How to Build Attacker Profiles By Using Domain Registration History Records

Posted on March 24, 2020

Consider this scenario: You just got wind that a prolific cybercriminal has recently been spotted. You want to avoid joining his/her list of victims, of course. The question is how you go about it. Building attacker profiles, notably with WHOIS, might help.

Of course, that has become harder now that much stricter privacy protection laws like the General Data Protection Regulation (GDPR) are in effect. Typical WHOIS searches for a list of sites to avoid may no longer work since many domain owners, especially in the European Union (EU), can opt to redact their personal information from registration records.

However, using historic WHOIS searches with tools like WHOIS History Search might still be relevant. At least, you can take action against potentially harmful domains registered before WHOIS record redaction became a thing.

In this post, we demonstrate how to build attacker profiles so companies can beef up their existing blocklists.

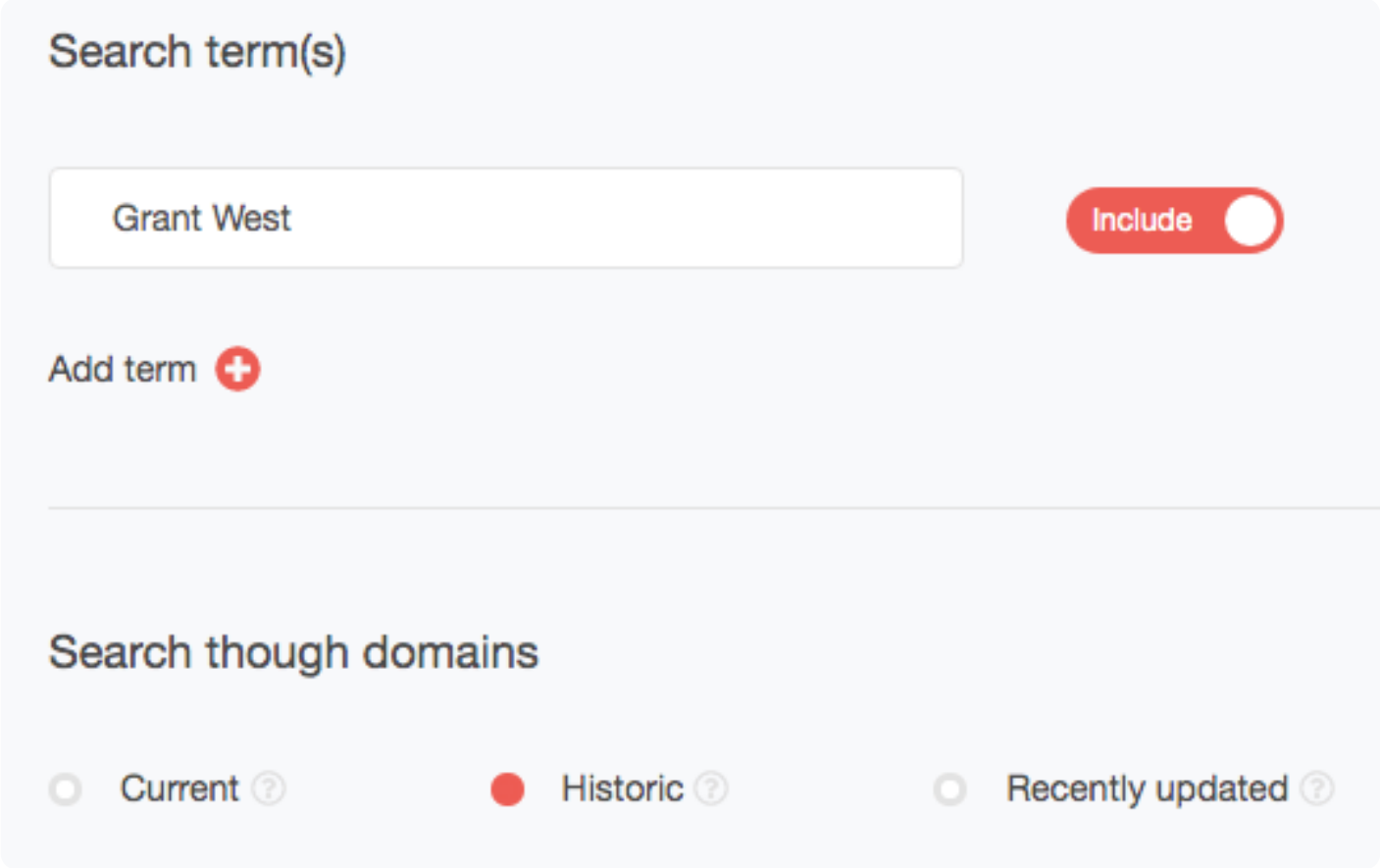
Attacker Profile #1: Grant West

Grant West was convicted just last year for defrauding around US$1.1 million off 100 companies worldwide. He is an EU citizen, so he'd be most likely enjoying the privacy benefits of the GDPR, allowing him to privately register domains.

