The Daily Scam Features WhoisXML API’s Domain Abuse Research

Posted on November 21, 2022

The Daily Scam is an online publication that exposes Internet-based scams. The website was developed by Doug Fodeman (Editor-in-Chief) and David Deutsch (Creative Director).

The Daily Scam and its founders acknowledge that online threats increase every year. With that, their goal is to educate people about these threats and how to avoid them. The publication has tackled several issues, including email scams, online and phone fraud, and two-letter country-code scams.

In a recent interview with WhoisXML API’s Head of Marketing and DNS Researcher Alexandre Francois and Senior Project and Contact Marketing Manager Anna Danilova, The Daily Scam helped bring to light the impact of domain abuse on different types of threats.

“It doesn’t matter whether you are targeted by a malicious text, email, fake ad, or social media post. A vast majority of these threats rely on using a domain name as part of the fraud. And that is especially true if the threat is a malware trap. A website is usually set up where the malware lies in wait and you are sent a trigger. That website is first set up with a domain name,” read part of The Daily Scam’s newsletter featuring the interview.

Domain Abuse Paves the Way for Scams

The Daily Scam and WhoisXML API collaboration focused on a recently published threat report entitled “Is Your Software a Top Impersonation Target?,” which was also published on the Internet development news platform CircleID.

The researchers found more than 20,000 domain names that mimicked some of the most impersonated software, namely, 7-Zip, TeamViewer, CCleaner, Microsoft Edge, Steam, Zoom, and WhatsApp. A deep dive into the cybersquatting resources revealed that very few could be attributed to legitimate companies.

Another alarming finding is that around 5% have already been reported as malicious by various malware engines. In other words, several cybersquatting domains have already been used in various forms of cyber threats.

Different Phishing Scam Angles

Threat actors are cunning and can exploit every possible angle. As Francois said in the interview, "Threat actors are very smart and fast. They take advantage of every angle, including the COVID-19 pandemic, celebrations like Christmas and Mother's Day, the tax season, current events, the e-commerce boom, and countless other events and incidents."

For instance, Amazon and PayPal account owners can easily mistake the following domains for the official web pages of the imitated companies:

- account-update1-amazon[.]com
- account-update2-amazon[.]com
- account-update3-amazon[.]com
- account-confirm-verification-amazon-sign2[.]com
- paypal-ticketid-158[.]com
- paypal-ticketid-173[.]com
- paypal-ticketid-174[.]com
- paypal-ticketid-178[.]com

Worse, threat actors often couple these domains with legitimate-looking emails or web content.

Another phishing angle discussed during the interview is the use of urgency-inducing words like login, register, pay, authentication (auth), signin, recover and update. When used alongside a company name, there’s a high chance that they can successfully lure victims.

—

The Daily Scam’s extensive effort to educate Internet users about online scams aligns with our vision of making the Internet more secure and transparent. Through this collaboration, we can educate Internet users about the dangers that look-alike domain names pose.

Reiterating the words of CEO Jonathan Zhang, “Cybersecurity requires collaboration between all stakeholders. WhoisXML API’s part is to provide contextual information in the form of WHOIS, IP, and DNS intelligence. Security teams can then use our data to enrich their processes and help contribute to a more transparent and safer Internet.”

Are you a member of the media and looking to collaborate with WhoisXML API? Please check our Research and Media Collaboration program for more information.