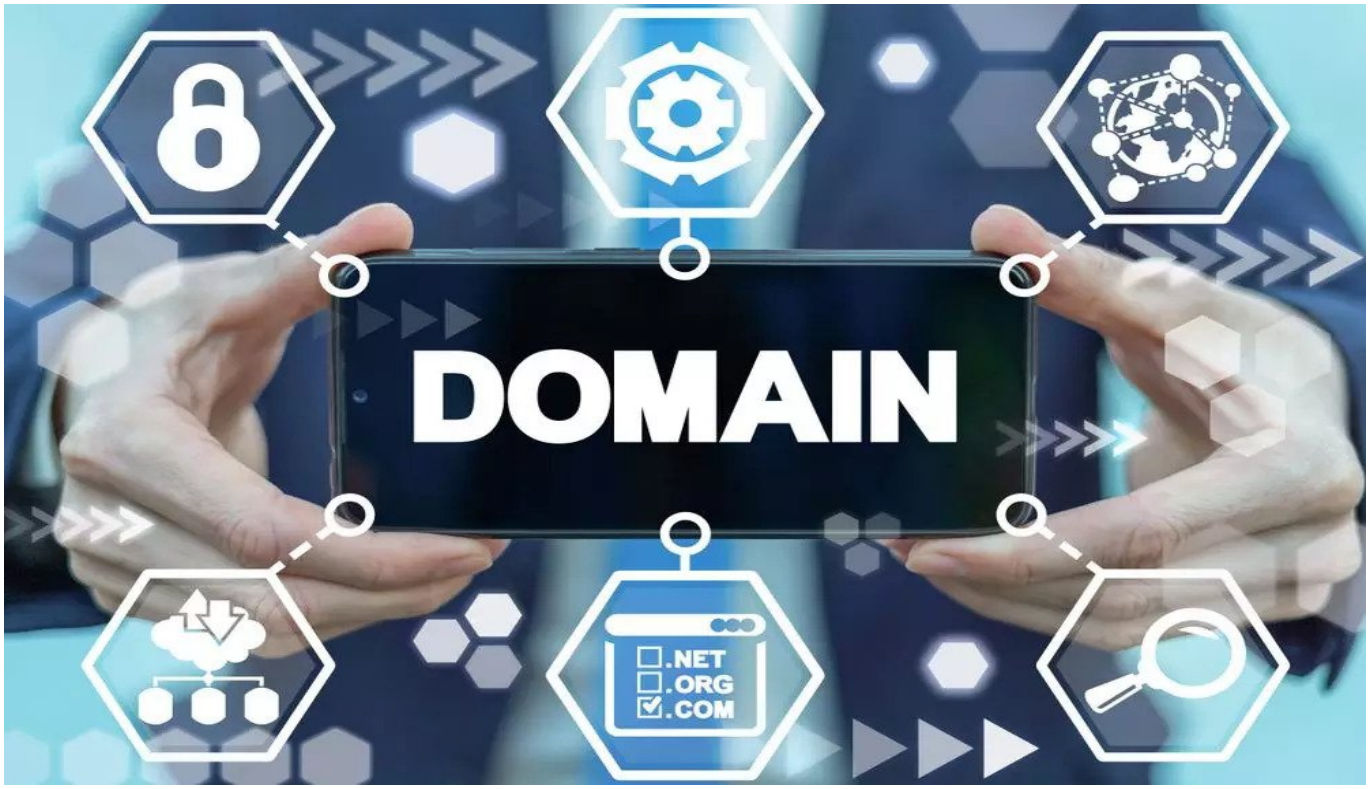


How to Find Out Who Owns a Domain Name with Reverse WHOIS Search and WHOIS Database Download

In the past, there was no way for users to find out what other domains, if any, a particular registrant owns without first translating a domain name into an IP address. But with the shortage of available IPv4 addresses, which resulted in the assignment of shared IP addresses to unrelated individuals or even companies, that approach has become riddled with difficulties.

Even if you can pinpoint the owner of an IP address, a shared one would provide users with a list of domains that may take a lot of time to sift through. If that IP address turns up as an indicator of compromise (IoC) in a publicly accessible report, affected users would have to go through each related domain's WHOIS records to get to the bottom of the issue. Imagine how long that would take if you had 30 domains or more to scrutinize.

Thankfully, domain intelligence providers like our company have streamlined this process with the introduction of tools like Reverse WHOIS Search and offerings such as WHOIS Database Download.