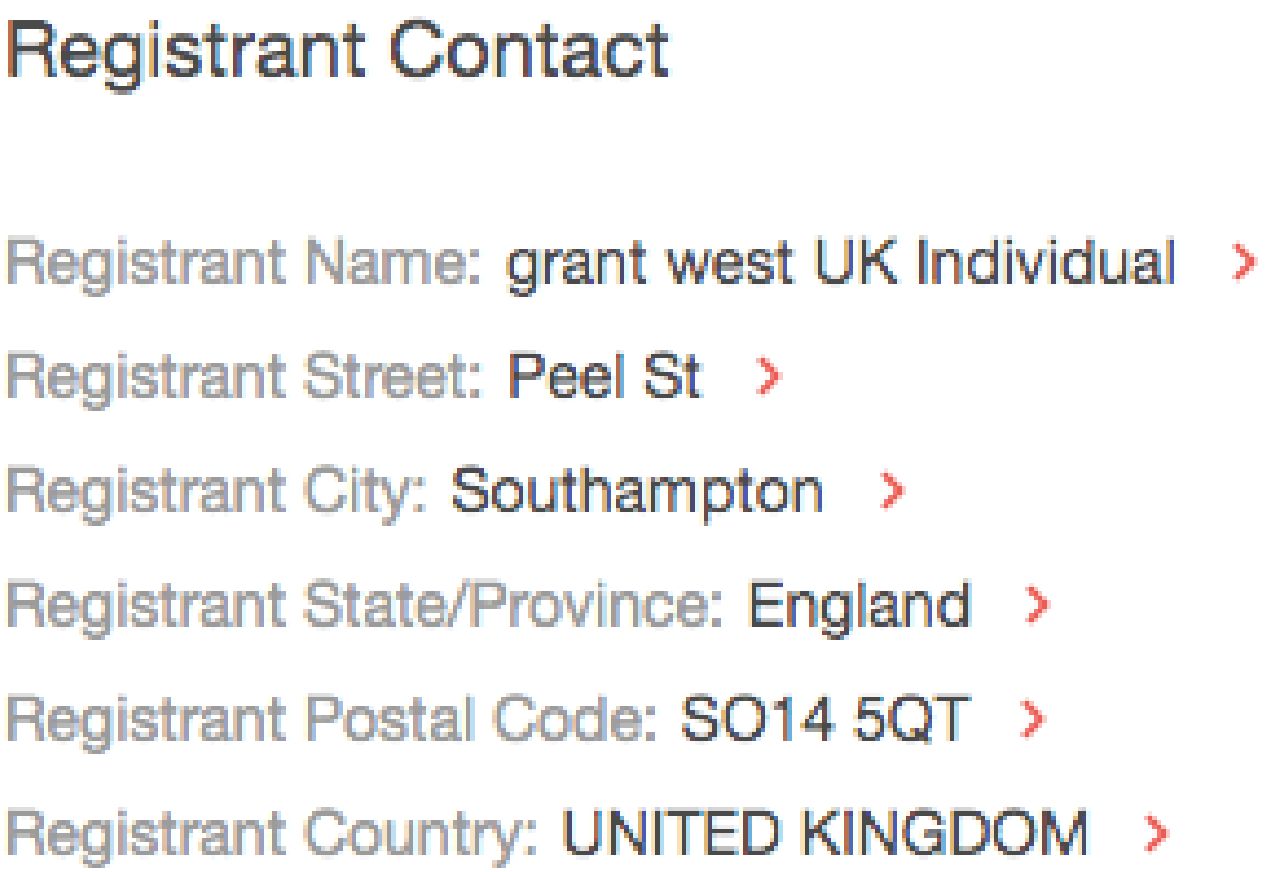
We know from reports that he phished popular brands that include Apple, Groupon, Uber, Sainsbury's, Ladbrokes, T-Mobile, Vitality, the British Cardiovascular Society, and the Finnish Bitcoin Exchange. He used the handle "Courvoisier" in his Dark Web dealings.

