Investment-Related Cybersquatting: Another Way to Lose Money?

Table of Contents

Executive Report

This year, the stock market is at its most volatile state due to several factors. Debates abound about whether 2022 will be as bad as 2008, but we'll leave that up to the experts. What we know is, because the stock and forex market status is attracting media and public attention, threat actors might be riding that particular wave.

This study analyzed thousands of web properties containing "nasdaq" as a string. And since the forex market has also been making headlines, we included the search term "forex" in our searches. Our key findings include:

- 760+ Nasdaq-related domains and subdomains added in the past three months, between 1 August and 31 October 2022
- 9,100+ forex-related web properties added within the same period
- Most of the properties were geolocated and registered in the U.S., but several also traced their origins to European and Asian countries
- About one-third of the resolving properties could be traced back to Hetzner Online GmbH as Internet service provider (ISP), while most of the domain registrations were under Namecheap as registrar

Analyzing Market-Related Cybersquatting Resources

To determine how dangerous the investment-related digital properties might be, we used our extensive DNS and IP intelligence sources to determine their locations, ownership details, and content. Below are four questions we sought to answer.

Where Were Most of the Web Properties Located?

The domains containing “nasdaq” and “forex” were mainly registered in the U.S. A significant percentage were also registered in Iceland, but mostly because the registrants employed the services of a privacy redaction provider based in that country.

About 90% of the properties had active IP resolutions, mostly geolocated in the U.S. and Germany.

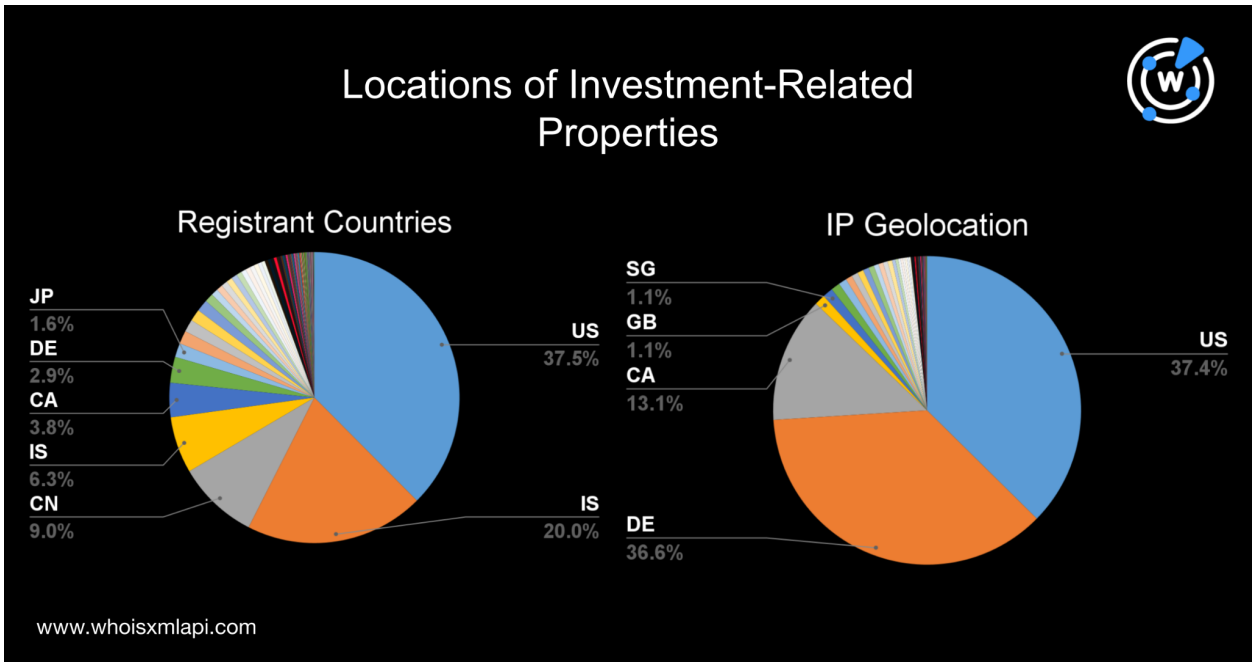


Chart 1: *Registrant countries and IP geolocations of the investment-related cyber resources*

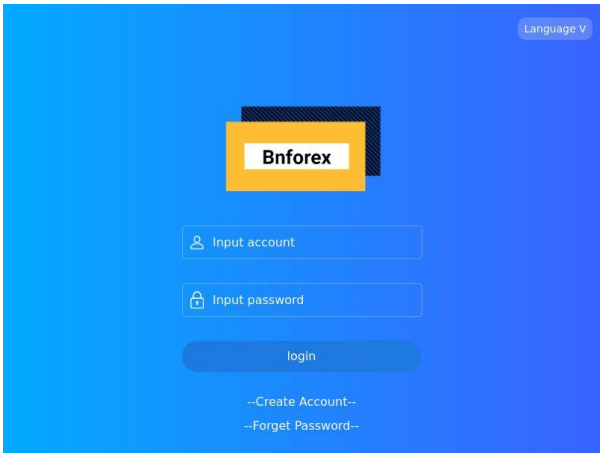
Who Were Responsible for the Cybersquatting Properties?

