How to Look up a Domain's WHOIS Record History to Bolster Cybersecurity

Posted on June 2, 2020

Data breaches could cost organizations an average of $3.92 million per incident. The average ransomware payout, on the other hand, stands at $41,198 per occurrence, with the largest payout recorded to date amounting to $1.14 million. It's essential to be meticulous when it comes to cybersecurity as a seemingly inconsequential hole in an organization's network could result in millions of dollars' worth in damages.

Covering every possible attack vector is, therefore, a must for cybersecurity teams, and one attack vector that cybercriminals often use is a domain name. Ransomware, for instance, usually gets injected into a victim's system through a phishing email that contains a link to a malicious domain. The threat could also unknowingly get dropped onto a victim's computer when he/she visits an infected website.

Therefore, every aspect of a domain should be inspected, including its WHOIS history records. That way, no stones are left unturned, and one cybersecurity product that could prove useful in this regard is WHOIS History Lookup. This tool allows users to look into the ownership history of a given domain, even before a possible redaction of WHOIS records.

Illustrating the Importance of Domain History Using a WHOIS History Lookup Tool

In 2016, researchers uncovered a new ransomware variant called "AlmaLocker." It uses AES-128 cryptography to encrypt selected files on a victim's computer. Upon infection, the actors behind AlmaLocker would demand a ransom payment of 1 Bitcoin within five days.

Source: BleepingComputer

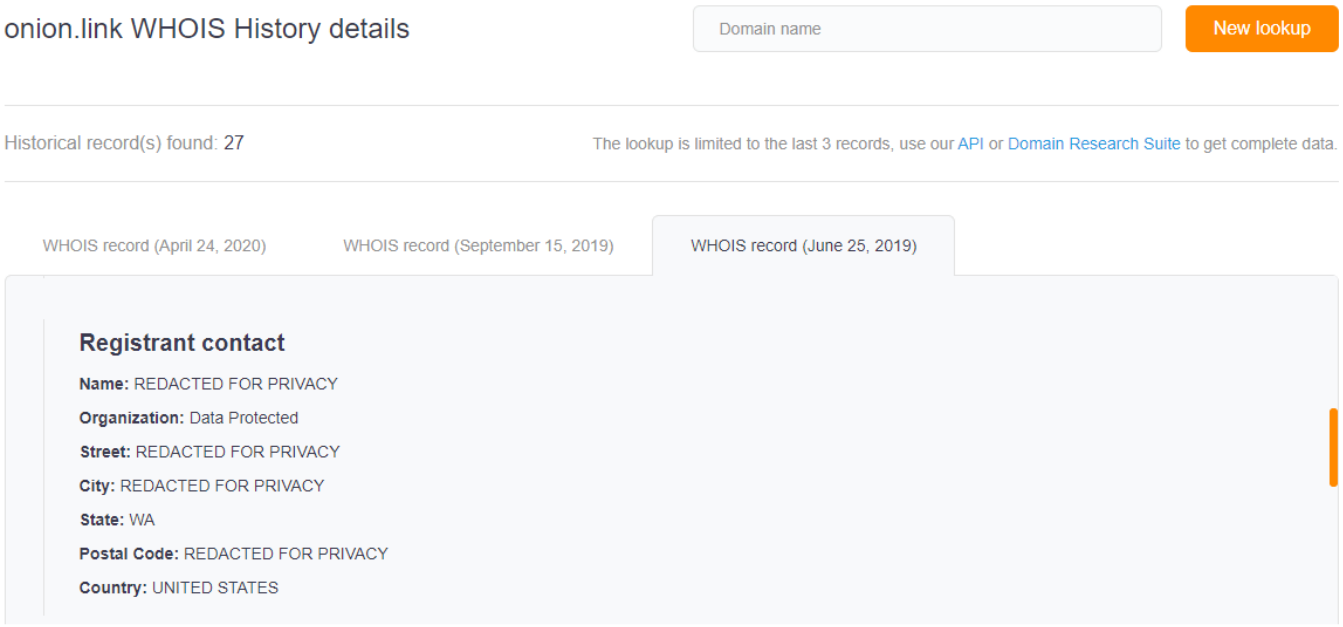
AlmaLocker was among a few ransomware variants released at that time and had a secure encryption algorithm, which meant that it was difficult to reverse-engineer. Still, some cybersecurity experts eventually developed a decryptor, although it did not work for all AlmaLocker types.