Through Domain Research Suite, which WHOIS History Search is a part of, we looked for domains that West registered. Our analysis started by using Reverse WHOIS Search, which allows identifying connected domains based on one or more identifiers typically found in WHOIS records. We typed in "Grant West" as our search term and then we chose to include historical and

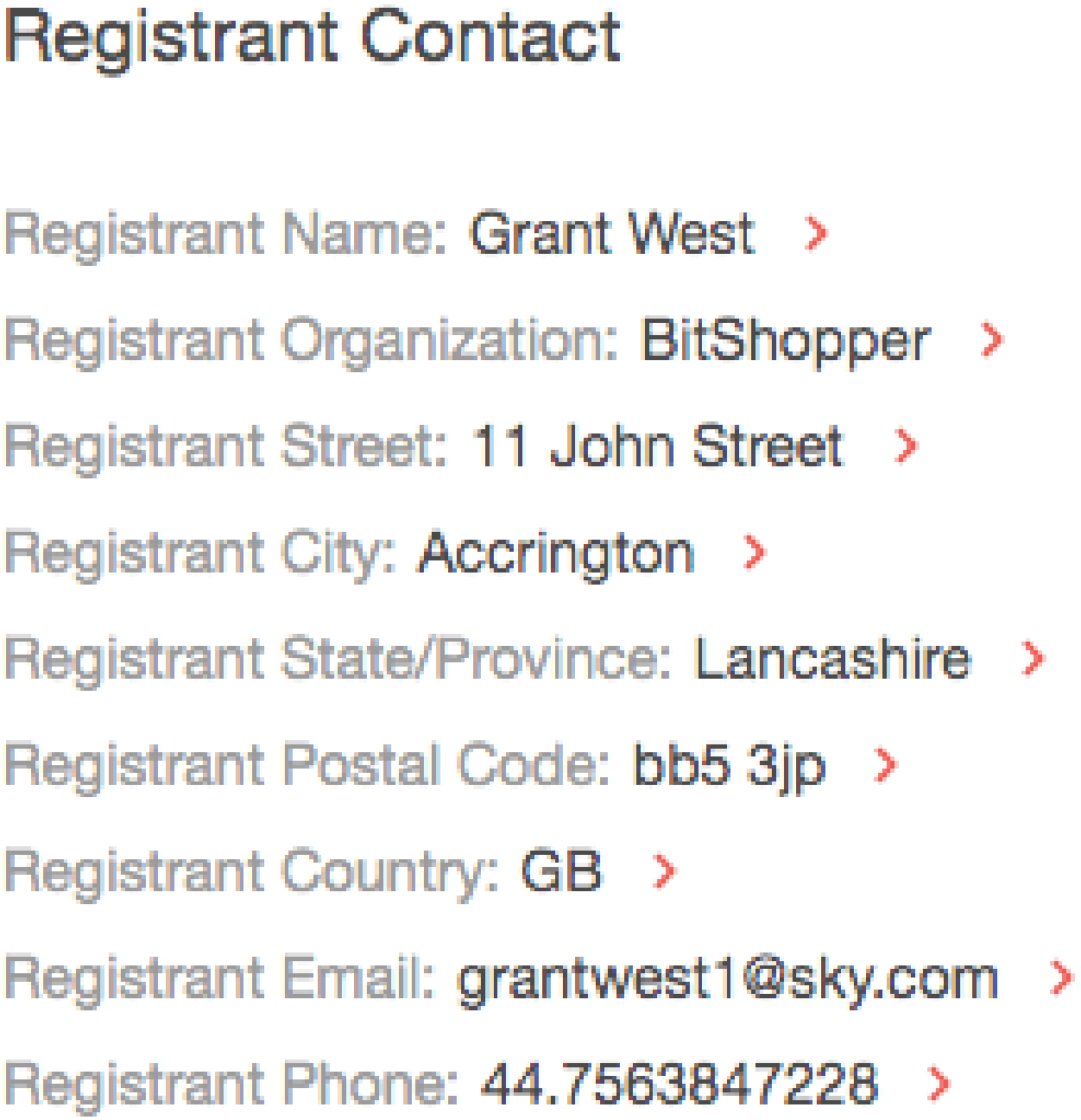
not just recent records.



Our search returned 53 domains. Among these, we built **domain registration history** reports for atlantic-refrigeration[.]co[.]uk, cryptopump[.]net, and soggycat[.]co[.]uk and found that they were indeed owned by an individual named Grant West. There may be others from the list.



