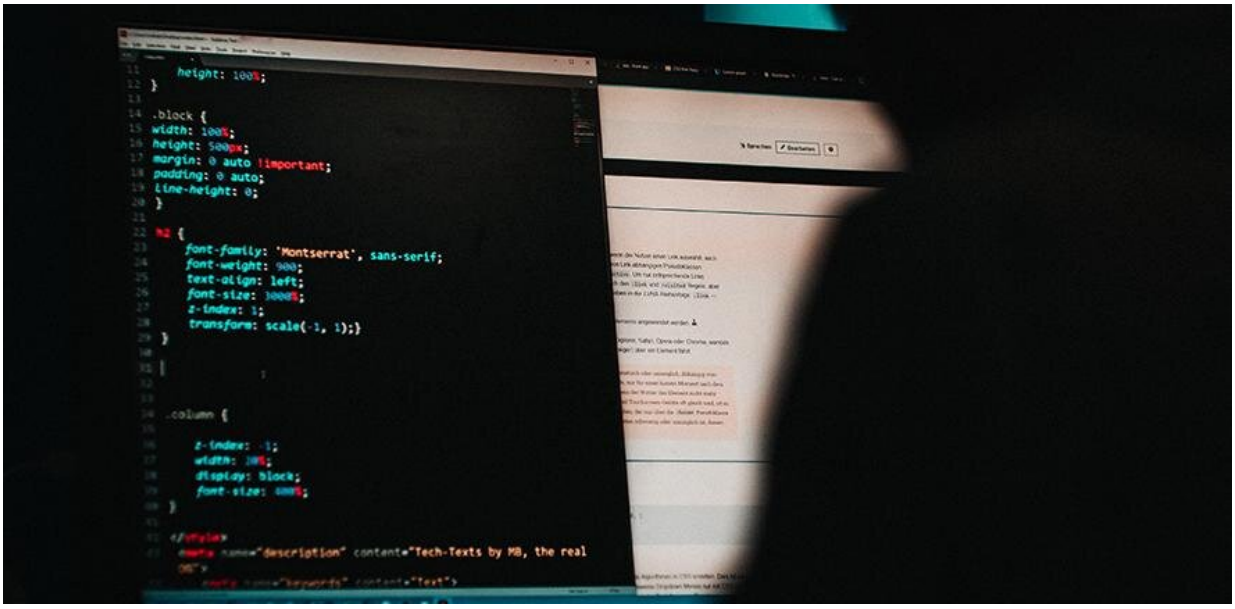
Honour among thieves: The study of a cybercrime marketplace in action

November 9 2020



Credit: Mika Baumeister on Unsplash

Researchers at the Cambridge Cybercrime Centre have revealed what they've learned from analyzing hundreds of thousands of illicit trades that took place in an underground cybercrime forum over the last two years.

Having seen a large rise in illegal transactions during the first national lockdown last spring, the researchers will warn at a workshop this

afternoon that the second lockdown is likely to result in another surge in cybercrime activities. But they will also be offering insights on how such activity can be disrupted.

The researchers have been collecting the data on illicit trades from HackForums—the world's largest and most popular online cybercrime community. Two years ago, it set up a market where contracts had to be logged for all transactions as an attempt to protect members of the community from scamming and frauds.

The contract system was introduced in 2018, and then made mandatory in spring 2019, for all market users. It logged all the illicit buying and selling of—among other things—malicious software (malware), currencies including Bitcoin and gift vouchers, eWhoring 'packs' (e.g. of photos and videos with sexual content), hacking tutorials and tools that allow users illegally to access or control remote servers.

Ironically, HackForums had introduced the contract logging system in response to its members' concerns that trades were being abused and they were being scammed. But in doing so, it unwittingly lifted the lid on the way such underground markets operate.

The data the contract logging generated has been collected by researchers here. And after analyzing it and using statistical modeling approaches, the researchers have been able to shed important new light on the way a cybercrime market operates, hopefully to the benefit of the security community.

