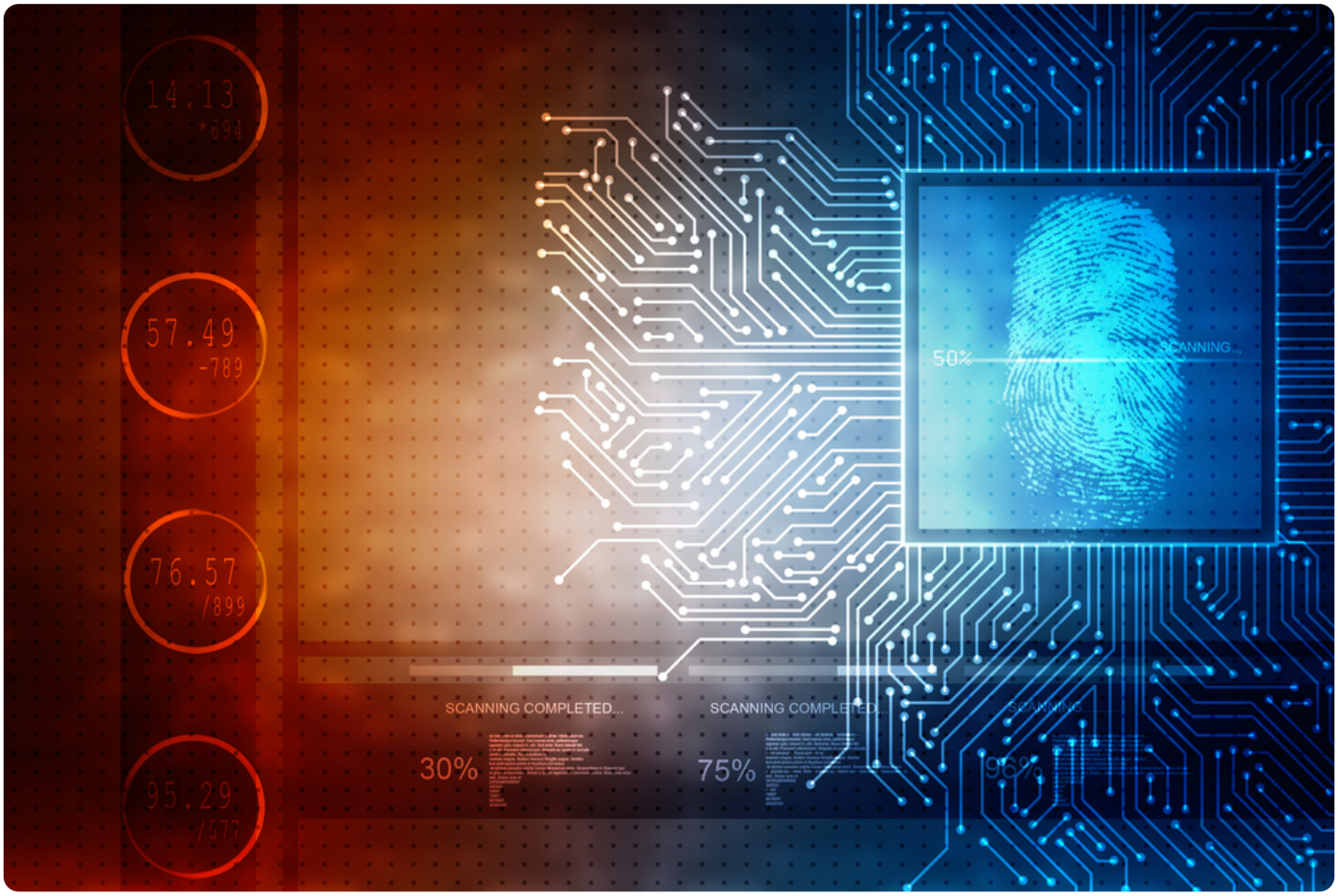
How a Domain Checker Helps in Digital Forensics and Incident Response

Posted on May 15, 2020



Digital forensics and incident response (DFIR) experts have a unique yet essential role in maintaining the overall cybersecurity of any organization. They are responsible for gathering data about ongoing attacks or attempts, mitigating their possible effects, and implementing post-attack actions. That includes digging deeper to obtain evidence to enhance their cyber defense as well as aiding in law enforcement efforts.