Historic WHOIS Record of atlantic-refrigeration[.]co[.]uk from December 29, 2016



Historic WHOIS Record of cryptopump[.]net from January 8, 2014

Historic WHOIS Record of soggycat[.]co[.]uk from June 22, 2017

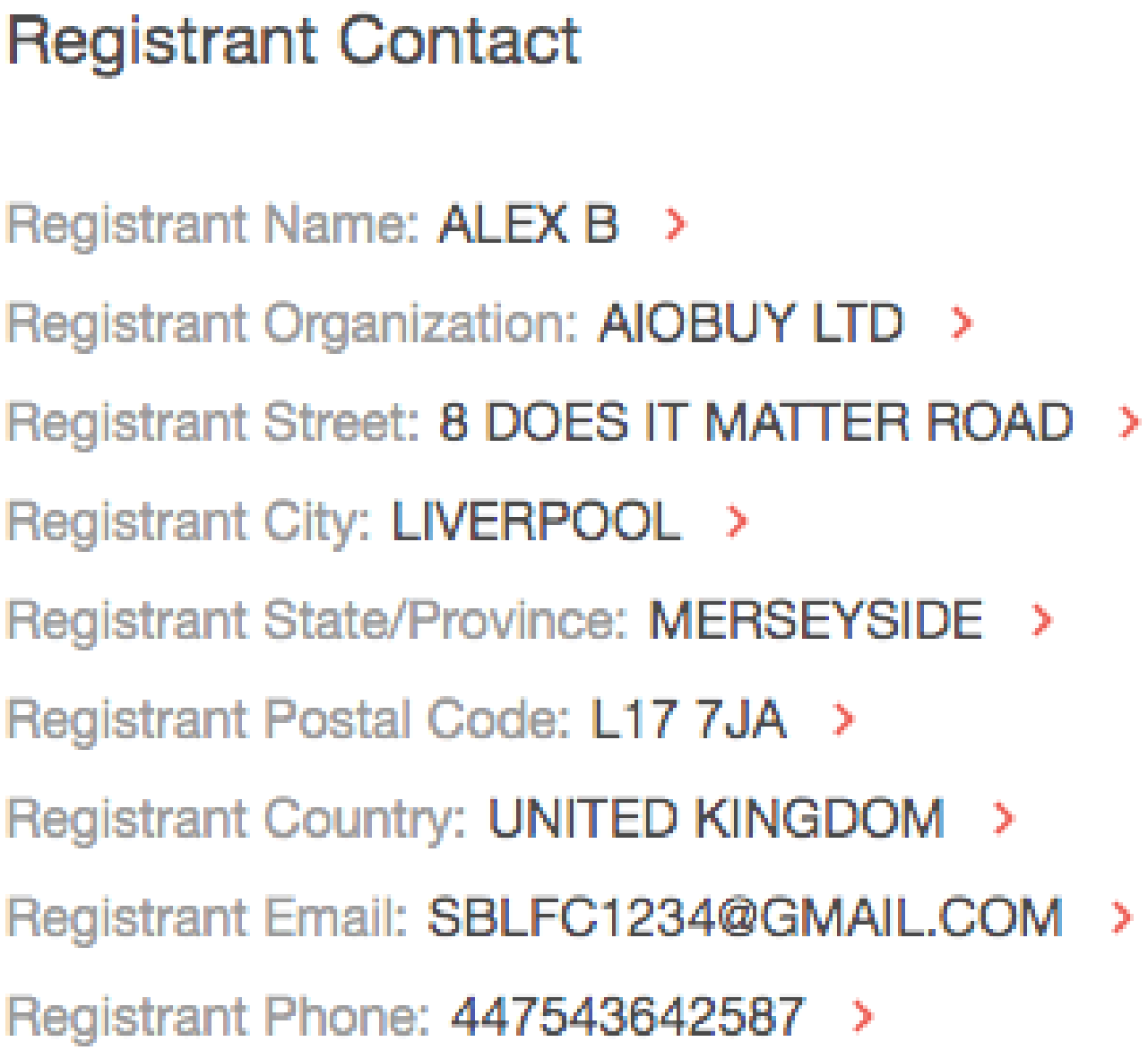
While we can't say for sure that this individual is the same person recently incarcerated for phishing attacks against companies and their customers worldwide, prevention is still better than cure when it comes to cybercrime. Any company that wants to protect its employees from phishing attacks can thus pay closer attention or even block access to these domains.

Attacker Profile #2: Alex Bessell

Alex Bessell was convicted in 2018 for running a botnet used for attacks against companies' applications, including Pokemon Go, Skype, and Google. He also owned a hacker shop called Aiobuy that sold malware and other hacking tools to fellow criminals in the Dark Web and made at least $65,000 during his career. Like West, he is a U.K. citizen.

We followed the same steps used to create West's phishing portfolio. We did not find domains registered by an Alex Bessell, though. But we also know Bessell's online shop's name, so we used

it as our search term, letting us find the domain aiobuy[.]net. We built a **domain registration history** report for the domain and found that on October 1, 2016, it was bought by an individual named Alex B. from the U.K.



