Cybersecurity Forensics Analysis Using Domain Intelligence Sources

Posted on September 14, 2020

Forensic science has crossed over to the digital world in what is now called “digital or cybersecurity forensics.” And just like their physical crime scene counterparts, cybersecurity forensics experts need to hold on to whatever evidence they have and use it to get one step closer to catching the perpetrator.

Evidence comes in many different forms, but cybercriminals often use domain names and Domain Name System (DNS) infrastructure since those assets are practically what makes the Internet work.

When creating botnets for a distributed denial-of-service (DDoS) attack, for example, threat actors need to infect hundreds or thousands of devices. Each of these devices has an IP address, and the requests they send to the target’s server may sometimes contain the command-and-control (C&C) server domain. Even with their most effective entry point - phishing emails - the bad guys need to use domain names and subdomains.

What Is Cybersecurity Forensics?

Cybersecurity forensics is the process of investigating pieces of evidence so they can be used effectively in a court of law. But it is not as simple as it sounds.

First, a clear set of steps has to be developed to serve as guidelines for investigators. Such a procedure is vital in order to ensure that whatever data gathered is handled appropriately. And then there’s the evidence acquisition process, which in itself has many roadblocks.

In most cases, investigators strive to uncover more evidence by digging through hard drives, social media platforms, and email accounts. They do so by using sophisticated tools and techniques. While these digital resources are valuable data sources, cybercrime investigations can get more context if domain and IP intelligence sources are considered as well.

How to Use Domain Intelligence Sources in Forensics Analysis?

To demonstrate the use of domain and IP intelligence sources in cybersecurity forensics, we used a real-life case of Behzad Mesri. The details of the case weren't fully revealed, but we know that Mesri used the alias "Skote Vahshat" and that he hacked HBO and leaked an unaired episode of "Barry" on one of the websites he controlled or owned.

The succeeding scenarios are hypothetical, and the goal is to illustrate how investigators can track a threat actor with only a domain name to start with.

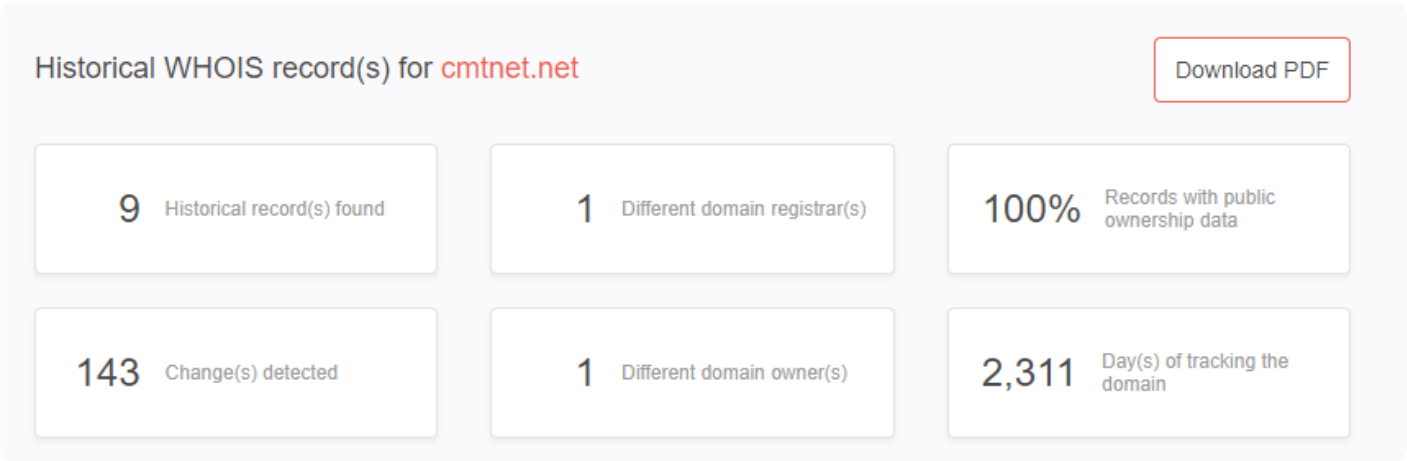
Now let's say that HBO executives received an email threatening to leak unaired episodes of several of its high-rating shows unless it pays a seven-figure sum. Undeterred, HBO ignored the threat, until an episode was released on a website with the domain cmtnet[.]net. Now, the crime has escalated.