Most of the web resources were managed by Namecheap, accounting for about 17% of the total volume. It was followed by GoDaddy and GMO with 9.5% and 7.5% shares, respectively.

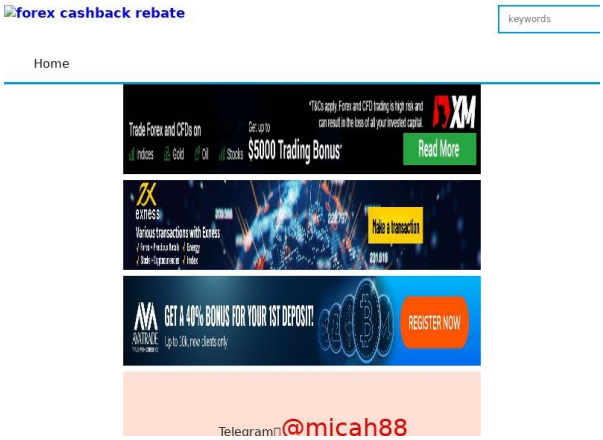
Also, note that almost all of the domains studied had redacted WHOIS records. About 80% of the registrant email addresses we retrieved through a bulk WHOIS search were anonymized.

Were the Cybersquatting Resources Malicious?

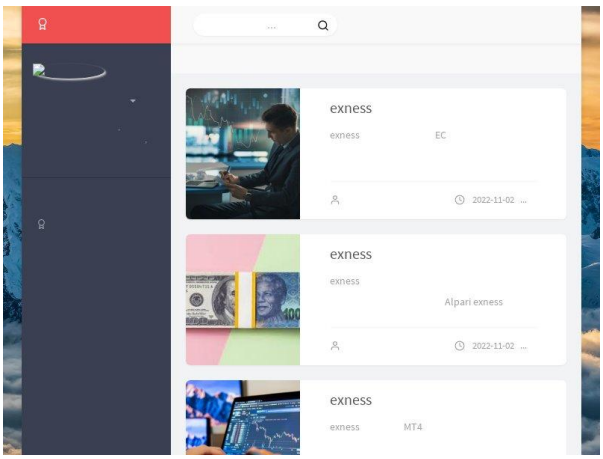
We subjected all the digital properties to a domain malware check and found that several have already figured in malicious campaigns. Despite having been reported, some continued to host live content. A few examples are shown below.