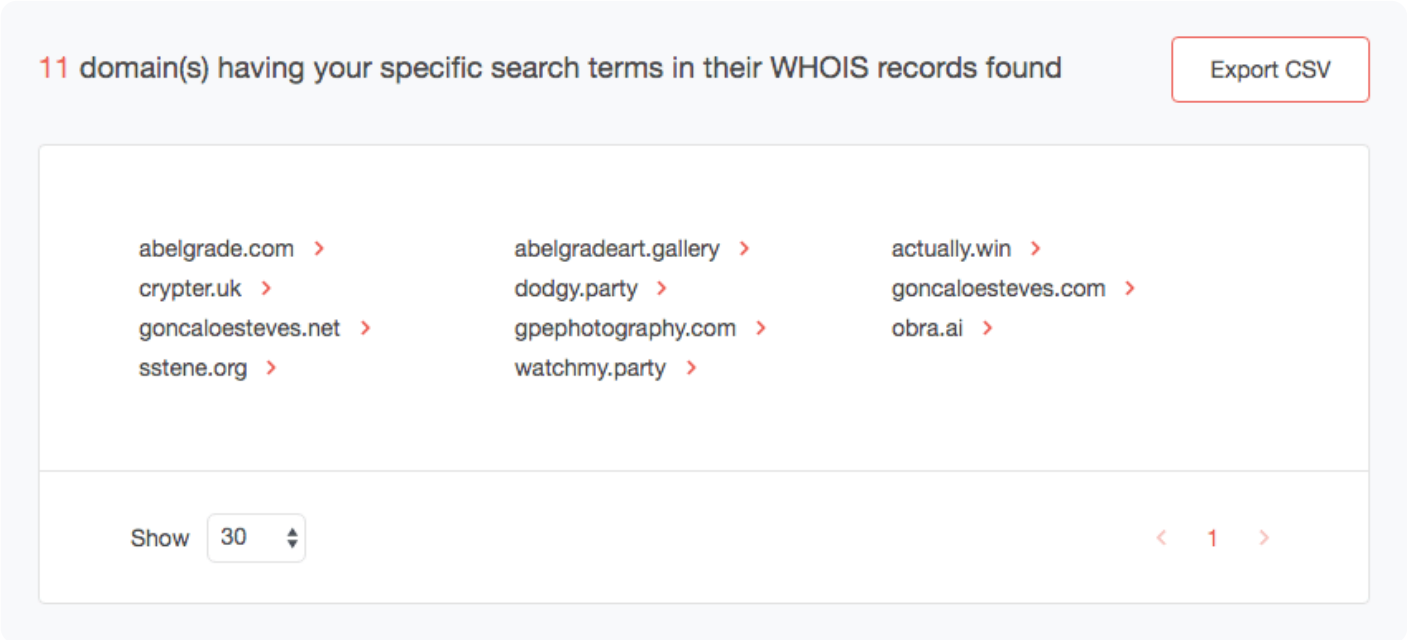
This domain could be part of Blessell's cybercriminal infrastructure. While his shop is located in the deep recesses of the Web that conventional search engines can't crawl, he still needed a way to

trick victims into becoming part of his botnet. He could have used this domain and so companies would do well to scrutinize it and all connected sites and pages.

Attacker Profile #3: Goncalo Esteves

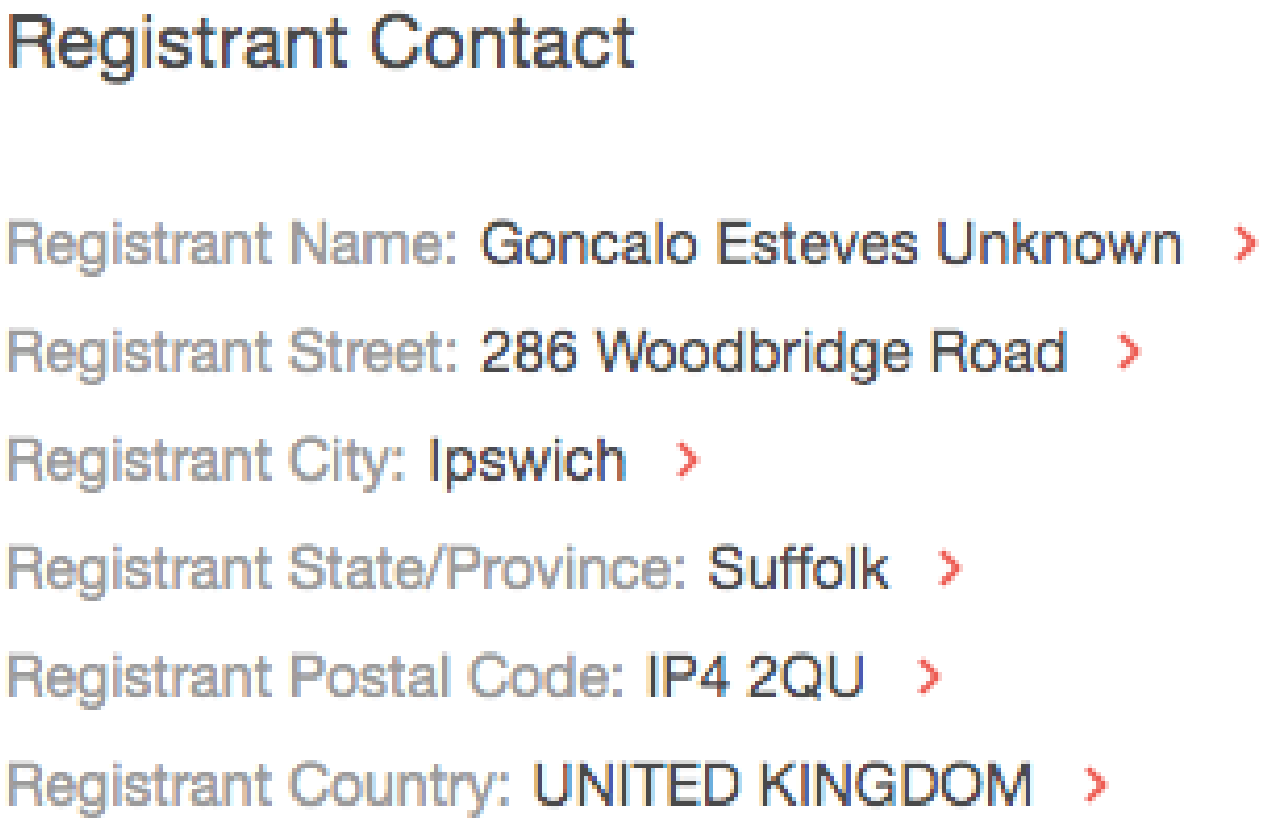
Goncalo Esteves was also convicted in 2018 for selling the antimalware evasion tool Cryptex to fellow criminals, along with money laundering charges. He ran a shop called reFUD[.]me using the handle “KillaMuvz,” allowing him to make around $42,000 in PayPal payments and $21,000 worth of bitcoins before his arrest.