Among the indicators of compromise (IoCs) for AlmaLocker was the URL jjuwnj2ejjmafg74[.]onion[.]link. Indeed, a quick check on VirusTotal reveals that the URL and the parsed domain name onion[.]link are malicious. Cybersecurity protocols would likely dictate that the domain name be blocked from any network so it won't cause any harm. However, if you want to bolster your organization's cybersecurity posture, you'll dig deeper.

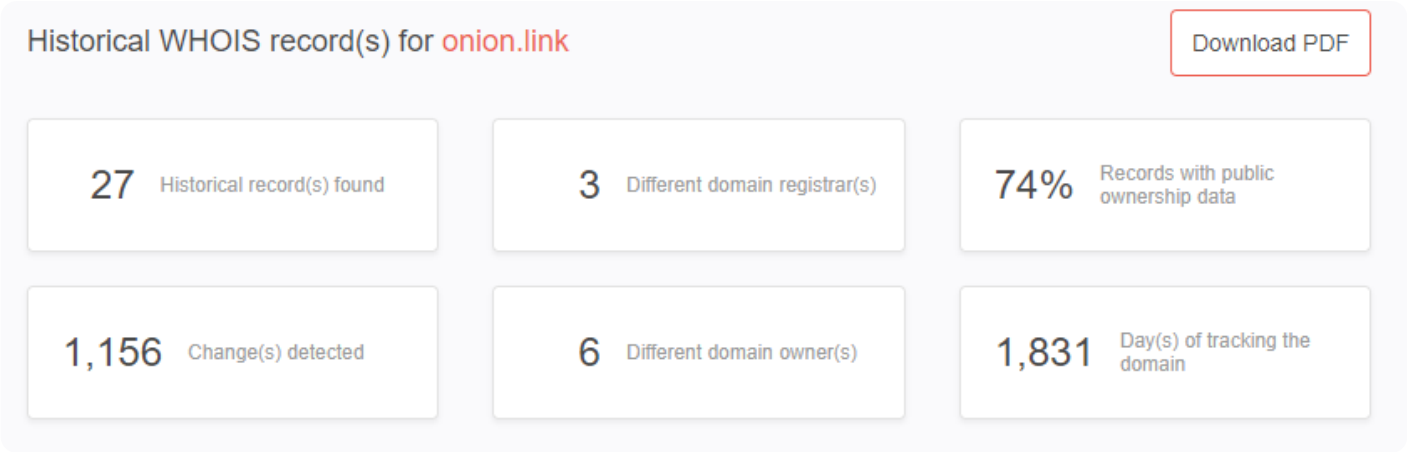
Checking a Domain's Record History via a WHOIS History Lookup

Running onion[.]link on WHOIS History Lookup will give you the three most recent ownership records of the domain with the following dates:

