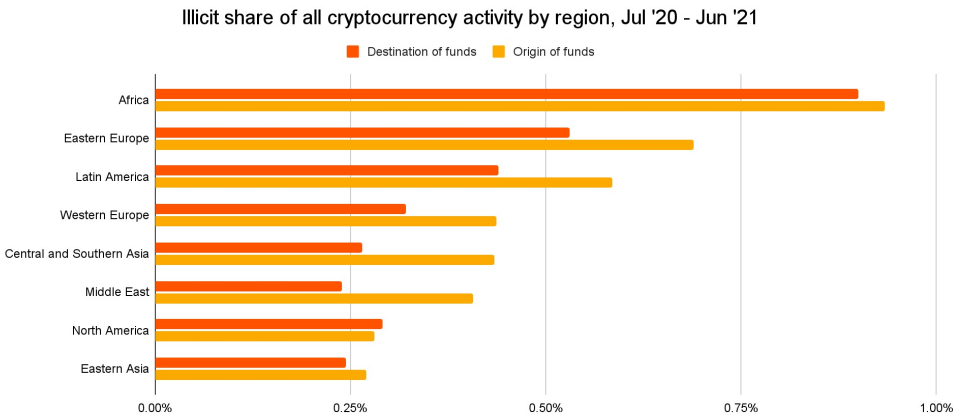
Eastern Europe's Crypto Crime Landscape: Scams Dominate, Plus Significant Ransomware Activity

This blog is a preview of our 2021 Geography of Cryptocurrency report. Sign up here to reserve your copy and we'll email you the full version when it's released this October.

Addresses based in Eastern Europe have the second-highest rate of exposure to illicit addresses behind only Africa.



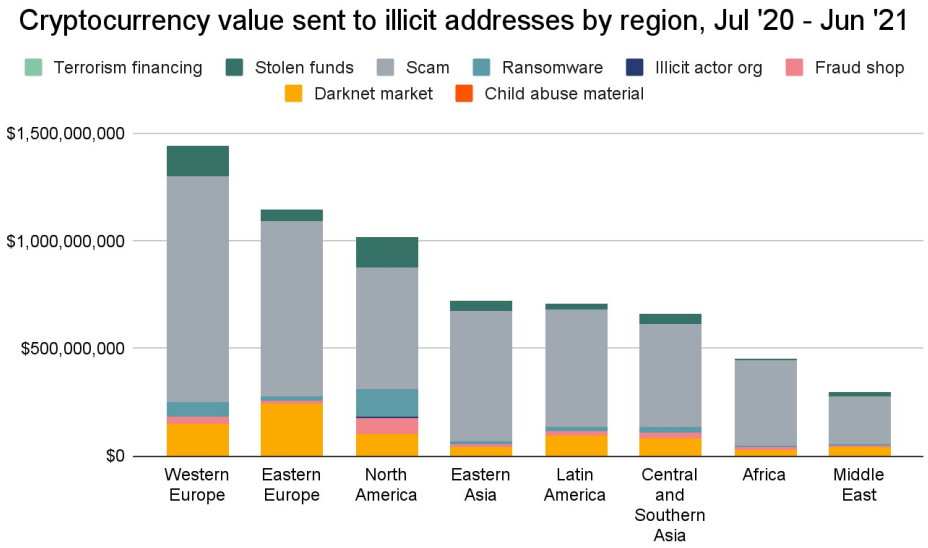
Keep in mind too that Eastern Europe has a much larger overall cryptocurrency economy than Africa, as well as Latin America, the third-ranked region for overall exposure to illicit activity. In fact, Eastern Europe is the only region with a total transaction volume of $400 million or more for which illicit activity makes up more than 0.5% of total cryptocurrency value sent and received.

In terms of raw value, Eastern Europe has sent the second most cryptocurrency of any region to illicit addresses, behind only Western Europe.