Of course, any company would also want to protect its employees from dealings with shady domains that Esteves may own. So we built his attack portfolio as well using WHOIS tools. We found 11 potentially malicious domains.

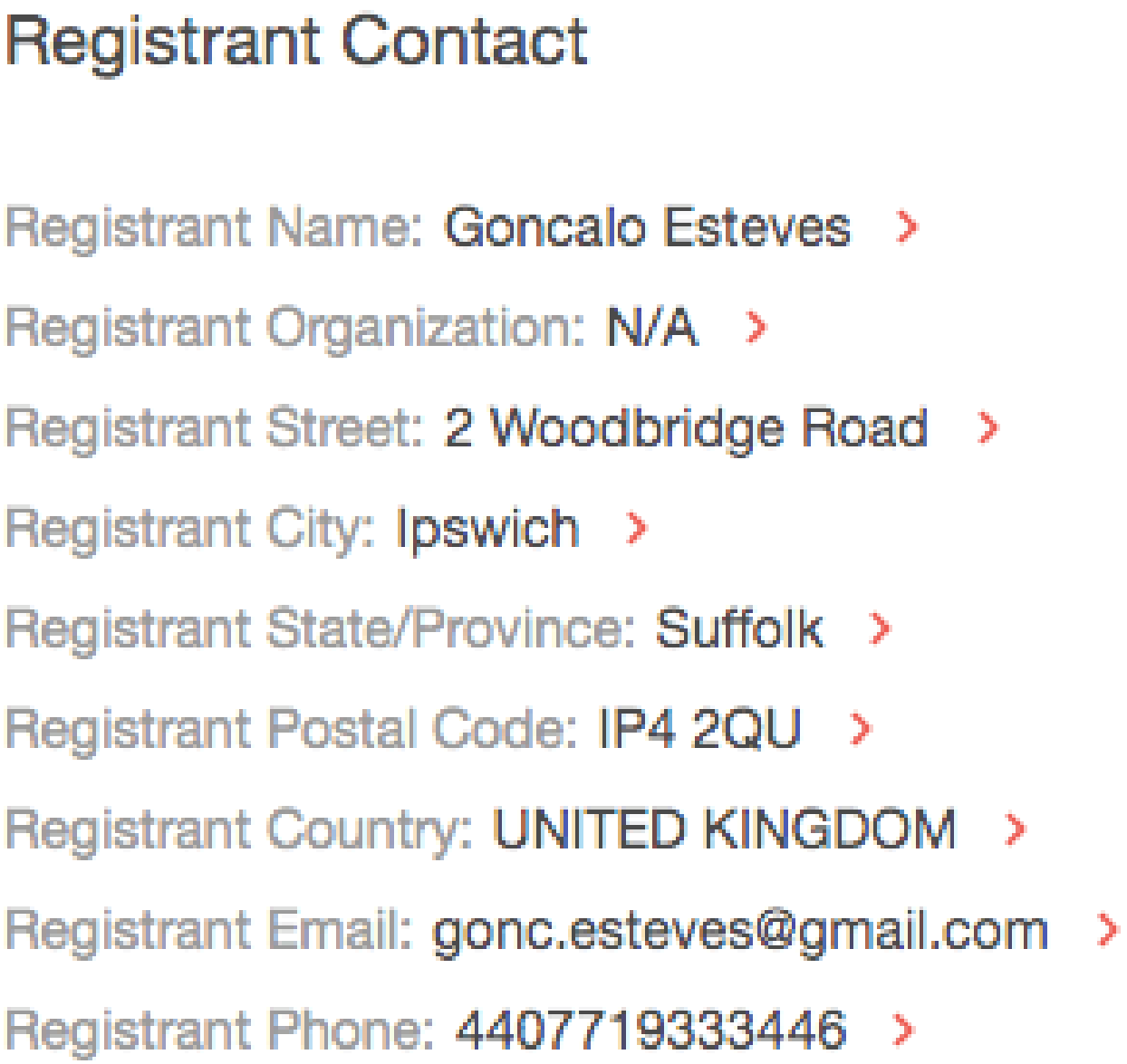


