CryptoCoin Rush:

The Next Mining Boomtown Could be your Corporate Website

With hacking for digital coins as lucrative as ever, RiskIQ deployed its crawling infrastructure to map the cryptocurrency mining landscape

RiskIQ's crawling infrastructure downloads and analyzes website content to identify the individual technical components that load when pages render to detect cryptocurrency miners across the internet. We found an influx of revenue-generating miners—which steal CPUs of prospects and customers of well-known brands—in websites in the Alexa top-10,000 and analyzed their attributes, such as prevalence, longevity, and associated infrastructure.

Top-five Top-Level Domains Seen Running Cryptocurrency Miners

Newly Discovered Miners Per Week

RiskIQ detected an average of 495 new hosts running cryptocurrency miners each week over the past 26 weeks.

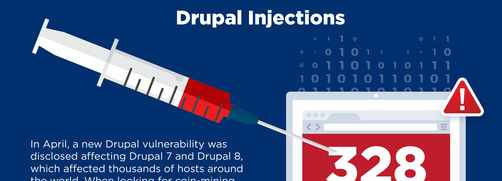
Cryptocurrency Miner Longevity:

Here's how long the longest-lasting cryptocurrency miners were active.

TOP 5

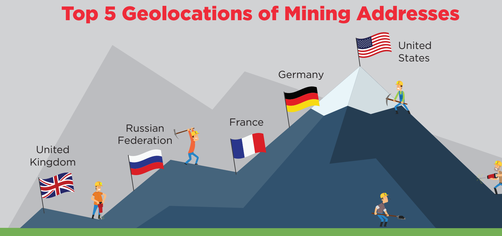
DAYS	DAYS	DAYS	DAYS	DAYS
159.8	160.5	161.7	161.7	162.9

Drupal Injections



In April, a new Drupal vulnerability was disclosed affecting Drupal 7 and Drupal 8, which affected thousands of hosts around the world. When looking for coin-mining scripts, we found drupal injections on 328 distinct hosts.

Top 5 Geolocations of Mining Addresses



Hosts Running Cryptocurrency Miners in the Alexa top-10,000

RiskIQ detected 415 distinct hosts in the Alexa top-10,000, showing even the world's most frequented domains are affected.

CoinHive, the World's Most Popular Cryptocurrency Miner

2,192

So far, RiskIQ has detected 2,192 distinct Coinhive site keys and adding more every day.

50,000

RiskIQ reported back in February that upwards of 50,000 total websites have been observed using Coinhive in the past year–many of them likely without the original owner's knowledge.

Top 5 Cryptocurrency Miners

".FM" TLD Campaign

3,027

RiskIQ detected 3,027 sites on .FM that were hosting cryptocurrency miners. These parked pages are mostly typosquats of famous and well-known trademarks that not only are likely to mislead the public, but also steal their computer resources in the process.

RISKIQ®