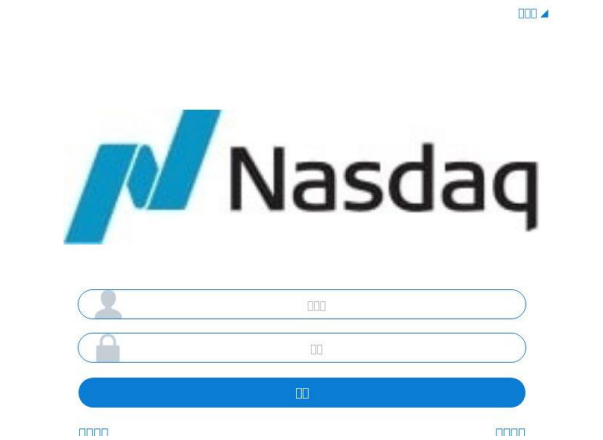
Screenshot of bnforex[.]cc



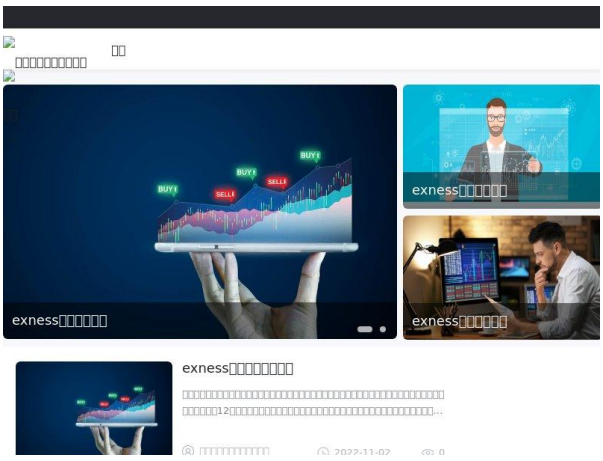
Screenshot of clever-forex[.]com



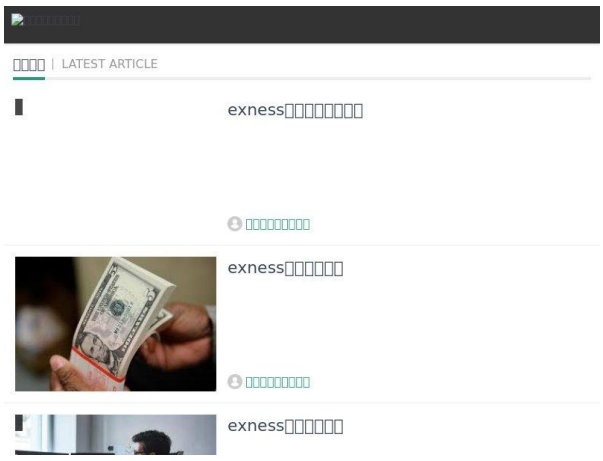
Screenshot of forextrackingnumbercheck[.]com



Screenshot of nasdaqtaiwan[.]com



Screenshot of cheaptabletforforextrading[.]com



Screenshot of forexnasl[.]com

We saw three types of malicious content used in different campaigns after a closer look at the sample malicious domains, namely:

- Login pages likely targeting Nasdaq and forex investors
- Pages that lured users by promising trading and signup bonuses
- Content repeatedly showing the word “Exness,” a popular trading platform

What Content Did the Web Resources Host?

A screenshot lookup on all the resolving resources revealed several domains that hosted the same content as those flagged “malicious.” Below are some examples of domains hosting the same Nasdaq login page as nasdaqtaiwan[.]com.

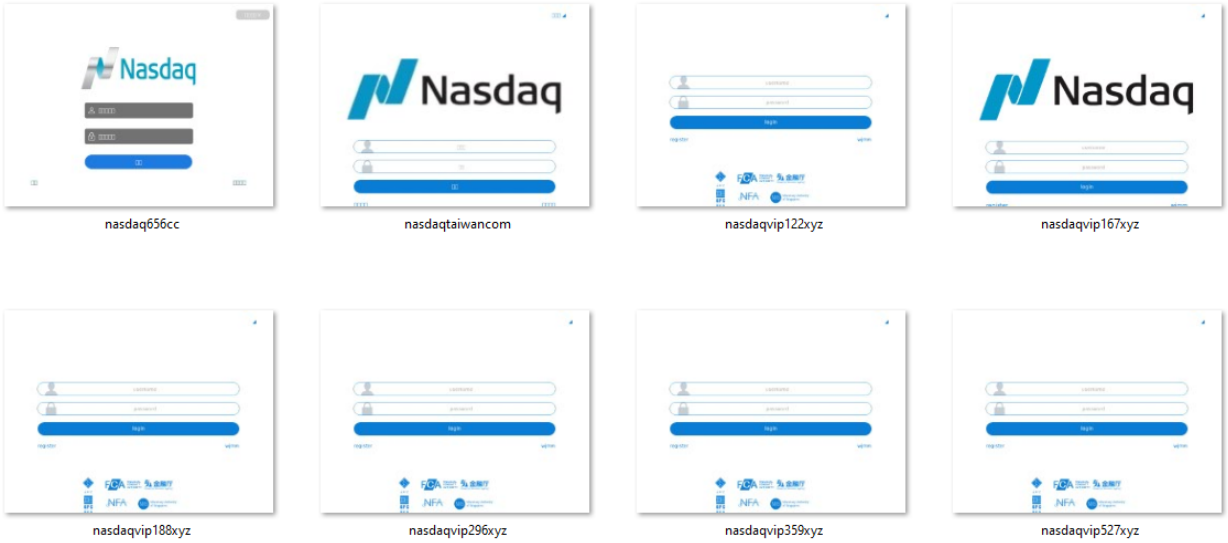


Image 1: *Screenshots of web pages hosting Nasdaq login pages similar to nasdaqtaiwan[.]com*

The following domains hosted content similar to the malicious domain clever-forex[.]com, a page that promised clients up to US$10,000 as a signup bonus. It also featured the same Telegram account.

Image 2: *Screenshots of web pages hosting content similar to clever-forex[.]com*

We also found dozens of domains that looked similar to forextrackingnumbercheck[.]com, with pages showing thumbnail photos seemingly promoting Exness. Several domains seemed to imitate the trading platform.