- 24 April 2020
- 15 September 2019
- 25 June 2019

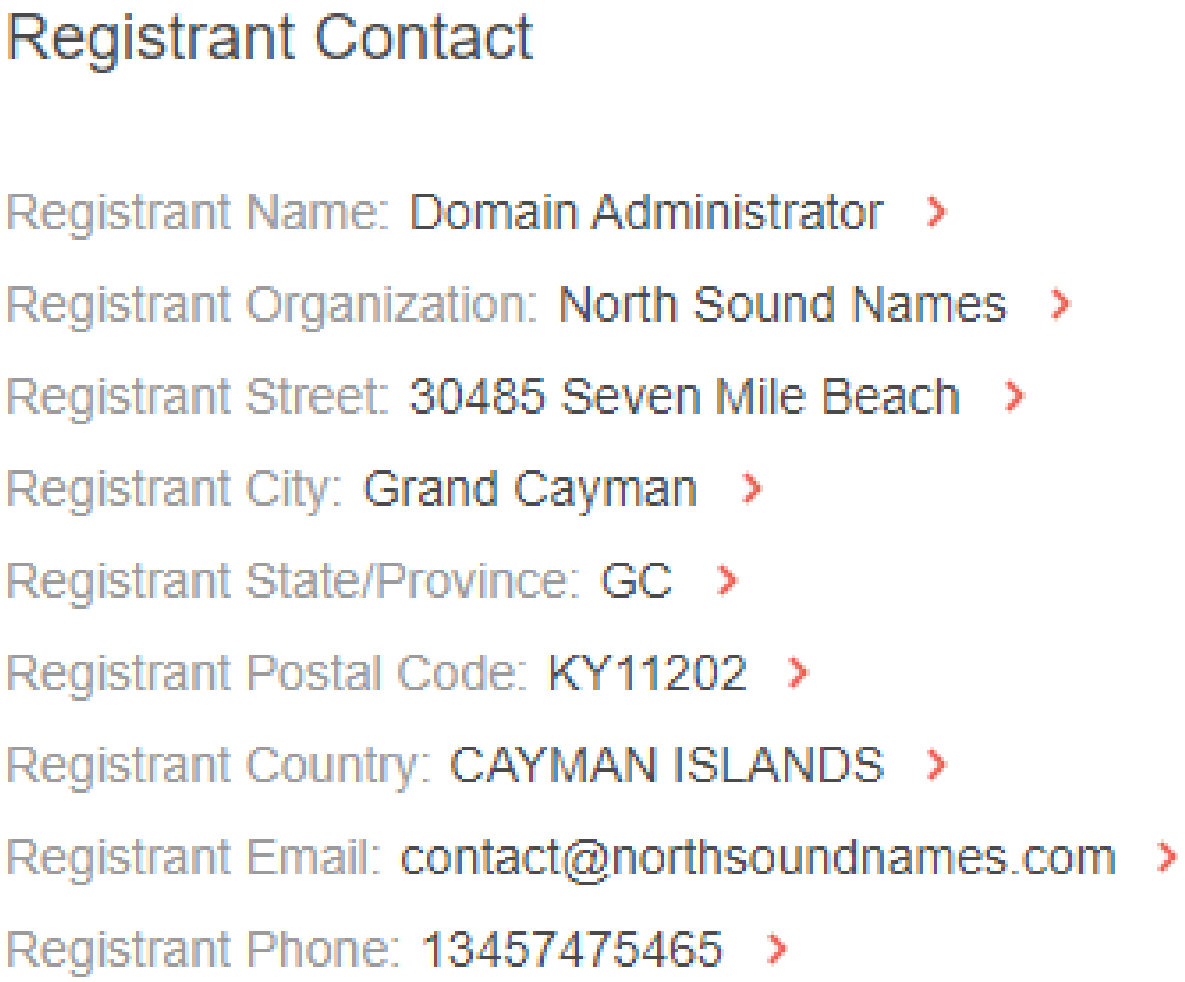


The General Data Protection Regulation (GDPR) was enforced in May 2018. As a result, most WHOIS records following that date have been redacted for privacy. However, WHOIS History Search revealed that the IoC was created way back in March 2015.



Below are the key facts we found about onion[.]link.

- **Its first owner was a domainer.** The domain was initially registered by an individual tied to an organization in the Cayman Islands called “North Sound Names.” As it turned out, North Sound Names was the name used by the top domainer Frank Schilling when he started in the business.