PUBLISHED
September 1, 2021

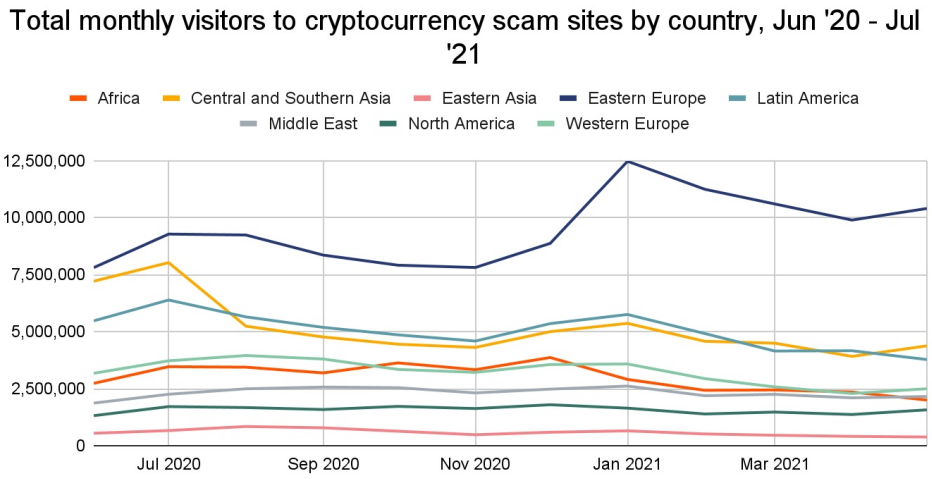
AUTHOR
Chainalysis Team

TOPICS
Chainalysis
Blockchain analysis
Bitcoin
Data
Geographic trends

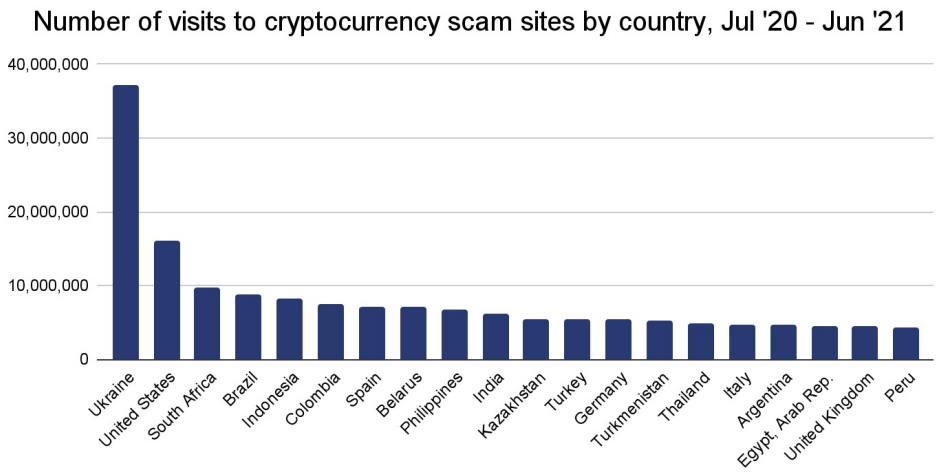


One thing that stands out is that Eastern Europe sends more cryptocurrency to darknet markets than any other region. This is largely due to activity involving Hydra Market. Hydra is the world's biggest darknet market and caters only to users in Russian-speaking countries throughout Eastern Europe. However, as is the case with all regions, scams make up the biggest share of funds sent from Eastern Europe to illicit addresses — we can assume that most of this activity represents victims sending money to scammers. Between June 2020 and July 2021, Eastern Europe-based addresses sent $815 million to scams, second only to Western Europe.

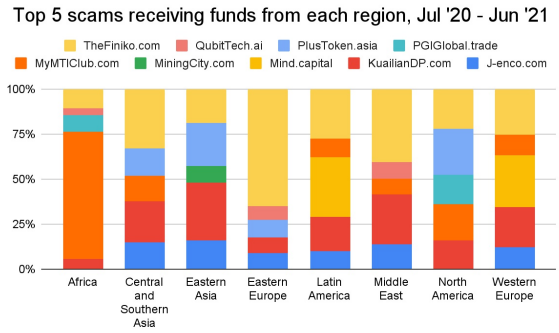
Eastern Europe also sent the most web traffic to scam websites during the time period studied by a wide margin.



Drilling down to the country level, we see that Ukraine accounted for most of this activity, and sends more web traffic to scam websites than any other country, more than doubling the total web visits of the second-ranked country.



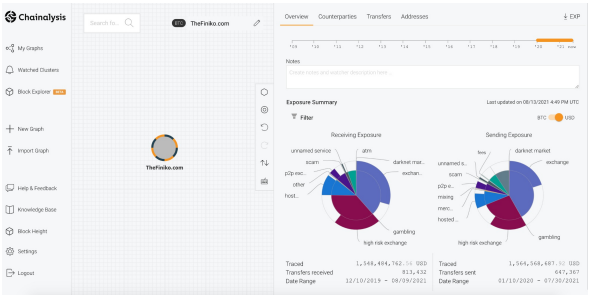
What scams are victimizing cryptocurrency users in Eastern Europe? More than half of the value sent to scam addresses from the region went to one scam: Finiko.



Finiko was a Russia-based Ponzi scheme that collapsed in July 2021, soon after users reported they could no longer withdraw funds from their accounts with the company. Finiko invited users to invest with either Bitcoin or Tether, promising monthly returns of up to 30%, and eventually launched its own coin that traded on several exchanges.

