348-6705-460a-8db0-d6cd0f4e42ce?cookieUUID=bacb7760-ce67-4f37-8981-ce332e4fef2a&cookieUUID=eda34016-054b-4c86-be03-b7a54a3fffb4.

While the URL is not reported as malicious, unsuspecting users clicking the link would see an order summary totaling US$997 and a button that allows them to pay via PayPal.



These are just a few analyses of the domains' screenshots, which brings us back to the need for unattributable domains to be scrutinized.

Malicious Domain Alert

A few of the domains have been reported "malicious." Threat Intelligence Platform (TIP) detected that the following domains are listed on blocklists, such as Bambenek Consulting OSINT data feeds, Virus Total, and Google Safe Browsing.

Malicious Domain	CEO Name	Company Name
timothybyrne[.]com	Tim Byrne	Lincoln Property Company.
renettejones[.]com	Rene Jones	M&T Bank
kevinjmurphy[.]com	Kevin Murphy	Ferguson Enterprises
brianmoynihan[.]com	Brian T. Moynihan	Bank of America
sundarpichai[.]com	Sundar Pichai	Google

Conclusion

CEO impersonation fraud or BEC, in general, is a billion-dollar business. In 2019, the Federal Bureau of Investigation (FBI) pegged the losses at US$26 billion, adding more than US$2 billion in 2020 alone.

The 2021 DBIR stated that threat actors didn't have to compromise email accounts for most BEC scams. As such, the return on investment (ROI) for cybercriminals is tremendous. They could register domains imitating brands and their top executives for a few dollars and use these domains to lure victims. The weapon could be any of the 98% of domains in this study that cannot be publicly attributed to the organizations.

This study on the domain footprint of the names of the top 100 CEOs suggests that CEO impersonation is real and present. It could be as harmless as fans creating websites for their CEO idols, but it could also be detrimental in that threat actors could redirect innocent users or employees to money transfer pages.

About Us

WhoisXML API is a cyber intelligence provider that gives enterprises access to one of the largest repositories of well-parsed domain, subdomain, IP, and DNS data that enhances cybersecurity platforms' capabilities and helps security teams gain superior network security.

The data that WhoisXML API provides comes in different consumption models, ranging from APIs, data feeds, monitoring tools, and lookup tools, all of which make the Internet more secure and transparent. WhoisXML API has more than 50,000 satisfied customers, spanning law enforcement agencies, cyber forensics analysts, threat hunters, and cybersecurity solutions developers.