This post shows how users can find out who owns a domain name in five simple steps.

5 Steps to Identifying All of the Domains a Threat Actor Owns

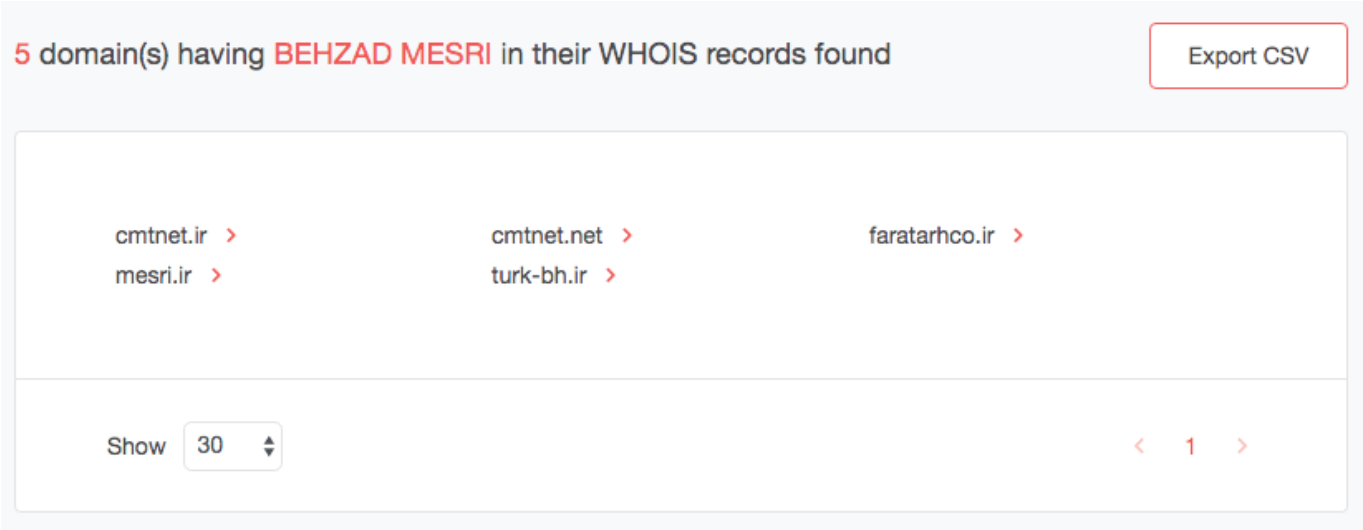
Avoiding the hassle of falling under cyber attackers' radar is one of the most effective ways to prevent a catastrophic compromise. As such, any organization's infosec team must be armed with a list of known cyber criminals to monitor their movements. After all, you might be next on their target database. We'll show you how to use Reverse WHOIS Search and WHOIS Database Download to search for domains by owner.

Law enforcement agencies like INTERPOL and the Federal Bureau of Investigation (FBI) have pages that warn all computer users about the most notorious entities behind the world's greatest online crimes. We chose to investigate Bahzad Mesri for our Reverse WHOIS Search demonstration.