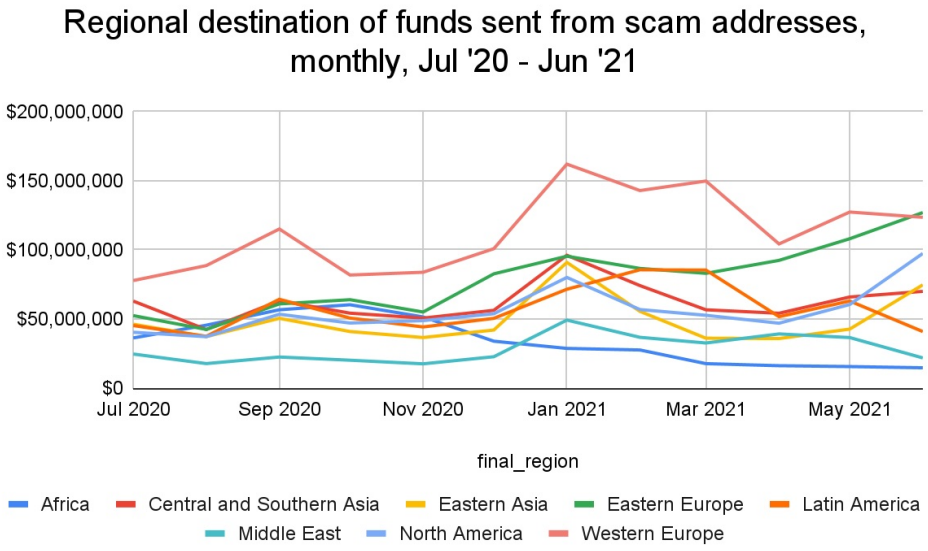
According to the *Moscow Times*, Finiko was headed up by Kirill Doronin, a popular Instagram influencer who has been associated with other Ponzi schemes. The article notes that Finiko was able to take advantage of difficult economic conditions in Russia exacerbated by the Covid pandemic, attracting

users desperate to make extra money. Chainalysis Reactor shows us how prolific the scam was.

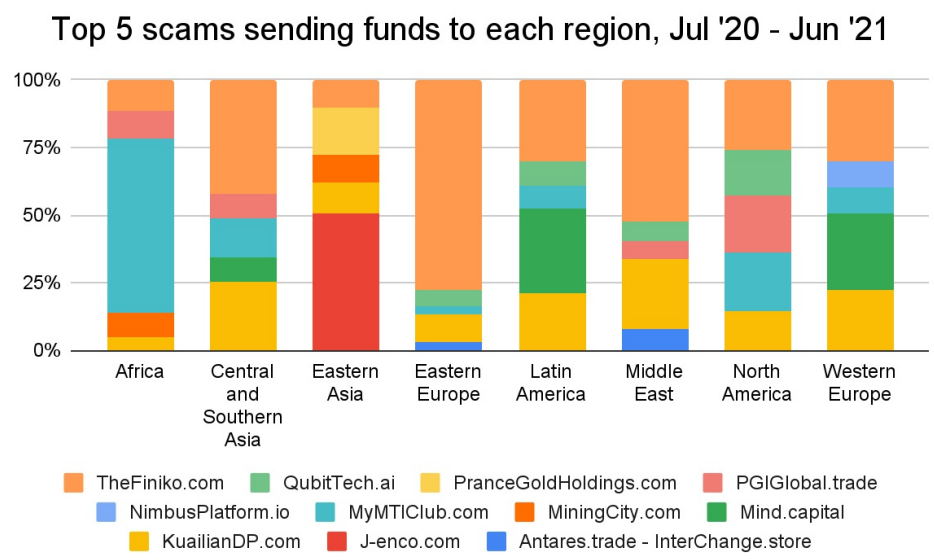


Between December 2019 and August 2021, Finiko received over $1.5 billion worth of Bitcoin in over 800,000 separate deposits. While it's unclear how many individual victims were responsible for those deposits or how much of that $1.5 billion was paid out to investors to keep the Ponzi scheme going, it's clear that Finiko represents a massive fraud perpetrated against Eastern European cryptocurrency users, predominantly in Russia and Ukraine.

Eastern European addresses also receive a great deal of funds from scam addresses, suggesting that many scam operators in addition to victims are located in the region.



The chart above shows how the regions receiving the most cryptocurrency value from scams have changed over the last year. During that time period, Eastern European addresses have received roughly $950 million worth of cryptocurrency from scam addresses, putting it behind only Western Europe. However, Eastern Europe's monthly totals have climbed steadily since March 2021 as Western Europe's have dipped, allowing Eastern Europe to surpass Western Europe in cryptocurrency received from scams in June. Again, Finiko accounts for more than half of that transaction value.