With only cmtnet[.]net to start with, how can cybersecurity forensics experts proceed?

Acquire More Evidence from WHOIS and WHOIS History Records

The first course of action would be to look at the WHOIS records of the domain. A WHOIS lookup would reveal the current registrant's details, but in most cases, WHOIS data is redacted for privacy. Thus, it's vital to employ the service of WHOIS history tools so you can see past ownership details.

Our WHOIS history tool revealed that cmtnet[.]net only had one registrant since it was created.



The name of the registrant is Behzad Mesri, with an address in Mashhad, Iran.

Registrant Contact

Registrant Name: Behzad Mesri
Registrant Organization: Computer Make Tomorrow
Registrant Street: Arman 12
Registrant City: Mashhad
Registrant State/Province: Khor
Registrant Postal Code: 91793
Registrant Country: IRAN (ISLAMIC REPUBLIC OF)
Registrant Email: behzadmesri@gmail.com
Registrant Phone: 989355695454

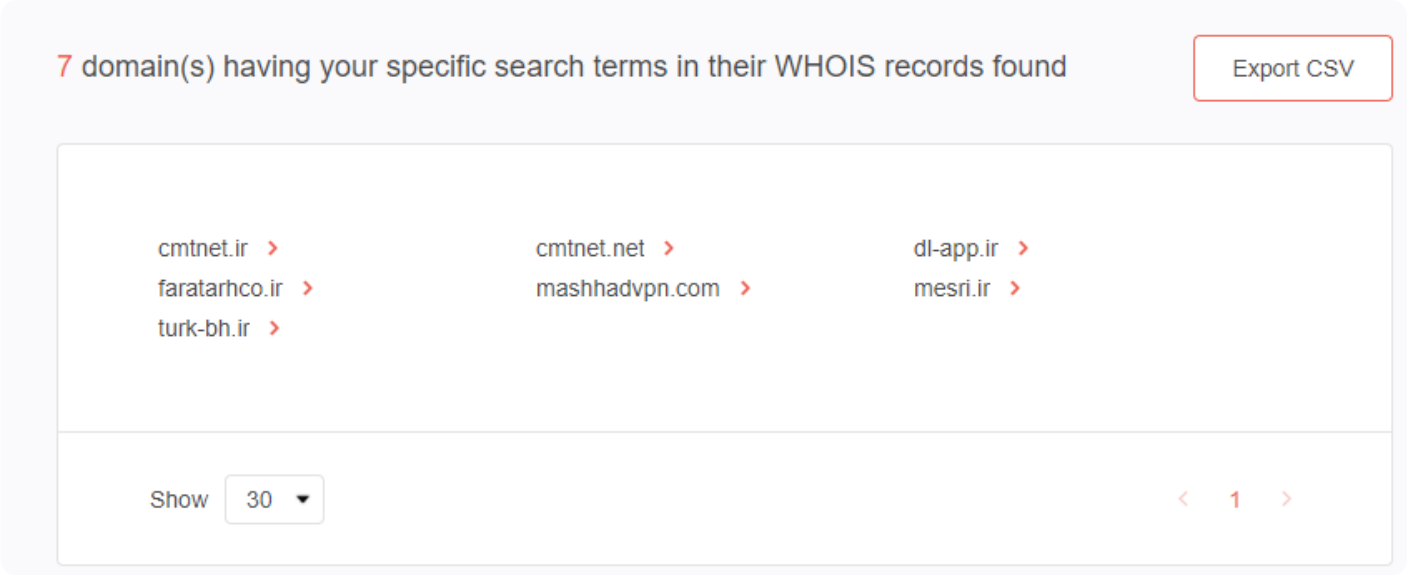
Cybersecurity forensics experts can perform more in-depth investigations to unearth social media connections and other associations by using the name, organization, email address, and phone number in the historical WHOIS record.