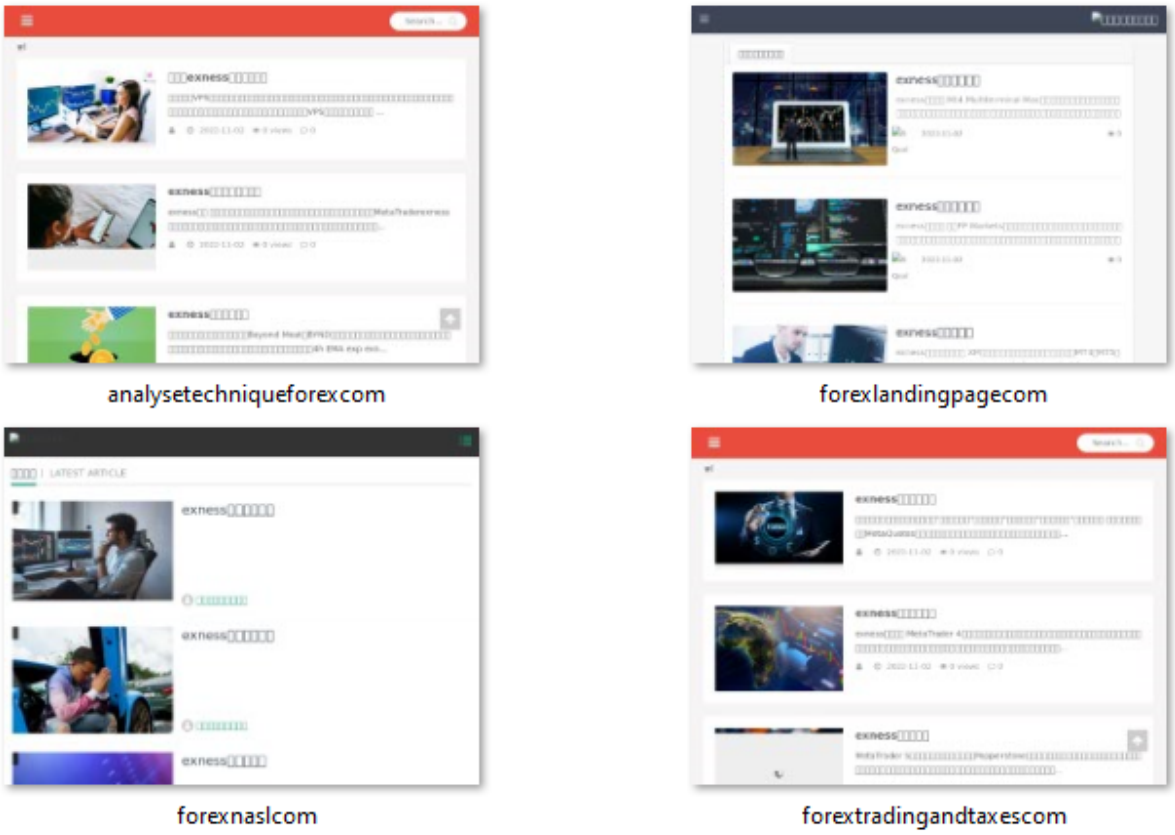
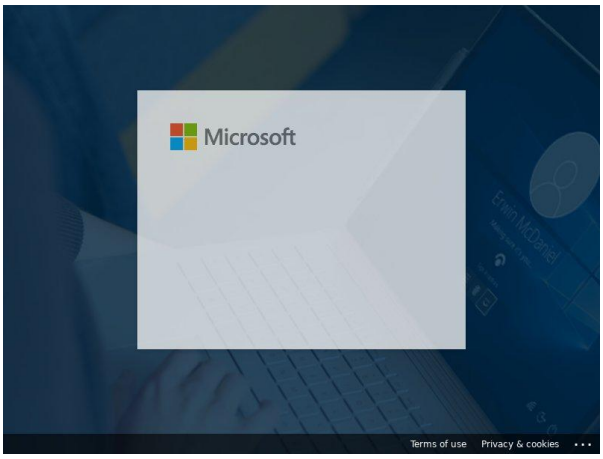


Image 3: *Screenshots of web pages hosting content similar to forextrackingnumbercheck[.]com*

Aside from Exness, some content was also made to look like those of legitimate websites. Here are some examples.



Screenshot of forexdevapifunctions[.]azurewebsites[.]net

Trading Forex

Screenshot of forex[.]lp2m-iainambon[.]id

—

While some of the web properties in this study may be operated by legitimate stock and forex brokers, several may figure in malicious campaigns targeting investors. We already found dozens flagged as malicious and more that could be potentially dangerous.

Aside from educating investors about the dangers of cybersquatting, regular monitoring of investment-related web resources can help detect suspicious domains and subdomains earlier before investors lose money to threat actors.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.