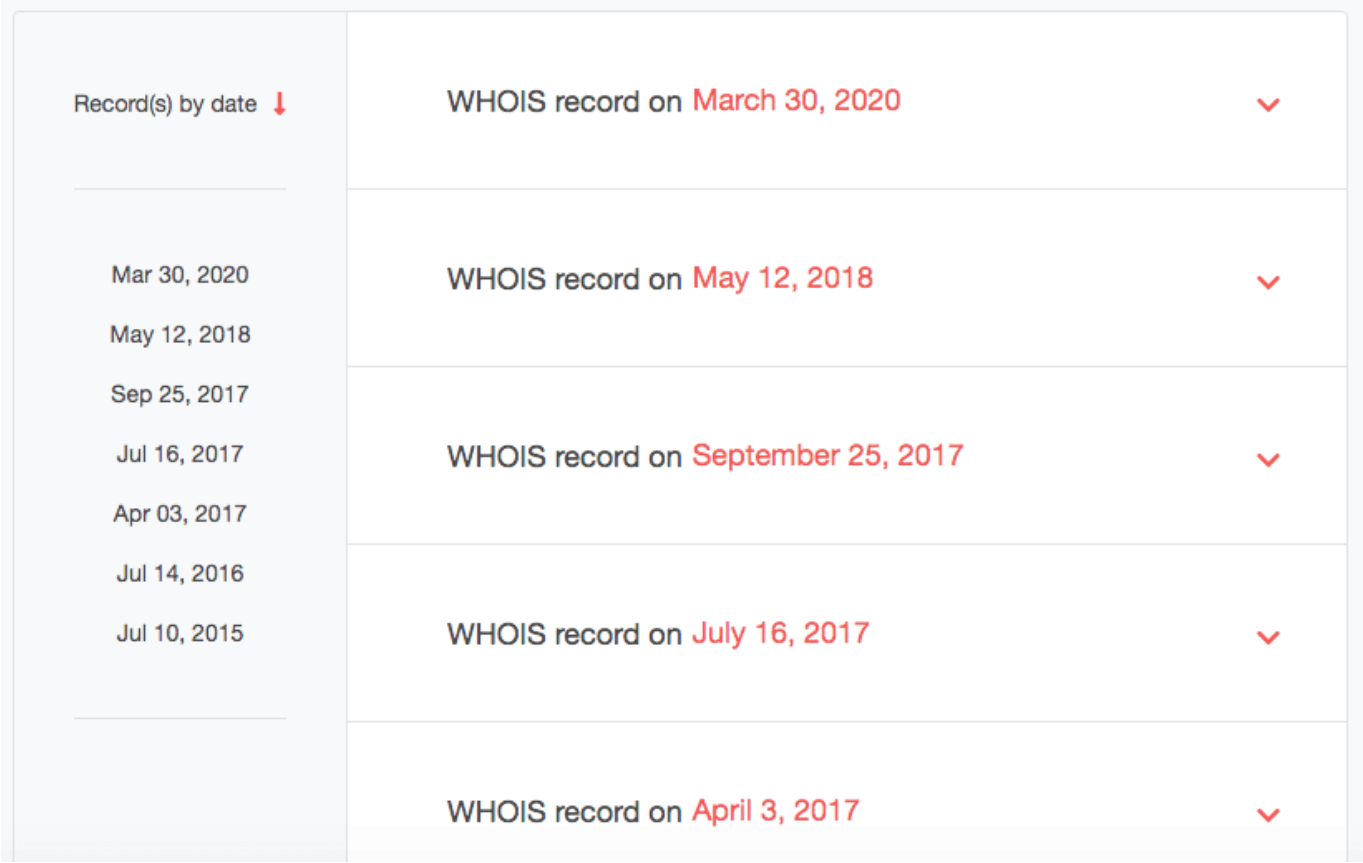
Mesri is wanted by the FBI for his alleged involvement in criminal activities that include computer intrusion and aggravated identity theft. He was the CEO of an Iranian entity that is believed to have worked for the Islamic Revolutionary Guard Corps (IRGC), which was reportedly involved in a malicious cyber campaign targeting current and former members of the U.S. Intelligence Community. A U.S. district court issued a federal warrant of arrest for him on February 8, 2019, after he was charged with conspiracy, attempted computer intrusions, and aggravated identity theft. He was previously charged with unauthorized access to computer systems, stealing proprietary data from said computers, and attempted extortion for approximately $6 million in Bitcoin on November 8, 2017.