Mesri has been wanted for the HBO hacking and other cybercrimes since February 2019. He is also believed to be working with a state-backed hacking organization, so exploring possible connections and associations is a must to prevent Mesri and his cohorts from victimizing other

organizations.

Look for More Connections with Reverse WHOIS Search

Armed with a name and other registrant details, cybersecurity forensics experts can pull up all associated domains by performing a reverse WHOIS lookup. There are seven domain names with “Behzad Mesri” in the registrant name field.



While some of these domains have already been dropped, others are still active according to WHOIS and subdomains lookup results. Below are the active domains that Mesri owns, along with their last update dates, expiration date, and nameservers.

- **cmtnet[.]ir:** Updated on 20 May 2017; expires on 21 April 2022; ns15[.]talahost[.]com and ns16[.]talahost[.]com.

- **faratarhco[.]ir:** Updated on 30 October 2017; expires on 10 December 2022; ns17[.]talahost[.]com and ns18[.]talahost[.]com. The domain has three

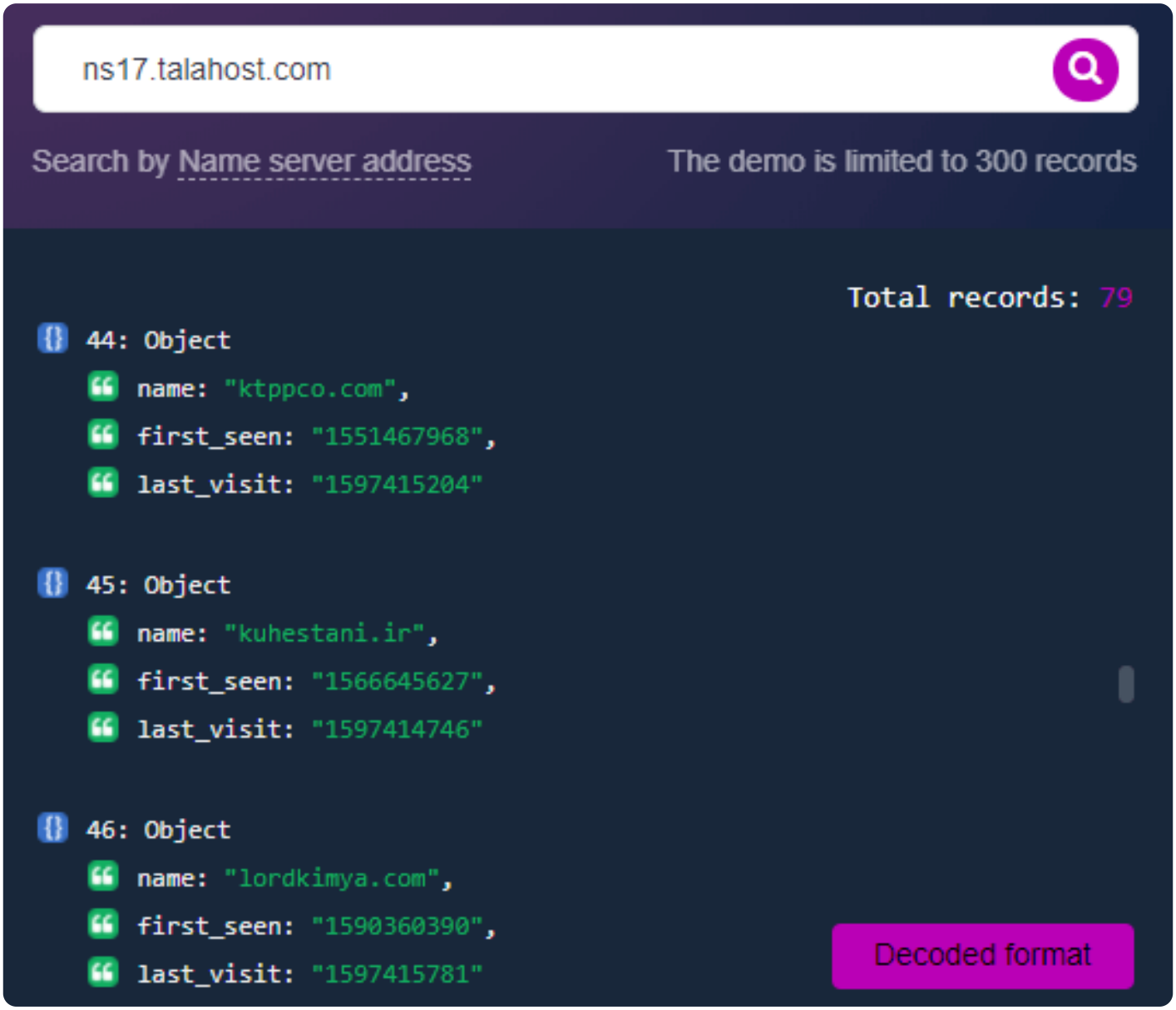
subdomains—webmail[.]faratarhco[.]ir, cpanel[.]faratarhco[.]ir, and webdisk[.]faratarhco[.]ir.

