Cyber scammers are scamming each other, and revealing dark web secrets along the way

Scammers are scamming scammers, and that's creating an unexpected window into their world.

Written by **Danny Palmer,** Senior Writer

Dec. 8, 2022 at 5:27 a.m. PT

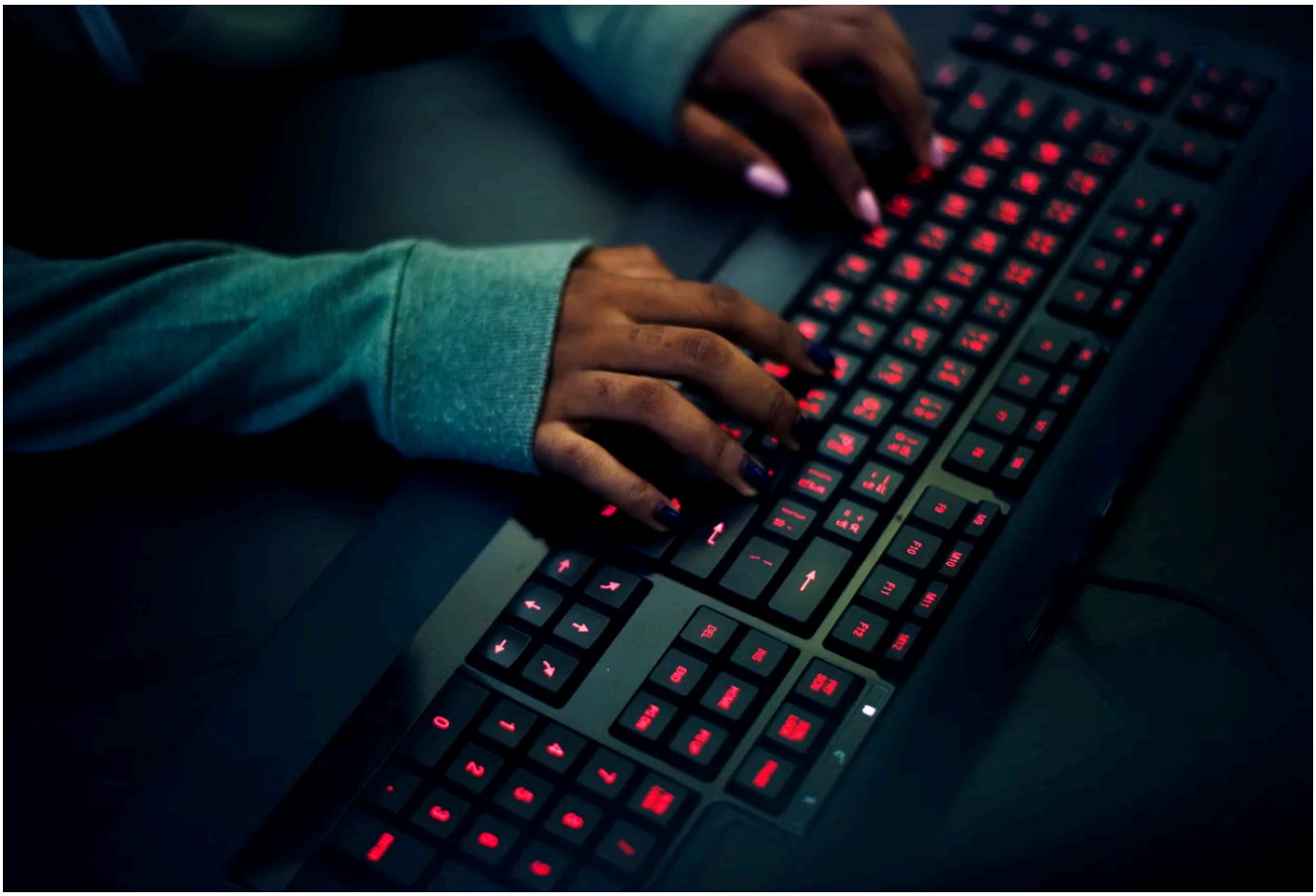

Image: Getty

Cyber criminals are losing millions of dollars to other cyber criminals after themselves falling victim to scams on dark web forums. And the way they're publicly complaining about it could help uncover the secrets of the whole underground economy.