We know that Esteves’s tool is called “Cryptex,” so we built a **domain registration history** report

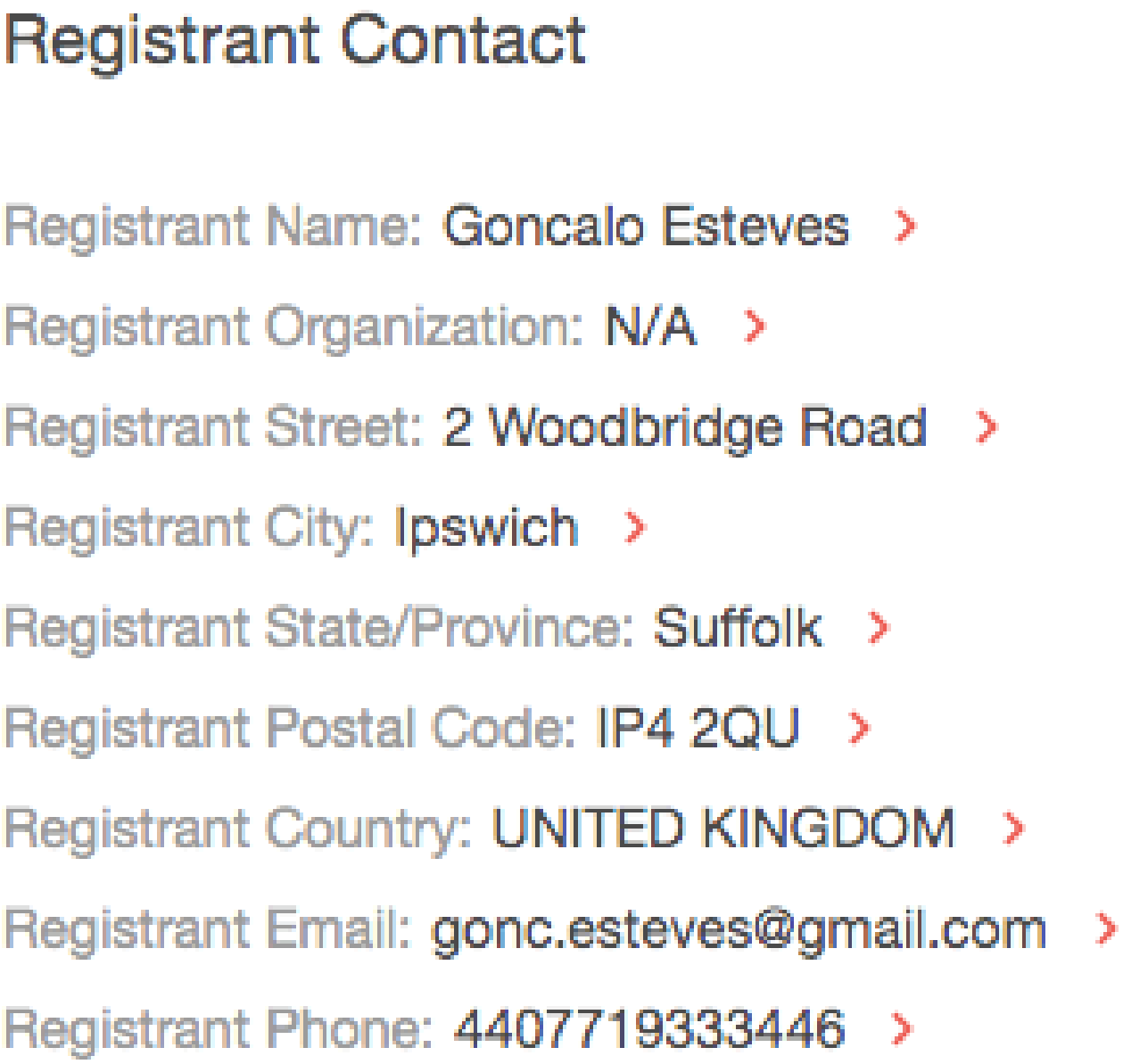
for crypter[.]uk and found that it was indeed owned by someone with the criminal's name who is also from the U.K.