- **mesri[.]ir:** Updated on 30 October 2017; expires on 2 October 2021; ns17[.]talahost[.]com and ns18[.]talahost[.]com. We found three subdomains for mesri[.]ir. These are webdisk[.]mesri[.]ir, cpanel[.]mesri.ir, and webmail[.]mesri[.]ir.

The domain turk-bh[.]ir is also still active as of the time of this writing although it is no longer owned by Mesri. Since 28 October 2019, it has been owned by a M. Zarghami with an address in Tehran, Iran, and the email address b***70@gmail[.]com. Although Mesri dropped the domain in October 2016, the connection between the previous and current owners could be worth exploring.

Nameserver Associations

At this point, we looked at nameserver associations of the three domains that remain active. The domain names use Talahost's nameservers, which, when run through our reverse NS tool, yielded 79 associated domain names.

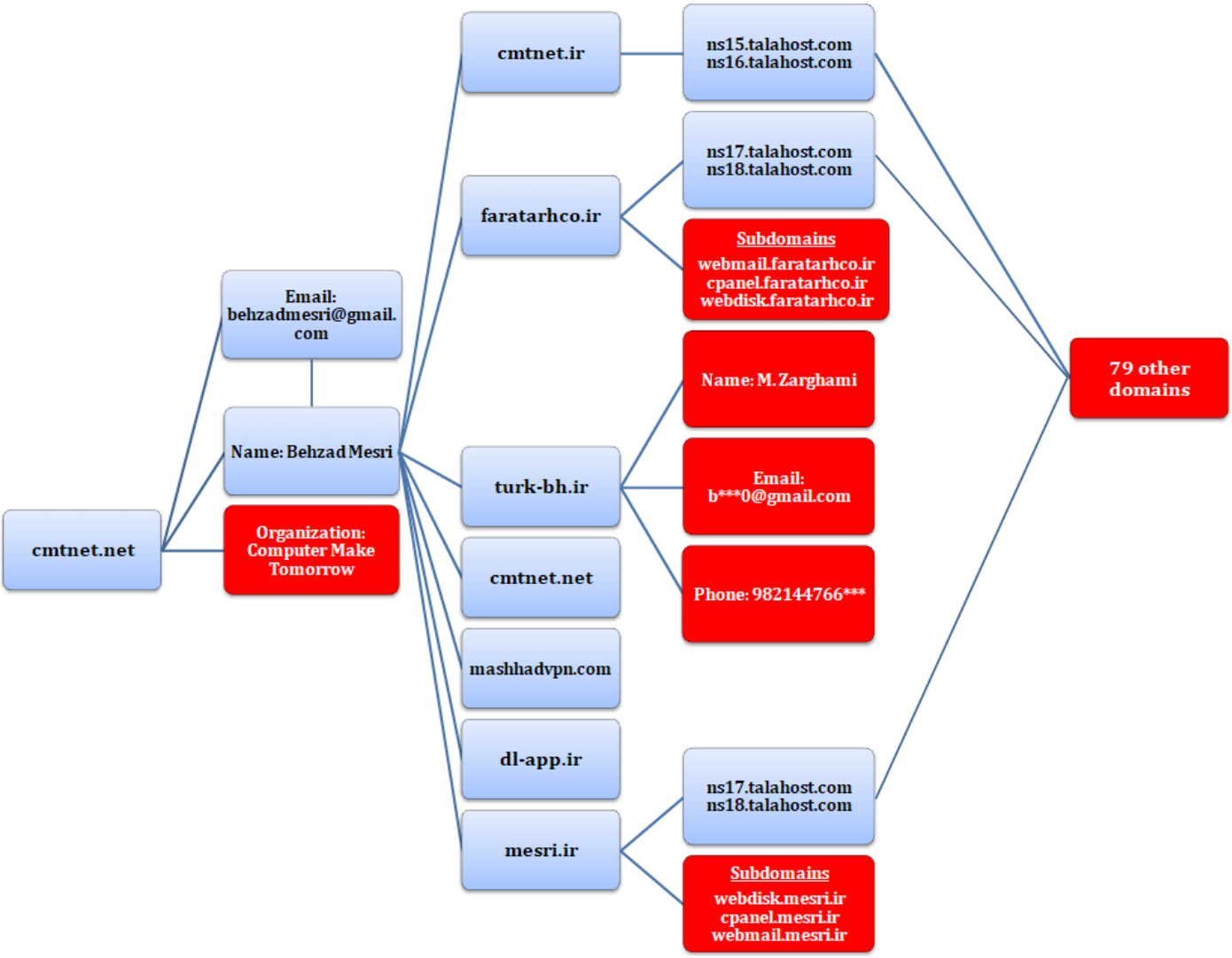


All these domain names should be scrutinized further to see associations with any of Mesri's friends.

To Recap

Although some of the sample case details are hypothetical, you can see how domain intelligence can take you one step further with each piece of evidence. To provide some perspective, the chart below represents how far we've come in uncovering Mesri's digital footprints. To recall the details, we started with the domain cmtnet[.]net and did the following:

- Ran cmtnet[.]net on WHOIS History Lookup to see data before the redaction of records for privacy.
- Used Reverse WHOIS Search to see what other domain names contain the registrant name and email address. Reverse WHOIS returned seven domain names.
- Of the seven domains, only four remain active. Except for turk-bh[.]ir, all active domains are still under Mesri's name.