How to Use Reverse WHOIS Search to Identify All of the Domains Owned by Mesri

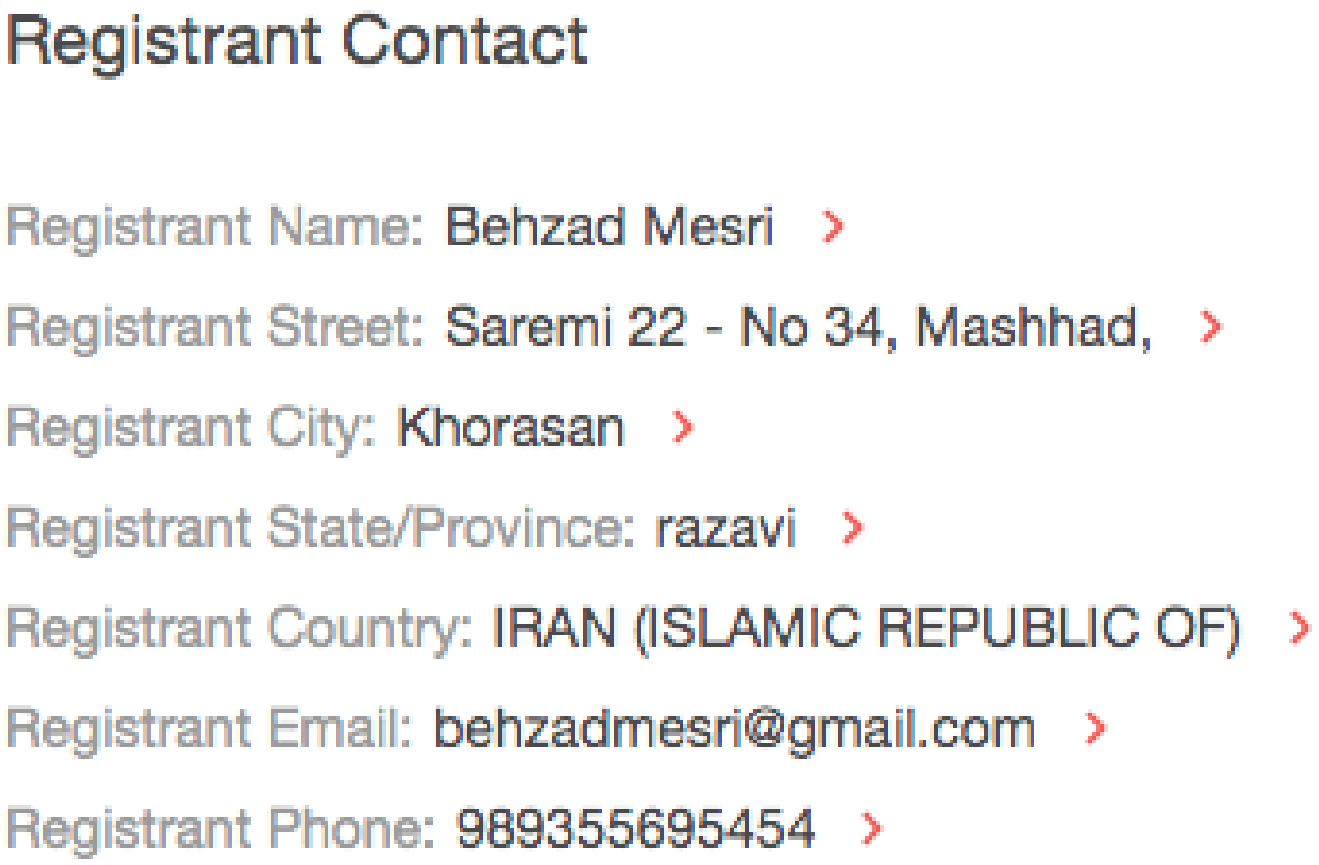
- Log in and access the Reverse WHOIS Search dashboard. Use the registrant's name (Behzad Mesri, in this case) into the input field and click "Search." The tool listed five domains whose WHOIS records contained "Behzad Mesri."



- We can't be sure that all of these domains belong to the same person, so we'll need to dig deeper. To do that, we need to take a look at their WHOIS records. Click the red arrow beside the first domain (cmtnet[.]ir). You should see a drop-down list, then click "Build historic WHOIS report." You will get a list of dates when the domain's WHOIS record was updated. Click the latest file, dated March 30, 2020.



- Take note of the registrant details. In this case, you now have an additional clue — an email address.



Do the same thing for the other four domains on the list. We found that Mesri also owned mesri[.]ir and discovered a potential accomplice's name and email address. That isn't surprising since Mesri was supposedly a CEO. Of course, he would have staff members that may include his domain's billing and technical contact.