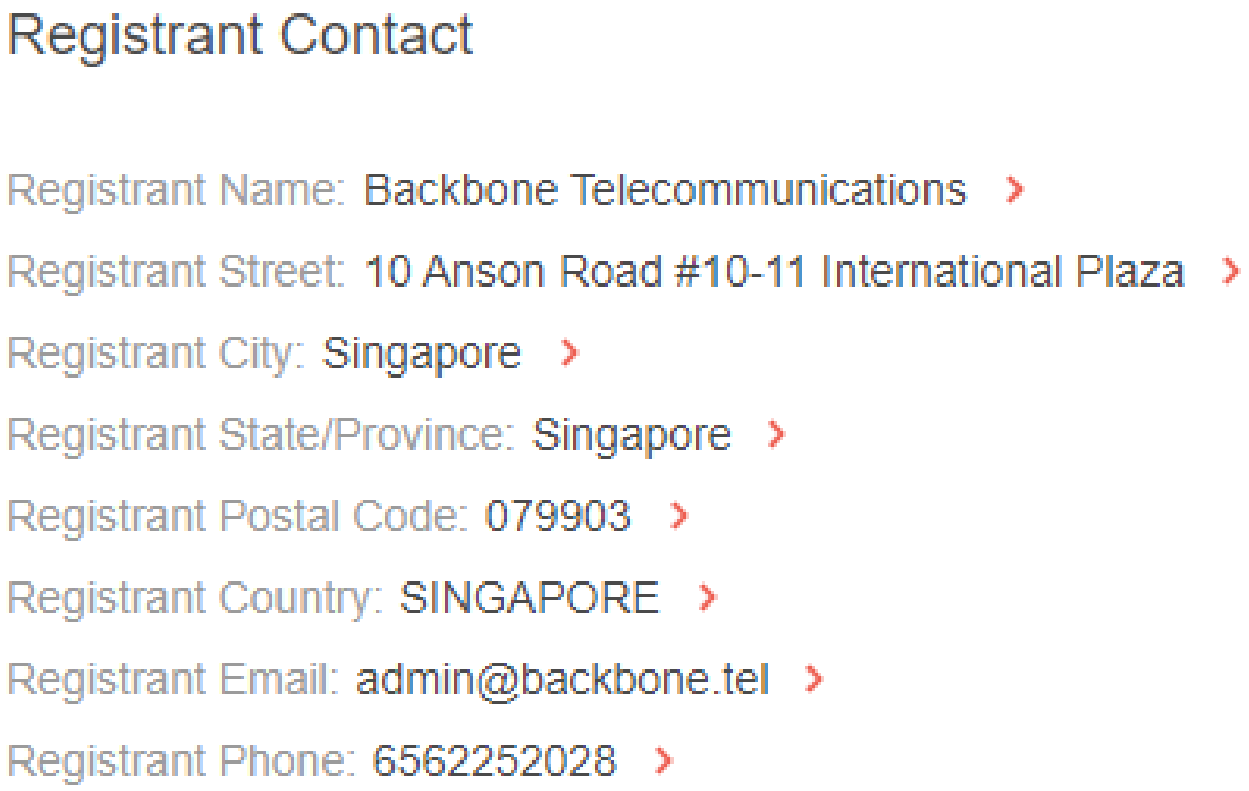


- **The domain was privacy-protected even before GDPR.** From September 2015 to February 2017, the registrant's name changed to "PrivacyDotLink Customer 548072." The street address also changed to P.O. Box 30485 Seven Mile Beach Grand Cayman, Cayman Islands KY11202.