The researchers watched the market initially function as a forum where many individual users conducted one-off transactions. Then it changed. As the contract system became mandatory, within a few months, the market was becoming concentrated around a small group of 'power-users' offering goods and services that were attractive to many.

"This small group of users—representing about 5 percent of all users—are involved in around 70 percent of all the transactions," said Anh Vu, a research assistant in the Cambridge Cybercrime Centre and co-author of the paper the Centre has just produced, "Turning Up the Dial: the Evolution of a Cybercrime Market through Set-up, Stable, and COVID-19 Eras' .

And then came the global declaration of the coronavirus pandemic in March 2020. The research team saw the virus and the resulting lockdowns that were introduced significantly "turn up the dial" on the number of market transactions.

"There was a big rise in transactions in what we call the "COVID-19 era,'" said Anh. "Looking at the discussion forums, we could see that a period of mass boredom and economic change—when presumably some members were not able to go to school and others had lost their jobs—really stimulated the market.

"Members needed to make money online and they had a lot of time on their hands, and so we saw a rise in trading activity. We expect to see another rise during the second lockdown, but we don't think it will be as large as during the first."

The increase in business during the pandemic also meant that contracts for transactions were concluded much faster. Where in the early months of the market, the completion time for contracts was around 70 hours, during the pandemic it dropped to less than 10 hours.

Online underground forums like HackForums are communities used for trading in illicit material and sharing knowledge. The forums support a plethora of cybercrimes, allowing members to learn about and engage in criminal activities such as trading virtual items obtained by illicit means, launching denial of service attacks, or obtaining and using malware.

They facilitate a variety of illicit businesses aiming at making easy money.

The Cambridge Cybercrime Centre researchers have done some previous work looking at underground forums. "But this is the first dataset we are aware of that provides insights about the contracts made in these forums," says Anh. Previously, while traders might meet online in a forum, they would likely trade offline via private messaging. But the introduction of the contract system means all trades are now logged—and can therefore be tracked.

Using the data, the researchers looked at a variety of trading activities taking place in the market. The largest activities were currency exchanges and payments—for example, exchanging Bitcoin (a very popular currency in illicit trading because people believe that it leaves no trace) for PayPal funds.

This activity was followed by trades in gift cards (including Amazon gift cards) and software licenses. "When you install a software package like Windows," Anh said. "You have to input a key to activate it. People often buy software keys illegally in a market like this because it is cheaper for them than purchasing it officially from Microsoft—and sometimes they can obtain it for free in exchange for other items."

Other products and services they found being traded in the underground market were hacking tutorials, remote access tools and eWhoring materials—photos and videos with sexual content that are sold to a third party, who pays for them believing that they are paying for an online sexual encounter.

They used several methods to try and estimate the values of trades taking place via HackForums and concluded that taking both public and private transactions into account and extrapolating by each contract type, the

lower bound total of trades was in excess of $6 million.

What the researchers learned about the operation of an underground cybercrime market is valuable, they believe, to the security community. The logging of contracts when goods were traded has allowed users to build up a form of trust and reputation and this in turn led to the rise of the 'power-users' in the market.

"And now we know a small group of power-users are responsible for a large number of transactions, it would make sense to focus interventions on them," Anh said. "As that will have a much bigger impact than going after a large number of individuals."

In their paper they suggest interventions to undermine the perceived reputations and trustworthiness of the big players—for example by posting false negative reviews of them and using other methods, known as Sybil attacks, that disrupt the market's reputation systems.

And the researchers are continuing to watch the market. "We're interested to know how the marketplace evolves during this second lockdown and afterwards," said Anh. "And will be looking to see whether any new trading activities emerge."

More information: Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras: www.cl.cam.ac.uk/~vv301/papers/imc20.pdf

Provided by University of Cambridge

cybercrime-marketplace-action.html