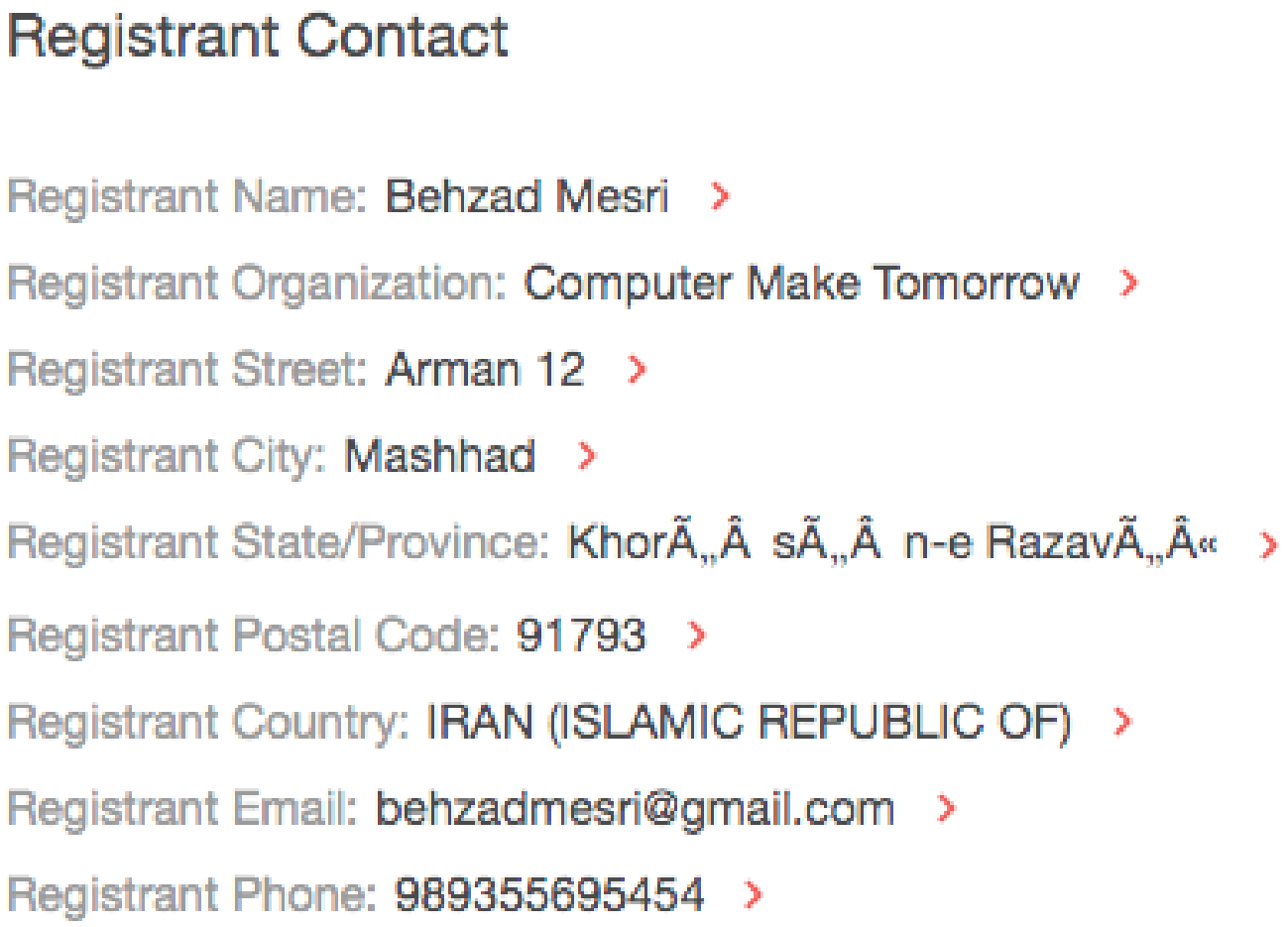
Registrant Contact

Registrant Name: Behzad Mesri
Registrant Street: Saremi 22 - No 34, Mashhad,
Registrant City: Khorasan
Registrant State/Province: razavi
Registrant Country: IRAN (ISLAMIC REPUBLIC OF)
Registrant Email: behzadmesri@gmail.com
Registrant Phone: 989355695454