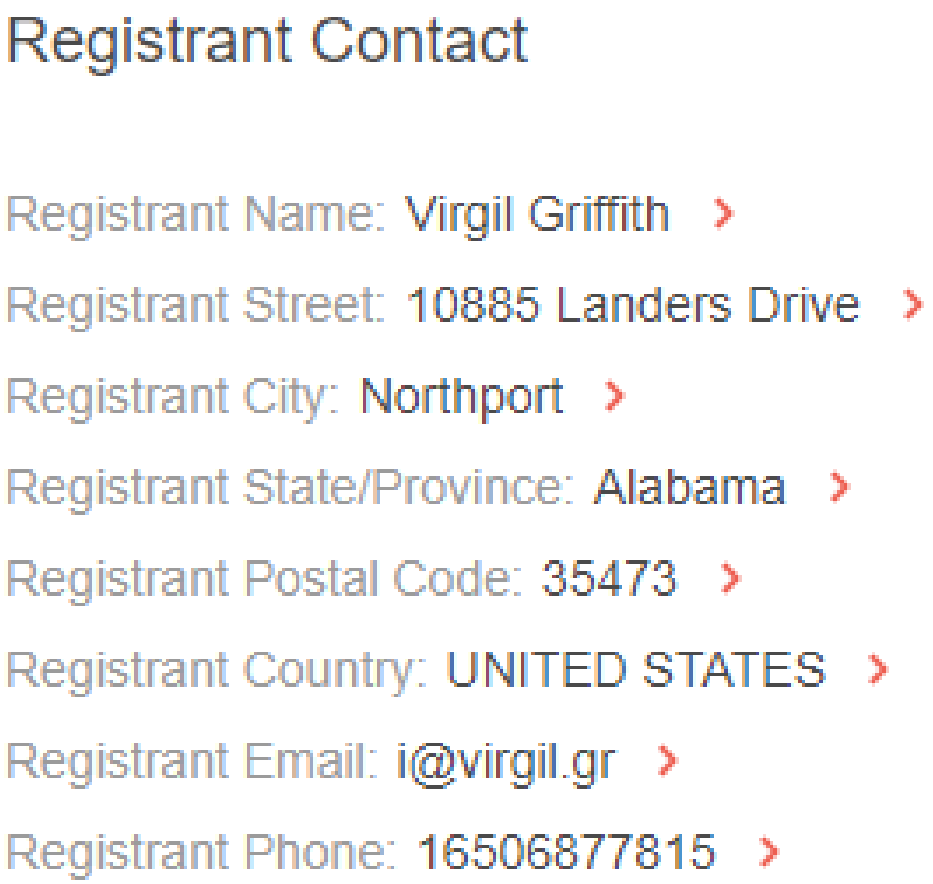
Remember that the domain was reported as an AlmaLocker ransomware IoC on 29 August 2016. That could mean several things: Frank Schilling may have owned the domain name when it was compromised to serve as an AlmaLocker host; or he may have sold it to another person who hid his/her identity before using the domain as an AlmaLocker distributor; or the said possible buyer

may also have been a victim when his/her recent domain acquisition got compromised.

- **A Singaporean company obtained it.** In March 2017, the domain name changed hands. It was registered under Backbone Telecommunications, an IT and computer services company based in Singapore. Records indicate that as of October 2017, the company hadn't renewed its licenses, and so was considered nonexistent. However, it retained ownership of the domain name until April 2018.



- **Programmer Virgil Griffith was its last owner.** In May 2018, the domain name changed hands again. This time, it was registered by Virgil Griffith of 10885 Landers Drive, Northport, Alabama. There weren't many changes to the domain's records until its ownership details were redacted in August 2018, perhaps in compliance with the GDPR.



Griffith is an American programmer, also known as “Romanpoet.” He has been invited to talk at various hacker events. He even went to North Korea to participate in a blockchain and cryptocurrency conference. It is believed that in that conference Griffith explained to North Koreans how to evade economic sanctions by using cryptocurrency. He was arrested on Thanksgiving Day last year.

What Do All These Findings from WHOIS History Records Mean?

Our investigation of the domain onion[.]link using WHOIS History Search proved exhaustive. The

domain that figured in the spread of AlmaLocker ransomware had ties to quite controversial personalities, from a top domainer to a no-longer-existent company to a mysterious programmer. How does this help cybersecurity teams, though?

For one, all the details can serve as a starting point for a more in-depth investigation so organizations can prevent future cybersecurity incidents. Since the domain had ties to the ransomware at the time it was registered under “PrivacyDotLink Customer 548072,” it may be a good idea to find all other domains and IP addresses under the same name – or at least be alerted about those that may belong to “PrivacyDotLink Customer 548072” in the future. Users can utilize the following tools:

- **Registrant Monitor:** Monitor any new domains registered by “PrivacyDotLink Customer 548072.”
- **Reverse WHOIS API:** Find all domains associated with “Virgil Griffith.”
- **DNS Lookup API:** Determine the IP address, nameservers, mail servers, and other Domain Name System (DNS) infrastructure details of the domain.

Tracing the WHOIS history of a domain can provide a wealth of information for cybersecurity teams. And in the age where information is power, organizations need as many relevant intelligence sources as possible. WHOIS History Lookup and Search, along with the tools listed above, can help bolster any organization’s cybersecurity posture.