The fact that attacks are getting stealthier and more sophisticated, though, in terms of tools, tactics, and procedures (TTPs) make DFIR experts' jobs ever more difficult. They must not only resolve issues in as little time as possible but also be there to prevent successful attacks from causing irreparable damage to systems or their companies' reputations.

Timely detection is, therefore, the answer. Then again, DFIR experts get bombarded by numerous notifications from security tools every day and thus can get easily overwhelmed by false positives. So they need solutions that can help them quickly verify the validity and quality of domains, IP addresses, and email addresses that their users come in contact with. Domain search solutions such as WHOIS Lookup and its API version WHOIS API may just be what they are looking for. Let's discuss the reasons why.

3 Ways to Use a Domain Checker for DFIR

We listed down at least three DFIR responsibilities that domain search solutions can help with below.

1. Thwarting Attempts to Steal Confidential Data

A proactive approach to cybersecurity prevents companies from suffering from the dire consequences of attacks. One way to do that is by beefing up their threat intelligence efforts. Doing so will help them come up with better security protocols and measures, especially in areas where they are likely to be hit.

Digital forensics requires checking network logs to scrutinize the domains, email addresses, and IP addresses that come in contact with network-connected users. DFIR personnel often configure systems to issue alerts when an unknown IP address is, for instance, trying to access a restricted

file.

A quick run through a domain checker can help DFIR experts identify the owner of the IP address in question or the ISP responsible for managing it. Overall, WHOIS Lookup gives them the following details:

- Abuse contact email address
- Registrar
- Registrant's name and contact details (if the IP address is connected to a domain name)

From this, DFIR experts can contact the suspicious IP address's owner or its ISP. If the address doesn't correspond to those of a given organization or has no other legitimate reason for accessing the file (e.g., it doesn't pertain to a business partner, etc.), it can be reported to the authorities and added to a blacklist.

2. Identifying Connected Domains and Other Potential Attack Sources

A study revealed that 200,000 newly registered domains (NRDs) are added to the WHOIS database every day. But what is more interesting to note is that 70% of NRDs are either malicious or suspicious. Given the volume of threat sources, it is often best to proactively identify and block access to all malicious websites.

DFIR experts can use indicators of compromise (IoCs) from published reports and publicly accessible threat databases as a starting point. Additionally, they will be the first to know about newly-registered domains through a repository of their WHOIS records.

From there, they can then collect all domains, IP addresses, and email addresses from these records to use as search terms on a domain search tool. That should provide them with name servers and other registrant details to help identify other potential threat sources that they can then either monitor or block access to outright.

3. Pooling Evidence to Help Law Enforcement Agents Catch the Culprits

What probably sets DFIR experts apart from other cybersecurity professionals is that they often get tapped by law enforcers to provide evidence for litigation purposes. They often submit their analyses and findings to serve as either leads or digital evidence for cases filed against attackers.

WHOIS Lookup often serves as a starting point when investigating cybercrime. It provides digital breadcrumbs that could lead to figuring out who is behind an attack.

DFIR is critical to any company that conducts business online. And so, when it comes to improving your organization's overall cybersecurity posture, it is vital to provide DFIR experts with all the resources they need to mitigate risks, thwart attack attempts, and respond to incidents in real time. One indispensable solution that their arsenals must contain is a domain checker such as WHOIS Lookup or WHOIS API. Start arming your DFIR team with the right WHOIS data now to help avoid the nasty repercussions of cyberattacks.