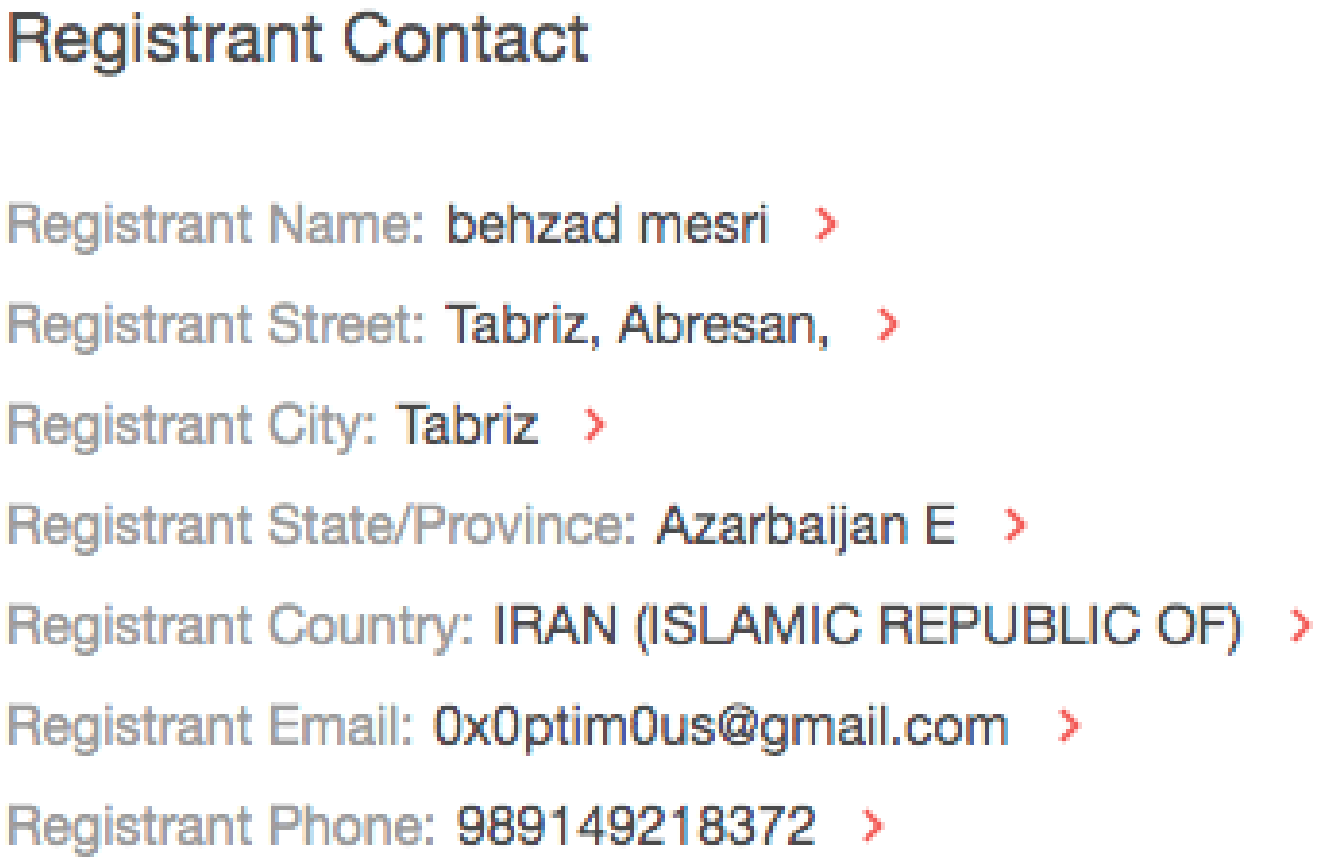
Billing Contact

Billing Organization: Rayan Dadeh Negar Dena
Billing Country: IRAN (ISLAMIC REPUBLIC OF)
Billing Email: rayan@talahost.com