- Ran the nameserver used by the three domains through Reverse NS API, which returned 79 other domain names.
- Looked up the subdomains of the three active domains using Subdomains Lookup API and found three subdomains each for faratarhco[.]ir and mesri[.]ir.



The red boxes in the chart above represent data points that you can explore further. A reverse WHOIS search on the new owner of turk-bh[.]ir, for instance, could reveal a connection with Mesri outside the domain name. Do they belong to the same hacking group? Or is the new owner only an innocent person who happened to become associated with one of FBI's most wanted cybercriminals?

The 79 domain names that share the same nameserver could also lead to more details and evidence that could have been overlooked had we not used domain intelligence in the investigation. On the other hand, the subdomains found for mesri[.]ir and faratarhco[.]ir should also

be monitored and investigated deeper as they could yield vital information.

A quick search on the company name “Computer Make Tomorrow” doesn’t yield anything conclusive, but a more in-depth investigation could turn up something that could help finding other cybercriminals.

Investigators need all the information they can gather, no matter how insignificant it may seem. We illustrated how domain intelligence sources can enrich cybersecurity forensics. With a single data point, investigators can uncover more data that could later prove to be useful. Each data point can help bring cybersecurity forensics experts closer to solving a case. And even when it doesn’t, each bit of evidence can be used to prevent more people or organizations from becoming victims.