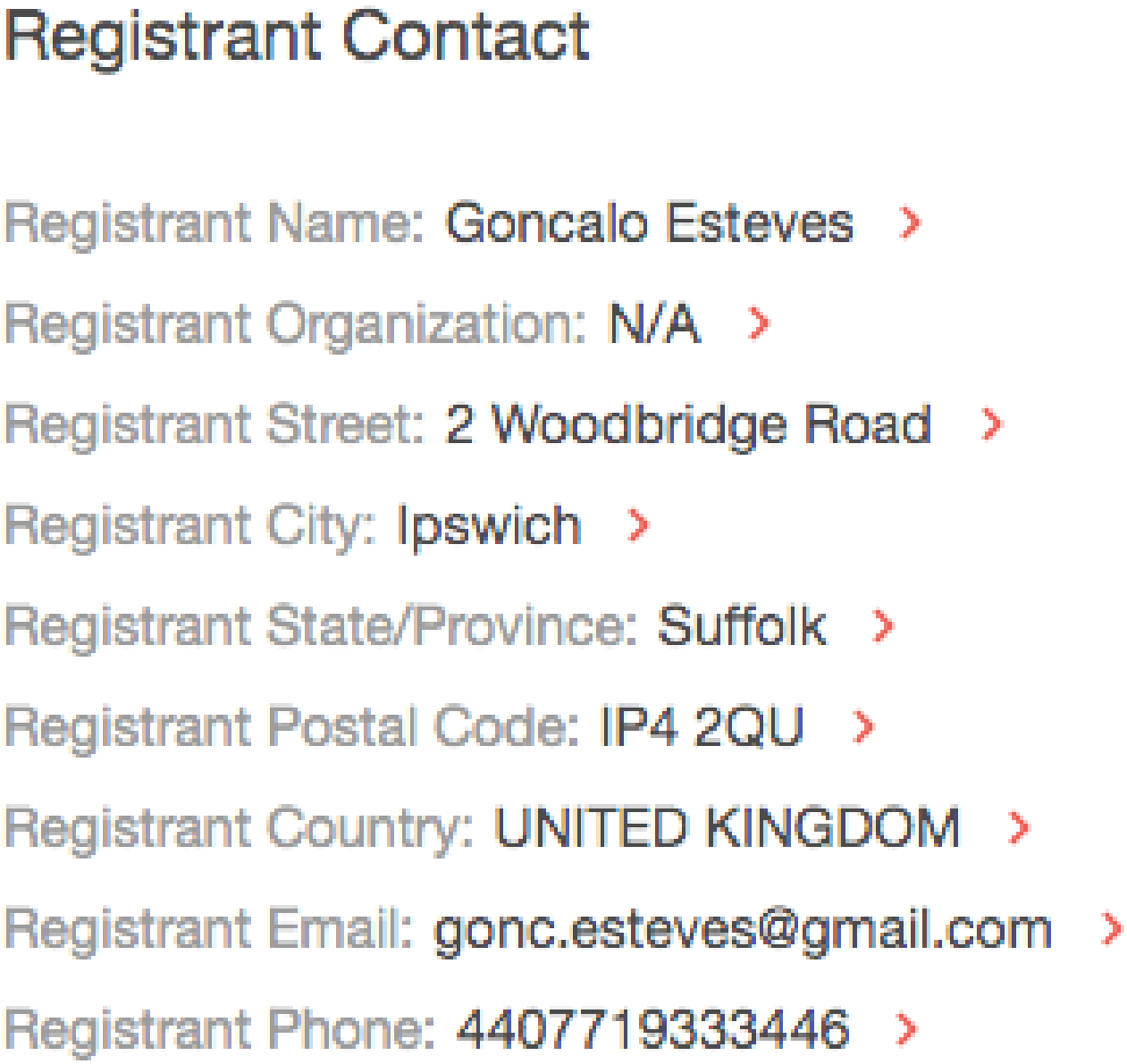
Then we built **domain registration history** reports for dodgy[.]party, watchmy[.]party, and actually[.]win and found that the same individual who owned crypter[.]uk owned them. It may also be a good idea to include these domains in your blacklist.



Historic WHOIS report for dodgy[.]party on August 19, 2015



Historic WHOIS report for watchmy[.]party on September 14, 2015



Historic WHOIS report for actually[.]win on June 17, 2016

While building attacker profiles may seem like a tedious task, it is an effective way of keeping employees and all of a company's digital assets and entire network safe from all kinds of malicious activity that could lead to a devastating breach. WHOIS History Search and other domain research

can be handy for cybersecurity teams who want to make sure their blacklists are up to speed with the latest news and developments in the threat landscape.