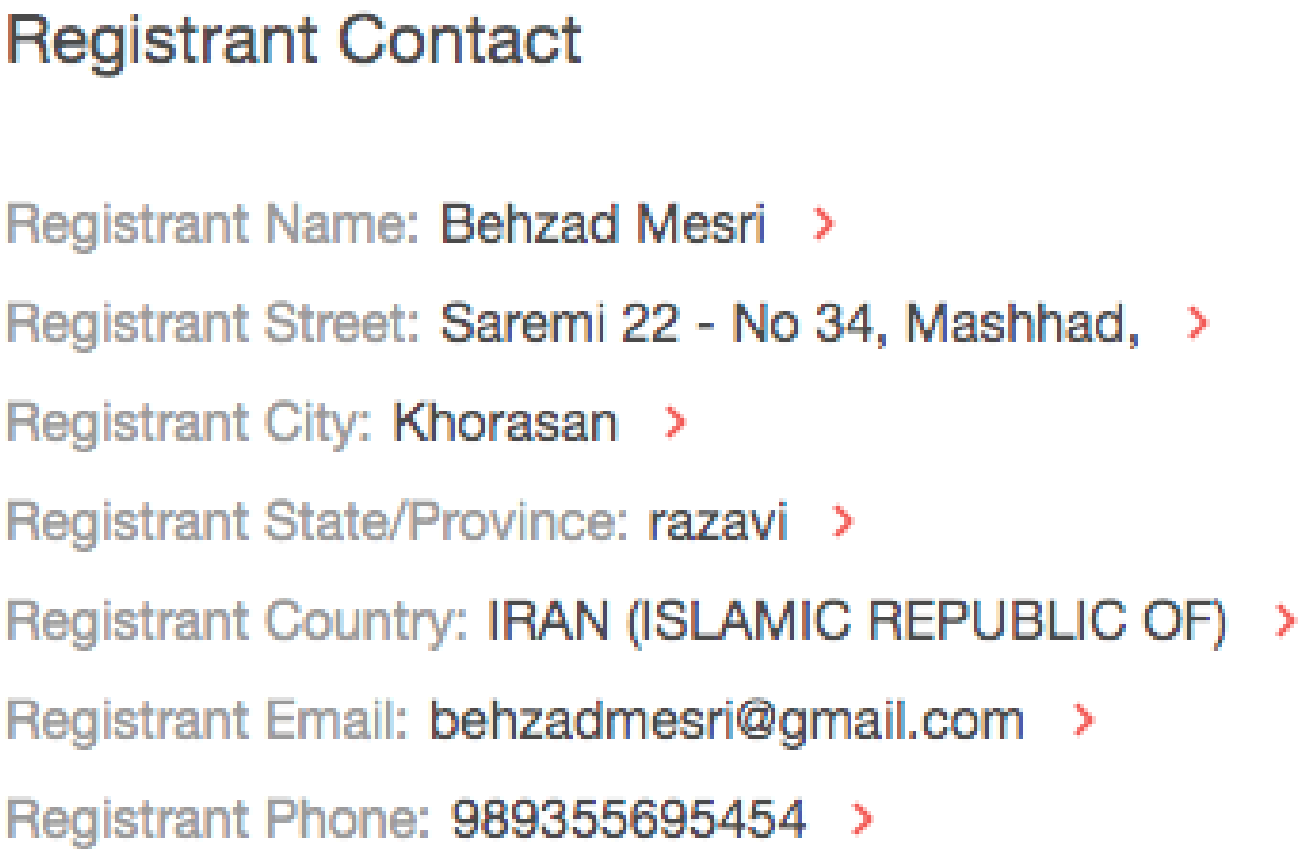
Cmtnet[.]net is older compared to its country-code top-level domain (ccTLD) counterpart (cmnet[.]ir) and mesri[.]ir. Notice, though, that the email address is consistent with the others. We also obtained a new clue — an organization name (Computer Make Tomorrow, “cmt” in short).



While turk-bh[.]ir sported a new registrant according to its March 30, 2020 WHOIS record, back in November 26, 2016, it was owned by Mesri as well. Note that he used different street and email addresses then.



Finally, faratarhco[.]ir remains registered by Mesri with the same details he did for cmtnet[.]ir and mesri[.]ir.



- While all five domains are now inaccessible, it won't hurt organizations that want to take all the necessary precautions against attacks to block access to cmtnet[.]ir, mesri[.]ir, cmtnet[.]net, turk-bh[.]ir, and faratarhco[.]ir. The blocking of the email addresses behzadmesri@gmail[.]com and 0x0ptim0us@gmail[.]com is also a great idea. That way, no communication from the domains and email addresses will get into their networks. It is, after all, fairly common for former accomplices to reuse sites for their malicious activities.

- The activities of Mesri's billing organization, "Rayan Dadeh Negar Dena," may also be worth monitoring. It could be harboring cybercriminals within its infrastructure (with or without knowing it).

This step-by-step guide shows how vital a search for domains by registrant is when all you have to ensure network protection is a suspect's name. A quick reverse WHOIS search is all you need to get a list of domains, email addresses, and organizations to include in your blocklist.

WHOIS Database Download should give you the same results. Users who prefer to perform in-depth investigations offline can use the database instead of the web-based Reverse WHOIS Search tool. All users need to do is filter the entries in the repository by registrant name and take note of their findings.

—

In an age where attacks may come from even the most seemingly benign sources such as a company that offers services to other organizations, it is essential to scrutinize every little detail before allowing it access to your network. Even so-called “CEOs” may not really be who they claim they are. Instead of relying on your gut feeling or first impressions, trust solutions like Reverse WHOIS Search and WHOIS Database Download that will let you dig deeper into domains and their owners.