Online scammers and fraudsters cost consumers and businesses billions every year, and it appears that even cyber criminals aren't immune to falling victim to scams.

/ security

Do you need antivirus on Linux?

6 ways to protect yourself from getting scammed online, by phone, or IRL

The best VPN free trials for 2024

8 habits of highly secure remote workers

How to find and remove spyware from your phone

According to analysis of underground marketplaces by cybersecurity researchers at Sophos, cyber criminals have lost at least $2.5 million to other dark web scammers during the past 12 months – and that's just on three prominent cybercrime forums, so the total figure is likely to be a lot higher.

Also: Watch out for this three-pronged PayPal scam

Scamming other cyber criminals can be an appealing prospect because there's little risk of the police ever getting involved. While some dark web forum moderators do offer arbitration processes if someone is accused of conducting a scam, the anonymous nature of the cyber-criminal underground forums means that, for the most part, the worst consequence a scammer is going to face will be a ban from the forum.

But this isn't just an opportunity to enjoy schadenfreude at the expense of online scammers and other cyber criminals – it's also a chance to gain insight into how cyber criminals work, providing intelligence on what attacks are being employed and how to stop them.

It can also potentially help identify who is behind the schemes, because while most cyber criminals are careful about hiding their identity, information they hand over during the arbitration process can provide clues – which could ultimately be used to find out who they really are track them down.

"Because forum rules demand proof to support scam allegations, wronged threat actors will often happily post screenshots of private conversations and source code, identifiers, transactions, chat logs, and blow-by-blow accounts of negotiations, sales, and troubleshooting," said Matt Wixey, senior threat researcher at Sophos.

"This hidden sub-economy isn't just a curiosity. It gives us insights into forum culture; how threat actors buy and sell; their tactical and strategic priorities; their rivals and alliances; their susceptibility to deception – and specific, discrete intelligence about them," he added.

Many of the scams are based around 'rip-and-run' schemes, where either a buyer receives a product but doesn't pay for it, or a seller receives a payment but either doesn't deliver the product or it doesn't work as advertised.

Also: Cybersecurity: These are the new things to worry about in 2023

This can even include providing an application or service as advertised, then secretly using it to plant malware on the buyer, stealing information or money from them.

They're called 'rip-and-run' schemes because the scammer rips their victim off then runs away, either by ghosting additional messages and complaints or disappearing from the forum altogether.

But there are also cyber criminals who engage in meticulously planned, long-term scams. For example, one scheme involved someone creating 19 fake criminal marketplaces, and then tricking users into handing over $100 'activation fees' to join.

Others, simply engage in scams out of spite, because they hold a grudge against another user – or they think they've been scammed themselves.

Also: My stolen credit card details were used 4,500 miles away. I tried to find out how it happened

When these disputes do end up in arbitration, it's often the case that one or all the parties involved receive warnings or get banned. On one forum, the ban is even accompanied by the personal information that's been submitted alongside the claim, partially doxing them in an attempt to deter other scammers.

"If there's a takeaway from all this, it's that no user is immune; any trade on criminal forums involves an inherent risk of scams. While there are both proactive and reactive (arbitration rooms) measures in place, scammers are not only common, but – judging by the data we gathered – often successful," said Wixey.

MORE ON CYBERSECURITY

- **Ransomware gangs are complaining that other crooks are stealing their ransoms**
- **Police just launched an e-commerce fraud crackdown. Here's how to protect yourself from scammers**
- **Dark web crooks are now teaching courses on how to build botnets**
- **Password-hacking attacks are on the rise. Here's how to stop your accounts from being stolen**
- **A security researcher easily found my passwords and more: How my digital footprints left me surprisingly over-exposed**