Eastern Europe-based addresses have also received significant funds from addresses associated with ransomware at $46 million, behind only Western Europe at $51 million. However, we believe that at least a portion of the ransomware funds labeled as traveling to Western Europe should likely be attributed to Eastern Europe. Our geographic attribution is based on web traffic to cryptocurrency services, so in cases where two regions use many of the same services, it's more difficult to attribute transaction volume to the correct service. The matrix below shows which regions have the heaviest overlap, with each cell showing the number of services for which the region in the column is ranked first in web traffic, and the region in the row is ranked second in web traffic.

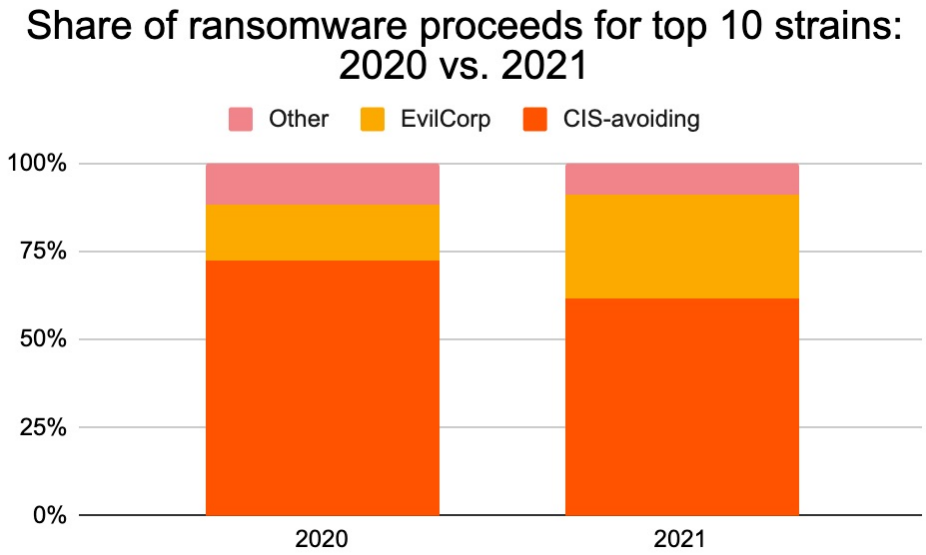
Number of cryptocurrency services where regions are ranked 1st and 2nd by web traffic for all region pairs, Jul '20 - Jun '21

	Africa	Central and Southern Asia	Eastern Asia	Eastern Europe	Latin America	Middle East	North America	Western Europe
Africa	0	58	1	8	4	3	17	23
Central and Southern Asia	9	0	20	37	18	20	15	38
Eastern Asia	1	19	0	12	7	2	24	24
Eastern Europe	5	81	7	0	23	3	24	160
Latin America	4	12	3	12	0	5	15	22
Middle East	0	5	1	7	4	0	3	20
North America	8	19	7	12	13	2	0	95
Western Europe	13	49	15	68	32	16	112	0

We see from the above that Eastern Europe and Western Europe have the highest overlap of any two regions, with 160 services for which Western Europe is first in web traffic and Eastern Europe second, and 68 for which Eastern Europe is first and Western Europe is second. Because of that, we believe it's likely that some of the cryptocurrency value labeled as traveling from ransomware addresses to Western Europe is in fact traveling to Eastern Europe.

Why are we so confident it isn't the other way around? As we've covered previously, many of the most prolific ransomware strains are associated with cybercriminal groups either based in or affiliated with Russia, such as the notorious Evil Corp, whose leadership reportedly has ties to the Russian government. However, there's another way to get a sense of how much ransomware activity Eastern European cybercriminals are responsible for besides looking at where ransomware operators send funds to cash out. Many ransomware strains affiliated with Russia and other Eastern European countries have code that prevents them from being deployed against operating systems in

detects as being located in a Commonwealth of Independent States (CIS) country — the CIS is an intergovernmental organization of former Soviet states. On the chart below, we quantify how much of each year's total ransomware revenue went to strains either associated with Evil Corp or that have code designed to avoid CIS countries from 2018 to the present.



Overall, for the time period studied, ransomware strains associated with Eastern Europe for the top ten strains account for 90% of all ransomware payment volume, a share that has been growing year on year. The data makes it clear that an important step in the ransomware battle will be to work with law enforcement in Eastern European countries to disrupt local ransomware operators.

This blog is a preview of our 2021 Geography of Cryptocurrency report. Sign up here to reserve your copy and we'll email you the full version when it's released this October.

NEXT ARTICLE

August 18, 2021

Introducing the Chainalysis Global DeFi Adoption Index